EPISODE 1243

[INTRODUCTION]

[00:00:00] JM: Decentralized applications, or dapps, are applications that feel like normal apps but are actually deployed on the Ethereum blockchain. That means dapps can't be taken down. They can't be censored or blocked. And they typically use Ethereum accounts as identity and would only experience downtime if Ethereum itself went down. There are a lot of things you can do with blockchain applications particularly decentralized finance. The company Compound develops protocols built on the Ethereum blockchain that establish money markets. Money markets are pools of assets with algorithmically derived interest rates based on supply and demand. The compound protocol represents assets as fungible ERC-20 token balances called cTokens. cTokens automatically increase in value from the amount of the initial underlying asset. The interest generated and managed through the compound protocol can be used primarily for long-term investing in Ether and tokens as well as dapps and other entities. Compound provides lots of documents and discords for infusing interest and liquidity and into dapps and related projects. This enables dapps to manage assets that generate interest and could lead to entirely new blockchain-based business models.

In this episode we talk with Jared Flatow, Director of Protocol at Compound. Previously he worked as a software engineer in Caffeine and founded the company Quasi Convex Union. We discussed the importance of liquidity and interest earning assets in DeFi and how Compound is helping enhance dapps and the role of growth of dapps overall as well as his goals for compound going forward.

[INTERVIEW]

[00:01:29] JM: Jared, welcome to the show.

[00:01:30] JF: Thanks. Great to be here, Jeff.

[00:01:33] JM: Today we're talking about Compound. I’m just going to ask you upfront, describe Compound in one sentence.

[00:01:40] JF: Okay. Compound is a protocol for efficient money markets on Ethereum. So you can supply assets to the protocol and borrow assets for the protocol and you either earn or pay interest.

[00:01:55] JM: And what does that mean to be able to supply assets and to borrow assets against those which you supply? Like why is that necessary?

[00:02:05] JF: I guess what's necessary is kind of a question in itself, but it kind of enables people to do things that they might not otherwise be able to do. People have collateral in different forms that we think in terms of collateral protocol. Every position, if you borrow from the protocol, you need to be over-collateralized, which means that you need to supply more of an asset that the protocol accepts and you can borrow an amount less than what you supply it. It depends what you supply and how much more and what you're borrowing, but that's kind of the basic idea. And like I guess the question is why would you want to supply more of a value of something and borrow less value of something else? And I think there's different answers to that, there's different use cases, but a lot of times people have some asset that they want to they want to maintain ownership of and they also want to have another asset that they can use for liquidity purposes or whatever they might be doing. There's a lot of kind of trader type people that are using the protocol so you can – There's ways to hedge different assets against each other as well using this mechanism.

But I think a lot of it is people who are sort of bullish on crypto overall and want to maintain their long exposure to the assets they're holding and then they want to be able to borrow like dollars against those crypto assets. And so they can keep their exposure but also have kind of dollars to use for liquidity, and they don't mind paying the interest rate because they expect their crypto of values to dominate the interest that they're paying.

[00:03:55] JM: So how does an interest bearing account or this interest rate that you've introduced with compound, how does this become a building block for more complex financial instruments?

[00:04:08] JF: One of the pieces that I guess the kind of broader industry that we're now part of is called decentralized finance, and there's this idea of contracts running particularly on Ethereum now since that's where most of this is happening. With compound, the assets that – When you supply, you actually get back what's called a cToken. So you supply let's say eth and you get back c-eth, and that token is transferable and it represents your collateral in compound. And there might be limitations on what you can do with it. If you're also sort of borrowing against it, because you have to maintain that collateral requirement, you can't necessarily transfer it while you have that borrow open. But that's all part of the contracts that are written that everybody knows how the contracts work. And so like the Ethereum network kind of takes on this role and the contracts that are running on it take on this role of the sort of the third party and enables people to stop trusting or not having to trust like middlemen really anymore, because the middleman is basically these contracts running on Ethereum.

And so the interfaces that the protocol provides and the fact that the balances are represented as tokens and the ability to borrow large amounts of any asset that's supported by the protocol, because there's quite a lot of liquidity in the protocol now, make it a really useful primitive for people trying to do all kinds of things. So one use case is people building applications who they may have for whatever reason have assets for a period of time and they can sort of put them into the protocol to earn interest while they're over that period of time. As far as like the broader financial system, there's a lot of things every day that we're seeing emerging, but kind of these markets by themselves in traditional finance are actually quite huge markets and it's kind of beyond my over my head a little bit is talking about traditional finance since I never really worked in in traditional finance. Fixed interest – So Compound protocol is variable interest, which is I think is a smaller sort of market than fixed interest markets, but the fixed interest markets are like absolutely huge, and that's something that you can actually build on top of protocols like Compound.

[00:06:31] JM: Let's roll back a little bit. Why do you need a token for this system? Like explain what the Compound token does.

[00:06:41] JF: So the compound token is actually our governance token, and that's a different token. The symbol for that token is Comp, and that was something that we added sort of only in the last year really, but like about two years ago what we did is we built the V2 of our protocol

and we instead of just supplying to the protocol and then you kind of don't have your assets, you put them in the protocol then you don't have them anymore. Instead with these cTokens, you get back a token representing your balance in the protocol. So if you supply Ether and you get back c-eth, that token is now like an interest bearing version of whatever you supplied. And the basically the only reason you really ever need tokens is because you want to transfer them. So that's kind of the purpose of anything being a token in my mind. And so cTokens are there so you can have these interest bearing kind of representations of your balance that at any time you can go and redeem them back for more than or equal to the amount that you pretty much more than because of the interest is continuously accumulating more than what you put in. That's kind of like why you want to have tokens.

But there's, again, between these cTokens and the comp token which we introduced about a year ago beginning of last year which is our governance token. Also in the last two years we've undergone this process of sort of decentralizing the whole protocol. So the protocol used to have certain admin keys that were controlled like sensitive things like doing certain upgrades that were possible in the system and setting certain parameters. There was also some special price keys for posting prices to protocol because the system does rely on liquidations which do rely on knowing what the prices and the relative values between the assets and the protocol are. But in the past kind of low upper year we managed to decentralize all those aspects and get rid of all the admin keys. And so instead of admin keys now, we have comp token that actually represents voting rights on all these decisions that get made and anything that can be done in the protocol, which is – So some of these contracts can be upgraded, and like all the parameters that can be set so the governance can do whatever it wants if comp holders agree to do that in a vote. So we have contracts in place that recognize kind of the balances of those tokens, and that's how the whole system is kind of controlled now.

[00:09:19] JM: Gotcha. Of course it's worth noting, there are people that are working on the Compound software. How are you monetizing this? How is the Compound company earning money?

[00:09:31] JF: Yeah. I mean the protocol is not the company anymore. So part of this decentralization process was sort of separating the protocol and having this governance token and now it's really its own entity. The protocol has been profitable since it's been alive, because

borrowers when they pay interest –Most of that interest goes to the suppliers of the assets that they're borrowing, but a percentage of it goes to the protocol itself, and we call it reserves, but it can be used for different purposes. And lately there have been various governance actions which have actually used those reserves for different things including paying some contributors to the protocol, and it's actually – I mean that's a whole other topic, but it's really a self-sustaining system at this point. And then as far as the company is concerned – So the company's VC-backed originally. I think we raised much money more than a year ago at this point and there's been a couple rounds, but I think we're out of pity and just because like our CEO, Rob, is kind of very savvy and has a more traditional finance background. I mean out of kind of like pity, I think the company is doing extremely well even though we're not like really trying to make a profit right now.

[00:10:56] JM: Is there a line of sight towards making money or is it more like you're just kind of building some infrastructure right now and you're going to think about it later?

[00:11:04] JF: Yeah. So the goal is to really just build infrastructure for the nascent kind of crypto ecosystem, and we're building a new blockchain now that's kind of our latest project. Yeah, I think profitability, we do have kind of thoughts about that. It's not something that we're publicly talking about yet, I think, but we definitely have ways in mind that we you can see towards being profitable, but we're really just focused now on building infrastructure that we think will be useful and can grow the ecosystem since we're fortunate to have kind of significant funds raised already and kind of other investments that the company made.

[00:11:49] JM: Okay. So let's get back to the actual core of what Compound offers. If I deposit some Ethereum into Compound, I want to bear interest on that Ethereum. Can you walk me through what happens under the hood?

[00:12:10] JF: Sure. So what happens is you basically – I don't know if you've ever used like Ethereum or MetaMask before. Have you used MetaMask? Or let's just assume –

[00:12:22] JM: I have used MetaMask, yes.

[00:12:23] JF: So I don't know if I should assume that people know what MetaMask, but MetaMask is a wallet that that sort of lets you interact with the Ethereum network. There're other wallets that you can use to interact with Ethereum. A lot of people use MetaMask because it's easy, it's open source. It has a nice Chrome extension. And what you can do with MetaMask is you can go to a sort of a website and if it's Web3-enabled you can connect to it with your MetaMask and it'll sort of light up your MetaMask and now you can interact with a normal web page using some of these kind of Web3 commands. And so you can actually send – You can make a call to a contract on Ethereum using this wallet and you can actually – So you can call the mint function on our contract. We have an interface. There's actually a lot of interfaces to the Compound protocol because the protocol itself is really just on Ethereum. And so anything that interacts with Ethereum or knows how to interactive with Ethereum can let you do this, and there are a lot of ways to do this now. If you go to like a compound.finance UI, there's buttons there that can lead you to click and say, "I want to mint 100 c-eths." And what happens is you just call this contract function, and in Ether there's this idea of a function can be payable, which means you can send it Ether. So you send this function call and you call this function and you send it Ether and the contract keeps your Ether and it writes down that, "Okay. Now Jeff has a c-ethere balance of this much," and it's an ERC-20 which is an interface for tokens on Ethereum. So the c-ether that you back is actually a token and in your wallet you'll see that you now have the c-ether balance. And it's kind of it. That's really all there is to a mint. But now that you have a mint and you have a balance in the protocol, any of the other connected markets you sort of have this liquidity to draw on, which is like your collateral value that you've supplied. And so as long as you maintain a collateral position in these contracts, you can also call other functions, like can call borrow now on another contract or even the same one particularly. Yeah, and then you would be allowed to borrow up to a certain amount of funds of the other markets.

[00:14:53] JM: And just out of curiosity, how do those returns compare to what you would get from like depositing money in a checking account? Like if I would deposit a USD in a normal money market account, how do those returns compare?

[00:15:09] JF: They are variable, it's hard to – And there's all kinds of market forces at play, but I think in the last few years we've seen them be significantly higher than what you would get from a typical checking account. I mean we can check kind of right now what – If you go to the Compound finance markets page, it's kind of up to date what the rates are. I think stable coins

are kind of very popular to borrow and I guess maybe less for supply, but they actually have gone down recently. They're somewhere in like the two to ten percent range. I would say usually when you check first as far as earning. But, yeah, it's a function of demand.

One of the things that we can do because these are algorithmic money markets and because they're completely controlled by contracts is the rates are actually completely determined by the supply and demand for each of the tokens. And so when there's more demand for a particular token or borrowing demand, then borrowing rates go up and in turn the supply rates go up there. There are other variables which come into play and including like what other things are happening in the market. So in the past kind of nine months we've seen a lot of protocols on Ethereum offering these sort of liquidity mining rewards taking — saving rewards, and it's been a bit of like a battle to get liquidity into different protocols. And so the protocols have been offering these sort of like crazy returns and usually in terms of like the native asset of their protocol and they can be very high. And those have impacts throughout the ecosystem. If a new protocol launches and it has a very aggressive sort of incentive going, then it can actually draw funds out of other protocols. If the supply in Compound goes down, then it actually drives the supplier interest rates up for the people that remain in the protocol. And so you'll see that thing happening all the time. Like in the last few days I think a bunch of supply rates went down because I think some programs may have ended and a lot of funds came into Compound and drove rates down. Still higher than what you would get with a traditional bank.

[00:17:31] JM: Can you explain – Just refresh me. What is going on when I put money into this protocol? How is it earning interest? Where is the interest bearing coming from?

[00:17:44] JF: There's a bunch of different assets sitting in these pools. So if you supply Ether, it goes into the Ether pool. If you supply Dai, it goes into the Dai pool. If you supply BAT, it goes into the BAT pool. On the other side, people are borrowing those assets. And when they borrow, their collaterals locked in the protocol and they have to be over-collateralized to a certain extent for this kind of the safety of the system. And so they have a borrow balance in the protocol when they initiate a borrow, and over time their borrow balance is increasing. And so what they owe back to the protocol is an increasing number, which means – And in the worst case what happens is if they don't want to pay back their borrow, their collateral will remain locked, and at some point if they get – We call it going underwater. If their borrower balance gets too high

relative to their collateral balance they can be liquidated, and liquidation is kind of maybe the magic sauce that makes things work. That means that – So if your borrow balance gets behind and you don't have enough collateral, somebody else can repay your borrow and take an amount of your collateral and they're given an incentive in terms of the amount of collateral they get in order to discourage you from wanting to be in that position and also encourage them to want to close your position.

Normally people are actually repaying their borrows. If they don't, liquidation comes into effect. But the way that your balance as a supplier goes up is because the borrower balances are increasing and what's owed to the protocol is sort of distributed to suppliers and also a little portion of it goes to the protocol itself.

[00:19:29] JM: Gotcha. With enough volume, is that the amount of money being taken by the protocol itself? Is that enough to earn the protocol to make the company wealthy or does that – When you say the money goes to the protocol, does that go to the company that's building the protocol?

[00:19:46] JF: No. No. It doesn't. So like we like made a very conscious explicit decision to never take those funds to the company. So this is before we sort of decentralized the protocol. We never touched sort of the reserves according to the protocol because we always wanted to decentralize protocol. And so those funds actually belong to the comp holders. They can do whatever they want with them. They basically accrue to a separate – it's called reserves in the contract. Each of the money market contracts has a reserves field I guess and it tracks what portion of the funds in that contract are owned by the protocol itself. And the only way to do anything with those funds is through a governance vote and a proposal and a vote which happens completely on-chain. So it's really completely owned by the comp holders.

And as far as like how the size, the magnitude of it, it has grown extremely large recently. So when I joined Compound a little over two years ago we had I think about 20 million dollars in assets under management in the protocol, and I think I haven't checked today, but it's about like 12 billion dollars now. So it's grown an enormous amount in the past like two years. Yeah, I mean the amount of interest being generated by which is accruing to the protocol and reserves and also which is being paid to suppliers is a very significant number. You can do all the math

on this if you look at the exact numbers on our markets page or just going to on Ether scan or something, looking on what's happening. All of it is completely transparent in like the Ethereum contracts.

[00:21:38] JM: So if I've got a bunch of money, let's say I have three thousand dollars in Ethereum sitting on Coinbase, is there a way to get that into Compound easily?

[00:21:49] JF: There might be even easier ways, but the kind of default easy way is you can send your Ether to any address which you own and then you can supply that into Compound. I think there's probably even one step ways to do that, and there might be even easier ways to do that. I'm not sure. But that's kind of like the easy normal way to do it.

[00:22:16] JM: Got it. So I would just use my transfer from my Coinbase wallet to my Compound wallet or Compound smart contract?

[00:22:26] JF: Coinbase is kind of like providing the service. So if you have funds in Coinbase, it's basically providing like – It's kind of like custody wallet service for you even though they have a separate custody product, and it's not normally – I'm sort of conflating that term here, but they're basically maintaining custody for you. So they have a wallet that that interacts with Ethereum that's holding your funds, which is basically just a private key associated with an address. You can generate any private key you want. You can buy a ledger or a hardware wallet or you can set up a – You can open up MetaMask and create an account. There're a lot of ways to create a private key and then try to track it. That's basically what a wallet is. So you can generate an account in MetaMask and you can say to Coinbase, "Transfer the funds to this address," and that address is controlled by whatever wallet you sort of have the private key in.

So you would transfer to any wallet. And then from that wallet you would initiate this. So then you could go to like the Compound interface and connect with your MetaMask if you transferred your MetaMask address and you could sort of just click a button and it would ask you, "Do you want to call this function on the contract?" If so, it would do the transfer for you and you would see your balance, your MetaMask balance. Your Ether balance would go down and your c-ether balance would go up.

I mean kind of the whole – The UI for interacting with Ethereum, at least a lot, still to be desired, but I think it's actually relatively simple and elegant under like if you can get past kind of just the lack of policy and like – I mean the fact that the whole thing is decentralized, I think it's kind of what makes some of the experiences not as fluid as they will be in the future. But, yeah, I mean basically it's just a transfer. And then the way to make it even simpler, I think there's probably a way to call the compound mint function from your Coinbase wallet. I believe they have this capability. I'm not sure actually how you do this in Coinbase, but the simple way that I hope will be the normal way in the future is like from Coinbase you could just click the button and have it supplied to come down.

[00:24:45] JM: Interesting. Yeah, that would be a lot smoother.

[00:24:49] JF: Yeah, for sure. I think there actually are ways. Again, I'm not the expert on like what the state of the Coinbase integrations are, but I do think they actually have these capabilities already.

[00:25:00] JM: So tell me a little bit about the engineering behind Compound. Give me the architecture for the smart contracts that are fulfilling the issuance of interest-bearing Ethereum or interest-bearing Bitcoin when I trade it in.

[00:25:19] JF: I guess are you interested in like the math of it?

[00:25:22] JM: I'm kind of interested in the software architecture. I would be interested in the math as well, but starting with the software architecture.

[00:25:30] JF: The great thing about building on like Ethereum and I think the reason why it's kind of exploded a bit in terms of DeFi, is that it's actually really simple architecture as far as building like a whole protocol. All you really have to think about is you have a set of contracts which run on this network and they all have the same state. All the machines in this network have the same state. So it's really simple in that sense and it's kind of also the problem like why Ethereum can't scale. But it's a really simple model. And so when you're building protocol, really, all you're thinking about is like I have these – how do you want to split up your contracts? And the kind of considerations there are it's really about risk management and the risk of exploits

and security vulnerabilities. That's really I think kind of the name of the game when you're designing a system on Ethereum is thinking through all of the bad things that can go wrong and how you want to sort of mitigate some of those things.

And so like the design of Compound E2 protocol, we split each market into its own contract, and this was partly I think because we wanted Eth1 to be an ERC-20 excuse and there was kind of a limitation on being — but also I think we wanted to – We did want to split the risk of having all the assets being one single contract in case there was any kind of issue with the contract that it was – Sort of they weren't all sitting in the same place. And then we sort of moved the – And actually initially we didn't have any of those contracts being upgradable. So if you want your contract to be – By default, everything's immutable on Ethereum. So if you deploy a contract, no one can ever change it. It will just exist the way it exists. But you can build in a function into your contract which says it makes it upgradable. You can make it as flexible or as inflexible as you want.

So our cToken contracts were originally immutable because I think early on there used to be more value in having immutable contracts. People I think felt safer when interacting with contracts that were immutable because they couldn't be changed beneath them. A lot of things have changed. And one of the biggest reasons that kind of sentiment I think has changed at least with respect to Compound is because of the decentralization protocol and because the only way that changes can actually get made to the contracts is through the governance process, and the governance process is intentionally sort of slow. So it's like three days minimum to take a vote and then two days minimum of time lock, which means that from the time that the vote passes. So on-chain you can see like, “Okay, the protocol decided to upgrade this contract or set the reserve factor of this contract into this amount,” or whatever you're going to do. So there's a time period where people can see those changes and they can actually exit the system or whatever they want to do. They can opt out before those changes actually take effect. So that whole system has actually mitigated a lot of the original design decisions where we made these contracts not upgradable and also to some extent splitting into separate contracts. But that's why we have this separate. We call it the comptroller contract. So the architecture of V2 is there's a comptroller contract. It’s like a hub-and-spoke model. So the hub is the comptroller contract and the spokes are the cTokens.

And so when each contract needs to ask these questions when it wants to do a mint or allow a borrow or allow a transfer it can say – You can ask the comptroller, “Is this account allowed to do this?” And the comptroller is the one that determines the value of this collateral is sufficient to cover the value of whatever is being asked to be done. If you want to withdraw, you have enough funds to withdraw. Do you want to borrow? Do you have enough collateral to borrow? If you want to transfer, you have enough liquidity and collateral to be able to transfer. But a lot of things have been added to comptroller since then, but that's sort of the hub and it's upgradable and it's controlled directly by the governance contracts which were added on top of that. Basically we designed the comptroller be this upgradable contract. It had an admin key, and we replaced the admin key with the timelock contract, and the timeline contract has an admin which is the governance contract. So it grew organically, but also I don't think we would have really designed it any differently had we not done this like progressive decentralization.

I think some things have changed. So the cToken contracts that we started as the spokes that were these immutable contracts, the newer ones are actually upgradable as well because the community has found a lot of value in being able to modify those contracts and because, like I was saying, it's fairly safe to do so since it has to go – The only way to upgrade it is actually through this this governance process and the community it's fully transparent. The community makes those changes itself and sort of audits itself and does all the things to make sure that whatever changes it wants to make are going to be sound. But, I mean, of course there's a lot more to it. I don't know if you want me to keep going on this topic, but I’m happy to.

[00:30:51] JM: Yeah. I mean it's quite interesting. Has there been much in the way of protocol changes with – Like have the governance tokens actually been used to vote on some changes to the infrastructure?

[00:31:07] JF: Yeah. We're actually at our like 42nd I think proposal now. I think 41 just happened. I got to check the numbers. If you go to compound.finance/governance you can see all the proposals that have happened and actually who's voting and the leaderboard and it's all transparent. You don't have to go to compound.finance. There're other systems now which are tracking the governance processes that are happening, because basically after we – We’re actually one of maybe the first like fully on-chain governance system. We built our governance contracts last January. It was when we released them actually. And then we built this other

system for distributing comp through our comptroller contract for people that were interacting with the protocol. And it sort of kicked off this whole like summary of DeFi just by the mechanics of it. But what happened is a lot of other protocols started cloning or using our governance contracts and also our governance token which is comp contract. By the way our comp contract, which is the governance token, is a separate contract from our governor contract, and the reason for that is the governor contract is upgradeable. The comp contract is not upgradable to it's mutable, which is really appealing for a token contract. So like Uniswap is actually using a modified version of that for their governance token now, and a lot of the protocol governance systems which have emerged in the last like nine months are actually very similar versions of our government system. And so there's actually systems now which are familiar with those particular contracts and are sort of able to integrate with the government systems of all these protocols because they're all using the same very, very much similar contracts.

I think one of them is called Liptally, which is a way – It's sort of a way of interacting with all these governance systems. But, yeah, I think it's very active and it's been getting more and more active. So it's a good time to get involved I think if people are interested. But what would happen actually the last – One of last rules this last week is the community grant proposal, the community grant committee, which is probably going to bring a lot of exciting changes because what happened – Before the only way that changes were actually getting made, there was a few members of the community that have been sort of writing code and contributing. And then what they do is like after they make some code changes, then they included in their proposal. In this slow governance proposal process they say like, "And by the way, like send me some comp or send me some side because this is how much I deserve for working on this." And so like the government sort of decides all at once, "Okay. We like this change, and we're going to pay you for it," but it was kind of bad because it is very limiting in terms of people contributing because a lot of people don't want – Who wants to develop and like not be sure if they're going to get paid. And so we actually – So now we have this – It was just voted and executed by this governance process that we now have a grants committee, which I think they we gave them like two million dollars first like a six-month program. Whatever they don't use they're going to return, but they can actually just – So they're actually doing everything in public. There's a comp forum, and then on our Discord channel there's a good grants channel now and they have a Twitter account. So you just kind of like apply to the committee. They sort of make it really easy to just get funds.

They're sort of establishing their process. Like this really happened like in the last few days, so it's like really being established now what the processes are looking like, but it's pretty cool. Like this just happened like completely organically and now there's this like expedited way of if you want to develop or build on protocol you can actually get like very significant grants to do so. And that's because the protocol has like a huge amount of assets now to allocate for this this type of purpose, but that's just one example of governance. So other things like governance often votes on things like adding assets to the protocol. There's talk of recently about changing the price oracle, changing reserve factors. Yeah. I mean, I guess you can look through the 40 proposals. Some of them are more boring than others.

[00:35:29] JM: Can you explain a little bit more about the cTokens? The ERC tokens that represent the assets that are held by Compound contracts?

[00:35:41] JF: Sure. Actually what in particular you're wondering about there?

[00:35:49] JM: Mainly like how they function? Like once I own one, like how am I earning the interest on it? Like where is that interest being tracked?

[00:35:58] JF: Yeah. So the way these contracts work is you basically – It's a program. You have a bunch of functions. So when you write a contract, you say like these are the functions that can be called on my contract and you also define like some storage slots, and this is the Ethereum model. It's like you pay gas. So when you want to do something, you want to interact with the contract or interact with Ethereum at all, every operation costs some gas. And so one of the more expensive things you can do, the most expensive thing you can do is write permanent storage. But that's the only consideration if you want to have storage in your contract. You can just add slots for storage. And if you use those storage slots in your contract it will make people interacting with them more expensive. They'll have to pay more to interact with those functions the more expensive you make them. But there's sort of like storage available – There's a single state machine, which is Ethereum. And if you want to write to storage in the Ethereum sort of state, then you can just do it in your contract. You just have to pay to do it.

And so this is basically how contracts do everything. They can't interact with the outside world except through – I mean all the Ethereum VM functionalities are either like read and write from storage or doing math operations and things like this. There's no network calls or anything. And so what the Compound protocol is basically you call comment. Mint does a transfer of assets, and there's some – It depends what you're transferring. There's actually different types of assets on Ethereum. Like Ether itself is like the native asset of Ethereum, and it's not an ERC-20, but all the other assets in Compound are actually ERC-20s themselves because ERC-20 is basically the standard for how you transfer things which aren't on Ethereum.

And basically everything that's happening is just through tracking storage and doing math on the Ethereum state machine. And so really all the contract is doing is it's keeping track of who supplied what. And then the way that the magic of interest happens is that it's actually implicit. So we can't loop through everybody's account and be like, “Okay. You get this much every –” And when would you even do that? It's like compounding every block. And so we every block loop through all the users accounts and be like add this much to their balances. So instead we use what we call an interest index, and whenever an action is taken in the protocol, which increases the borrow interest that's owed to the protocol, which is actually – So this happens every block. Every time somebody interacts with the protocol, one of the first thing that's done is there's an accrue interest function that's called. And what that does is it – We call it truing up. It trues up the borrow index. So the total borrowers that are owed to that whichever contract that you're in. So in the cToken contract, it’s the c-Dai market you're interacting. First thing that happens when you're minting or doing anything, the first thing that happens, managing or borrowing or transferring or withdrawing or re-bank or liquidating, the first thing that happens is accrue interest. It says, “What was the interest rate since the last time that we've accrued interest? How much interest has been accrued?” And then it actually allocates that to different places. So there're really only two places it can go. So it sort of takes a little fraction of that and puts it into the reserves and then it takes the other large fraction of it, puts that into – It gives it to suppliers, and the way it gives it to suppliers is it ticks up the exchange rate. And so when you're holding a cToken balance, the amount that you can redeem it for is increasing via the exchange rate. And so like basically you don't have to update everybody's balance. Instead they just have a cToken balance. The exchange rate is going up. And when they want to redeem their cTokens for the underlying, you can do so at an increasing value.

[00:40:35] JM: Gotcha. Can you tell me more about the actual development of the protocol and how like software engineering proceeds? Like how does testing work and how does a deployment work? Just give me an overview of the software engineering practices.

[00:40:54] JF: So the main consideration with Ethereum has been, like I was saying, like security. The thing with – And especially earlier on, and like things have definitely been evolving on Ethereum. So I guess I'll maybe go through the journey a bit, but like very early on like it felt a bit like you're like deploying these like spaceships or something. Once you put them out there, because a lot of them – Because they're basically immutable by default, and you can't really change them. It's a lot more like hardware. You do like deploy them. You can't really necessarily do anything to fix a problem if it happens once you've deployed them. So we put like a ton of effort into making sure that, first of all, that we don't have problems once things are on-chain. And second of all that like we have the right like knobs and levers to be able to fix things when they go wrong, but also like not too many knobs and levers that people – That there's like admin powers that people need to be afraid of. And it's actually like it's a tricky balance to get right, and I think that's the hard part of like building on Ethereum. But the way that we sort of make sure that we don't have problems when we get to the chain, and of course there's really no way to like guarantee that, but that's why we have like a sort of multi-tiered approach to this through – Basically there's a QA process where we – So the first thing we do when we're building a new contract or anything is we do an in-depth detail spec document. I would say this is usually like the longest part of our process where we actually specify it in as great as detail as possible like all the different angles of the system and how things should work. And that lets us, when we get to actually writing the contracts, focus on the key things that we really care about and not have a lot of other noise and back and forth on code when we get to actually writing the code and we can keep the code very like streamlined and very transparent as to what it's doing and try to be very clear about it. And then what we do is once we have a spec we start writing this code and then we'll add unit tests as we develop the pieces in the specs. Basically the contract itself should be are generally like one to one with these spec docs and then the unit testing is just a matter of making sure that those functions like do something reasonable, do reasonable things that they're supposed to, but they should cover like every branch that can happen in the contracts. And then the next level testing is like integration testing and simulations. And I think simulations are actually the most powerful way that we have of checking that the contracts will behave the way we expect them to.

And like nowadays when – So we're not doing the main development of the protocol itself anymore. It's actually the community is very much doing the development now. And so like the processes we had as a company for developing contracts, we tried to empower every everybody in the community to follow these guidelines so that they'd be able to make changes and get them approved by governance. But, yeah, so like this phase of like simulating what the effect of your changes will be or what your contract will do is a very cool kind of powerful thing that you can do with Ethereum and other blockchains. So you can like basically fork the state of the network and then you can do these hypotheticals of like, “Okay. Like basically I have a clone of Ethereum. Like this was the state at this block and now I do all these other things,” and pretend like all these other things happen and you can like see if your expectations are better or not. And you have to do a lot of thinking about what sort of scenarios you're testing there, but it's a very powerful way of checking what will happen after you make some changes.

And then kind of the other piece of the process that I think is very important not just because of the results, so it's formal verification. So we work with a company called Certora that has a tool to formally verify solidity contracts and or really EVM byte code. What you do is you write down what they call CVLs, Certora verification language. There's other formal verification frameworks as well. It's just one that they've been using. But you basically write down like invariants that you expect to hold in a way that you can sort of ask the verifier to try to prove that those things hold. Or really what they do is they try to find exceptions to your invariants. So they either say like, “Okay, can't find anything.” And you say like, “Okay. Then I’ve proven this thing.” Or they find sort of an instance of a state of the contract or of the EVM which violates your assumption.

For example, you could write down a verification rule that's like exchange rate. If I check the exchange rate and then I do some action in – I call any function on the contract and then I check the exchange rate again. The second exchange rate must be greater than or equal to the first exchange rate. So you can write down that kind of thing and it can actually prove that like, “Yes, that's the case. There's no function.” There's no way to actually make that state – Get to that state without giving these functions in – Given this contract. Or they say that's not true. This can actually occur. But what you get there is you don't get that all the ways that occur. You just get like – You sort of have to think they're like, “Well, why did this – How to define this counter example to what I was trying to prove?” So this is definitely whole process of if you're finding

those kind of issues you have to think a lot. So that's why I say the results of the formal verification aren't the most useful part of it, because the technology is actually still pretty nascent and there're a lot of things you still can't prove, but sort of the thought process going into it and trying to think about the contracts in this way and thinking about the invariance in the system is I think a very important part of the process and trying to make sure that the contracts do what you want and expect them to do it. But, yeah, I mean that's basically the process.

So we go through those QA steps typically, and then there's an auditing process usually for bigger changes, and community views things typically. Again, then it's up to – If somebody makes a proposal, you have to have a certain amount of comp to make a proposal, or you can go through these – You still need a certain, like a much smaller amount of conp, but you can make a community proposal which says it sort of doesn't really get proposed until it gets enough support and then it becomes a real proposal which people can vote on. And then once it's proposed, we'll start voting. And if it gets enough support, it'll be passed, which means you can view it in the time lock. And then after enough time, elapses in the time lock. You'll be allowed to execute it. And then if nobody executes it after a certain amount of time in the time lock – So like specifically like two days. And it takes at least two days, and then if nobody called it for like two weeks, which has never happened, but like if that happened, then at some point you can't call it anymore. It would expire and it would effectively be cancelled. But that's pretty much the whole process for how people make changes for the protocol now.

So we've started to – As I've said before like, we're actually working on our own chain now. So we are still doing Ethereum development. We still follow this process for how we do the contracts that are on Ethereum, but not everything is on Ethereum anymore. So we're starting to sort of expand this process to try to apply in a less restricted system. So the EVM is very restricted to the training system, which is nice for being able to think about safety in a lot of ways. I mean when you're building the blockchain itself, you don't necessarily have – You don't rely on the assumptions that you necessarily do when you're working within the EVM.

[00:49:02] JM: So the new chain that you're building, you're building an entirely new blockchain for Compound?

[00:49:10] JF: Yeah. It's called Gateway. So there's actually a project called Substrate, which is a framework that Polkadot — rebuilt for Polkadot, and it's actually it's a Rust sort of framework. Well, technically like it's the WASM interface. You could actually build a Substrate chain not in Rust, but really a good practice. It's a Rust framework for building a blockchain and a really bunch of libraries building blockchain. So we've been using that. Our code is actually open source ready for this and we've launched our test net. We're in the process of adding validators to the test net. Yeah, it's its own chain. It's starting out as a proof of authority network. The idea is to eventually be staked by comp, but it introduces this asset called Cash, which is an interest-bearing stablecoin, which is in a lot of ways similar to the V2 protocol we've been talking about on Ethereum, but it sort of takes all of the learnings that we've had from the V2 protocol and it tries to make like a reimagined like way better V3 in a way, but it sort of connects to other chains, which is the reason it's its own chain.

We call them star ports, which is like the contract which connects to the compound chain to the gateway on whatever chain that it's talking to, but the idea is you can lock assets on Ethereum into the star port on Ethereum and then they magically are part on Gateway then. And then you have this cash asset that you can actually transfer between any of the connected chains. So people on Ethereum will be able to move assets onto Gateway and sort of use their liquidity on Ethereum if they want to go and use some cash on a different chain like under Polkadot or Solana or Tezos or whatever star ports get built for a Gateway. But the idea is it's a cross-chain chain. It's like a network chain for moving value between chains, but it's also kind of the V3 protocol.

[00:51:19] JM: Very interesting. Sounds ambitious.

[00:51:21] JF: Very ambitious.

[00:51:22] JM: We should begin to wind down. I'd love to get your picture for how DeFi unfolds in the next five to ten years and just what the overall landscape is going to look like from your perspective.

[00:51:38] JF: I mean I don't know. It's really amazing. It's been a really amazing journey. I've only been at Compound a little more two years and it feels like much longer than that. So many

things have changed and it's just exploding now. When I started I thought like, “This is amazing.” It's really hard to keep up with all the awesome developments that happen like every week, but it's like so much harder now. Yeah, just like a ton of really smart people working in things and like trying to really change the world I think, and I think I think they're going to succeed. I think we're going to succeed. Like I think in five to ten years the whole sort of financial infrastructure will look different. I think it's already happening, and I don't really know exactly what it's going to look like, but I do think in order to succeed, like things have to become way more usable. That’s got to happen. And like less focus on like innovating and breaking things and more focus on how do you make things work for people who don't necessarily understand like what's happening under the hood. And I think like with respect to like protocols like Compound, like I think the way that I would like to see things expand is in terms of the collateral, the types of collateral that you can use. I just thought that Compound is kind of like a basis of trade so you can – Yeah, it's just a way of if you have some value, which is not necessarily liquid, to be able to take advantage of that value and use it in a more liquid way. And so I think people have – There's like all kinds of collateral that people have, their houses, cars, whatever and even more abstract things than that that they're not able to really tap or leverage the value of. I think you know as more things are brought on to chain and represented in ways on chain that are good representations where you're not losing values, you have to be able to reliably represent things, which is kind of the challenge for getting new collateral types onto the chain. Yeah, that's certainly my goal over the next – Or what I hope to see happen over the next five, ten years, is like really having a broad set of things that people can represent on the chain and do – Pretty much, I think even if you could do all the same – Do various similar things that you could do today, but with all these other types of assets it would just be really amazing. But I’m excited to see, because I’m sure that everything that I think will happen now is you will be dwarfed by what actually happens.

[00:54:14] JM: Yeah, sounds amazing. And I’m kind of a believer at this point too. I’m trying to keep up with the space best I can, although it's such a big animal at this point and to try to keep up with it concurrently with the rest of the world of. Software engineering is quite a trial.

[00:54:29] JF: Yeah, it sure is. I don't think anybody can really keep up with it. Yeah, you just got to pick some things that you're interested in and try to pay attention. But it's a good problem to have I think.

[00:54:41] JM: Well, Jared, thanks for coming on the show. It's been a real pleasure talking to you.

[00:54:45] JF: Yeah, you as well. Thanks for having me, and glad to be part of it. Thank you.

[END]