Demetri Kofinas: 00:00:00 Hey, everyone. I've given you guys time codes to navigate the content more efficiently in the description, but there are some important updates in the intro that you won't want to miss, especially if you're already familiar with permissionless blockchains like Bitcoin, for example, because although we do make comparisons between Hedera and Bitcoin during the episode, it's important to be absolutely clear that even though Hedera's network goes public today - and I discuss this during the intro - it remains a hybrid system on the permission side with a roadmap to becoming permissionless, which involves its own challenges, which we get into during the full episode. So, the comparison is imperfect, and I want you guys to always keep that in mind.

Demetri Kofinas: 00:00:46 Hedera and Bitcoin serve entirely different use cases, and if you want to learn more about Bitcoin, I've done some great episodes on it with Pierre Rochard - Episode 75 - and more recently with Nic Carter, a great episode on Bitcoin's ontology - number 97 - so be sure to check those out as well. Also, for Hidden Forces patrons, I'm giving you guys early access to an episode that I recently recorded, and which won't be released for a few more weeks, so look for that on your Overtime feed. And for anyone who's new to the show, you can find out more about our Patreon subscription and about how you can support the podcast at Patreon.com/HiddenForces, where you can also get a full transcript to this week's episode, along with the show rundown. These are educational documents full of links and references to material covered during the podcast. With that, please enjoy this week's episode.

Demetri Kofinas: 00:02:03 What's up, everybody? The episode you're about to hear was recorded on the 16th of May, during Consensus Week in New York City. A redacted version of this episode has been available to Hidden Forces Patreon subscribers since early July. It was redacted because in this full version, Leemon and Mance share news about council members who were only recently announced to the public, companies like Worldpay, which was purchased in the interim by FIS, which, for those of you who don't know, is a huge player in the payment space. They process roughly 75 billion transactions annually, and move something like $9 trillion around the globe every year. Tata Communications, part of Tata Group, one of India's largest conglomerates, a combined market cap of about $145 billion, with over 700,000 employees.

Demetri Kofinas: 00:03:02 IBM. You all know IBM, one of the largest multinational corporations in the world, and a leading provider of Enterprise solutions, including their work with Hyperledger Fabric. But

most exciting for me has been the announcement of Boeing joining Hedera's governing council, the world's largest aerospace company, the largest airline manufacturer in the world, and the biggest manufacturing exporter in the United States. These are just the latest announcements. Mance goes through the entire list of companies that have been announced so far, as well as some of the responsibilities and duties of the Hedera Governing Council and its role in the path towards decentralization, which is how Hedera has described the process by which their ledger will move from its currently permission to state to a fully permissionless one where individual nodes would be anonymous and where anyone in the world will be able to run a node, which is part of the company's vision.

Demetri Kofinas: 00:04:03 It's something that Leemon has talked about since they announced the public ledger in March of 2018, and I think it's part of what he means when he talks about Hedera Hashgraph becoming the trust layer of the internet. Also, as many of you already know, and as I've discussed on the program multiple times, I am a seed investor in the public ledger. Hidden Forces was the first media company that I know of to cover the technology in late September of 2017, and then again in mid-October with our panel at the Assemblage, and I've been an enthusiastic supporter of the team and Leemon in particular ever since. I understand that no matter how much I try to be objective, I'm still invested, not just financially, but reputationally, and to some degree, emotionally, in the success of the project.

Demetri Kofinas: 00:04:59 Also, I've developed a rather close relationship with some of the founding members, Leemon in particular, in the years since, so I fully recognize it. I own it, and I want all of you to keep that in mind at all times. This is not a normal episode. It's me sharing news and information and my own personal excitement about a venture, a project, a technology that I believe in, that I'm invested in, and that I've watched grow for the last couple of years, and which I am hopefully will be able to transform a great deal of what we think of as commerce, security, and identity on the internet today. That said, Hidden Forces is still my baby. It's my priority, and I want to continue to be able to use this platform to have conversations with people and projects in the space, and that means encouraging a critical analysis of Hedera, its implementation, and a great example of that was a recent back-and-forth on Twitter with a number of folks in the Bitcoin blockchain space that produced a series of responses by Hedera with respect to the details of their fair ordering, how they're measuring transaction throughput at launch, some of their

initial trade-offs, why they're making them, and I've linked to the most recent response in the summary text, and I encourage everyone who listens to this episode to engage with the team, whether it's on their Telegram channel, which I've also linked to in the text, or on Twitter, or through some of the webinars that they're going to be doing, where they're going to be fielding questions from the community about the platform and whatever else comes up in the future.

Demetri Kofinas: 00:06:44 Also, before I give you guys the official, "This is not financial advice," disclaimer, because I've already done three past recordings with Leemon, two of them on video after the initial episode we did in September of 2017, and one with Mance as a panel at the Assemblage, my intention with this episode was to make it to go-to audio for anyone who is new to the technology, or even for those who want a refresher. I wanted to spend an equal amount of time on the tech, the governance, and the use cases, but unfortunately, we ran out of time towards the end, and I made the decision to cut from the use case section, only because I felt like we couldn't afford to skimp on the tech, and even on governance, we couldn't do as much as I had hoped.

Demetri Kofinas: 00:07:34 However, don't despair. Paul Madsen, Hedera's technical lead, hosts a weekly podcast where he speaks with different developers and entrepreneurs who are building on Hedera and spends a lot of time discussing use cases, so you should totally check that out. The name of the podcast is Gossip About Gossip, and I believe it's available across all major podcasting platforms. Also, there are a few dozen distributed applications working on the network today, with, I am told, a few hundred more developer teams working in toe on apps currently under development. All council members will be running nodes at OA, which again, is today. OA is Open Access. It means the network is now fully public, anyone can join it, anyone can use it.

Demetri Kofinas: 00:08:25 This also means that HBARS, Hedera's native currency used to stake nodes, conduct transactions, and make API calls, are now trading on some exchanges. If you care to learn more about that, I suggest you figure it out yourself. I am not here to shill my alt. Seriously, nothing I say here can or should be viewed as financial advice. All opinions expressed by me and my guests are solely our own opinions, and should not be relied upon as the basis for financial decisions.

New Speaker: 00:09:00 Now, having said all of that, I am so excited to finally get to share my conversation with Leemon Baird and Mance Harmon. So, Leemon Baird and Mance Harmon, welcome to Hidden Forces.

Leemon Baird: 00:09:21 Thank you.

Mance Harmon: 00:09:21 Great. Thank you. Good to be here.

Demetri Kofinas: 00:09:22 It's awesome having you guys here.

Mance Harmon: 00:09:23 Thanks.

Demetri Kofinas: 00:09:24 We're recording this during Consensus Week. Consensus just ended, as well as the other blockchain related conferences.

Mance Harmon: 00:09:30 Yeah, Digital Asset Summit. That's right.

Demetri Kofinas: 00:09:33 I want to ask you guys how those went. The reason we're recording this now is because you're in New York. You guys are based out of Dallas. I don't know that you'll be back here again before Open Access, and I wanted us to do this and basically talk about everything that you're going to be able to discuss once OA hits, including a lot of important council member announcements and other things as well. First of all, what's been your impression this time in New York, this week, with all the events?

Mance Harmon: 00:09:59 Wow, so the activity level is really high. You know, what's interesting is in past years, I've been able to watch some of the events, you know, see people on stage. For me personally, this year, that's been much harder, but my impression is that while in past years, there's been a lot of focus on protocols, and still there is a lot of talk about protocols, but in addition to that, we're now seeing more discussion about other infrastructure in addition to protocols, not just infrastructure that makes it possible for the industry to mature, but dapps applications, that sort of thing. It feels to me like even though we've been in the midst of crypto winter, there's a lot going on, and the industry is moving forward, clearly.

Demetri Kofinas: 00:10:44 Do you think it's been beneficial that there's a crypto winter for development on the platforms?

Mance Harmon: 00:10:49 Absolutely. Leemon and I, going back years, I don't know when we first started talking about this, but we always understood and believed that there would be a crypto winter, and knew that when it happened, it would be good for the industry, right? If you look back in 2016, 2017, there were the ICO craze, and while there were good projects, there was a lot of noise, and there was a lot of fraud, and the crypto winter has begun to

weed that out. Those projects that are still getting the money are now the ones that have real value.

Leemon Baird: 00:11:23 Every technology goes through this path where you have hype, and the main things going on, and there's bubbles, and then you have a crash, and you have a crypto winter equivalent, and it comes out healthier. Now, perhaps, we're actually seeing the end of crypto winter, which is an exciting time.

Demetri Kofinas: 00:11:36 Yeah, the cycles are compressed in the crypto world.

Mance Harmon: 00:11:39 Yeah, it sure feels that way, doesn't it? You go crypto winter was only coined as a term in late fall, early winter, right, and here we are five months later, and people are now talking about crypto spring.

Demetri Kofinas: 00:11:53 It's really interesting how things have changed. Let's move onto the most important announcements. First, let's talk about ... Well, you guys can decide how you want to do it, but there's obviously the big news of the council members. Maybe you can also start by telling us the council members that already have been announced, and then tell us the new members that will have been announced when this episode airs.

Mance Harmon: 00:12:11 Sure. Well, so back in February, we had our first council meeting in Seoul, Korea, and at that time, we announced the first five council members, Nomura, a major bank financial services organization out of Tokyo, Deutsche Telekom, of course, the largest telco in Europe, Swisscom Blockchain, the blockchain arm of Swisscom, which is another major telco in Europe, DLA Piper, one of the top global law firms, and Magazine Luiza, which is a major online retailer in Latin America, based in Brazil. Those are fantastic names. Since then, given that this is airing at OA, we have just recently announced the next tranche of council members, and so Boeing is a council member in the United States, of course. Everyone knows Boeing.

Mance Harmon: 00:13:02 IBM is a major council member, now that we're partnered with, and we'll talk more about the work that we're going to be doing with IBM. Worldpay, which is maybe not a name that the average consumer knows and understands, but they play a role in just about 50% of credit card transactions globally, and Tata Communications, a Conglomerate, out of India. These are huge names, and what we always understood was that the first five council members would be the hardest. Getting those first five would be the hardest, and then once we got that next tranche of council members, things would get a lot easier. Now that we are there, the pipeline is fantastic, and the council is growing,

and there's a lot of excitement and work with the council. We've had our second council meeting now, at the end of Consensus here in New York City, and there's a lot to talk about in the work that we're going to be doing with them.

Demetri Kofinas: 00:14:08 Yeah, they're remarkable names. I mean, is there any in particular that you're more excited about? I think what's interesting with IBM is that's the one that I think will surprise a lot of people, because of IBM's relationship to blockchain with Hyperledger.

Mance Harmon: 00:14:20 Yeah, so what we just announced a week ago was that we joined the Hyperledger Foundation, and Leemon, you want to talk about the work we're going to be doing with them?

Leemon Baird: 00:14:31 Absolutely. So many people join the Hyperledger Foundation. They contribute code. We're contributing code. We're doing all those things. In addition, the code we have allows it to inter-operate with our ledger, and that's pretty cool. You can do things in the Hyperledger, and you can then have calls to use our files, or use our smart contracts, or use our cryptocurrency, but then we're doing something more fundamentally to the whole system, and that is the ordering service. The ordering service allows you to send messages of some kind to our system. We put them in order. We give them time stamps that are consensus, and that are fair, and we send them back.

Leemon Baird: 00:15:08 You can organize them by what they're about, and then you can just see the ones in the area that you're interested in. This, we are doing with Hyperledger, so that Hyperledger can use it to do its operations. It can use it as its ordering service and as its consensus layer, which allows you to build extremely fast applications. You know, you could build a stock market, and you could build it directly on top of Hyperledger, get all of the advantages of the entire Hyperledger ecosystem, and your consensus is being done by Hedera. You have all the advantages of knowing that you have the trusted nodes, you have the trusted council governing it, and you have the speed and the fairness and all those things.

Demetri Kofinas: 00:15:44 We're going to get into more detail about this, but for a quick explanation for our audience, why is it that Hyperledger can't put transactions in order? We'll get into more detail about this, but what's the reason that they want to use Hedera? Why can't they do this themselves?

Leemon Baird: 00:15:57 Oh, they do. They have software, and if you have computers that everybody in the world trusts, then you could run it on

your computers, but you need to have computers that everyone in the world trusts, which is what we're bringing, and for some applications, you need fair ordering, so it isn't just one computer that decided what the order would be, and so we have this consensus fair ordering. Not every ledger does fair ordering, but we have fair ordering. There are some cases where, "Fine, you and three friends can run your computers, the network's fine," and then there are cases where you want the broader base for the type of trust that you get from that, and now we can do both.

Demetri Kofinas: 00:16:32 Okay. Great. This'll be an opportunity to get into distinctions. I drew a bunch of distinctions here that I wanted to get into. Are there any other announcements, by the way, that you wanted to make before we proceeded forward?

Mance Harmon: 00:16:44 I think those are the announcements that will have been made.

Demetri Kofinas: 00:16:47 Okay, super. We'll talk about what Open Access is, but I wanted to begin by drawing some distinctions. Leemon, you and I, in our first episode together, and in a few subsequent ones, went through Hashgraph's consensus protocol. I've dubbed my first conversation with you "The Hashgraph Holy Shit Moment" that I had about halfway through. I think the time was 36 minutes in or something. I have it on the transcript, and it's when I realized that the events themselves functioned as the voting participants. I realized, as I've told you subsequently, that the way I think about Hashgraph is that it answers the question of what is the minimum amount of information needed to run a voting protocol, and that in a sense, it isn't so much that you've reinvented the wheel.

Demetri Kofinas: 00:17:27 It's just that you've found a way to deploy a voting protocol at scale, right, and to maintain all those same security properties, which is remarkable. There are distinctions I want to make. The first one deals with finality, and so that's a way of talking about what is the difference between Hashgraph, which is the consensus protocol, and we'll get into this distinction between Hashgraph consensus and Hedera Hashgraph, which is the distributed ledger technology that's built with Hashgraph consensus at its core, but this distinction between Hashgraph and Nakamoto style consensus, which is what blockchain databases use, which is proof of work, pretty much.

Leemon Baird: 00:18:02 Yes, so that was a whole bunch of questions.

Demetri Kofinas: 00:18:05 Yeah.

Leemon Baird: 00:18:06 Finality means that when the ledger reaches consensus, it knows it has reached consensus. Guaranteed, we are done, as opposed to every time there's a confirmation, you become a little bit more sure, and then over time, you say, "Well, I got six. Maybe I'm sure enough, or maybe it's really important, so I'll wait for 12, and then I'll be sure." No. With finality, there's a moment when you know for sure that it is true that everybody will have the same consensus, that no one will change their mind, and that you're guaranteed. What does that mean? Well, for one thing, it gives you better speed. We have finality within a few seconds, and at that point, there is no question you have it. If I go to your store, I pay you some HBARS, you give me a product, and within a few seconds, you know that it has cleared and that you definitely got those HBARS, and then I can walk out of the store. That would be different if we had to have this probabilistic way that I just get more and more sure and it takes an hour to reach certainty.

Demetri Kofinas: 00:18:57 Can you explain that, though? How does that probabilistic way work? Why does it take 10 minutes and an hour to verify a transaction on a permissionless blockchain database like Bitcoin, or like Ethereum, or some of these other platforms?

Leemon Baird: 00:19:11 You never really know for sure that we have consensus. What we have instead is a chain of blocks that we're building up, in a blockchain system, and people can add onto the top of the chain. They have to solve a hard math problem and waste lots of electricity to do it, so that slows them down. The whole point of proof of work is to slow it down, so hopefully, we'll all end up adding them one at a time, and we'll know about them before the next one's added, but maybe not. Maybe two people add at the same time. Even with proof of work slowing us down on purpose, we might still add two at the same time, and then your nice chain forks and becomes a Y shape. That'd be bad.

Demetri Kofinas: 00:19:44 Mm-hmm (affirmative).

Leemon Baird: 00:19:45 What we then, as a community, have to do is figure out which of the two sides of the Y to continue extending, and so everybody tries to extend whichever one they think is longer, and over time, eventually we kind of start to agree on which one's longer, and that's the one that gets extended, but sometimes you might think that one is longer, and then you realize, "Oh, I see. Everybody else thought the other one was longer," and then you have to jump back over to the other one. You thought it was true, and it wasn't. How long does it have to grow before you can be really sure it's true? Six? Six is usually enough, although they've even had rollbacks of six, and there

have been attacks on other systems that have had a rollback of vastly more than six.

Demetri Kofinas: 00:20:21 Six represents 60 minutes. It represents an hour.

Leemon Baird: 00:20:24 On average, yeah.

Demetri Kofinas: 00:20:25 Just to clarify a few of the things that you're saying, proof of work, besides the network layer security function that it provides, and we'll get into that, between proof of work and proof of stake, it also allows for leader elections through a non-algorithmic lottery system, because blockchain needs leaders to propose new blocks, right? Because then the entire network decides which chain to build on, and that brings us back to the point about keeping the network's growth slow enough so that the network can decide what chain to build on, so you don't get a hydra head.

Leemon Baird: 00:20:53 Exactly. You don't want a hydra that keeps splitting faster than you can chop off the heads of the hydra. The way that it works is whoever solves the puzzle first gets to put the next block on. You could say that they're like a leader because they get to pick what's in their block. They could leave out your transactions. If they don't like you, you have to wait another 10 minutes and then try again.

Demetri Kofinas: 00:21:12 The answer first is an uncomputable number, right? It's a number that you have to guess. It's the reverse hash.

Leemon Baird: 00:21:17 Yes, it's inverting a hash, and so you just keep making guesses until you hit the right answer.

Demetri Kofinas: 00:21:21 Did I describe that correctly?

Leemon Baird: 00:21:22 You did.

Demetri Kofinas: 00:21:22 Okay.

Leemon Baird: 00:21:23 You are trying to find a partial inverse of a hash, and so it's just a hard math problem that has little use.

Demetri Kofinas: 00:21:26 It's a lottery.

Leemon Baird: 00:21:27 It's a lottery where you buy your ticket with electricity and a supercomputer. Then they can have this forking thing, and so you never really know. Is the chain long enough that it won't get reverted and turn stale, and have to go to the other branch?

With voting algorithms like what we're using in Hashgraph, then it's just there's a mathematical proof. Once I have a certain amount of information, I know for sure we have consensus, period. We're done.

Demetri Kofinas: 00:21:51 Let's break that down a little bit more, because I think one of the questions I get asked a lot when I try to explain your technology to people, and to smart people, one of the first questions I get immediately, almost predictably, is, "What are the trade-offs? Come on, there have to be trade-offs, right?" What I try to explain is that of course there are trade-offs. There are trade-offs in terms of latency and throughput and those things, but those trade-offs are different in Hashgraph because it is a different paradigm, and it's a different paradigm because of bringing it back to the point about using a voting algorithm, and that you've managed to scale that, right? Explain to our listeners how it's possible. How can this be possible? We all live in a paradigm where there are these trade-offs, that we're trying to get above 10 transactions per second, right? That's sort of the paradigm and blockchain, somewhere around there. Everyone's been trying to figure out how to make a faster horse, right? How on earth can it be possible that you would be talking about hundreds of thousands of transactions per second, perhaps millions with database sharding? How are you talking about seconds of latency? How is this possible?

Leemon Baird: 00:22:54 Yeah, so it's a good question. You have to get your information out. When you make a transaction, you may have to make sure all the nodes know about it, and then the nodes have to come to a consensus on the time stamp on it, and then you can put them in order by the time stamp. The way to get the information out, the fastest way you can do it is gossip. If you have an internet, and you can have pairwise communication, there's nothing faster than gossip, which just means I tell a random person. Now two of us know. Then each of us told a random person. Now four of us know, and then each of us tells a random person. Now eight of us know, and it just grows up exponentially, how many people know it. The gossip is the fastest way to get the transaction out. Every ledger pretty much uses this.

Demetri Kofinas: 00:23:32 Exactly. That's not special.

Leemon Baird: 00:23:32 It's not special.

Demetri Kofinas: 00:23:33 Yeah.

Leemon Baird: 00:23:34 Then the hard part is oh, how much talking do we have to do to get to consensus, or do we have to solve a really hard math problem to get to consensus? Turns out, back when you were doing the gossip part, if you just added two hashes to each of your messages, if I just, every time I send a message, I make a little note of what the last message was that I created, and the last message I received. That's it. Tiny bit of extra information on each message. Then, for free, now, you get a complete history of how we've talked to each other. You can see the entire history of how information flowed through the network, but if you can do that, you can take 30-year-old voting algorithms that are really strong and horribly slow, and get them to run in your head without talking to anyone. You can do a voting algorithm with no voting. You just do virtual voting, and so that's how we end up with pretty much the theoretical limit for how little information you can send out and still have an ABFT system that does this voting, has all these strong guarantees, because you're doing it all in your head based on your knowledge of the history of how we talked to each other, and that's what the hashgraph is. It's the history of how we talked to each other.

Demetri Kofinas: 00:24:42 Let me see if I can try to break that down even further, and you can let me know if I have it correctly. Normally, all the information that's normally gossiped represents some amount of information, right, that all the nodes in the network have at any point in time, and if you wanted to run a voting protocol, you then have to cast votes across the internet, and that would be a tremendous amount of information and overhead bandwidth, all that stuff, right? What you're basically saying is you realized, you came to a realization that all of the information needed to run a voting protocol is almost all already on each node of the network, and that the only thing they needed was an additional amount of information represented in the hashgraph, that's generated using these two hashes, and which is basically a genealogical tree of the network's communication, and if you have that hashgraph, along with all the information that already needed to be gossiped, each node on the network can independently run a voting protocol, where they virtually represent the other nodes on the network and cast votes.

Leemon Baird: 00:25:42 That's it exactly.

Demetri Kofinas: 00:25:43 But no votes are actually cast, so there's actually no voting happening.

Leemon Baird:	00:25:47	There's no actual voting. We never send any votes over the internet, so the whole world of this for the last 30 years has been debating, "Is this an order-n squared algorithm, order-n cubed algorithm, order-n algorithm?" Yet we're in order 0, in that part.
Demetri Kofinas:	00:25:58	So when I say that to people, I get blocked sometimes.
Leemon Baird:	00:26:00	Oh, I know. I know.
Demetri Kofinas:	00:26:00	I get blocked sometimes on Twitter.
Leemon Baird:	00:26:05	The truth is if you want everyone to know the transaction, you have to use enough bandwidth to send everyone the transaction, and gossip is the best way that we know to do that, you know, humanity, the best way known to do that. If you add this tiny bit of information, the two hashes, now you have a complete history of how we talk to each other, and it just turns out, you don't actually have to send any votes at all over the internet. You now have enough information in the hashgraph, in that history, to do everything, and you're done.
Demetri Kofinas:	00:26:32	On top of that, you guys can do fair transaction ordering. How are you able to order transactions? What we're discussing here is that you can process a tremendous number of transactions in a very short period of time, which means that you're competitive with any major payment processors, right, or clearing houses, or whatever, but how are you able to put transactions in order, and why can't blockchain put transactions in order?
Leemon Baird:	00:26:56	Blockchain puts transactions in order. Whoever wins the lottery gets to put a block on, and they are the king. They get to decide whether your transaction goes in or not, and maybe they don't like you, or maybe you didn't pay them enough as your bribe to get put in, and maybe you'll have to wait a long time until someone takes your bribe and gets put in. There is a leader. There is a king that decides that.
Demetri Kofinas:	00:27:17	It's a leader based system.
Leemon Baird:	00:27:18	Well, that's proof of work I was just talking about. Then there's things called leader-based systems, which are even worse. One king is king for multiple blocks, maybe, or maybe they take turns. Maybe each block comes from one person, but the leaders take turns.

Demetri Kofinas: 00:27:27 But even in a permissionless database like Bitcoin, there needs to be a leader elected at some point, in order to put together the next block of transactions that the entire network decides to build on.

Leemon Baird: 00:27:37 Well, we don't talk about leader election in Bitcoin. What you talk about is that whoever was able to solve that puzzle is able to put on the next block.

Demetri Kofinas: 00:27:43 Right.

Leemon Baird: 00:27:44 But what's in that block? Hey, it's all up to them. They get to choose. In fact, there have been protocols that have seen half the blocks are empty, because you can make more money by churning out blocks than actually putting stuff into them, which is ridiculous. But what we have has no leader. Think about it. Because of the hashgraph, because we're putting these hashes, we see the history. I can see how this transaction spread through the network, and I know what time each person in the network received it. Well, if I look at all those times, and I make a big list of them and sort them in order, I can take the middle one.

Leemon Baird: 00:28:19 That's when it reached half the people in the community, and if a few people lie and say, "Oh, I received it a million years ago, or I received it a million years in the future," well, when we sort it, they're at the top or the bottom of the list. The guys in the middle are still the same numbers, and you're still getting from that group of numbers in the middle, and so they can't manipulate this time in a bad way. There is no leader who decides, "Here's the time on this transaction, or here's the order of this transaction, or even whether we want to have this transaction or not." Everybody sees it, everybody knows when everybody sees it, and everybody knows the consensus time. Completely fair.

Demetri Kofinas: 00:28:57 Because most people are not going to be able to necessarily follow the details of what you're saying, besides the validation of the governing council members and investors and other people in the community who have validated, in one way or another, your approach and your protocol, have there been any formal methods applied to prove the validity of hashgraph consensus?

Leemon Baird: 00:29:18 Yes. Of course, you know, we just talk to people and explain it, and mathematicians tend to look at it and say, "Well, of course, that would work." That's the early things. Then we wrote a math paper that has an extremely detailed math proof that

proves that it's actually ABFT, and does all these things that I just said.

Demetri Kofinas: 00:29:34 Asynchronous Byzantine Fault Tolerant, which is the most secure you can get as a consensus mechanism.

Leemon Baird: 00:29:39 It is. It's the most secure you can get. It guarantees that you have finality. It guarantees that only a small group of people can't do any harm, even if the bad guys control the internet, even if they can DDoS people and shut down computers with distributed denial of service, DDoS.

Demetri Kofinas: 00:29:51 Right, and just to clarify for those who don't know already, Bitcoin, contrary to what some people think, is not even Byzantine fault tolerant, and by Bitcoin, I don't mean just Bitcoin, I mean any permissionless blockchain implementation that exists currently is not BFT.

Leemon Baird: 00:30:05 None of the proof of work systems are BFT. Proof of work is a different paradigm than would allow it to be BFT.

Demetri Kofinas: 00:30:09 It's probabilistic consensus, which is why it's not BFT, right?

Leemon Baird: 00:30:12 Right, so you never have finality. You also don't have the strong guarantees. There're all sorts of reasons, if the bad guys can control the internet, then they can actually manipulate things in really bad ways with Bitcoin. They can shut down every computer on the internet except one, and that one gets to be the leader for every block.

Demetri Kofinas: 00:30:25 To bring it back to what we were discussing ...

Leemon Baird: 00:30:28 To bring it back to what we were discussing, we have this math proof that it is ABFT, that it has the strongest kind of security that you could, better than just BFT. It's ABFT. Then we went beyond that, so you can download that. The paper is years old. You can read the math proofs. What we did-

Demetri Kofinas: 00:30:44 You're talking about the Swirlds white paper?

Leemon Baird: 00:30:45 Yeah, the Swirlds white paper.

Demetri Kofinas: 00:30:46 That's 2016, yeah.

Leemon Baird: 00:30:46 2016. You can go read that, but what we did is Karl Crary, associate professor at Carnegie Mellon University-

Demetri Kofinas: 00:30:54 Say that name again.

Leemon Baird: 00:30:55 Karl Crary. Great guy. He spent the time to create a Coq proof. Now, Coq is a program that allows a computer to check math proofs, because even humans make mistakes when they're checking math proofs. He wrote this all up as a Coq proof, so he basically translated it from human language into computer language, and the computer checked the proof and said it is correct. What he wrote up is also downloadable from the website, and has been for a long time now. You can download that. You can look at his thing, and so we've gone beyond this. We had an idea that was cool, but then we did the math proofs, and then we wrote it up as a formal math proof, and then we've actually done the formal methods, which means having a computer able to check the math proof.

Demetri Kofinas: 00:31:39 How long did it take him to translate it?

Leemon Baird: 00:31:41 He is a master at this. I can't believe it. It only took him a few months. There are only a handful of people on the planet that are good at Coq. I personally, as a computer scientist, think that formal methods like Coq is the future of computer science, and it is really rapidly growing right now, but at the moment, there's only a few people that are true experts in it, and Karl is one of them.

Demetri Kofinas: 00:32:03 How long does it take for the computer to check the proof?

Leemon Baird: 00:32:06 A fraction of a second.

Demetri Kofinas: 00:32:08 I guess I just wanted to point out how stupid we are.

Leemon Baird: 00:32:11 Humans are very stupid.

Demetri Kofinas: 00:32:12 We actually just did an episode. I just recorded one. It'll be out long before this comes out, dealing with the evolution of prediction science, essentially, but it focused a lot on machine learning and the challenge of moving into a world where machines increasingly provide better and better predictions that we are increasingly less and less able to understand, so the methodology behind those predictions, you know?

Leemon Baird: 00:32:32 Oh, that's true. Neural networks, I used to do that a lot. I did that for years.

Demetri Kofinas: 00:32:36 So I don't have to tell you. This is a big deal. The fact that you've done a Coq proof of the consensus protocol is nothing to sneer at.

Leemon Baird: 00:32:44 It is nothing to sneer at.

Demetri Kofinas: 00:32:45 How different is this approach to what we have in this community currently, in this industry currently?

Leemon Baird: 00:32:49 Oh, this isn't the way it's done. It's not done this way. The way it's done right now is mostly you make up a protocol and you have no math proofs, or you proof things that don't actually prove security. Some protocols have a math proof, but they're BFT, but they're not ABFT. Then, as for doing formal methods? Almost nobody goes that step to prove the formal methods, and honestly, I think it's the future of computer science. Everybody's going to do this in the future, but right now, it's really hard, and so only a few people are doing it, but we've got to do it. You know, computer programs have bugs. Our algorithms have bugs. Protocols have bugs. People find these bugs all the time. We've got to fix it. This is the only future.

Demetri Kofinas: 00:33:23 It's interesting. I don't know if either of you have heard this, but I had an episode that I did with Cal Newport, the computer scientist from Georgetown University, whose specialty is consensus. He apparently had been in contact with you by email, I suppose. I don't know if you remember this, but he mentioned that he had been in touch with you, and that he had come across the Swirlds white paper, and he was excited by the prospect of someone from academia, like yourself, coming into this community because he was talking about how the academic community has sort of, in a sense, fallen behind in terms of the implementation of much of the work that had been done for decades in academia.

Demetri Kofinas: 00:34:00 He actually referred to you as a Rosetta Stone for consensus, which was very [crosstalk 00:34:03]. All right, so let's take everything you just said about theoretical alternatives to Hashgraph. Let's assume that Hashgraph would be able to provide the fastest, most secure way to process transactions on a permissionless database at scale, assuming a successful deployment along the lines of the path towards decentralization that you guys have laid out, and that we'll get into, but could there be theoretical alternatives that would be competitive to Hashgraph in the future?

Leemon Baird: 00:34:31 Oh, good question. First of all, if you want the trust of a ledger, you have to have a number of people involved. You have to

have more than one computer involved. If you don't need that kind of trust, use a server. Don't use a ledger. Don't use a blockchain, don't use a ledger.

Demetri Kofinas: 00:34:43 A permission database.

Leemon Baird: 00:34:44 Just use a permission database. I mean, why not? If you trust the person running that database, just trust them, but if you want to have distributed trust, then you have to have a number of people involved, and they all have to see this transaction that we're getting consensus on. The bare minimum bandwidth that you need is you have to at least make sure that that transaction gets sent to everybody. Either you send it to all the other computers, or maybe you send it to one who sends it to one who sends it to one, and it eventually gets to everybody. Gossip is very efficient. Theoretically, could you use less bandwidth? Well, not if you wanted everyone to get the message. You have to send the message to everyone, or send it to people who send it to people, but the total bandwidth used by the network, you can't get less than that. You can add on these two little hashes to get the hashgraph. Even theoretically, you can compress those down, so it's just a tiny bit of effort, and then our voting protocol uses zero bytes. I don't think you can reduce it below zero. A little bit hard to go negative.

Demetri Kofinas: 00:35:37 Your contention is it would be very difficult to provide a faster solution that is this secure at scale for consensus on a permissionless database.

Leemon Baird: 00:35:48 Nope, you can do it.

Demetri Kofinas: 00:35:49 You can.

Leemon Baird: 00:35:49 Yup, you can beat it. Here's how you do it. Now, the way that you beat it is that we've already got the bandwidth down as small as I said, if everybody needs to see the transaction, but if you really want to go to scale, what you do is you do sharding, and so the only thing better than a single shard doing this is you have a bunch of shards. Then you get the really interesting question. What kind of security can you ensure for the big system? Having each little shard secure, does that make the big system secure?

Demetri Kofinas: 00:36:17 Let's stop one second and tell people what database sharding is.

Leemon Baird: 00:36:22 What we're doing, and sharding is a word from databases, as you pointed out. It's also used in the blockchain world, and in

the ledger world, so DLTs shared the same way. The idea is that we have all of these distributed nodes, these computers, running our ledger. We're going to break them up into groups, and we'll only give your transaction to one group, all the nodes in one group, as opposed to making every single node in the world look at your transaction. If you do really good sharding, as opposed to saying a ledger with side ledgers hanging off, but if you do truly decentralized sharding, where every shard is sort of equivalent, then your cryptocurrency account could be stored by any of the shards. Any one shard could have it. If you store a file, it'd be stored in any one of the shards, but within the shard, every computer has it. That's how you get the trust. Then the question is, well, can you make that secure? It turns out that if you don't have finality, it's really hard.

Demetri Kofinas: 00:37:15 Why?

Leemon Baird: 00:37:16 Because a shard is going to have to take the word of another shard and believe it, but when do you believe it? You'd have to be 100% sure. Well, if you don't have finality, you're never 100% sure, and so then your uncertainty exponentially grows if you have to have one shard trust what another shard said about what another shard said.

Demetri Kofinas: 00:37:33 What you're saying is if an application is running on top of the database, the larger network, and it needs to be able to reconcile computations that have happened across different shards, that you need to have finality within each shard in order for that to happen?

Leemon Baird: 00:37:46 You have to. Imagine Alice wants to give some money to Bob.

Demetri Kofinas: 00:37:49 Who's Alice?

Leemon Baird: 00:37:51 Alice and Bob are just two random accounts.

Demetri Kofinas: 00:37:53 It's a term used in computer science to describe ...

Leemon Baird: 00:37:55 Yeah, you're right. In computer science, it's always Alice and Bob and Carol and Dave. It goes back to a movie title.

Demetri Kofinas: 00:38:00 ABCD.

Leemon Baird: 00:38:00 ABCD. They always start with the letters of the alphabet, so if I ever use examples, it's always Alice and Bob, because I taught cryptography as a professor for years. It was always Alice and Bob and Carol and Dave.

Demetri Kofinas:	00:38:10	Go ahead.
Leemon Baird:	00:38:10	But not Eve. We don't like her. You know what Eve does?
Demetri Kofinas:	00:38:13	No, I don't.
Leemon Baird:	00:38:13	She eavesdrops.
Demetri Kofinas:	00:38:15	Is that a joke?
Leemon Baird:	00:38:16	No. It's actually what's used in cryptography.
Demetri Kofinas:	00:38:19	That's so funny. I didn't know that.
Leemon Baird:	00:38:21	Yeah, okay. Anyway, so if Alice and Bob are two just people who have accounts on this system, they have cryptocurrency, Alice wants to send Bob some, but they're stored in different shards, then the shard that has Alice is going to say, "Hey, Alice is now sending some HBARS to Bob. Trust me, Alice has enough. She didn't just do a double spend." Okay, but if you don't have finality, you only sort of trust, so now what do you do? You put the money into Bob's account, but only a little bit trust that Bob has it? Now we have to get consensus on whether Bob got this transaction or not before he's spent, and so then it compounds. Now, you really need finality, and you need ABFT if you want it to be hard to shut down. You really need ABFT within each shard, and then it turns out you can do sharding.
Demetri Kofinas:	00:39:08	This brings us back to the point that you made earlier, which is that in current blockchain databases, you don't have finality. It's probabilistic, and so you're basically compounding the security issues that you face on one database across all the different databases that you have, because now you don't have finality on all these different ones.
Leemon Baird:	00:39:25	You've got it.
Demetri Kofinas:	00:39:25	It's logarithmic.
Leemon Baird:	00:39:27	Yeah, it's terrible, so if you want to do sharding right, you have to make sure you get it right inside of a shard, which means you need finality and you need ABFT within each shard. Then you can do it right for sharding.
Demetri Kofinas:	00:39:35	Let's distinguish between something else, which is a directed acyclic graph, otherwise known as a DAG, and blockchain, because these are also points of confusion. You fall within the

category of a DAG, but for example, there are other implementations like Holochain or Iota. I don't know all the rest of them that also use this type of data structure, but it's comparing apples and oranges. Let's help our listeners understand what the distinction between these two things are, and how you differ from, let's say, other implementations.

Leemon Baird: 00:40:08 Yeah. Blockchain is telling you something fundamental. It is storing a chain of blocks. That actually means something. DAG, in a very real sense, doesn't mean anything. There are lots of tools in computer science. You use numbers. You use arrays. You use DAGs. They're used all through computer science, and if anybody makes up a new protocol, they might use some numbers in their protocol, and they might use arrays in their protocol, and they might use DAGs in their protocol. It's just ways of implementing things, but that doesn't mean that there is a category of number-based programs, or a category of array based. I mean, they're just tools, so DAGs are another tool, and so you'll find that there are different protocols that use DAGs, but they use them for totally different things.

Leemon Baird: 00:40:44 All a DAG is is something you can draw out as a bunch of circles connected by arrows. We use a DAG. Other ledgers use DAGs, but the circles mean something different, and the arrows mean something different, and the way you're using the whole picture means something different, and the properties of it mean something different. They have nothing in common. Just the fact that you use circles and arrows doesn't mean that there's anything in common. They are radically different things. Most of the systems that use a DAG are not using it the way we are, simply as a history of how we've talked to each other in order to do virtual voting. Instead, they're doing things that are not ABFT and aren't even BFT. They're just doing completely radically different things.

Demetri Kofinas: 00:41:24 Yeah, I'm not even sure if some of these, or any of them, have consensus mechanisms. I'm not sure. Are there any inherent advantages of one database architecture over another?

Leemon Baird: 00:41:35 For ledgers?

Demetri Kofinas: 00:41:36 Sure.

Leemon Baird: 00:41:37 Sure. Proof of work was the first one. It's sort of the generation one, but it uses ... Bitcoin itself uses more electricity than Ireland, and it's expensive to buy the mining rigs, and so what do you find? Consolidation, and it's all in one place. Proof of work has some issues. Then people started going to leader-

based systems that don't have to have proof of work. You have a king, and you let the king decide what happens. Let's work, and then if the king gets shut down, we switch to a new king, and if the attacker keeps shutting down everybody, well then, the whole system shuts down. It's a real problem, but at least you can get away-

Demetri Kofinas: 00:42:10 That's PBFT?

Leemon Baird: 00:42:11 PBFT is an example, sure, and Paxos has a problem, as an example, and Raft as an example. These are all leader-based systems. DPoS systems, delegated proof of stake, are also leader, where you take turns being leaders, and so the problem is you have the fairness problem, because the king gets to decide what's in the next block. You have the DDoS problems that if you shut down the king and follow the leader, as the leader changes-

Demetri Kofinas: 00:42:31 And you can have that even in a permissionless database if there's a virus, for example, in the network, right?

Leemon Baird: 00:42:35 Any system will be crashed if you can crash all the computers. The question is could you freeze the system by just crashing one computer at a time? Proof of work typically doesn't have that problem.

Demetri Kofinas: 00:42:47 Right, because it's random.

Leemon Baird: 00:42:48 Because it's random.

Demetri Kofinas: 00:42:49 It goes back to the reverse hash.

Leemon Baird: 00:42:50 Exactly, and so you really can't DDoS the leader because you don't know they're the leader until they've already finished leading. That's an advantage of the proof of work, but then it's very inefficient. It's also not fair, and it also leads to consolidation, which gives you problems. If it's all under one government, you have some issues. You have, then, the leader based systems that are faster, but they still have the fairness problems and the DDoS problems, but they're better in some ways, and then you have voting based systems that are super secure, but horribly inefficient, because you have to send all these votes over the internet, and you can try to merge leader with voting and say, "Well, we'll just have a few leaders and let them vote," but the simplest thing is a radically different thing, which is don't have any leaders, just do the gossip, add in two hashes, and then you actually know how we talked to each

other, and we're done. That's what we do, and you get all the strongest securities properties with the speed of very little bandwidth needed, and along with the total fairness of there's never a leader, even for a second. We don't even take turns.

Demetri Kofinas: 00:43:48 Mance, you've been sitting here. How are we doing so far?

Mance Harmon: 00:43:51 Always enjoy it. You know, Leemon is a master educator, right?

Demetri Kofinas: 00:43:55 I've been watching you as you're-

Mance Harmon: 00:43:56 I never tire of hearing him talk about this.

Demetri Kofinas: 00:43:58 I can say it's amazing. It's amazing. Inherently, we're never going to be able to address every single question. I think we've done pretty well so far. We've talked in various ways about proof of stake versus proof of ... Well, we haven't really talked about proof of stake much. We've talked about proof of work. That's come up a lot. I want to talk about the distinctions between proof of stake and proof of work for network layer security, Sybil attack resistance, for example, and then I also want to talk about the distinction between the deployment of POS, proof of stake, in Hedera versus the way it's been discussed in some of these alternative blockchain implementations, because there's so much confusion there, and I would love to address that. First, let's talk about the network layer security aspect of this. How does proof of work provide network layer security, let's say in the case of Bitcoin, the most prominent example, and how does proof of stake offer that, in terms of Hedera, and then we'll get into why you think proof of stake actually works better for Hedera, whereas perhaps it wouldn't work in some of these other implementations.

Leemon Baird: 00:45:05 Sure. The whole thing we're worried about is we want to be decentralized. We're afraid we're going to stop being decentralized, and have one attacker control the network. That's the fear, and they can do it with Sybil attacks. If you allow anonymous nodes, they can do it with Sybil attacks, which means one person creates whole bunch of computers and pretends to be a lot of different people, sock puppets, and then they all get too much influence, so how do you stop that? There's really either you have a totally permission network, where you have to have permission to run a node and everyone knows who you are, or you have some kind of a scarce resource, so you could pretend to be a million people, but then you have to split your scarce resource a million ways, and you still don't have much of a vote. It has to be one or the other. In proof of work, the scarce resource is the computational power, which

means buying a supercomputer and feeding it lots of electricity. That's the scarce resource.

Demetri Kofinas: 00:46:00 It's revving your engine.

Leemon Baird: 00:46:02 It's revving your engine, and so one person could pretend to be a million people, but they can't each have a supercomputer, because then you'd have to buy a million supercomputers, and if you buy a million supercomputers, you might as well just admit that you're one person. There's no advantage to pretending to be many. That's how you have the security, but because of the expense ... Well, it's expensive, which is bad. It's inefficient, which is bad, and that also drives consolidation, which is bad.

Demetri Kofinas: 00:46:22 I'll interrupt a second just to point that out, because I think that is important. There are huge economies of scale associated with proof of work, and that causes centralization, right? Not just in terms of the ASICs, right, that are used, which are difficult for most people to have, applications specific integrated circuits, but then there's also advantages to pooling the resources, of course, of these classic economies of scale. The more computers you have, the cheaper each additional computer will be. Also, certain geographical areas subsidize electricity, or electricity is cheaper in certain areas, so there are all sorts of ways in which proof of work causes centralization, right, and anyway, please continue. I just wanted to make that point.

Leemon Baird: 00:47:01 That's absolutely true, and I think it's widely recognized that proof of work is not ideal. It causes centralization for the very reasons that you said, because you have to buy an expensive computer, and there's economies of scale, which means the small person can't just buy a tiny piece of that computer. They have to buy a big thing, and you have to feed it lots of cheap electricity.

Demetri Kofinas: 00:47:18 I also actually want to make one more point. The way that proof of work works, in terms of the lottery, it makes it increasingly expensive if you're operating a single computer, because the chance that you'll win the lottery at any point in the lifetime of the CPU is very small, so it's to your advantage to pool together lots and lots and lots of machines, because it's smoothens out the volatility of the cost versus the reward of actually winning the election and having the opportunity to propose the next block, right?

Leemon Baird: 00:47:43 Yes, and this actually adds to a whole other layer of security problems.

Demetri Kofinas: 00:47:46 It's a question of fairness, too, in terms of compensation.

Leemon Baird: 00:47:49 Exactly. If you said, "I will make some money, but I'll only get paid once every 10 years with my computer," even if on average, I make enough money to justify doing it, I won't do it, so what do I do? Well, I get into a pool with a bunch of other people, and we all agree, "Well, whoever wins will share with everybody." But how do you know that I was actually mining while we were running? I get my share if you win, but how do you know that I did my share part-

Demetri Kofinas: 00:48:13 The free riding problem.

Leemon Baird: 00:48:14 The free riding problem. It gets even worse when you have forks that use the same protocol, because now I can pretend to be part of pools of different protocols, and I'm actually going back and forth which one I'm actually doing the hashing on, and so then you have all sorts of questions. How do I prove that I tried to solve the problem and failed, as opposed to, "I spent my time on somebody else's network, and I still want to get paid"? There're all sorts of issues that happen with that. Pools are not ideal. With a proof of stake system, which I'll explain in a second, you can just get paid every day. You don't ever need pools. I like not having pools. It's much cleaner not to have pools. It's much more decentralized. I mean, by definition, a pool is some guy who's running the pool, and it's becoming more centralized.

Demetri Kofinas: 00:48:51 Yeah, absolutely.

Leemon Baird: 00:48:51 You have problems across the board, so we have to have a scarce resource. If your scarce resource isn't going to be electricity and supercomputers, what will your scarce resource be? Well, it can be tokens of some kind, so you could use the cryptocurrency itself as the stake in the network, or you could use something else to stake, but it has to be something that is widely spread out to stop the Sybil attack, and it also has to be valuable enough, or somehow hard enough to transfer that one attacker can't get all of it, because then they would dominate and destroy you. I think the world as a whole is coming to the understanding that proof of work was a great v1, great generation one, but now we need to move onto something else.

Leemon Baird: 00:49:29 Proof of stake is sort of a catchall term that basically covers everything that isn't proof of work, and that's really the way to go is that you want to have a proof of stake system. Okay, so you asked about our proof of stake system. Hedera Hashgraph is proof of stake. That's good. That allows you to spread out and

become decentralized, and have anonymous nodes. You don't have to worry about Sybil attacks. You have proof of stake, but of course, you always have, then, the chicken and egg problem. You can't have a secure network with anonymous nodes until you have the widespread valuable stake, but you can't have the widespread valuable stake until you have a working network that everybody is using, so it's a chicken and egg problem. How do you solve that problem? Here's how you solve that problem.

Leemon Baird: 00:50:13 You create a council that everyone can trust that can run the system, and then you go starting with just a few computers run by them, which then expands to computers run by people we know, which is permission, but broader, which then expands to anonymous nodes. Anyone can run a node, which now is permissionless, and so you have this continuum of building up to that. You have staked from the beginning. You have coins from the beginning, and over time, they are spreading out. People are using them around the world. They're buying and selling them. They're using them on the network. They're becoming more valuable as the network itself becomes more valuable, and it becomes valuable because of all the things built on top of it, and so by the time you have spread out to anonymous nodes, the Sybil attack is not a concern.

Demetri Kofinas: 00:50:58 I want to get into more detail here, because I have a lot written out about proof of stake and the way the voting works and everything else. Before we get there, and we've done a good job, I think, so far, really hitting on all the points I've written down here, I do want to clarify for those who don't know the distinction between permissioned and permissionless. We might have actually touched on it already. I mean, we definitely touched on it, but I don't know if we were clear about it, and the difference between public and private networks, and then also perhaps a little bit between distributed and decentralized, because those words get thrown around a lot. Maybe we could start with public and private network. Hedera is a public network, as opposed to a private network. What is that distinction?

Leemon Baird: 00:51:35 Yeah, so public and private refers to who can use the network. Permissioned and permissionless says who can run the network, and so we have, in Hedera, a network that is public from day one, and becomes more and more permissionless over time. It starts off with just a handful of nodes that we're controlling. That's permissioned, but then it evolves to have more and more and less and less control over who's doing it, until it's millions of random people around the world who are running nodes. They don't have to say who they are. They don't have to tell anyone

who they are. They just say, "I want to run a node." They can stake their stake, and they can run a node, and they influence the consensus. They can make up shards, and all that stuff. There is a continuum that you go from. You can have private versus public. Both are useful. We are public, purely public, from the beginning, and then you have permissioned versus permissionless, and we're on the path to allow that to happen as the stake allows it to be done securely.

Demetri Kofinas: 00:52:35 All right, so great, so here we are now. We're on page four of my rundown. Path to decentralization, that's what you're talking about. It's the path from a permissioned network to a permissionless network, and that brings us back to proof of stake and why this path is necessary. Let's go back to where you were before. We were talking about proof of stake and how that works on Hedera. Let's get back to that. Can you explain how proof of stake works, and then we'll continue along this conversation?

Leemon Baird: 00:52:59 Sure, so proof of stake works by the nodes helping the consensus, and the amount of weight they have in the consensus, the amount of influence they have in the consensus is proportional to how much stake they have. If you spread out the stake, everybody has sort of equal weight, and as long as not too many of them are bad, we're okay. It is inherent in the math that if the bad guys work together, so you really have one bad guy, one attacker, and they have a third of the stake, then they can do bad things. They can corrupt the whole network, and this is inherent in every system, even systems that say, "We have a 51% attack." They do have a 51% attack, but they also have a 34% attack if you have firewalls, if the internet is controlled by the attacker too. Some systems actually have a firewall around the country that it's mostly inside of. You can have this problem.

Demetri Kofinas: 00:53:45 Stake refers to financial stake, right? It's 100% of the stake of the network is equivalent to the market capitalization of the network.

Leemon Baird: 00:53:54 For what we're doing, yes. We're using the HBARS as the stake, and that's the most common thing. Typically, in a ledger, you use the cryptocurrency as the stake. That's a common thing. Theoretically, you could do something else, but that's what we use, and so it has to be spread out, but it also has to be hard for one bad guy to get them all, and so that means they have to be expensive enough that one bad person couldn't get them all. If we just released all the stake on day one, it is entirely possible

that we would have whales, and you have the Gini index that says, "To what degree do you have whales?"

Leemon Baird: 00:54:25 It's entirely possible that the whales could get a third of all the coins that are in existence, and if you have a fixed supply of coins, they never get any more, once a whale has a third of all of them, you're kind of out of luck forever. On the other hand, if you have a fixed supply ... We have a fixed supply of 50 billion coins. There'll never be more HBARS, but if you release them slowly over time, okay, on day one, maybe a whale gets a third of all the ones released on day one, but that doesn't mean they're going to continue to be able to do this over time. As it grows, as the price of the coins or the total value of all the circulating coins, I should say, goes up, then it becomes really hard for, 10 years from now, a whale to be having a third of all the coins.

Demetri Kofinas: 00:55:08 So the security of your network is contingent upon a sufficiently large market capitalization, and the high market cap makes it difficult for any one particular or conspiracy of actors to accumulate one third of the HBARS on the network in order to attack the network.

Leemon Baird: 00:55:26 That's exactly right, and we don't have to have it on day one. We just have to have it by the time we have those anonymous nodes.

Demetri Kofinas: 00:55:32 Yeah, so you'd have to be super careful about how you release your HBARS into the market, and this is the explanation for why you have elected to follow the release schedule that you have.

Leemon Baird: 00:55:44 Exactly, so most people don't publish release schedules for their token. We've done so for the whole 15-year period, because we think it's important.

Demetri Kofinas: 00:55:51 So it's a 15 year release schedule.

Leemon Baird: 00:55:54 It is a 15 year release schedule.

Demetri Kofinas: 00:55:55 That's a long time, Leemon.

Leemon Baird: 00:55:55 And it is linear. Yes.

Demetri Kofinas: 00:55:55 I thought about it. It made me feel old when I thought about how old I'd be when it'd be done.

Leemon Baird: 00:56:01 Oh, I know. Seriously-

Mance Harmon: 00:56:04 It's short compared to Bitcoin.

Leemon Baird: 00:56:08 Not really, because Bitcoin's not linear. Yeah, it takes 100 years to get that last Bitcoin, but right now, we're already, what, 18/21 of the way through it?

Demetri Kofinas: 00:56:16 But it is important, and obviously, I knew the answer to this question, but the reason I wanted to make the point is that there's a good reason why you're doing this, because we know this, there's FUD. There're all sorts of misinformation in the market, and one of them is this idea that somehow ... In fact, one time I mentioned this on Twitter, and I explained it, and someone said, "Yeah, sure. That's really the reason," but if your objective was somehow to make a quick buck, you wouldn't want to release these over 15 years. You'd dump them into the market as soon as you could, make your money, and close the scam.

Leemon Baird: 00:56:47 Of course. Our goal is to build a 100-year company, that this company's going to be around for 100 years, and to build a ledger that will be around for 100 years. We want this to become the infrastructure of the entire planet for generations to come, and we're serious about that. One indication of our seriousness is that we're releasing our coins over a 15-year period. Another indication of seriousness is that the founders themselves have locked up their own coins to dribble out over seven years. In your typical scam, rule one of Scam 101, don't dribble out your profit to yourself over seven years. In fact, the majority of our coins are after year five.

Demetri Kofinas: 00:57:23 Well, I mentioned at the beginning of the intro of the show that I'm an investor, and I'm more than happy to have lockups because I think that what's important is that this be successful. Do you envision this being the next layer of the internet?

Leemon Baird: 00:57:37 It is. I absolutely do envision that. The bottom layer of the internet just gets bits to move around, but the layer on top of that creates trust, and we need to have that, and so I absolutely do see this as the trust layer of the internet.

Demetri Kofinas: 00:57:52 It could be cool, if we had time towards the end, to talk a little bit more about how the internet protocols allowed for decentralized or disintermediation of the communication layer, and that this sort of does that for being able to say something about that communication in a trustless, decentralized way. Maybe there's a better way to describe it. We'll see if we can get into that. Did you want to make a point, Leemon? Actually, I see you want to make a point.

Leemon Baird: 00:58:16 I do.

Mance Harmon: 00:58:17 Probably worth it.

Leemon Baird: 00:58:18 I don't know, so this is not the whole internet. You do not want the whole internet to be a public ledger. There's room for private ledgers as well.

Demetri Kofinas: 00:58:26 Well, it wouldn't work. In some cases-

Leemon Baird: 00:58:28 Some things are private.

Demetri Kofinas: 00:58:28 Yeah, yeah, yeah.

Leemon Baird: 00:58:29 Some data is private, which is why we're doing the ordering service with Hyperledger to allow you to have private networks and public networks, but more importantly, have them work together, and so the stuff that should be public can be public, and the stuff that should be private can be private. That's the future of the internet.

Demetri Kofinas: 00:58:47 At this point now I've got three more pages here, and I think we're going to end up having to jump around, because the next point I wanted to discuss, and maybe we can try to discuss it a little bit here and then we can move forward, because I had a section around network protection, and one of the things I wrote down here are theoretical attacks. For whatever reason, I kind of get off on thinking about this stuff, and you guys do proxy staking, for example, right? Now, there's an example of how let's say your market cap is $100 million. Not only would it cost you at least $33 million to get a third, but as you get closer to that number, the market is a dynamic system. Market participants see that the price is going up.

Demetri Kofinas: 00:59:26 They're going to start speculating that something's happening, and they want to pile into HBARS, and that drives the price up higher. It's very difficult to corner the market. I think the Hunt brothers got something like 10% of the silver market, and that was a big deal, and there was Fisk and Gould with trying to corner the gold market in the 1870s or something, so it's extraordinarily difficult to corner a market, and the reason why is because it becomes incrementally more difficult. People see that the price is rising, and they pile in, but you guys offer something known as proxy staking, so first of all, let's discuss that, because we didn't get a chance to discuss that, and then we can use that as an example of ways in which theoretical attack vectors open up for economy based systems, and how

you deal with those, and how you will deal with those in the future.

Leemon Baird: 01:00:14 Yes, so the proxy staking allows you to take your tokens and choose nodes you think are reliable or going to be around for a while, and say, "It gets credit for my HBARS. It gets credit for my cryptocurrency, in the consensus algorithm." First of all, you want to proxy stake to somebody who's not going to shut down, because if they shut down, you don't get paid. You have motivation to try to find nodes that are reliable, that are being up reliably. Maybe they've been up for a long time because that has greater indication of reliability, and then people will be proxy staking to those nodes, but they can't have too many people proxy staking to one node, because there's a cap, and so you'll end up spreading it around the nodes that you believe are reliable.

Leemon Baird: 01:01:01 You can imagine an attacker is going to try to stand up lots of nodes to do an attack on the network. First of all, on day one, no one's proxy staking to them, so maybe they have a multi, multi-year attack plan where they stand up these nodes and build up a reputation, each of the nodes building up its own reputation separately. This is difficult. This is a long time, and they have to convince lots of people to do it, and there has to only be one attacker doing this. If you've got four attackers doing it, we don't care, because none of them is going to get a third of the proxying.

Demetri Kofinas: 01:01:29 You'd need to be something like a credit worthy borrower with a long history and a great credit, where you'd be able to leverage up tremendously. That's one way to sort of describe it. I know it's not borrowing, exactly, but-

Leemon Baird: 01:01:40 It's borrowing good will, or borrowing your reputation, or something. Yeah, it's manufacturing reputation, so it's a reputation-based system that way.

Demetri Kofinas: 01:01:46 But the idea is basically that you wouldn't need to actually purchase the HBARS in the market. You'd actually be able to borrow them, basically.

Leemon Baird: 01:01:53 Well, you could think of it that way.

Demetri Kofinas: 01:01:53 Yeah, it's not exactly borrowing them.

Leemon Baird: 01:01:53 Someone is lending them to you for that purpose. Yeah, it's not exactly borrowing.

Demetri Kofinas: 01:01:57 I should say another thing, also. Another way in which I don't literally communicate this, but metaphorically ... It's an imperfect metaphor. Another aspect of this is I talk about taxi medallions, because you can own a taxi medallion and not operate a taxi. You can own HBARS and not operate a node. You can allow someone else to operate that node.

Leemon Baird: 01:02:17 True. What you are doing, as an ordinary person proxying your coins, is you're helping the network be reliable by figuring out which nodes you think are reliable, and you can look at their reputation, there can be online reputation things. In addition, you don't have to make all those decisions yourself. I imagine lots of people would be writing wallet software, and they can help you out, and they have even more motivation to do even more good on this. Now, if there were only one wallet software company in the world, then of course, they might be able to redirect lots of people, which would be bad, but we expect a huge ecosystem with this.

Demetri Kofinas: 01:02:49 You're purposely introducing competition into this market so that it can evolve.

Leemon Baird: 01:02:53 Exactly. We have competition at every level, so we have competition among the nodes trying to be reliable so that people will proxy to them. We have competition among the people trying to decide which nodes they want to proxy to. We have competition of the wallet developers with each other, and then they can help people proxy, and they can maybe have defaults for proxying, other ways to monetize proxying, and again, it's okay to have attackers. If you have four joined attackers, they can't do any harm at all. You have to have one big attacker that gets a third of everything, and so we have multiple layers of protection here, and this is why we don't say that proxy staking gives you a payment that's just a handout.

Leemon Baird: 01:03:29 We say you're actually earning it by making the network better, and it's actually true. The people doing the proxy staking are making the network better with no risk, and I've got to talk about this. You asked with the difference between different staking systems. We have no bonding, no slashing. Let's talk about what those words might mean. If you want to stake coins because you have a node, or you want to proxy stake coins because you like getting paid to proxy stake, you can do so. As long as the node is running, it gets paid once a day, and as long as you're proxy staking to someone who's running and they're not over the limit, the cap, you get paid once a day. You do not have to freeze your coins and promise not to spend them. At every nanosecond, you can spend all your coins if you want.

Demetri Kofinas: 01:04:13 Your HBARS.

Leemon Baird: 01:04:13 Your HBARS.

Demetri Kofinas: 01:04:14 Yeah.

Leemon Baird: 01:04:14 You can spend them anytime you want. You can spend all the HBARS in your account at any moment, and you simply don't get paid anymore after you spend them.

Demetri Kofinas: 01:04:21 The same HBARS that are being used to create network layer security to stake the system are also being used in order to conduct transactions and pay fees, et cetera.

Leemon Baird: 01:04:31 Exactly.

Demetri Kofinas: 01:04:31 At the same time, the same ones.

Leemon Baird: 01:04:33 At the same time, and you don't have to color them differently. You don't have to say, "I'm setting these aside just for my proxy staking." No, no, just put them all in your account, proxy stake all of them, and then whenever you want to buy something, just buy it. Whenever you want to do a transaction, use this to do the transaction fees. You don't have to set them aside and bond them. Even better, there's no slashing. If you do something evil, we're not going to take away your coins, and a lot of systems, what security they can get is based on, "Well, we'll slash people, and that will motivate them to not do anything bad," and then you have to say, "Well, did you slash enough to stop them from doing something bad? Maybe they could make enough by doing something bad to pay for the slashing." We say, "Well, no. It's inherent in the math. You can't do anything bad until you get a third of the coins, period."

Demetri Kofinas: 01:05:15 What if your computer is compromised, and there was a virus running, which was conducting an attack, and it was using your computer and your stake without your intention?

Leemon Baird: 01:05:24 Yeah, as long as it's less than a third of the coins, it has no effect.

Demetri Kofinas: 01:05:26 Yeah, yeah, no, I just meant in terms of the slashing. I don't see how that necessarily would be helpful.

Leemon Baird: 01:05:30 Ah, you're right. Let me say what you just said, because it's a really big point. People say, "If a rational economic actor has their coins at risk, and if they do anything wrong, I will take

away their coins. That will make them not do anything wrong," but you're saying, "Wait, they're not a person. They're a computer. It could be hacked. It could have a virus, and it could decide to do something wrong because it doesn't mind if its owner loses their coins." That's a really good point. There's no risk to proxy stake, and we do the proxy staking because it makes the network more secure, but we're not using this to drive up the price of the coin or at. It's not a lot of money that we pay to proxy stake. It's just a little bit to encourage people to do it. It encourages them to help the network become more healthy.

Demetri Kofinas: 01:06:12 Let's talk about that. Let's talk about network fees.

Leemon Baird: 01:06:15 Yeah.

Demetri Kofinas: 01:06:16 Because those are a little complicated. They're one of the more complicated parts of the white paper, because there are a lot of different fees, and they function in different ways. Maybe you can help break that down for us here.

Leemon Baird: 01:06:26 Okay, so for geeks that are interested in the details and the guts of the system, it's really complicated, and there's lots of reasons for all the parts, and we can talk about it, but for users, it's actually very simple. Whenever you do a transaction on the network, you pay a fee, and if you want to know how much your fee is, the SDK tells you. The SDK has built in the ability to figure out how much your fee is for a given transaction, or if you're using a program, the program can be telling you how much your fee is going to be. In fact, we even have this great tool.

Leemon Baird: 01:06:57 It's a web page that you go to and it shows you what your fee will be for a transaction. You can describe the transaction, and it tells you what the fee will be, and you can say how many of different types of transactions you're going to do. It has almost like a shopping cart where you say what the transactions are, and how many of each one you're going to do, and it tells you what your total fee will be. It's a beautiful tool, and so transaction fees are really simple. Technical us your transaction, we tell you what the fee is. Under the hood ... As a mathematician, I love all the complexity, and as a computer scientist, it's just really cool, but it's simple for the user.

Demetri Kofinas: 01:07:27 Maybe also the more important point is that fees are extraordinarily low, and this is why micro-transactions are possible on the platform.

Leemon Baird: 01:07:34 Exactly. If you charge a fee of $1 a piece, or 10 cents apiece, you can do something useful, but if you charge a fee for a fraction of a cent for each transaction, it opens up new kinds of things that you can do. You can do things like surfing the web and paying a fraction of a cent to read each web article that you're reading, and not have advertising, not have someone spying on you, but you can only do the if the fee is a fraction of a penny. If the fee was 50 cents, you can't do that, so we have extremely low fees for that reason. It's because we can do payments very fast, so we can afford to charge a very low fee for each payment.

Demetri Kofinas: 01:08:08 Just in the interest of time, let's actually go to governance, because I want to make sure we hit on this before we possibly run out of time, because I got you guys for another, I think, 30, 40 minutes or so. Mance, maybe this question is directed at you. Top level, how does governance work on Hedera Hashgraph, and how is it different than, let's say, other platforms, and why is that important?

Mance Harmon: 01:08:33 Sure. Well, let's start with the other platforms first, right? When we talk about governance, what do we really mean, right? In our case, what we're referring to is the body of decision makers that are deciding on what features to add to the platform. When do those features get released to the network? What are the fees that are charged for the use of these services? What are the rates paid to those nodes in the network that are processing the transactions? Those are the kinds of decisions that we're referring to when we talk about governance. When we look at Bitcoin, for example, there are a dozen core developers that are making decisions about what the features should be, and then there are a set of miners that are deciding whether or not they want to adopt those features, and so in that sense, it's bicameral governance. If we talk about Ethereum, there's a foundation, and there are core developers, and you know, each platform has some form of council, if you want to use that term, that's deciding on the decisions for the network as a whole.

Demetri Kofinas: 01:09:42 It just may not be institutional.

Mance Harmon: 01:09:44 It may not be institutional. It may be very loosely coupled, but nevertheless, it's a relatively small number of real decision makers. I mean, people will say that there are thousands of contributors to Bitcoin or Ethereum, and that may very well be true, but the decision of what goes into the platform lies in the hands of just a few.

Demetri Kofinas: 01:10:07 Is governance the same thing as talking about where power resides to alter the software? Is that the primary?

Mance Harmon: 01:10:13 That's a major component of it, absolutely. Who has the authority or the power to decide what the "product roadmap" is going to be for the software that enables the network? In our case, what we've done is we've just recognized that fact publicly. We recognize that there always is a decision body, and we've deliberately made the decision to try and create the most decentralized governing body of any of the public networks. What that looks like for us is a council of 39 global organizations, blue chip organizations, that are trustworthy, they have great brand respect by their markets, and also, some of the largest companies the world.

Demetri Kofinas: 01:11:03 Some of which we mentioned at the top of the show.

Mance Harmon: 01:11:05 Yeah, exactly, the ones that we talked about at the beginning. They're chosen across 18 sectors of the market. We want full representation from all the different markets, in terms of what the product roadmap should be, and then also, they are geo-distributed. We're not pulling members just from a certain jurisdiction or certain geography. We want a global representation, and then finally, they're term limited. We don't want a council that is stagnant. We want a council that is dynamic, and so these council members can serve up to two, three-year terms for a max of six years before they have to rotate off the council, and they're replaced by somebody else.

Demetri Kofinas: 01:11:46 Can they come back on at some point?

Mance Harmon: 01:11:47 Theoretically, but the reality is that if we're talking about 18 sectors of the market, I mean, today, for example, we have two Telcos, and there are a lot of Telcos that have an interest in participating, and so over time, it's possible that there may be a Telco that leaves the council and ultimately comes back, but we want a dynamic representation across the industries.

Demetri Kofinas: 01:12:13 Is the desire for industrial distribution, distribution across all sorts of industries, geographical distribution, and of course, the term limits, is that because you feel that Hedera can offer solutions for all sorts of industries across all domains, and you want to be able to get that level of representation and stakeholdership, in a sense?

Mance Harmon: 01:12:33 That's absolutely the case. That plays into it. We want the platform, the features in the platform, to be the right features

that support general purpose use cases across industries, not for a specific sector or specific market, and so we want that broad distribution of representation. It's also the case that we have the council, and we don't want the council members to be aligned, in any sense, motivated to collude, and so it's far less likely that the council members would collude or form constituencies within the council to try and have more influence than they ought if they're cross-sector and geo-distributed and distributed through time as well. This increases the trust in the council itself by structuring it this way.

Demetri Kofinas: 01:13:31 The council members come to decisions through supermajority voting?

Mance Harmon: 01:13:36 Oh, well, there are range of decision categories. You know, the simplest is 51% vote, and in some cases, it's a supermajority, and in a few cases, rare cases, it may be-

Demetri Kofinas: 01:13:49 Unanimous.

Mance Harmon: 01:13:50 ... a unanimous vote that's required.

Demetri Kofinas: 01:13:52 What are some of the more important things that the council can do, and then what are some of the things it can't do that are important to note here? With obviously understanding that we can't go through everything.

Mance Harmon: 01:14:03 Yeah, so here's an example of something that would be really hard to do, and we would highly discourage. We have minted 50 billion tokens, and it has been our intent from the very beginning that that does not inflate. If it were the case that some council members thought that it should inflate, or that we should mint more tokens in the future, that kind of decision would take a unanimous vote, but if we're talking about what are the next features that should be including in the platform, well, there are actually committees that are structured to deal with every part of the organization.

Mance Harmon: 01:14:42 There's a tech steering committee, for example, and council members that have technical expertise will likely contribute at the tech steering committee level. There's a legal and regulatory committee, for example. Same deal there. The committees will make recommendations to the council of various forms, and the council will then vote on what those committees recommend. I mean, hypothetically, or theoretically, the council can do anything they want. Practically, the council is incentivized to do

what's in the best interest of the network, and disincentivized to do what's in self-interest.

Demetri Kofinas: 01:15:17 Let's talk about that a second, because this is a really great point, because also in Bitcoin, theoretically, there is a fixed supply, but of course, it can also be changed because it is software. The security and confidence that the market puts in Bitcoin's price is borne out of a culture of crypto-anarchism and an ideology, an Austrian hard money ideology at the core of the developer community, in Bitcoin. In terms of Hedera, certainly it's obvious to me why you would want to limit supply, because first and foremost, you want a high market cap, because you're motivated to have a high market cap, and you're also motivated, interestingly enough, to have as equal distribution as possible of ownership of stake, because that maximizes the security of the network, right? So, what would be potentially a motivation to increase the supply of HBARS?

Leemon Baird: 01:16:10 Frankly, I don't think there is one. The traditional answer might be, "Well, if people need more coins just to do an economy, you need more coins," but these are almost infinitely divisible, right? You can go down to a hundred-millionth of a coin. That argument wouldn't apply.

Demetri Kofinas: 01:16:24 Or maybe if, let's say one of the council members or a group of council members wanted to give themselves new HBARS, right? That's where it would make sense.

Leemon Baird: 01:16:31 Sure, so there you're embezzling. Here's what goes on. I mean, that's basically what we're talking about.

Demetri Kofinas: 01:16:35 Right. Yeah.

Leemon Baird: 01:16:36 That's why we've structured it in such a way that it is extremely hard. The council has to agree to change this bedrock commitment that it has made, but now wait a second. This is a commitment that Hedera has made to the world. We're going to stay at 50 billion. We're not going to do more. What is the reputational cost to all these giant companies of trying to do such a thing? It is enormous, and you have to get them all to agree to it, and they're all in different countries, and they're all in different sectors. It would be harmful to all of them, and they would have to all agree to harm themselves in this way to break our promises in this way by doing inflation. It becomes very hard. It might be easier to bribe a handful of developers on another ledger to do an inflation thing than it would be to do this.

Demetri Kofinas: 01:17:19 So Mance, you said that you've already minted all the coins. The coins that haven't already been allocated to investors, employees, Swirlds, which is the parent company, are in the Hedera treasury. I want to quickly just touch on that, and then I want to move into open source versus open review. I think we talked about forking, but the role of IP, what is the role of your IP in terms of governance, and a few other important points before we finish. But let's clarify that really quickly. What percentage is the Hedera treasury, which is going to be part of the release schedule and sold to the public, and how does the rest of this ownership break down?

Mance Harmon: 01:17:56 Yeah, well, in terms of percentage that is in treasury, on day one, it's less than 5% that is going into circulating supply, which means it's over 95% that remains in treasury. The total release schedule, as Leemon mentioned earlier, is over a 15-year period, and we've split that up really into conceptually three different five-year periods. The first five years will likely see the first third, or 33%, being distributed over that first five-year period-

Demetri Kofinas: 01:18:30 Combined with treasury and also people that are able to sell their HBARS? Is that how that works?

Mance Harmon: 01:18:35 Yeah, exactly, so those that have invested in the token earlier, through the SAFT mechanism, they're getting their token allocation over that period. The employees are getting their token allocations over that period. As an organization, there are tokens that are reserved just to incent the community in various ways, and there may be treasury sales as well, but that entire five-year period will result in approximately 33% being released over the period, and that's true for the next five years and the following five years, with a fairly straight, smooth curve, if you will, for the token release schedule itself.

Demetri Kofinas: 01:19:21 All right, let's talk about this distinction between open source and open review.

Mance Harmon: 01:19:24 Right.

Demetri Kofinas: 01:19:25 You guys are open review. The industry is open source. I want to really nail down those distinctions.

Mance Harmon: 01:19:34 Yeah, so open source simply means that, at least in our industry, means that anybody that chooses to make a copy of the existing public ledger and go and create a competing public ledger may do so, and that results in some negative consequences for

anybody that's built an application on the ledger, where the state of that application gets copied and it's part of that process, and when that happens, for example, let's just hypothetically say that we have a land registry application that's running on a public ledger, and the registry itself records ownership of land parcels. Well, there's software out there running on computers and smartphones, maybe, that is used to update the land ownership in that registry.

Mance Harmon: 01:20:27 If the product, or the platform, rather, is pure open source, then it's possible for some of the node operators or miners to become disgruntled, say they're going to copy that, go create a competing network with a competing cryptocurrency, and when they do that, that land registry now gets copied and it exists now on two separate networks, and that same software, the client software running on computers and phones, it still connects to the same total set of nodes, but now some of the nodes are in the old network and some of the nodes are in the new network, and you have that land registry diverges, and it creates chaos for the application developer. You have to solve that problem fundamentally.

Demetri Kofinas: 01:21:13 Is that something that enterprises have told you is a concern for them?

Mance Harmon: 01:21:17 Well, what I can say is that we have council members that are building on top of us because the ability to prevent that from happening is an enterprise feature that the enterprises absolutely will care about over time. Now, it's still the case that most people in this industry don't even recognize this as an issue yet, and that's in part because there haven't been a lot of enterprise use cases built, period, on public networks, because of some of these issues.

Demetri Kofinas: 01:21:49 Also, an important point is there is a culture of open source, but open source in something like Linux is very different than open source in something like permissionless databases and base layers that are monetizable, where so much of the financial opportunity is in the base layer, is in the protocol.

Leemon Baird: 01:22:05 Absolutely. I'd like to give the answer to that one too. I thought it'd be useful to hear both.

Demetri Kofinas: 01:22:09 Sure.

Leemon Baird: 01:22:10 Open source and open review, open source means that anyone can take the software and read it, and they can also stand up

competing networks that are doing going to same thing. Open review means anyone can read it, but they can't stand up a competing network, and so we would be doing an open review rather than open source for the software to stop the network from forking. The goal is to make the network be stable for the people that want to build on top of it that don't want their network forking. When we have seen forks, we have seen confusion as to, "Well, which one is the real one? Which of the two is the real one and which one is a new network that's coming off of it? Which one is the ledger that's just sort of the new upstart?" It's not always obvious which one is the real one, and it isn't obvious which one people should go to.

Leemon Baird: 01:22:49 If you have software on your phone that goes to the ledger to get information, it's not clear which one to go to, so one of the mechanisms that we're using, one of several mechanisms to stop forking, or to combat that, is the open review rather than open source for the ledger software itself. On the other hand, we're open sourcing lots of stuff. We're open sourcing the mirror nodes. Anybody can run mirror nodes. We're open sourcing the software that does the wallets on iOS and on Android. We have a Chrome plugin that lets your browser actually let you browse websites and pay for articles. We're open sourcing that, and we have a WordPress plugin that allows you to monetize your own site. We're open sourcing that, so we're doing lots of open source. The SDKs have some open source versions, but we're not going to open source the core network. We're going to open review it.

Demetri Kofinas: 01:23:35 That's so important, though, because I really, really, really want to drive home what that is, because some of these words, they have strong values associated with them, and you are as open as open can be. There's nothing that's not transparent. People can copy and recompile your code. They simply can't legally redeploy it. In fact, they can illegally redeploy it, and the only reason they can do that is because it's openly accessible. For example, Apple is an example of a very closed ecosystem, right? Not only is it a black box ... In other words, you don't have access to Apple's code, but Apple also prevents companies from developing on their platform without a license.

Demetri Kofinas: 01:24:15 Same thing with Sony PlayStation, for example. Strong amounts of control. Android opens it up to developers. They don't need a license to develop on Android, but you cannot look at the code. You don't know what's running on Google's servers. For you guys, it's wide open. It's there for anyone to see. It's full transparency. The only thing you're saying is that you're not allowed to copy this code and redeploy it and call it something

else, and compete with Hedera directly and cause confusion among the ecosystem of application developers or enterprises that have built on this, that are relying on a stable platform.

Leemon Baird: 01:24:50 That's exactly right, so it's just dealing with the forking issue. The transparency is there, because you can see the code and know what's going on, and when you're running a node, you can even see the code of what you're running, and know it's inter-operating with the others, so you even know that the code is correct. You actually have a way of checking whether the code is truly the real code. You can build on top of us, with a dapp or whatever, without talking to us. Any anonymous person can create a smart contract and deploy it to the network, and anyone can write a program that uses the network for cryptocurrency or for files. There's transparency there. There's openness to allowing people to do that. We have all these tools to build on is that we are open sourcing, and we're trying to have as much transparency as possible in the process to hold the council accountable, and that's part of the reason you trust the council is because they care about their own reputations. They don't want to do something nefarious because they'll get caught immediately.

Demetri Kofinas: 01:25:38 Unfortunately, we're speeding up along this way. I would like to spend more time in each one of these points, but just given the amount of time we have, I want to ask one more important question, and then I'll let you guys add anything else you want to ask about governance before we move into application development, because I want to get into the stuff for the devs. World governance. That's my subtitle for it, but what I mean is how would you respond to a legitimate question, which would be, "Oh, you've got 39 multinational corporations? Is this just some kind of corporate multinational power grab? How do we know that this is not some sort of multinational corporation supplanting national governments, and that this is what Hedera will evolve into, whether intentionally or unintentionally?"

Leemon Baird: 01:26:18 This is not a multinational corporation grabbing power, because it is balanced by 38 other multinational corporations.

Demetri Kofinas: 01:26:26 Well, how about this, a potential cabal of multinational corporations?

Leemon Baird: 01:26:29 This is a really big cabal. It is a bigger cabal than the cabal that is running, you know, some of these developers that run some of these other ledgers. No, the goal here is cabal implies some very close buddies that are very closely aligned. That's why we have the decentralized council. They're on different continents in

different industries, with different interests, so they can collude with various things, but to a large degree, they're balancing each other with checks and balances, plus we have the transparency. Even the meeting minutes get published. Total transparency. The code can be seen. You can see what they're doing with the code base. If they do something truly nefarious, like inflate the money supply, the backlash to them will hurt substantially, and again, it's not like they're all in the same industry, and they're in smoke filled rooms doing backdoor deals. These are people spread around the planet. They're east and west. They're northern hemisphere and southern hemisphere. They're different continents, and they're different industries.

Demetri Kofinas: 01:27:29 That's a good point. Actually, this brings up another question that I have further along, which has to do with you guys have taken a squeaky-clean approach from the very beginning, and you've actually generated a lot of backlash among the community, which had become accustomed to this ICO model, which also, of course, ironically, is the source of so many scams. Your approach has been the opposite. You have, at every turn, sought to minimize risk of regulatory backlash or doing anything that would put you under a negative spotlight. I think the reason for that is obvious. I know it, and it's because you, from the beginning, have felt that you've solved consensus, and that you have, as Leemon said, a platform that you want to be around for decades, if not centuries, and you didn't want to eff it up, I think is the simple way to put it. Just talk to me a little bit about the approach you've taken in order to be regulatory compliant at every turn, and your relationship, Hedera's relationship, to governments, and how you see that platform fitting into all of that.

Mance Harmon: 01:28:30 Yeah, well, there are two parts to that answer, right? One is our posture, as it relates to the regulators, when going to market with this global network, and then second is what we've built into the network itself that is intended to make it possible for the regulators to be able to do their job, and so when we started all of this, it was recommended to us by a lot of people that we not be domiciled in the United States, and that we not sell tokens or SAFTs to US citizens, et cetera. Because of the regulatory unclarity or ambiguity in the United States, we decided to take exactly the opposite approach, and it's for the reasons that you've already articulated, and that is that if you're wanting to build a 100-year company, then the decisions that you make are very different than if you're just wanting to make a bunch of money in the next few years.

Mance Harmon: 01:29:24 We decided to domicile in the United States. We've engaged with the regulators very directly now in a dialogue that's almost a year old, and we've made it very clear to them our plans and our approach, and so far, so good. We're going down a path that appears to be the best path that we can take at this moment in time. We haven't had any negative feedback from the regulators, and so that's been the posture, and it has everything to do with the fact that we're wanting to build a company that's going to be around for 100 years. Second, we also recognized that in the platform itself, there needs to be a capability or a feature set that makes it possible for the regulators to be able to do their job, and so, Leemon, I'm going to toss the ball to you on talking about the claim system.

Leemon Baird: 01:30:18 Yeah, so we have live hashes. We used to call them claims. You may have heard that previous. We have live hashes. We have this way that if you have an account that holds HBARS, it can be anonymous. You don't have to tell us who you are. You can do whatever you want, and if you want to go spend it at a store, or you want to transfer it to a bank, as long as the store and the bank are okay with it, you can do so, but if there are jurisdictions where they want to put restrictions on their stores or on their banks, they could say, "We want you to only have trusted accounts that are able to interact with our stores and our banks," trusted being whatever they want to define trusted to be. It's up to them, and so if you want to not be part of that, it's entirely your power.

Leemon Baird: 01:30:58 If you want the power to convince them that you're a good person, then you have the power to do that. It allows you to attach things to your account that give it some kind of authentication. We don't get involved in what the authentication is. We've just made mechanisms where you can do the attachment, and so you can have certificates that show something about yourself, maybe a lot or maybe a little bit, but enough to convince the bank or the store in that jurisdiction that it's okay in that jurisdiction to do business with you, and that it is possible for whoever issued that credential to revoke it. It's like a revocation service. Then the store or the bank can check whether it's been revoked.

Demetri Kofinas: 01:31:32 This might actually be a good way to transition into use cases, because one of the issues that has been coming up a lot lately, and even more so as we move into what's known as synthetic news or deep fakes is trust in information, trusting the source. How do you know, for example, if you get an article that seems like it's coming from the Washington Post, or a video that looks like it is the President of the United States making an

announcement? How do you verify the authenticity of that? How does Hedera, for example, provide a solution to that problem?

Leemon Baird: 01:32:01 It's a layer above us, but here's how we help people doing the things at the higher layer to do it. Basically, you have to sign your video, or digitally sign your picture, and then it's your reputation as a photographer or videographer that people have to trust. There's really no way around that, and if people are willing to trust untrustworthy people, then they're going to be fooled, and that's a problem, but you at least want to be able to sign things. You could say, though, that I would like the ability to un-sign something if, say, a hacker got into my computer and started signing things on my behalf. I'd like to be able to revoke it, and if you want ability, we can help. We can create revocation, and ways of revocation where you attest that you really did take this picture, and in the future, if you want to remove your attestation, you can do so.

Demetri Kofinas: 01:32:42 There's also actually something else that you can do. There's obviously an infinite number of things that you can do with this platform. We did an episode with Bruce Schneier. Actually, also with Josh Corman, both on cybersecurity, and we discussed all sorts of possible attacks against all sorts of different industries. One of the easiest, dumbest attacks you could do is to hack hospitals, which are notoriously insecure, and scramble blood records before surgeries. You could take a snapshot of that database, of the hospital's database, right, and then the hospital could authenticate, or could verify that the blood records had not been altered before every single surgery, and that would not be a very costly thing to store on Hedera, right, that snapshot, right, that hash?

Leemon Baird: 01:33:25 Exactly. Yeah, it'd be a hash, and so there's no privacy indication problems because you're not storing patient data, you're only storing a hash of the patient data, a fingerprint of it on the network. But yes, you can do that to show authenticity. There's a lot of areas where you want authenticity. You said hospitals, but the pharmaceuticals that they're using are even more important. You might want to know the history of the pharmaceutical and what all hands it went through, and which factories produced it, and all that. All of that can be stored in the ledger, or a hash of it can be stored in the ledger, or a combination.

Demetri Kofinas: 01:33:52 We're running out of time. You guys know this. I also was an advisor for Helix, which is an Accelerator that seeded 10 different projects that were building applications for Hedera.

		I've seen some really amazing interesting projects, some interesting applications, some of which will be ready to go on day one. There're all sorts of potential, decentralized car sharing applications, all sorts of things. I think one of the really cool things about Hedera is the market has already been educated about the types of use cases that can work on such a platform, but up until now, the problem is that none of them actually worked because the platforms couldn't scale, and this is basically a situation where the market's been educated, and now a platform comes along that actually can do all of that. Tell me, how many people, how many companies, how many projects are being built right now? How many do you expect to be available on the platform at OA?
Leemon Baird:	01:34:48	We know of over 500 being developed right now that have just bothered to tell us. Many haven't even talked to us, but over 500 different dapps that are building on top of us. Many of them have told us, "Hey, we're ready for OA. We will release at OA. Open Access day, we will be deploying right on top of you." We know the Helix Accelerator that I find amazingly exciting. A whole Accelerator to help startups that are going to build on Hedera. We didn't do it. They did it themselves, and I'm just very excited that they decided to do that. They believed in it enough, they wanted to invest, and then they wanted to incubate these companies, and they fund the companies that they like.
Demetri Kofinas:	01:35:24	It seems like a pretty big no-brainer for either you guys or members of the team, or whoever, to set up some sort of fund to seed projects and startups that are using Hedera software. Is that something you're considering?
Mance Harmon:	01:35:38	We will certainly have a market development fund. The structure and size of it is-
Demetri Kofinas:	01:35:41	How does someone get in that?
Mance Harmon:	01:35:42	Yeah, I know, that's right. TBD. If you want more info, call me, but even beyond that-
Demetri Kofinas:	01:35:47	That's exciting.
Mance Harmon:	01:35:50	... what's exciting is that we know of others that are building their own funds, ecosystem funds, specifically for Hedera or Hashgraph related applications.

Demetri Kofinas: 01:36:01 We talked about so many big things here. First of all, I'm so happy how much we managed to cover in what looks like about 90 minutes or so. You also made some big dreams, put out some big dreams about, again, second layer of the internet, and how long it'll be around. We talked about proof of stake, which has to do with security and market capitalization. How much business do you imagine, in terms of dollar value, could be conducted using Hedera?

Mance Harmon: 01:36:28 You know, when we started, we've always assumed at scale that our platform could very well be processing or contributing to the transfer of trillions of dollars of value, right?

Demetri Kofinas: 01:36:41 Per year.

Mance Harmon: 01:36:42 Per year, and who knows where we end up, but given that assumption, we understood that the network would very likely be attacked, and that was the real motivation for Leemon pushing to achieve asynchronous BFT, and why it took years to get the algorithm in the first place. We've assumed that if this market matures the way we all believe it will, then it's a huge market, and we will see that in the next five years.

Demetri Kofinas: 01:37:13 Guys, Zenobia's pinging me, and I am very good on time, and I was getting us to wrap up anyway. There is so much more I wanted to talk about, and if we had the time, I normally do overtimes, I would switch us to overtime at some point at the end, and I would love to have just, you know, shoot the shit, and have just a much more personal conversation about what this has been like for you. I know some of it. I had the great pleasure to get to know both of you. Leemon, I've gotten to spend even more time with you, and it's been so wonderful. I have been so excited to watch this progression. I've been so honored to be part of this effort, and it's just been just wonderful from the very beginning, when the first time I read the paper, and I just, like I said, I got stunted by the claims, and then had the call with you, and had that, as I said, the Hashgraph Holy Shit Moment halfway through the conversation. Then we put on that panel, and I put on that panel in New York in October, Mance-

Mance Harmon: 01:38:09 That really kicked everything off.

Demetri Kofinas: 01:38:10 Yeah, and then Mike, Mike Maloney, longtime friend, did the documentary that came out in December, and that just blew up, and it's just been wonderful, and we've all been waiting patiently for this moment, so I'm just so excited. Thank you so much for coming in today.

Leemon Baird:	01:38:25	Oh, thank you.
Mance Harmon:	01:38:26	Thank you for having us. It's a pleasure, always.
Demetri Kofinas:	01:38:30	Today's episode of Hidden Forces was recorded at Creative Media Design Studio in New York City. For more information about this week's episode, or if you want easy access to related programming, visit our website at HiddenForces.io, and subscribe to our free email list. If you want access to overtime segments, episode transcripts, and show rundowns, full of links and detailed information related to each and every episode, check out our premium subscription, available through the Hidden Forces website, or through our Patreon page at Patreon.com/HiddenForces. 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 at Facebook, Twitter and Instagram at HiddenForcesPod or send me an email. As always, thanks for listening. We'll see you next week.