Announcer: Bulletproof Radio. A state of high performance.

Dave: You're listening to Bulletproof Radio with Dave Asprey. Today's cool fact of the day is that there is a new prime number over 23 million digits long, and why might you care about this? Because prime numbers are cool, and it turns out this one is 23,249,425 digits long, which is completely ridiculous. And this is core math stuff that you might not hear about.

And what's cool about this is, this was found by an electrical engineer in Tennessee using software provided by something called the Great Internet Mersenne Prime Search. Why does this matter? Because, well, if you're looking at anything having to do with cryptocurrency or cryptography, prime numbers are very, very important for that stuff, and I might be foreshadowing what we're going to talk about on today's show.

If you've been a Bulletproof Radio, we've never had an episode about crypto or cryptocurrency or even some of the hard technology that's been the focus of my career. And what you're going to hear about today is a new company called Swirlds, and what they're doing is revolutionary in changing technology around. And I want you guys to meet its inventor, but I also want you to understand exactly how he got to be an inventor. So this is a chance for us to dig in on a really smart guy's brain, learn something about cryptocurrency if that's interesting for you, but this is really about the process of invention, creation, and discovery, and how you can apply that into your own world.

And today's guest is a PhD from Carnegie Mellon, and his name is Leemon Baird. Leemon, welcome to the show.

Leemon: Oh, thanks. Appreciate being here.

Dave: I'm actually really excited to interview you, because being a fellow geek, it's just fun to be able to geek out a little bit. And you invented something called the hash graph distributed consensus algorithm, which we're going to get into. That's going to be very exciting for people, trust me, it will. But before we get there, tell me a little bit about what made you decide to become a computer science inventor kind of guy. How did you get where you are?

Leemon: Yeah, so what made me decide? In junior high, I discovered there's these things called programming languages, and you can write programs. And even before that, my dad, when I was in fourth grade, had a programmable calculator, and I was able to write a program that would let you guess numbers by saying higher and lower. And it was just, it was amazing.

It's this cool thing, it's like Lego blocks, but it can do anything. And you put them together, and then things happen. It's just mind-boggling that you can do that. You can create whole worlds just by imagining something in enough detail, and that just was mind-boggling to me, and I just played with that and I got really into it in junior high and high school, and started creating stuff.

Dave: That's a very typically geek story. I remember the first time we got computers, I was maybe in ninth grade or something, and within 20 minutes, I changed one of the video games to actually have swear words in it. It was ninth grade, after all. But that's kind of the hacker mindset.

And so you were kind of born with this, it sounds like. You've always had this intense curiosity. But intense curiosity is something that almost all kids have unless something bad happens and they're taught not to be curious. But you somehow, it seems like you maintained this different mindset, because you created this whole new data structure and algorithm that got patented, and I think is a very meaningful addition to our overall set of technology that allows some of what we're doing as humans to scale.

But how do you go from, okay, I was a curious guy in middle school where I just realized you could stack these things together ... How did you know how to stack them together in this way? Did you sit down and say, I'm going to solve this big problem, and then create a path there? Did you have a crazy dream? What happened?

Leemon: No, no, none of that! For whatever reason, I've always been into these puzzles my whole life. A problem will grab my attention, a math problem or whatever, and I'll just think about it and try to solve it. It's just fun. It's just a game.

And I have problems I've been working on for decades and I'll probably never solve them, but sometimes, they just kind of sneak up on me and say, I want you to think about me for a little while. And so I think about them for a little while. And some of these problems are useful. This hash graph thing turned out to be kind of useful. Some of them are completely useless, like I've done stuff in cellular automata that has no use whatsoever! And I've published really cool math papers on them that nobody cares about.

It has nothing to do with whether it's useful or not. It just grabs my attention. I want to understand and then for whatever reason, this problem grabs my attention and I keep working on it. And so I've got lots of problems I work on like that. And they're all different fields, it has nothing to do with whether they're important or not or what field they're in, and for whatever reason, five years ago, I wanted to be able to do shared worlds with a distributed database kind of thing. And it gnawed at me for years. I don't know why.

Dave: Wow. So you just have this set of things ... Do you write them down, do you keep journals of the problems you want to solve, or is there some sort of mental construct in your head that does this?

Leemon: Yeah, I just kind of remember them.

Dave: Okay, you just kind of remember them.

Leemon: And then just, often I'm just daydreaming, and one of my long list of problems comes back and I kind of work on it for a while, and then I'll set it aside or I'll solve it and write a paper and publish it, or whatever. Or start a company. I've done a bunch of companies.

Dave: Do you have ADD?

Leemon: I do not! No. So I focus. I am the exact opposite. When I am focused on something, I don't hear anything around me. I will be so focused on it that the whole universe is just the thing I'm thinking about. So some people are really good at multitasking and some are really good at focusing, and there's sort of this continuum. I'm way over on the, I can't multitask, I only focus, side of that scale.

Dave: Okay, so deep focus is kind of your superpower for inventing, and you sort of go ... It sounds like almost an altered state, you don't really hear people around you 'cause you're just thinking.

Leemon: Oh yeah, absolutely. Right. Sure.

Dave: Got it. And I would say that there's more people who are either ADD or Asperger's in ... I was on that spectrum, we'll put it that way, until I changed some of my nutrition. But if you look at computer science in particular, those are the default characteristics there. So you're one of the more deep math kind of guys, and there's ... Mathematicians have different brains than typical computer science guys, although they're kind of merging together.

Okay, so you have this ... I'm just going to make a joke here. You have this distributed ledger in your head of ideas and things. What gives you the spark when ... You have 10 different problems, and sometimes you know you just want to work on one of them. What gives you the spark to work on one of them versus another one? Is this a conscious thing, or does it just happen?

Leemon: Absolutely just happens. Why do you enjoy playing some games and not others, or why do you enjoy watching some movies and not others? This is just what's fun for me. It seems to be inborn, I don't know why. And some problems I find very boring and I really don't want to think about those problems. And other problems are fascinating and I'll spend decades trying to solve these math problems or invent algorithms for these things. I don't know why, it just is.

Dave: So it's driven mostly by joy and pleasure, it sounds like.

Leemon: Oh yeah. The two things in life that bring me joy are research and teaching. Absolutely.

Dave: Now, teaching is something that actually puts you in a flow state-

Leemon: Yeah.

Dave: -if you look at the research on flow states. And actually, research, I'm the same way. I taught for five years at the University of California, and teaching, public speaking, and research also put me into this really focusing, I don't know what the heck's going on around me.

And, okay. So you're working on these problems. Do you do things to enhance your ability to solve the problems? Like, do you go for a walk, do you breathe deeply, meditate? Do you have any things that you do that put you here, or is it so organic and natural that you just do it?

Leemon: So it is organic and natural. What I have found, and this is not choice, this is just self-observation, is that sometimes I will just sit in a recliner and stare into space for hours on end working on these math proofs or trying to develop these algorithms or trying to design some complicated architecture.

On the other hand, I like to take walks, and I take lots of walks. I now live near a path through the forest that goes for 40 miles. It's a beautifully paved path, it's gorgeous, here in Texas. But other times I just walk on city streets or whatever. But I like going for long walks. And so sometimes I will be walking for miles while working on these math problems, and other times I'll just sit in a chair and stare into space while working on these math problems. Seems good either way.

Dave: And when you're solving them, are you doing visual stuff? Are you doing 3D structures in your head, or are you thinking in words and numbers? What's going on in there, 'cause I think there's a lot of people wondering, okay, here's a top inventor. So what happens in there?

Leemon: It is absolutely visual, and I try very hard not to do this when I'm driving. I don't know if this is dangerous or not while driving. But yes, I visualize things. I view everything visually, not as equations, usually, but as visual, whatever visual things I can use.

I was actually in a job at one point where I was ... Probably shouldn't say this out loud. But I was in this job where I had to go to a meeting every day. And it was completely worthless. And-

Dave: Like most meetings.

Leemon: Like most meetings. There was nothing that I had to say and there was nothing that I needed to absorb, really, or I could use 1% of my brain to absorb it, because every five minutes someone said something. But I couldn't get out of it and I couldn't use paper because then it looked like I wasn't listening.

And so I was spending an hour a day for years on end, it was actually several years, that I had to go to this one hour a day meeting. And I got really good at doing math proofs entirely in my head. And in those three years of going to these one hour useless meetings, I invented or proved some theorems that later became the basis of a whole string of journal articles and things, that were just really cool. That were really fun.

Deep math is kind of useless in that case, but I got to where I could visualize this and I could hold quite a bit in my head at once, just using scratch paper purely mentally, which was just fun. And then I'd do that.

Dave: So how long did it take you to get good at that? You said, three years, an hour a day? Was this something ... After six months of this, you were pretty good at having these scratch papers in your head? 'Cause that's an unusual skill, but it's one that's trainable.

Leemon: It probably is trainable, and I would imagine that the skill increased over time, but I wasn't aware of it. I don't know, I was just playing with it for fun to while away the time while sitting in a useless meeting.

Dave: So there's a trick for everyone listening. If you're in a really boring meeting, practice visualizing stuff in your head. And it's funny, because there's some research. I've actually got it in my next book that's coming out, about the power of visualizing. And if you look at what the Tibetans would do when they were meditating, is they would actually have the teacher tell you, now visualize this with incredible detail, so you could hold these very detailed images in your head. That was actually part of what they were teaching people who were seeking enlightenment to do, was to be able to have these powers of visualizing and remembering and zooming in. There's the memory palace technique and things like that.

But yours is all just organic. It's just out of, I was bored, I wanted to do something fun and joyful, so I sat here and I just pondered.

Leemon: Yeah.

Dave: So you're a super ponderer, is your ...

Leemon: I suppose so. And I've read about this stuff. So you have memory palace and things. You have a path and you put images along the path, and you can use the major system to turn numbers into words, and all that stuff works. I've played with that a little bit, but I've never really been into it. I've never really been into trying to memorize stuff well. But all that stuff works.

Dave: Yeah, yeah. You don't need to memorize stuff, we have this thing called Google, it memorizes it for you. It's kind of done.

Leemon: Exactly.

Dave: Okay. Well, that is fascinating. All right, tell me about what is a distributive consensus algorithm, and why it's important.

Leemon: Yeah, so it's useful, if you have a bunch of computers, to have them come to agreements, even if you don't trust any particular computer or any particular person. So if a group of us over the internet can come to an agreement on something where we don't trust any one person, then we can actually have a more trustworthy system. Now, if you don't trust anybody, even big groups of people, to be bad, then you're out of luck.

But imagine that we have a case that ... We're a bunch of businesses, and we want to have some shared information. Some shared information where I don't tell you a different set of my books than I tell someone else. I want to make sure that everybody sees the same message from me. And I don't think you personally are going to try to cheat me. I don't think any other one ... I'm sorry, I don't trust you, sorry. I don't trust you personally at all. I don't trust, but I don't think that some big group of us are going to do something bad. Like, I want a dark pool. I want this little stock market for a set of banks. I don't think that a third of the banks are going to gang up on me and try to do something nefarious.

But I don't trust you personally at all. I don't trust any one bank at all. And it's possible that any one bank might send me one set of books and send you a different set of books, or one bank that I'm talking to might later deny that he signed a contract with me. All those things, I don't trust.

So what I want is distributed trust. We're all seeing the same shared information, even if one or two bad apples are in the barrel, and I don't know who the bad apples are, and as long as I start from a position where I trust no big group of us to do bad things, then I can trust that the group as a whole absolutely is 100% trustworthy. That what we as a whole say was the information, is the information.

And if we're doing things, if I do something and the group as whole says yes, Leemon did it, then it's true. And if you do something and I do something, if the group as a whole decides that your something came before my something, it is true. Guaranteed, and we will all agree on the order of things that we have done. And if the group agrees that you did something at noon on Tuesday, then it is absolutely trustworthy that no one person could have cheated and got that time to be really early or really late. It really is at noon on Tuesday.

This is what distributed ledgers are all about. It's creating a trustworthy set of information, ordering of what we've done, timestamps on what we've done, and we can 100% trust it. And not only that, we can prove to a third party. I can take something to a court and prove to the court, you know, I really did this on Tuesday, noon on Tuesday, because look at all these people that as a group agree that I did it. That's what distributed ledgers [crosstalk 00:14:59]-

Dave: And basically having witnesses. Lots of them.

Leemon: Exactly. It's a group of witnesses, where you don't have to trust any one person. Powerful concept.

Dave: This is terribly important, not just in cryptocurrencies and things like that, but inside our bodies, we have something called quorum sensing. And quorum sensing is what we're talking about here, and this is the idea of, how do we know what's going on around us?

So one of the areas of quorum sensing that completely screws us up is biofilms quorum. In other words, you live in a or you just enter a space that has toxic mold. The toxic mold will change the bacteria in your sinuses so they form biofilms. And to do that, they do quorum sensing to figure out, okay, who's around me and what should I be doing now? And so there's this cross communication between individual bacteria that allows them to form a cohesive community and then repel antibiotics and things like that.

So if you can disrupt quorum sensing, they can't form biofilms. And so some of the advanced treatments we're looking are exactly how to break what you're building. So this idea of biohacking, of hacking the human body, it's the same algorithms that support life, that you're looking at replicating here. And this really is building a global brain.

So one of the ways of having consensus is leader based consensus. Okay, well, the king said it, so it must be true, and that's how it is, right? Can you walk me through the other ways of driving consensus? And I'm going to tie these back to biology when I can, but I'd actually love it if you'd tie these to cryptocurrency, and also, why should we care? If we don't own Bitcoin, how are these going to be changing the world?

Leemon: Sure. And I love the way you brought up biology. You talked about biofilms, there's also things like slime mold. A slime mold is really a bunch of little independent things, but they work together to form a single thing that can solve mazes, it can do all sorts of things. It's acting like a creature, but it's not! It's a bunch of little independent things!

Dave: Very cool.

Leemon: Very, very cool stuff. And then neural networks are cool, and in a previous life, I was doing machine learning, and that's the same sort of thing. That's what my degree's in. So we'll forget about all that stuff and talk about ledgers, 'cause ledgers are really cool. But it's all about an emergent behavior from a bunch of little things acting independently. You could even say markets are like that. Democracies are like that. There's all sorts of places in nature and in human created stuff that is a bunch of independent things all doing their own thing. But the emergent properties are powerful and trustworthy in some way.

So you said, how does this tie to cryptocurrencies or whatever? Here's an example. Suppose I want to make up a kind of money. Okay, what we'll do is have a computer that remembers how much money you have and how much money I have, and when I want to send you money, we'll just make the number in the computer for you get a little bit bigger, and the number for me get a little bit smaller, and now I have sent you money. That's all it is. That's how your bank works.

Oh, but wait a second. Who gets to run that computer? What if I don't trust my bank? If my bank wanted to, it doesn't have to just move money between accounts, it could create money in an account out of thin air. That would be bad.

Dave: Isn't that called fiat currency?

Leemon: No, if a bank does it, it's called a crime. If a government does it, it's called fiat currency.

Dave: Oh, there you go.

Leemon: But this is it. So wouldn't it be cool if it could do something like a fiat currency, except we don't have to trust any one entity to do it? And maybe we could set it up so that the money supply is always constant and that no one entity can inflate the money supply? And as long as less than a third of us are evil, the money supply is physically incapable of being increased. That would be cool.

So instead of having these two numbers, the number that knows your bank account and the number that knows my bank account, sitting on a server somewhere with a guy we trust, no, we won't do that. We'll let everybody hold the two numbers. And we as a group will come to an agreement on when money should move between them.

So, for example, when I want to send you money, I tell the whole group, hey, I want to send him money, and I digitally sign it ... If we're using a good cryptography system, you can trust my signature. Ah, but we have a problem. What if I only have a dollar in my account and I digitally sign that I'm sending you a dollar, but I also digitally sign that I'm sending Alice a dollar at the same time? And I tell you that I'm sending you a dollar, please sell me something from your store and give me your product. But I tell Alice that I'm sending her a dollar, and ask her to give me something from her store at the same time. Double spend.

Dave: It's bouncing a check, basically.

Leemon: It's bouncing a check, which works fine. I can bounce checks if there's float. If it takes a while for the bank to figure it out, I can write two different checks and get two different products. That's a disaster. Basically I'm creating money out of thin or whatever.

So what we do is we as a community decide which of my two checks came first, and that's the one that's real. If I gave you the money first, then you get to keep the dollar, and Alice is out of luck. And vice versa. And so that's why consensus on order sounds very abstract and useless and mathematical, but it's the core of the whole thing. If we have some way as a group of coming to an agreement on order, we can create money, and it's good money, and we can trust the money.

And we can put deeds to the houses, and I can make sure I only sell my house to one person. I don't sell you the Brooklyn Bridge after I've sold it to somebody else. And that's enforced. And we can do more complicated contracts where I give you some land and you give me some money, and we make sure that both halves of that both happen at once. Everything becomes possible once we have this ledger where we reach agreement.

Ah, we have a problem. How do we reach agreement? Well, the simplest way is what you said. We'll have a king. We will have a leader. So when I want to send you money, I send the leader my transaction. When I send Alice money, I send the leader my transaction, and the leader decides which of the two comes first, and that's when the one that comes first ... The leader tells everybody, everybody says, leader, yes, I approve, and we're done. And we actually have a group consensus. And it actually is more trustworthy than the leader just having a server, running a server of their own, because this goes out to everybody and everybody agrees to it. So it really is truly a group consensus.

Except. What if the leader is just bad and always leaves out your transactions? If we're in a stock market, that's not fair. Or what if we're in a stock market and I put in a bid on a stock and you put in a bid on a stock and I bribe the leader and they always put my transactions before yours when they shouldn't? That's not fair.

Dave: You sound like an investment banker all of a sudden.

Leemon: Exactly. So the fairness of the ordering doesn't matter for some things. For other things, it matters a lot. If we're playing a video game and you shoot me and I dodge, we care a lot about which one happened first. And we don't want me to be able to bribe the leader, or maybe I'm the leader, and put my dodge before your shoot when really, your shooting happened first.

So leader based system has some problems with fairness, it has some problems with fairness of access and fairness of ordering and fairness of timestamps. And there's the DDOS problem. Distributed denial of service attacks. What if a whole bunch of computers on the internet all decide to flood the leader with packets and shut down the leader? Then the whole world freezes.

Dave: And so the big problem with having a king is that a) the king is probably corrupt, and b) the king only scales so much, 'cause kings have to sleep, and so no matter how smart or big the king is, you're going to have a problem with that. So-

Leemon: That's it.

Dave: -we can see that in the evolution of our society, kings basically, there aren't that many kings left. So they're mostly figureheads, because of this problem. And so the next step for us societally was to ditch the king and move to phase two here. But I don't really know, in a societal perspective, is there something that you can talk about in the consensus algorithm besides just voting? There's some other things in the middle there.

Leemon: There is. In fact, the voting came first. 30 years ago, people figured out how to do consensus with voting. Byzantine fault tolerance, asynchronous byzantine fault tolerance, all these wonderful math proofs, and 30 years later, nobody does it because it's so incredibly slow. And the reason it's slow is that we have to send gazillions of votes across the internet and maybe even receipts on votes, and it's just totally impractical. But it's very nice, there's no king.

So we have this pure democracy thing from 30 years ago, but nobody can actually do it in the real world 'cause it's so slow. Then we have the dictatorship. That works beautiful. Leader based systems, except that it's unfair, and you can do a DDOS attack, and even when the leader gets shut down, when we vote for a new leader, we can now DDOS the new leader and we can shut down the whole network forever with just doing one person at a time.

Dave: Is that pretty much the US government right now?

Leemon: Probably. Yeah, that's a problem. And there's also a bottleneck problem. If the leader has to individually call each person and tell them what the order is, then you have this n-fold slowdown because you have a leader involved.

So what can we do that doesn't involved a leader and doesn't involve voting? You know what we could do, is we could just let anybody send out some transactions whenever they want, but we're going to make them take turns by making it really hard to get the right two next set of transactions. In fact, we could say, the only way you're allowed to do it is if you buy a supercomputer and buy lots of electricity and solve these useless math problems, and then you get the right, when you finally solve one of these problems, you get the right to put some more transactions onto the list.

That is called proof of work. Your computer has to do lots and lots of lots of work, use lots of electricity. I just read today, the prediction is that next year in Iceland, more electricity will be spent on mining with proof of work than is used by all the houses in the country put together.

Okay. This is not entirely green, and we'll go into other problems with that. But it is a way of doing it. And it was a clever way of doing it, and there's no leader and you don't have to be sending the votes around. All you have to do is buy a bunch of supercomputers and use 1/1200th of the planet's electricity usage right now. And growing. Rapidly. Okay.

Dave: Wow.

Leemon: Yeah. So maybe proof of work isn't the best possible consensus algorithm. But it works, and it was really cool.

Dave: In our society, I suppose, if you work really hard, you make more money. And then you get to spend more money. So it's basically kind of an economy based system.

Leemon: So then we have what I call an economy based system. This is a little bit different. This is where we do some kind of almost gambling money, and the economic incentives make you gamble in the right way in order to reach consensus. And these systems are kind of weird. They're very complicated, and are they secure? I don't know. Well, can we mathematically prove they're secure? I don't know. Nobody ever has. They look really hard.

But there are systems that, for example, we all are kind of voting on what we think the next transaction should be, but we're voting with our money, and whoever ends up voting with the majority earns money, and whoever votes against the majority loses money. So we all have a motivation to be the majority. And so if the majority of us want to be with the majority, we all reach a groupthink and we all get an answer.

Dave: If you think about, if you ever see a flock of birds all change direction at the same time-

Leemon: Beautiful.

Dave: -they're doing an algorithm similar to what we're talking about here. We are literally figuring out the math that drives huge numbers of biological behaviors, and we're doing it in the context of cryptocurrency and distributed ledgers, which is really cool, 'cause what you're describing there is exactly that. If one bird goes sideways, what's going on? So there's all sorts of sensing going on, and it's not just one leader bird that does that. And we've been trying to figure this out in biology forever, and I think that what you're doing with math and computer science is actually going to describe that behavior better than probably the biologists have.

Leemon: Yes. So what you're describing is fascinating. So flocking behavior, or schooling behavior for fish, it looks like you could have a very, very simple algorithm. Basically, each bird says, follow the middle of where everybody else is, but never get too close to anyone. That by itself is enough to give you gorgeous flocking behavior.

I love watching flocks of birds, because it is counterintuitive how they work, it is beautiful. By the way, I got to see bats coming out for the night once, and it's totally different behavior. Have you ever seen it? They follow a single line of bats. Totally different.

Dave: I was actually bitten by a vampire bat when I was eight years old.

Leemon: Wow.

Dave: I woke up with it feeding on my neck. So I only saw one of them, but I saw it up close and personal.

Leemon: Wow, that is horrifying! So did you turn into a vampire?

Dave: It was kind of cool.

Leemon: Do you have special powers now?

Dave: I'm not saying. I'm not-

Leemon: Okay, I will not bring garlic anywhere near you. That is cool.

But the flocking behavior for bats is radically different from the flocking behavior for birds. It's a different algorithm. It's fascinating to me.

So this is cool. And human economies also have the equivalent of this. You have Adam Smith's invisible hand of the market that just makes things work out right. Supply and demand end up working out as long as you have a big enough market that's sort of efficient in some sense. Slight problem, though. It is also chaotic. It is sensitive to initial conditions. It does weird things for no reason. Could you mathematically prove that the US stock market will never crash again? No! We don't know that. In fact, a mechanic system is complex, is sensitive to initial conditions, there is no way we can prove it will never crash again, and in fact, I'll bet you money, it will someday crash again. It happens all the time. You can't stop it.

So any complex system like that, there really is no way that you can prove that it's going to work correctly. Even worse, there are really subtle attack you can do if you own some subset of the nodes in the network, and your goal is not to make money, your goal is to be disruptive. How many birds does it take to steer the flock? Maybe not very many. How many birds does it take to cause the flock to split into two different flocks? Actually, maybe not very many at all. Could we mathematically prove that it will never happen? No, we're into a realm of math that's too complicated for us, in many, many ways.

Could we use game theory? Well, when you get to game theory beyond two people, there may not even be an Nash equilibrium and all that stuff. And even if there is a Nash equilibrium, it's P space complete to find it. It's totally really hard.

So these economy based systems, I think are really cool, and I actually spent more than a year trying to find one that I could prove would work. And I failed. I was never able to prove one that works. Which left me in a quandary. The proof of work systems are bad because they require proof of work. And the leader based systems are bad because they have a leader. And the economy based systems are bad because I can't prove anything. Maybe somebody else can someday, but no one has yet. And the voting based systems are mathematically beautiful. The only problem is that they involve votes, which is totally inefficient.

So what are you left with? Well, that's it. Except you could do virtual voting. And that's what we came up with a couple years ago. And virtual voting is a voting based system without any votes. And you have all the math proofs of a voting based system. But there's no votes. It's totally efficient, and it's really, really fast. That's it.

Dave: And so how does something with no votes work for voting?

Leemon: Yeah, it sounds like you might need votes for voting. That would make sense. Turns out, first of all, we just talk to each other in the simplest, most resilient way I know of, which is gossip. How fast does gossip spread through the office when someone hears a juicy rumor? Everybody knows it immediately. And how does it work? Well, you just talk to people at random, and you tell them everything you know that they don't know. You say, hey, did you hear the latest rumor about so and so? And they say, no, I haven't. And you tell them the latest rumor. Or they say, yeah, I've heard that. Then you stop, you don't have to tell them.

And you just pick people at random. And people are wandering around randomly bumping into each other, and it explodes outwards exponentially fast. The rumor mill is the fastest known form of communication known to humanity. And so when you want to get your transaction out, you just gossip and people gossip and they gossip their gossip and soon everybody knows it. Really fast.

Dave: Wow, that sounds a lot like the congestion control algorithms that we use underlying a lot of the internet infrastructure. That used to be my area of expertise.

Leemon: So our routing algorithms are also random, and it works for the same reason. And the internet treats censorship as damage and routes around it. There's all those things. Exact same thing. However, that doesn't put things in order.

Dave: Not at all.

Leemon: You're going to get the transaction really fast, but everyone's going to receive the transactions in a different order. That doesn't help you.

So then the question is, how do we do consensus? And the answer is, well, forget about consensus. Let's do one little tiny addition. When I gossip to you and tell you all the messages I've heard, I also tell you the last message I created and the last message that the last person I talked to created. That's it. When I create a message, I put inside of it references to these other two messages. They're cryptographic hashes. All I do is put two hashes inside this message. It's a tiny increase. It's 1% more bytes that I'm sending you. Other than that, we just do random gossip. That's it.

And it turns out that then when you have a big pile of messages sitting in your computer, you see these little links between them. If you have a bunch of circles with links between them, you call it a graph. I was using cryptographic hashes for the links, so it's a hash graph. You have this hash graph sitting in memory, and it gives you, basically, almost for free, a complete history of how everybody talked to everybody. Not only do you hear all the juicy rumors almost immediately, exponentially fast, but you know exactly when everyone in the world heard those messages for the first time.

In fact, you even know what time they claim to have received all those messages. Again, you're getting this almost for free. In fact, when I did a transaction, you can tell when each person in the world heard that. You can sort all those times in order and take the middle one. Basically, you could tell when I had first reached a majority of the world, and you could say, that's the timestamp on when you did it. The consensus timestamp. And since we all see the same hash graph, we all have the same answer. We're done. It's a consensus.

Dave: And you invented that, and now we're rolling that out, basically, as part of the crypto system out there.

Leemon: That's it.

Dave: Now, timing is something that, if you're not a computer science guy or a computer science woman, I should say that 'cause my aunt actually taught computer science at Stanford, so she would beat me if I didn't mention her. But it turns out that timing is, when am I going to go to a meeting and when am I going to go to sleep and all, but timing is massively important biologically. And as computer science progresses, we're doing the same thing on biological science. The Nobel Prize, for instance, this year, or I guess in 2017, was one of the most awarded for circadian biology, which is what time happens.

And we talked about distributed systems and little things like slime molds and emergent behaviors. Well, it turns out throughout our body, there's a quadrillion or so little independent entities called mitochondria inside the cells. And these are ancient bacteria, by where they come from. And we have this problem. If we are a slime mold ... We're not really a slime mold, but we are a collection of bacteria in a Petri dish, from one perspective. And if some of the Petri dish thinks that it's midnight and some of it thinks it's daytime, the timing doesn't line up.

And the same thing happens with banking transactions you just talked about. Same thing happens inside your computer processor. If there's isn't a clock inside your computer so that every part of the computer knows exactly down to the microsecond what time it is, everything stops working. And what we're finding out now is that there is a distributed system inside the body. I would argue, and this is theoretical, but it works really well, that even our ego is an emergent behavior driven by bacterial algorithms to enhance survival.

And we see this thing rolling up throughout our body, but if the timing system is broken on the internet, if the timing system is broken in a ledger system so you don't know which check got cashed first, or if the timing system is broken in your body, the same things happen. The whole system starts to fall down. What I think has happened with hash graph is that you've actually created an algorithm here that works better for quorum sensing and for consensus driving than what we have on board in our own bodies. Would you buy that?

Leemon: Yes! In many ways, it allows a community to come to a consensus timestamp of everything, put everything in order. Relativity says it's impossible. This would actually, you could make a galaxy spanning system where we all had a unified clock in this way. Relativity says there is no standard preferred time frame, or frame of reference. This would create a preferred frame of reference, in some sense.

And the biological link is really fascinating. For example, your heart has a pacemaker, a biological pacemaker. But even aside from that, if you put a heart through the blender and put the pieces into a Petri dish, all the little fibers will start twitching totally out of sync, and over time, they will start to synchronize with each other. You put a bunch of fireflies in a dark meadow, and they will all be blinking out of sync. And over time, they will all start syncing with each other.

You even put a bunch of metronomes on a table, and they're ticking out of sync, and there's YouTube videos of this, and you just watch them get in sync. And what we are seeing is the same thing with our system. All the computers can have clocks that are out of sync. They can be people that are out of sync. You could have some malicious people trying to get us out of sync. And as long as less than a third of us are trying to disrupt us, we sync perfectly and we don't need a single pacemaker. We do it as a community. It's an emergent behavior.

Dave: That is elegant and beautiful. I gotta ask though, do you have a mathematical proof that less than a third of people are evil?

Leemon: No. So this is cryptoeconomics. So let's talk about this. What we have is a mathematical proof that this particular algorithm does all the right things if less than a third of us are evil. That's a math proof. Furthermore, there is a math proof going back a long ways that says, any consensus system can be broken if a third of the people are evil. Any system. If you have control of the internet, if you have malicious firewalls and so on. Any system can be broken if a third of the participants are attackers. Or a third of the weight. Maybe you do a proof of stake system, but it's weighted by something. If a third of the weight is evil, you're out of luck. There is no way to get consensus and have, anyway, all the good stuff that you want.

So this is a math theorem. You can never do better than one third. You have to achieve a third. The question is, how do you achieve a third? And there are lots of ways to set up economic systems to try to achieve a third, but I have to remember the quote ... It was one of the founders of our country, but I don't remember which one it was. But they went to the Constitutional Convention, and they decided, hey, let's set up a republic. They came back home and somebody asked them, so, what kind of a government did you give us? And the answer was, we're a republic, if you can keep it.

And many of the writing of the founders of this nation said a republic is a great system of government as long as most of us are honest. If you get a large subset doing the wrong thing, you will collapse into anarchy, guaranteed. Horrible things will happen, you'll eventually become a dictatorship or something terrible. But as long as most of you are okay, a republic is a great way to run a country. And what we're seeing is the same thing here.

Dave: So now I may be super far out there, but I keep seeing this, okay, the formation of a republic, the growth of democracy, was because the king-based systems didn't work. And then we moved into these economic based systems right now, and where I'm hopeful that crypto, not necessarily cryptocurrency, but just this whole distributed ledger system, is actually going to lead to this next form of human decision making. And this is something that plays out over hundreds or thousands of years. And we're just making it happen really fast 'cause we can model it now on all these cloud computing things.

But what do you see the societal implications of hash graph to be? Put on your futurist hat, 10, 20, 30, 50 years in the future. What's it going to look like?

Leemon: Yes. So this is absolutely exciting. With distributed ledgers, we have this new ability for a group of people to come to consensus on orders and even little programs running. So what? Well, then you start building layers on top of it. You can set up a distributed organization that is controlled by voting, by whatever system you want. And it can be a pure democracy or it can be a republic or it can be even weirder things. And you can even set up a dictatorship. But whatever you want to set up, and we can try different experiments of things, the rules then are enforced by the system itself. You can trust the voting system. And you don't have any one person who's the head of voting that could actually rig the voting system.

You can have trust in the voting system, which means we could set up these autonomous organizations. You could even have total anonymity if you wanted such a situation, where everybody is voting completely anonymous, we don't even know who each other are, but we have guarantee rules enforced onto the system as a whole. And you could set up a system with a certain number of shares that are not duplicatable, so that one person can't set up a million sock puppets. There are whole news ways of organizing human behavior that you can set up autonomously that doesn't have to respect boundaries of who knows each other or boundaries of countries or boundaries of corporations. You can just be setting up these autonomous systems that just exist in cyberspace and yet are completely trustworthy, as long as at least a third of you are trustworthy.

And what's the right way to do it? I don't know. But we can do them all in parallel and see what works! And over the coming centuries and millennia, we can try lots of different systems and see what works. The whole space of what is possible is open now. And we can try it.

Dave: Because we have the technology that supports it.

Leemon: Exactly.

Dave: Well, there's some interesting companies out there, companies like Valve, the company that created Half Life. And this is a company that has no managers, and there's been a few experiments over the last 10 years. Most of them have failed miserably, to be perfectly honest, in companies, where they're saying, we don't have any managers here because this king problem is such a big deal, and managers are little miniature kings, right.

So managers don't scale. You can have seven people working for you, then you have to have multiple managers. So these are companies saying, well, people just rotate right now projects. But there isn't a lot of infrastructure to support that. And do you see companies running based on a system like this?

Leemon: Yes. So let's talk about ... Okay, so I do not want to predict the future, but let's talk about possible futures.

Dave: Come on, predict the future. Tell us the most possible future. There you go. That's not a prediction.

Leemon: I don't know what the most possible is, but let me tell you some possibilities. So already we're seeing a fascinating thing, and in the industrial revolution, you had the corporation being created, which is a very powerful concept. And so what you end up with is, a bunch of investors invest in a corporation, the corporation becomes a hierarchy, and suppose you want to have a corporation built to build phones.

So what you do is you have a small group, maybe, within the corporation, that's designing the phone. Another small group that's managing the factory, the building. Another small group that's building a separate small group for each component of the phone. Another one for the chip, another one for designing the layout of the gates on the chip. Lots of different little groups inside your corporation. Each group is like a little tiny corporation inside the big corporation, which is what you're describing. This is what we can thank the industrial revolution for giving us, and it was a powerful model. And I'm sure it's powerful model for lots of use cases in the future.

But then you look at what's happening now. Most people, like, say, Apple, end up outsourcing lots of these little subcomponents that I just mentioned. And so you might have a small group that is designing the factory for how it's going to build the component, a particular component of an iPhone. And Apple doesn't do that. And you have a different one that's designing the layout of the circuits on the chip, which is a separate group. Actually, I think Apple [inaudible 00:42:46] that one in house, but lots of people outsource that. And then you have an entirely separate out group that is the chip fab that actually builds the chip. And Apple does outsource that.

You have this new way of talking. Furthermore, you have the rise of software shops, and some company can outsource to a software shop, which is a separate legal entity and a separate corporation. What used to be little units within one company are now independent companies that are contracting with each other to act as a virtual entity. But they're not a company. They're just an ecosystem of pieces that know how to work with each other.

Maybe this is the future, or the future is not megacompanies, the future is millions of little companies that all work with each other. Maybe there is a role for individuals to be a little company of their own. Well, sure, we call them consultants. Maybe the future is consultants on steroids, where a consultant ends up being a little piece of lots of bigger virtual companies.

Okay, so right now we have outsourcing shops. We have consultants. We have megacorporations. Maybe the lines start to blur. But we can't do that unless we have a very efficient way for doing negotiations, and for doing buying and selling, and for doing markets. Supply chain right now, maybe my factory has to contract with the widget supplier to supply widgets to my factory so I can build my pieces, 'cause a widget is a component of my piece. But what if we could add, at an instant's notice, create a little market for widgets, where several factories are bidding on buying widgets, and several widget suppliers are bidding on selling them, and we could instantly, in real time, set up a new little market and have them marketing or buying and selling with each other?

Oh, but wait, who do we trust to match up buyers and sellers? Whoever runs this market has enormous power. Maybe that's why it doesn't exist right now. Dark markets are a similar thing. It's like the little stock market, but there's terrible problems. What if you could just magically set one up in any moment and trust that the market is working efficiently, as long as not too many of us gang up on the others?

This is what ledgers enable. And so maybe they allow us to move to this totally new system of organizing society as a whole, that isn't just consultants, isn't just outsourcing shops, isn't just megacorporations, but is some blurred combination of all of the above and other things in between that we don't even have names for. Maybe that's the future.

Dave: Now, this gets really interesting, because let's look at what's going on inside our bodies again. Somehow, we have a liver and we have kidneys, just as an example. And there's all sorts of distributed stuff that they do, and there's many different layers. Inside cells, outside cells, hormone systems and all that. There's at least three different, probably four different signaling systems between the two.

But we end up essentially a group of eight cells at the very beginning of life. Something tells those cells what to grow into and then how to interact. And it's a distributed system that has emergent behaviors. And what you're describing here is the core unpinnings of technology to allow what we do as a big human organism that ... Well, if Elon Musk is right, we'll soon be on multiple planets. Anyway, to allow us to specialize in a way that companies have always done, but to allow us to specialize more like organs, where there's multiple layers and multiple things like that.

And so the core information field that probably drive the way our bodies form their different organs and things like that, and there's debate about why they do that. Stem cell guys are hacking that right now. But I think the core algorithmic things that are happening in the body that we are still discovering mirror exactly the work that you're doing with hash graph, which is why I wanted to have you on here, because I wanted to know a) what makes your mind work this way, 'cause it's interesting, but I'm hoping for our listeners, that this is kind of a little education about, how do decisions get made? How do we know what's happening, how do we know who to trust? That that's helpful, because it's affecting our societal structures, it's affecting our biology, and it's affecting our economic structures. And it's kind of happening now.

Now, what would you tell to someone who's, let's say, 22 years old, just maybe finishing school or something like that, going, what the hell do I do with all this knowledge, knowing that this kind of change is happening right now? What should I be paying attention to? Do you have any advice for them?

Leemon: Well, that's easy. What you should pay attention to? Everything. But seriously, oh, there's the famous Heinlein quote, "Specialization is for insects. A human being should be able to do everything." But this is true. It's interesting, his list includes a lot of agricultural things that I don't think are important. But what is important is a lot of different things.

So I think that being a specialist that can only do one thing, you don't know of anything outside of your field, maybe there's some use for that in the future. But we're all going to become more renaissance people and need to have more broad skills. We're about to undergo a revolution that is hard to even grasp how big it is as automation eliminates many jobs and creates new jobs. It's hard to even grasp what the nature of that's going to be.

If you are a young person in high school or junior high, or a new college graduate or whatever, what you should be doing is trying to gain as many skills as you can in as many different fields as you can. And what do I mean by that? STEM is really important. Science, technology, engineering, math. If you're interested in that stuff, it is the future. More power to you, learn as much as you can, not just in one narrow field, but in a lot of them, because the innovations happen in the cracks between fields that connect fields.

If you are interested in anything involving human beings, more power to you because the future belongs to people like that. So if you're interested in entrepreneurial things, if you are interested in any kind of sales and customer support and things that involve dealing with other people, if you are interested in consulting type things, being a life coach, being a ... the person at the gym that helps people work out. Being the person who helps manage someone's schedule for them. Being the person who gives advice.

If you want to have a vlog and make a full-time living vlogging on YouTube, if you want to make an entire living doing unboxing videos, I have to honestly admit, I don't understand that. I do not understand what the appeal is. That's okay. But I know that that's there. You could find millions of people that will watch you open boxes, or watch you play a video game while talking about whatever flows through your mind about your life. And you can make a full-time living at it, and it will grow over time.

If you can do the connecting to people thing, this is important for the future. If you can do creative things, as we automate more and more things, if you can create the music and the writing and the videos and the books and the blogs and the whatever, more power to you, because that is the future. In many ways, robots are a threat because they're going to threaten all the jobs that are subhuman and robotic to begin with.

Dave: All the boring jobs are going to go away.

Leemon: Exactly. And I laugh about it. I do not want to minimize the pain, we can talk about the pain and I think it's enormous and I think we should be doing ... Anyone who can do something to alleviate that pain for other people needs to be working right now really hard. I don't want to minimize that. Pain is bad because it hurts and it's hurting real people. But in the long term, this is enabling, this is a good thing. Humanity as a whole is going to allow us to achieve potential in ways we can't right now.

Dave: If you look at the dumbest technologies that you would never think of as a modern human, do you know how much drudgery baking powder has eliminated? I'm not kidding.

Leemon: I have no idea.

Dave: There were trade wars over baking powder because the amount of time that, frankly, mostly women, if you look back historically, spent kneading dough and waiting for it to rise so they couldn't go out and do other things. Dishwashers. All of these things eliminated huge amounts of the most drudgery kind of work you can think of. And hey, baking's fun, but it's not fun if you've gotta wake up at 5:00 every morning and do it for your entire life. It's actually horrific at that point. Washing machines for laundry.

These technologies, we used to wring it out by hand. All these things have been a continuous march. Fast food is there because cooking takes a lot of time. All these things are part of this continuum, and now we're at this point where we're actually going to remove almost all drudgery, and if you make your money doing drudgery things, that's scarier than hell. And you want to make sure you're fed and taken care of. But I've never been more excited in my life, because all the stuff that doesn't really take advantage of that power of being human that we have, we're going to be able to get rid of a lot of it, assuming we don't break the planet while we do it.

And I'm hopeful that hash graph and the stuff you're doing at Swirlds is actually going to contribute to accountability so that we can actually eliminate all this drudgery and have less people dumping mercury into the ocean, and doing bad things that currently are not trackable, because they will be trackable. So I'm hoping accountability comes as we unleash a lot of humanity. But yeah, it is absolutely scary on many fronts.

And I say this, I actually worked for five years putting auto parts in boxes when I was in college, because it was the most reliable source of income. And in fact, when I sold the first product ever sold over e-commerce, I was still working during summers, putting parts in boxes, 'cause I needed my $12 an hour, which was three times the minimum wage. And there was nothing more drudgerous than putting parts in boxes. It sucks. I'm not going to do that again, and if I could free every human on Earth from doing that again, I would do it in a minute.

So that's the peril and the positive upside of what you're talking about, and it's fascinating. And I'm really hoping that your technology does that. Now, I have one more question for you, Leemon.

Leemon: Yes.

Dave: If someone came to you tomorrow and they said, look. I want to perform better at everything I do as a human being. Not just my work, but being a human, what three most important pieces of advice would you have for them?

Leemon: My goodness. So have a passion for what you're doing. Find something to have a passion, cultivate a passion, have a passion for what you're doing. It's almost impossible to be good at something unless you have a passion about it, because you've gotta do 10,000 hours of intent work on it, not just doing it. Have a passion. Also it makes life more fun.

Learn everything you can. Learn everything about the thing you're interested in. Learn everything about the things you're not interested in. Learn about how the world works and how the pieces go together. Learn everything you can.

And connect with other people. We are hard-wired as social creatures. We are designed as social creatures. The whole ... What's the point of living as a hermit? You aren't even helping mankind and humanity is not benefiting from your existence. You will be happier if you're connecting with other people. You will be fulfilling your purpose if you are connecting with other people. That is crucial, you've gotta be doing this with other people.

And if you decide to start a company, get the best people you can and just really work together. Take care of people, take care of the people under you and over you and beside you and all of that. I don't know, I didn't pre-rehearse an answer to the question you just asked. But these are good things.

Dave: Passion, community, and taking care of others.

Leemon: Yes, and I said learning in there too. That's not a bad idea either.

Dave: All right. Good deal. Well, those are powerful answers, and I've asked that question of everyone in almost 500 episodes now, just to see ... When people are working to change the world, and I tend to target people who have broken out in a field or achieved something, and I always want to know, what matters most to you? And for you, it's really clear, the passion. It shows in just the way you answer questions and the way you solve problems. Like, I don't know, that was something I cared about. And I think that's fascinating.

And I'm hopeful that for our listeners today, that if you take one thing away from this, it's that have passion for what you do. But I have kind of a bonus question for you, Leemon. What advice would you have for someone who has passion for something that has very little economic value? Like the follow your passion, well, if my passion was doing something that actually won't put any food on my table, any thoughts about that scenario, 'cause I've seen that more than a few times.

Leemon: Yes, yes. And that's why I didn't say the words follow your passion. I didn't say it.

Dave: All right.

Leemon: What I said was, have a passion for what you're doing. And I even said, try to cultivate a passion for what you're doing.

Dave: Ah, so learn to care about what you're doing.

Leemon: Learn to care about what you're doing. In addition, hobbies are great. Have a passion for your hobby. In addition, try to find ways that you can project what you're interested in onto the space of things that are actually useful to humanity as a whole, because you may find that there's something very close to what you're into that would actually benefit the world. And you said in terms of economics, maybe, or maybe what other people care about, but of course, if it's benefiting the world, then it does have economic value, and people do care about it.

Dave: Yes.

Leemon: And so I didn't say, major in whatever sounds like the top thing on your list for being fun, because that may not be the best use to humanity or yourself.

Dave: Right, right.

Leemon: What I said is have a passion about what you're doing.

Dave: Very cool nuance, and I'm really glad you called that out, because I think following your passion can be dangerous if you want to eat. But it's incredibly joyful, so finding a way to have passion about what you do is different than doing what you have passion in.

Leemon: True.

Dave: So order of operations seems to matter, in math as well as in your career.

Leemon, your company is called Swirlds. I'm guessing people want to learn more about what you're doing with hash graph. Swirlds.com.

Leemon: That's right.

Dave: Cool.

Leemon: You can also go to hashgraph.com.

Dave: Hashgraph.com is probably easier to remember. That's hash graph, not hash craft, just for people who are listening for that. And thank you for sharing your knowledge and wisdom, and thanks for your passion and curiosity, and for inventing really cool new stuff that the world needs. I am genuinely grateful for it.

Leemon: Well, thank you. I really appreciate you having me on the program. Thank you very much.

Dave: If you liked this episode, you know what to do. Go out there and get yourself a big basket of cryptocurrencies. Okay, maybe not, but you can if you want to. But what I would love it if you would do, if you liked this interview, two things. One, I haven't interviewed a hard technologist like Leemon in quite a while. If you liked this conversation, tell me on Facebook. Leave a review on ... bulletproof.com/itunes will take you to the review site. But just let me know, if you want more of these, I am listening to you guys. I will interview the type of people about the topics you care about, as long as I also care about them, 'cause I'm going to follow my passion here too, right?

So anyway, thanks for listening to this show, thank you for subscribing and just downloading these episodes. I'm doing them because I love this stuff, I care about this stuff deeply. Bulletproof is growing, it's becoming a national company with all sorts of Bulletproof Coffee everywhere at Whole Foods and e-commerce and all that stuff. But I do this every week, I spend a lot of time on this because I think it matters. And so if you think it matters, just tell me, and tell me how to do it better and I will. Thank you.