EPISODE 1237

[INTRODUCTION]

[00:00:00] JM: A smart contract contains the terms of a blockchain transaction between a buyer and a seller as well as the capabilities to execute those terms. In order for smart contracts to include outside data from the world such as stock market data, weather, sports data, etc., the contract needs a third party service called an oracle. The industry standard blockchain oracle is Chainlink. Chainlink is a decentralized and open source oracle network that connects to any blockchain with seamless API connections. Their nodes connect to trusted data with cryptographic proofs that make their network tamper-proof. Chainlink is used with smart contracts that secure billions of dollars of value for blockchain projects. Their oracle network greatly expands the value of smart contracts and is used to create cutting-edge modern blockchain applications.

Sergey Nazarov is a co-founder of Chainlink and joins us to talk about their platform.

[INTERVIEW]

[00:00:55] JM: Sergey, welcome to the show.

[00:00:57] SN: Thanks for having me, Jeff. Good to chat with you.

[00:01:00] JM: You work on Chainlink. Can you give an overview for what Chainlink is?

[00:01:04] SN: Sure. Chainlink is a centralized oracle network, which is a fancy name for a new type of consensus and decentralized computation. So blockchains generate their own decentralized computation about the specific topic of generating a block, and that block houses transactions, and those transactions in those blocks are then connected to previous transactions which gives them a certain immutability and tamper-proofness that no other data structure or data storage mechanism has. And that's the focus of the decentralized consensus of a blockchain.

An oracle network, in our case a decentralized oracle network, arrives at consensus about events that are not on a blockchain, right? So a blockchain can arrive at consensus about the transactions inside of it, which means it's a relatively limited universe of transaction types that mainly relate to moving tokens, generating tokens, accepting signatures, combining signatures, and that's what Blockchains do with their consensus. Oracle networks actually reach out to the external world and they arrive at consensus about external events. And in arriving at consensus about external events, you make the events highly reliable, highly accurate, highly tamper proof and essentially reliable enough to control the value within a blockchain. So I think it's important to understand that blockchains are very good as immutable data structures, as tokenization mechanisms, as places to run smart contract code, which people should use application code, and then they should view the blockchain almost as if it's a database.

The oracle and oracle network is really all of the services that people are used to connecting to application code, but the difference between an oracle network and the centralized version of a service is that the oracle network has to provide the same service in a decentralized way in order for that service to meet the high standards of a smart contract. So, for example, when we reach out and get market data, we get that market data from multiple sources. That data goes into multiple independent nodes run by multiple independent teams and then there's a consensus mechanism and you arrive at a final kind of definitive truth that can automate billions of dollars in value transfer or financial product movement or anything else. And this is really what an oracle network achieves, is it achieves this additional layer of decentralized services that blockchains don't provide but that the smart contracts running on a blockchain need to go beyond tokenization and beyond now voting and some of the initial use cases of blockchains, which is why oracles are exciting to some people, it's because they're that kind of services piece of the puzzle that's missing from making smart contracts about the global financial system, the gaming industry, the ad network industry, the global trade industry. All of those examples, they would need an oracle network to go and get information or prove things about other systems to a smart contract which is kind of the final building block of making smart contracts useful in all of these categories of transactions.

[00:04:24] JM: That sounds really appealing, but it also sounds less possible, because you're talking about being an oracle for real-world events. Give me a rough overview and we can dive deeper into that, but give me a rough overview for how that's possible.

[00:04:40] SN: Sure, of course. I think what you need to think about is how do blockchains and decentralized infrastructure generally arrive at their guarantees and then how can a version of those guarantees be extended to these non-deterministic systems and these less secure systems and so on? So if you look at what blockchains really do, they're part of what's called decentralized infrastructure, and what the centralized infrastructure does is it arrives at a highly redundant cryptographically-proven computation, right? It arrives at something called decentralized computation.

Decentralized computation basically means that a lot of independent, provably independent parties, computed the same thing in completely separate instances, in completely separate environments, separate servers, and the entities and the key holders computing those things are all separate from each other. And on the basis of certain cryptographic techniques and primitives they've all arrived at the same conclusion, they've come to consensus, and then their consensus is memorialized in the form of a transaction that's put into a block in the case of blockchains. But at the core of what blockchains do is they arrive at this kind of consensus, right?

So the question then is how can I arrive at consensus? How can I arrive at decentralized computation about these external events? And then the question starts to evolve into, “Well, what are the layers of risk and what are the layers of separation between the final value and the risk that each problem inherent to making this type of consensus adds?” Right? So what are those layers? There is a layer of the people who come to consensus about a value and then there's the layer of the place where the data comes from, right? And really in our experience the maximally decentralized, and therefore the maximally tamper-proof version of this, is decentralized in both the layer of people that make consensus about what the value is and in the layer of data sources. So what this practically means is if you look at how we generate a lot of the data that we put into defi, we have 20, 30 or more nodes coming to a single value about the price of Ether or Bitcoin compared in a USD conversion rate from multiple sources, right? So there're over 10 sources that go into each of these networks, and those sources then cover the hundreds of exchanges where all market activity happens. So they then source their data from all of the world's kind of cryptocurrency exchanges, both the on-chain exchanges and the off-chain exchanges. And it's really thinking about how do I progressively decentralize more and

more of the process? And in some cases you can't always get enough data sources, and that's when you start to apply more cryptographic techniques to assure that the data sources that you are getting things from are being accurate and truthful and you're actually getting data from them. So it's actually two dials, right? One dial is lots more decentralization, lots more redundancy both on the data source side and on the note side. Sometimes data sources run their own nodes. So in certain cases they can be the same. And then it's also the application of various cryptographic techniques to make sure that the data is coming from the appropriate source, that it's being combined correctly. And between both of these kind of approaches you arrive at a highly reliable source of data at least in the case of data.

And then oracle networks also have more advanced capabilities where they can do computations themselves to generate randomness or to generate certain computations that you don't want to generate in a blockchain, but that's a more advanced topic. If we're just talking about highly validated data, what you're essentially doing is applying the decentralized computational model to both the consensus layer and to the data sources as much as you reasonably can.

[00:08:47] JM: What's a good example of an application that might want to use Chainlink?

[00:08:51] SN: Yeah, sure, of course. We right now power anywhere between 50% to 80% of defi depending on the day. Defi is essentially financial products built in the smart contract format and they can be anything from lending protocols to derivatives protocols. So let's take a derivative protocol. Derivatives protocol basically derives its value from essentially an event, often a market event, and price and certain factors that determine the value of the derivative and the settlement and basically almost all the characteristics of the derivative. And people have now made you know smart contract derivatives. Derivatives is probably the largest global industry probably ever valued in – Literally, the estimates I've seen is something like a quadrillion dollars in value and derivatives. It's actually a large risk due to lack of transparency in the global financial system that can hopefully be solved once those derivatives migrate on chain, but that's a separate topic.

I think derivatives is a very good example because they're heavily driven by data, and the degree to which they receive accurate data is very important because it determines their value

and their settlement and that's really just how a derivative functions. So you have an unchained contract that represents the value of something else and that representation of value is based on the data that proves what's going on with a market price of an asset somewhere. And that data, in the case of smart contracts or universally connected smart contracts as we call them, is provided by an oracle network. Because if you were to simply connect the smart contract itself to – Well, first of all, you couldn't connect a smart contract to an API on its own. You would need some kind of oracle because blockchains are inherently limited. And then your goal would be to connect it to the most reliable source of data that you could, which in the decentralized computational world would be an oracle network. And so you would have an oracle network with something like 30 nodes like many of our networks have. Those nodes would reach out to something like 10 data sources. They would aggregate data from those 10 data sources and they would give you a definitive kind of price that defines the value of that derivative and then people would be able to purchase or sell or settle or do whatever they want to do with that derivative. So this is what defi really is.

Defi is the combination of the world's data with financial products on chain, and defi really wasn't able to exist before you could do that. It's not a coincidence that around the time that we have started putting the largest amount of data on chain ever, a lot of decentralized financial products have appeared. Because if you look at what a financial product really is, it is the combination of application code with data. And if you couldn't have data on chain before you had oracle networks, well, then you couldn't have financial products on chain before oracle networks. But once oracle and networks appear and once data is made accessible to smart contracts, that's the point at which people can build decentralized financial products.

[00:11:50] JM: Tell me a little bit more about the data sources for Chainlink. Like how do those data sources get vetted and how does the data make its way onto the chain?

[00:12:00] SN: Right, absolutely. So there're actually two approaches here and I think they're both important and the flexibility of how you acquire data is important. The first approach is that you have an oracle network and that oracle network is a collection of nodes that are incentivized just like blockchain miners and Bitcoin miners are incentivized. Those nodes are incentivized to go out and get accurate data in order to generate the most accurate, highly reliable result possible.

In the first version of how data is put into a smart contract, this oracle network of anywhere from seven to over 30 nodes basically goes to an API at a data provider that is considered a high-quality data provider. Often that's determined by users. So users will say, “Hey, we want that data provider.” Chainlink also has a reputation system where we track how well each node, and even more and more now how each data provider is performing. And so better data providers get to continue selling their data to Chainlink networks, whereas worst data providers are kind of not as used by node operators because they're either not responsive or not returning the right results. And so there's actually a reputation system baked into Chainlink, and it's quite fascinating because the system inherently puts all of the data on chain and generates a lot of proof about what's going on with the oracles.

In any case, in the first variant of the system you can go to any data provider, you can go to really any API in the world and you can request from it and you can come to consensus on the data from that source assuming you can get other sources or you can come to some model of consensus that the user wants around that data. And that doesn't require the data provider to do anything, right? So the benefit of this system is that you have a layer of consensus and you have a lot of proof that the data was acquired from a data provider and the data providers don't need to change anything about their infrastructure, right? So the data providers just continue to provide their APIs, operate the way they have always operated and just do what they're supposed to be doing. This is the system through which a good amount of the data is acquired and then the data providers are more than happy to sell their data to Chainlink nodes because it's consumed into these applications which they're all excited about.

The second version is when a data provider runs their own Chainlink node. And what that basically means is the data provider gets a lightweight signing appliance. They basically get a lightweight signing application that allows them to connect their APIs internally to their own official node. And then that node publishes a contract on-chain, and that on-chain contract is a representation of that data provider. So now there's an on-chain contract that's the representation of that data providers services. And that on-chain contract gets requests from other smart contracts for data to be given to them because, once again, a blockchain cannot talk to an API. A blockchain has to have an oracle to speak with any API in the outside real-world.

And so the second variant is where data providers that are more interested in kind of selling their data to the blockchain ecosystem or more convinced about that, and we have many data providers already doing this live. We have data for sports events, weather events, market events, all kinds of things out in the real-world already live on production with data providers running their own production nodes. This variant allows you to get data essentially directly from an official node run by a data provider. It has the benefits of getting data directly from a data provider running their own node. It has the limitation in that the data provider now has to be able to make sure that they are properly connected, that their APIs stay up according to the node and all these other kinds of nuances. The benefit that they get is they are connected to many different chains all at once. And in reality this variant basically requires the data provider to want to opt-in to some kind of infrastructure. It requires them to want to say that, “Hey, I want to kind of run a function in the cloud or I want to run some kind of node myself and I want to make a technical investment in that.”

What we found so far is that the majority of data providers just want to sell their data to somebody and they want to provide that to an oracle network that just retrieves their data and sells that data successfully to a smart contract. There are some data providers that want to run their own node and we're working with a lot of those, but I think that's something that's going to evolve more slowly.

[00:16:33] JM: You mentioned this reputation system for how data gets verified as quality. How does that reputation system work? How do you vet and ensure quality data?

[00:16:45] SN: So once again there's two levels. There's one level of the node operators and assuring that they're operating properly and then there's the level of the data providers responding properly. In terms of the node operators, the way that the Chainlink system works is that node operators are committing to certain service level commitments, right? They're basically, in many cases, on-chain committing to a certain degree of service. And they're committing to that because the on-chain activity that they do is immediately public to everybody as soon as it happens.

So I think the big nuance difference between a reputation system in the web world and a reputation system in the blockchain world is that data is immediately available publicly. It is immediately available for people to know that a node did not respond for a certain period of time. And that lack of response is recorded on-chain immutably for everybody to analyze. And we actually have multiple ecosystem teams. We have multiple kind of block explorer-like things and marketplaces that are all able to analyze the same data about both node operators and data providers.

So basically the way that it looks is that the node operators are expected to perform to a certain degree on-chain. Those expectations are clear. They are then able to perform, or in some cases if they're not able to perform, they are not able to stay on that oracle network. And then the data providers themselves, for the ones that run their own nodes, it becomes pretty clear what their responses, are and if their responses are often wrong, then you know once again that data provider and their node might not be used in an aggregation. They might not be applied to that aggregation.

In the cases where a node operator gets data from a data source, a lot of that data is actually more internal to the oracle network and that data is something that's in the process of getting published on chain. So there is a certain amount of insight that node operators have about the responsiveness of different data providers and different data sources. At this point the reputation system extends to node operators and to the node operators that are data sources. It will continue and is already being extended to cover data providers. And that's another kind of piece that's coming and is already working for node operators in how they choose data providers and is something that's going to be made more public.

[00:19:13] JM: Let's talk a little bit about the architecture of Chainlink. Can you tell me about the different types of smart contracts that are stood up to compose what Chainlink operates as?

[00:19:26] SN: Sure. Sure. I think the simplest way to think about Chainlink is that you're creating an on-chain interface between an off-chain service resource or computational environment. So what you're really creating is you're creating an on-chain contract that can receive transactions from other contracts that basically request specific types of data, specific

types of computations like randomness and in many cases require you to make a commitment to provide that, right? And it actually varies in terms of the use cases.

So there're variants of chain-link networks that create something called reference data. Reference data is a piece of data that's used by many different contracts, and we have some of the top defi protocols using our reference data to settle their protocols and transactions and in lending and derivatives and insurance and various other financial products. And what reference data does is it creates an on-chain aggregation from multiple nodes and then that aggregation is then provided through an interface, through another interface that allows people to read that data and to use it in their contract. So that's one way to interface with Chainlink validated data.

Another way to interface is something called the request model. The request model is when you actively request a specific computation, a specific piece of data, a specific randomness from something like Chainlink VRF where you basically have a designation, a job ID that you feed in and you use to trigger a request. So I think that the nuance around understanding what oracle's do and what Chainlink is is around both the interface, the interface that allows people to consume all this data in different ways, and it's kind of a roundabout answer to your question because it's as varied as the different use cases want to consume data, which is quite varied, and also the type of data they want to consume.

And then this interface is replicated across all the different blockchain environments, but in many cases goes back to the same kind of core oracle network for that piece of data and then that retrieves the data from specific sources. But I think the simplest way to think about an oracle in an oracle network is that you're creating an unchained contract that is acting as the interface. Just like APIs are an interface into people's web backends, oracles are kind of another onion layer on top of APIs that act as the interface for people to interact with those services from a smart contract. And those interactions are very varied. They can be on a schedule where you tell the interface that you want them to send data at a certain point in time. Or in some of our keepers functionality we actually can watch contracts and the oracle network chooses when to send them data based on the certain conditions that contracts have or haven't met. And so it's more and more advanced depending on how people want to receive the data or how they want the off-chain service to interact with them.

[00:22:35] JM: Walk me through the series of events of an API call to Chainlink.

[00:22:44] SN: Yeah, sure. So I think the way this looks is that you have a function called get latest price. Get latest price allows you to get an answer ID from a specific round, and a round is the specific kind of aggregation that was, for example, most recent. You would kind of send that transaction to get the latest price, and the latest price would then be returned to your defi contract in order for it to settle its transaction or value the asset properly, right? And then there's an on-chain contract that's the interface for that where you send that request and you get the latest round of information. You can also request data about a previous round or you can kind of try and understand what the collection of data from multiple rounds was. But at the simplest level you basically go get latest price on-chain. You make a transaction with that request from your smart contract. It gets a response. And then it uses that value to calculate the value of an asset or of a derivative or of an interest payment or of whatever the decentralized financial product needs to do.

[00:23:53] JM: And how much volume is going through these Chainlink smart contracts on an average day? Like do you have any analytics on that?

[00:24:04] SN: Sure. Sure. I mean it varies by day because value shifts up and down within the defi ecosystem. It shifts between the protocols that we service. I think at this point it's anywhere between 10 and 15 billion, maybe between 10 and 20 billion. That's keeping in mind that all of defi is somewhere between 30 and 50 billion, 30 and 45 billion in total value locked. So it's anywhere from 50 to 80 percent of defi is what we generally see. There're a lot of shifts in defi value. How much of it is secured by the protocols that use us? How much of it flows into a decentralized exchange or something else? So it's hard to pin down a number, but it's a very sizable percentage because we are basically viewed as the most secure source of data and access to off-chain services generally. And people in the defi ecosystem, because they've made everything so programmatic and so automated, once they have some value secured, I think they become very sensitive to the security of their smart contract in an end-to-end way. So while they have traditionally focused on the smart contract code and the security audit of that code, the decentralized financial kind of developer I think now has understood that the end-to-end of their security is really what's important. And so when they evaluate what the top mechanism is to provide data or access to external services or access to randomness, they basically realize

that the top protocols use us and they do that because of the guarantees that we provide. So I expect that as the defi space grows, I think that those percentages will hopefully stay within that range. And as the space grows, more of the value will be secured by Chainlink.

[00:25:47] JM: Can you tell me more about the security considerations that you've had to put into implementing Chainlink?

[00:25:55] SN: Sure, absolutely. I think one of the things that's important is the reputation system proving that nodes are high-quality and one in a reliable way. There're actually certain hurdles that people need to meet to join oracle networks at all. I think another point is civil resistance. Civil resistance is proving that nodes are actually separate from each other, that they're not actually run by the same person. We use multiple mechanisms for this such as security reviews and also key base. Key base provides PGP-signed identities. And those are two of the large considerations in addition to decentralization.

I think generally the larger strategy is to have a very decentralized system, right? It's to have all the top note operators working together to come to consensus. They're proven to be the top node operators because the reputation system generates all of this proof on-chain. Having the largest amount of data providers that are out there actually using Chainlink and providing data to it, that's the second layer of decentralization. And then also the consensus methods that we use to aggregate signatures, the aggregation of signatures and something like OCR where we actually get the value from each node and put together a digest that proves what each node submitted. I think it's really a collection of these various kind of cryptographic techniques, the ability to prove things about nodes and the application of a maximum degree of decentralization.

In addition to that we actually have a number of trust minimization guarantees. So those are our kind of guarantees within the contract and the protocol itself that it can't deviate beyond a certain point. So for example we have a capability called circuit breakers where if the price deviates too much from a previous round it can be not included. We have ways for people to have flags around smart contracts where if there is a certain flag around that contract their system can automatically be paused. So it's really a collection of decentralization, good reputation system that proves things to you about the security of the nodes involved in consensus. A number of good use of cryptographic primitives that we put together with people

like Ari Juels, who was previously the chief scientist of RSA, was the co-author on our white paper together with me and our CTO and has now become our chief scientist. And then it's also kind of a few trust minimization techniques that minimize risk in regards to the oracle network such as circuit breakers and others. So it's really a big combination of all these approaches to manage risk and attack factors from all of these points of view.

[00:28:27] JM: So what aspects of Chainlink are managed off-chain versus managed on-chain?

[00:28:35] SN: That's an interesting question, because what Chainlink really is, is a middleware, right? It's a really secure, really reliable middleware with security baked in and data validation baked in and consensus baked in and all these mechanisms to assure that what is making its way on-chain is highly reliable, right? So the portion of it that's on-chain is the interface. It's the ability to interface with the data to request the data, to come to a service agreement with a smart contract, to assure them that they'll be receiving the data and that they'll be receiving a certain service quality or responsiveness. So the interface is an important part of what an oracle and what Chainlink does on-chain and all the various ways that people can interface and request the data.

There are those circuit breakers and other risk mitigation techniques and trust minimization techniques that are done through the contract themselves. And then there're a number of things around minimizing risks on updates and making sure that people can access the data in kind of a reliable way so that the wrong values don't make their way to a contract. So there's some validation that can happen on-chain.

I think the thing that happens off chain is the redundant connection to many data sources. For example, on many of the Chainlink networks that secure the largest amounts of value, each node is actually connected to multiple data sources. So it isn't the one for one where one node is connected to one data source. One node can be connected to three or more data sources. So it's the implementation of a decentralized model as far as data is concerned. That happens off-chain because you inherently have to connect to the data off-chain.

And then the arriving at of consensus, right? The arriving at of consensus happens on-chain in a cryptographically kind of proven manner and then the final results of that are broadcast from the

off-chain world into the on-chain world through this interface according to the conditions that were set up between the oracle contract and the user smart contract. I think that's probably the simplest way to think about it. I think the way it's going to evolve is the interface is going to become more robust. You're going to have more ways to request data, more capabilities for the data to be given to you in whatever format or way or schedule or under whatever set of conditions that you want. I think there will be more checks that happen on-chain against the data. That's going to be lower and lower cost to do because chains are becoming more scalable and therefore the computations to provide those checks will cost less, and so more and more of them will be baked in on-chain even though I think we have the largest number of on-chain checks out there right now.

I think the thing that will happen off-chain is there will be more and more off-chain computation that happens in addition to the provision of data, right? So right now what you see Chainlink doing is basically coming to consensus, validating a lot of data, connecting to a lot of data sources, increasing the depth and quality and security of data in verticals like market data, in crypto data, in forex data. And then you also see breadth, right? So you see more data sources across different types of data. Recently we had something about the value of different watches. So people could make NFTs off of that, and then sports data, weather data for insurance. So the breadth of data is expanding.

But off-chain, I think what's also going to happen and is already happening with something called VRF, which is our verifiable randomness solution, which is used to create NFTs, is the ability to do a computation in an oracle network. And the reasons for doing a computation in an oracle network that you don't want to do in a blockchain for scalability or privacy reasons in my opinion is increasing by the day. So I think the right way to think about Chainlink is not just as a data source or an abstraction layer getting data to smart contracts, but it has a set of decentralized services built on a set of oracle networks that provide all of the highly validated data and trust minimized off-chain computation that blockchains cannot provide.

What I think is going to happen is that there will be more and more reliable checks on-chain, more and more data coming on-chain both in quality and in quantity across different types of data and there will be more and more computation done within oracle networks because those computations are things people won't want to do in a blockchain for scalability reasons or they

won't want to do them in a blockchain for privacy reasons, because that part of the computation is something they don't want on a public blockchain, but they still need that computation done in a trust minimized way and they still need it provided in a way that proves that it was done correctly through various proofs, which is what the consensus of the off-chain oracle mechanism will provide.

[00:33:24] JM: What are the biggest engineering problems you've encountered when implementing Chainlink?

[00:33:29] SN: I think it's what you hit on initially is that you're trying to take a world of non-deterministic, less secure or less reliable data and turn it into some kind of definitive truth or deterministic input. And I think people underestimate the complexity of this problem, right? They're used to using APIs, right? They're used to using an API and they're used to maybe triggering something with the API that isn't immediately being attacked by an adversary or isn't under threat of being manipulated. So a lot of the development world has gotten to a place where thanks to APIs, which is absolutely great. People can go and compose those and build whatever they want to build for their core code very quickly. And a lot of the security issues or the data quality issues or anything else is kind of abstracted away from them. And then if they have an API that doesn't meet their needs or doesn't do what they want, they find out about it the hard way, it fails on them or it returns the wrong result, then they switch it for another one, right? That's actually another interesting thing that I think Chainlink will have a very good solution for, is we'll have a huge amount of data and publicly available data about the quality of different APIs that's proven and guaranteed to be accurate in its own way.

I think the real challenge is how do you create definitive truth and create highly reliable inputs into smart contracts in a way that can automate – Kind of hyper automate billions and eventually trillions of dollars in value? And there are different approaches to this. I think what happens is that the approach that wins is the one that can successfully scale as the amount of value secured by an oracle scales, right? So what you really need is you need a system that can, in a flexible way, connect to all the data sources that you could ever need regardless of if they want to run a node or if they don't want to run a node. You also want an option for the data sources that can provide or do want to provide data in a signed format to do that very easily, and

Chainlink right now has the largest amount of data providers running oracles and signing data on their own.

And then what I think you need is a system that allows the size of an oracle network and the security of an oracle network to scale with the value that it secures. And what that comes down to is the ability to add a more decentralization to it and more data sources regardless of if those data sources want to run a node or if they just want to run their own API and to kind of scale that in a quantifiable logical way. And that's why I think the reputation system is quite important, because we already have oracle networks of different sizes. We have oracle networks of seven nodes, nine nodes, 16 nodes, 21, 31 and growing, right? And the sizes of the oracle networks are growing relative to the amount of value secured by those oracle networks. And then the oracle networks themselves are also getting better and better data providers, better and better nodes because the value they're securing is larger and larger.

So I actually think there're two problems. I think there's a problem around how do you successfully arrive at a tamper-proof, highly reliable way to come to consensus about the external world? Whether that's about randomness generation or agreement on a value from a data source or some computation that you need that a blockchain can't do. And then how do you scale that in an efficient way to meet the demands of different value contracts, right? Because if you don't scale it efficiently, you're going to have certain people with very low value contracts being forced to use a system that's not efficient and that they probably need to either overpay for or be subsidized to an extreme degree which has its own questions. Or you arrive at a system where the amount of value secured determines the security of the oracle networks and those oracle networks should scale to meet that in an efficient way, which is how our system has been architected from the beginning.

[00:37:45] JM: From your work on Chainlink, you have a front row seat to how defi is developing. Give me a preview of what develops in the next five to ten years.

[00:37:55] SN: I think what happens – Look at it this way. Let's just talk about a progression of how this probably evolves, and I don't know in what timeline this evolves, but this is probably the progression. The first thing to look at is that if there's between 30 to 50 billion in the defi format today and the interest rates you can get on defi from stable coins or some kind of

cryptocurrency is something like four to eight percent, while what you can get at a bank is below one percent. And there's also one point – What is it now? I don't know. 1.8 trillion in the cryptocurrency format which is the format for value to be in in order to use defi. I mean, that's a really, really small percentage, right? That's something like two percent or less depending on the day of the total amount of value that can be in the defi format that is currently in the cryptocurrency format, right?

So there is a huge amount of value yet to be transitioned into the defi format and that alone suggests that that 45 billion or 50 billion number is likely to have another zero behind it relatively soon, because the ability to get a four to eight percent return on your crypto holdings and even your stable coin holdings is something that is attractive to the crypto user of which there's 1.8 trillion dollars in value of right now, right? So that's probably the first shift in how more value flows into defi, and that shift has not even really started. It's just slowly getting going. It's just slowly moving along now. At a certain point the floodgates are just going to open, it's going to accelerate in an unbelievably quick way.

The second version of this is when the average person is presented with the choice of whether they would like one percent or less from a bank account or if they would like four percent or three percent or two percent, if they're comfortable with their dollars being turned into crypto stuff and that crypto stuff being put in a defi protocol. I think the reality is that the vast majority of people have no idea where their savings account gets its percentage return from. They don't know if their bank does commercial loans or residential loans or the credit score or the capital reserves or who's on the – They don't know these things, right? They just know that that CD over there gives me X-percent and that savings account over there gives me Y-percent, and that's bigger. I'm going to go there.

So the next shift is the shift where people start putting value into the crypto format in order to use defi to get a rate of return, and logically speaking I think that'll all be very heavily exacerbated by two things. The first thing is inflation. Inflation is really scary. Inflation basically means that the value that you've worked your life to create and accumulate is suddenly through kind of a money printing tax, in this case, is being taken away from, the purchasing power of that value. And I think inflation is going to become a very, very relevant and top of mind issue and school children are unfortunately going to know the word inflation, which is kind of scary in

its own way. And so everyone is going to seek to combat inflation. Everyone is going to seek to preserve the purchasing power of their assets that they've worked their entire life to accumulate. And then the question will be where do they go to do that?

Right now defi has the best yield of anywhere that I know, and it has the best yield plus a lot of the best risk dynamics because you know exactly where your money's going. You know exactly how it's being used in a protocol. You know exactly what the capital reserves of the protocol are. And there are more and more tools to make this clear to people. So I think the second iteration of all this is where the average person begins to use defi in many cases not even knowing they use defi, because applications, whether it's Robinhood or whether it's some other trading application or whether it's a bank, we'll just begin to offer them a two percent rate of return as long as they're comfortable check boxing a form that says, “Yeah, I'm comfortable with you putting my holdings into a stable coin and putting that stable coin into a defi protocol.”

I really think that this shift is what's going to change our industry from being about let's make a token and wonder what its value is and kind of debate that in a market to the world's financial products and financial contracts should work this way and the average person is very comfortable and actually wants that. And then I think the third thing that will happen that'll accelerate society's overall adoption of all of this is that the existing financial system will run into more and more situations where it fails. Robinhood and Gamestop is a very good example of this, right? People thought the world worked one way. They thought their relationship with their assets was that they have control over those assets and that they were free to trade and they were free to do whatever they want. And everywhere you look the word freedom to choose and freedom to do things is plastered all over the place. And then guess what? In the critical moment, it gets taken away from them, right? For a number of reasons related to settlement and any number of other questions. But for users that doesn't matter. Users want a certain relationship to their economic life. They want to combat inflation. They want a rate of return and they want predictable risks that they can reasonably manage, right? That's generally what the global financial system seeks to provide to users.

I think in the longer term, this is probably on the five or ten year horizon, as more and more of the world's financial systems show how disconnected they are from users expectations through their failure, through their inability to deliver what users think they do, not what they actually do,

there will be a massive shift in trust. There will be a shift towards wanting to use a financial system that actually delivers on the promises that people think they already have. And in the long term what that will mean is that decentralized financial products and blockchain-based smart contract applications will just be something that society wants. And when society wants something, the political process begins to give it to them, right? It begins to say you have to do it this way. You have to do a smart contract if you do a certain type of financial transaction, because a smart contract can avoid fraud, mitigate risks for users and provide transparency to the government about what's going on.

And the fascinating thing is that all of that is completely true. All of the features of smart contracts manage risk better, put users in a better position and actually allow governments to manage the global systemic financial risks in a more clear transparent way. And so it's on the basis of that truth that you know I firmly believe that on the five to ten year timeline society will just decide that this is the way that they should do things because it is better. It is fundamentally ten times better. People just don't realize it yet. I mean I realize it because I work with this all day and people in the defi world realize it because they've learned all these esoteric words and phrases and nuanced details. But behind all those nuanced details and esoteric like industry-specific words is a fundamental truth, and that fundamental truth is that the centralized finance is what people want. They want fair, reliable, transparent markets. They want fair, reliable, transparent ways to get a return and they don't like surprises where they thought they controlled their assets or their economic life in one way and it turns out that that control doesn't exist. And so that's the foundational truth of all this regardless of the fancy words or the specific technical details or words of how it's achieved. I think people just don't realize that. And I'm pretty convinced about this because in the cases where I've taken time to explain it to people and I've explained to them the differences and I've asked them, “Well, you as a rational economic actor, would you like a contract that's less reliable where it can be changed on you and you can get something completely different than was guaranteed to you? Or would you like to have agreements that are kind of guaranteed by cryptography and mathematics and physics and are guaranteed to occur the way that you expect them to?” Once people understand the choice, know nobody says, “Yeah, I'd like the highly risky contract where some big bank can just take my money away from me and put me in a really bad position.” So I think that's really the fundamental truth that is important to understand here.

If you find all these ideas about definitive truth, oracle networks, the next generation of smart contracts, how decentralized finance will change, the global financial system, how decentralized insurance will change the world, NFTs and how randomness is important for them. If you find these things interesting and you're looking to join a great team that's building the future infrastructure that will enable all of this, feel free to talk to us. We're hiring developers, product managers, all kinds of people that want to see this future happen. We're excited to talk to you. And you can go to chainlinklabs.com/careers and we have a lot of interesting detailed technical problems to work on and a lot of things related to how blockchains work and learning how they work that I think is going to be interesting and useful for more and more people to learn in their career. So if this is interesting for you, please contact us. We're excited to work with great people that want to see this change in the world happen as much as we do.

[00:47:42] JM: All right. Well, very interesting road map for the future. Sergey, thank you so much for coming on the show. It's been a real pleasure talking to you.

[00:47:50] SN: Thank you, Jeff. It's my pleasure chatting with you as well. It's been immensely interesting. Thank you.

[END]