

EPISODE 372

[INTRODUCTION]

[0:00:00.4] JM: Cryptocurrencies have seen a surge of value recently. People are starting to see that Bitcoin, Ethereum other cryptocurrencies are not just for speculation. At worst, they are a store of value, like digital gold. At best, they are a tool for micropayments, smart contracts, and an entire decentralized financial platform. Coinbase is a company for buying and selling cryptocurrencies.

This episode is the first of three interviews with different members of Coinbase. In this episode, Linda Xie and Jordan Clifford explain why crypto currencies are important and how products that Coinbase builds make cryptocurrencies easier to use. This is the first in a series of episodes about Coinbase, and tomorrow we're going to discuss antifraud with, Soups Ranjan, Director of Data Science at Coinbase. I'd love to hear your thoughts on this series and any other suggestions or feedback you have. You can send me an email, jeff@softwareengineeringdaily.com.

This episode — This series can be thought of as a sequel or a continuation of the series that we did with Stripe a few months back. You can listen back to that episode. We did three different episodes with Stripe, and it was really popular. I hope we do the same with this series, and I'd love to hear your thoughts on it.

[SPONSOR MESSAGE]

[0:01:37.8] JM: Hosting this podcast is my full-time job, but I love to build software. I'm constantly writing down ideas for products; the user experience designs, the software architecture, and even the pricing models. Of course, someone needs to write the actual code for these products that I think about. For building and scaling my software products I use Toptal.

Toptal is the best place to find reasonably priced, extremely talented software engineers to build your projects from scratch or to skill your workforce. Get started today and receive a free pair of Apple AirPods after your first 20 hours of work by signing up at toptal.com/sedaily. There is none

of the frustration of interviewing freelancers who aren't suitable for the job. 90% of Toptal clients hire the first expert that they're introduced to. The average time to getting matched with the top developer is less than 24 hours, so you can get your project started quickly. Go to toptal.com/sedaily to start working with an engineer who can build your project or who can add to the workforce of the company that you work at.

I've used Toptal to build three separate engineering projects and I genuinely love the product. Also, as a special offer to Software Engineering Daily listeners, Toptal will be sending out a pair of Apple AirPods to everyone who signs up through our link and engages in a minimum of 20 work hours. To check it out and start putting your ideas into action, go to toptal.com/sedaily.

If you're an engineer looking for freelance work, I also recommend Toptal. All of the developers I've worked with have been very happy with the platform. Thanks to Toptal for being a sponsor of Software Engineering Daily.

[INTERVIEW]

[0:03:39.9] JM: Linda Xie and Jordan Clifford work at Coinbase. Guys, welcome to Software Engineering Daily.

[0:03:44.6] JC: Thank you.

[0:03:44.6] LX: Thank you.

[0:03:45.1] JM: Today we're going to talk about a variety of different cryptocurrencies, the cryptocurrencies that Coinbase supports. Let's start off with the broad definition, what is a cryptocurrency?

[0:03:56.4] JC: Broadly speaking, a cryptocurrency is a digital asset that is secured using cryptography. Cryptography gives us a lot of primitives that we can use as building blocks to create an overall system that administrates a digital asset. That's cryptocurrency.

[0:04:16.1] JM: What's the blockchain?

[0:04:17.0] JC: A blockchain is widely misunderstood. A blockchain really isn't enough information to describe almost anything, but a blockchain, generally speaking, is a chain of blocks, just like it sounds. Each block contains a list of transactions or state transitions for the units of account or the tokens. On a Bitcoin blockchain, we store transactions and these transactions has inputs and outputs and the transition from input to output just tells the whole network that these coins have moved from one place to another and we aggregate those transactions into blocks and we have each block reference the last block. It's an append only ledger that gets created.

[0:05:00.5] JM: Linda, why is it useful to have a variety of cryptocurrencies? Because people have been talking about Bitcoin for a while. Now, there's a lot more cryptocurrencies that have made — Well, a few more, at least, that have made it into the mainstream or the mainstream discussion as far as engineers, at least. What's the use of having a variety of cryptocurrencies?

[0:05:20.7] LX: Yeah. I think that everyone just has different ideas on what they want out of cryptocurrency. It started with Bitcoin where I think everyone wanted to have a way for a decentralized source of money where you could send money from one person to another. It's instant, global. The problem that some people had with Bitcoin was also that they didn't want all their financial transactions shown on the blockchain, because every single transaction is public.

You got a group of people that also value privacy, so then you started having interest in other privacy focused currencies, like Minera and Zcash and Dash. You had that privacy group and people wanted more powerful digital currencies, so the ability to write conditions in. That's where you kind of had smart contracts coming along, so that's where Ethereum come along and there's also other ones like Tezos where people are getting interested in being able to write conditions, being able to write decentralized application.

It's all different kind of use cases out of it. All of them I think can coexist together, and as you have more infrastructure for any interblock connection, you can actually just move freely between blockchains, I think, in the future, but it's just a matter in that specific use case what you want to have that or your digital currency.

[0:06:29.4] JM: People sometimes get tripped up because they don't understand why cryptocurrencies had value in the first place. When Bitcoin was first instantiated, the people who were buying into it, why were they doing that? What incentivized it?

[0:06:46.6] JC: The earliest days, Bitcoin was extremely fringe. It started about out of — It came out of a cyberpunk mailing list, and Satoshi Nakamoto which is a pseudonym for the creator or creators of Bitcoin kind of got some curious people into this purely as a total experiment. For the first year or two, Bitcoins had almost no exchange value. People would toss around thousands of them like they were not nothing, because they were nothing. Only through a process of kind of just experimentation and people seeing it is a toy did it finally emerge as an actual medium of exchange. It is kind of an interesting chicken and egg problem that Bitcoin got over purely through curiosity, I think.

[0:07:31.7] JM: I feel like the first use of Bitcoin was essentially speculation/curiosity, let's tinker around with this thing. We've gravitated towards a place where, now, the primary use of Bitcoin is store of value, I think, or maybe you can correct me if I'm wrong. What's the utility of Bitcoin today?

[0:07:53.8] JC: The utility of Bitcoin today is a money that lives independent of other entities. There's no banks governments, there's no governments, there's no intermediaries, there's no custodians required. That really allows us to do bit money in a peer-to-peer way, purely peer-to-peer. This opens up all kinds of possibilities for new markets to open new market corridors, all kinds of transactions that just never would've been allowed or never were feasible under the old system can now happen. We have ways for any two parties in the world to do business with each other without trusting each other and without trusting a third-party intermediary.

This is really revolutionary in the sense that now we can transfer value over the internet without any trust. This intermediation of the financial systems is something that we're all very excited about here.

[0:08:47.4] JM: Now, I understand why Bitcoin is useful for sending money around. There's also secondary capabilities of it where you can send messages that are not just financial transaction,

that you can only send information. I guess is the Bitcoin blockchain useful for sending messages that are not financial transactions or is that just like a secondary aspect of it?

[0:09:09.9] JC: There's a lot to unpack here. At its core, Bitcoin is very useful for this type of thing. The way Bitcoin is structured is nobody coordinates with each other. Everybody acts selfishly, and out of this, we have this append only immutable ledger that just get continues to move forward as time marches on.

The way it's constructed is blocks are added and it's provably hard to add a block over and over and over. The deeper ends of the blockchain, you have your money transaction or even just a bit of information that you want to keep as a permanent record. As time marches on, it becomes impossible to reverse those records. As a way to create an audit trail, as a way to monitor your supply chain, as way to really record anything that you want to stand the test of time, the blockchain is perfect for storing it in a way that will never be temperable.

[0:10:06.7] JM: The Bitcoin blockchain.

[0:10:08.8] JC: Yes, the Bitcoin is the most secure, largest blockchain as of today.

[0:10:14.2] JM: Linda, where does Coinbase fit into this? If we've got this big decentralized open source world of transactions, what is the purpose of Coinbase?

[0:10:26.9] LX: You definitely need a way of getting into this world of decentralized currencies. Coinbase we see as the fiat rails for this, so we are the trusted place where people can link up there bank account really easily and buy and sell digital currency. At the same time, not everyone is able to understand how to store their private keys, so we're able to be a means for people to easily store their funds through us and feel that their funds are safe.

I think that Coinbase is really important for getting mass adoption to happen because a lot of less technical people are not going to want to learn all these stuff and how to store these different digital currencies.

[0:11:03.0] JM: Bitcoin was the first currency that Coinbase supported. What was required to implement the support of Bitcoin for Coinbase?

[0:11:13.1] LX: Yeah. It's definitely a lot regulatory and legal work, especially, because you have to have a conversation with regulators and law enforcement and banks to say, "Okay, here's what Bitcoin. This is why it's not just used by people buying drugs on [inaudible 0:11:26.6]. This is actually really valuable use case for people doing remittances to get paid out in Bitcoin in their other countries."

We had to form that narrative, and so there's a lot of work involved by our compliance and legal teams to try to get that trust of Coinbase and why they should be willing to support Bitcoin too and how we could just work with them in general in just understanding exactly like what is Bitcoin, what does the blockchain do? There's a lot of that kind of work.

[0:11:55.3] JC: Just to add on to that. What it actually took to get it off the ground was a lot of security key management work. One of the things we pride ourselves here on Coinbase is being security first. Security trumps everything else. We take a lot of precaution to make sure that no single person has control of our called storage. We geographically distribute the coins. This key management solution is really what allows us to store customer funds in a safe way. Then we also had to do payment integrations with our banks. Current banks typically use ACH, so we have to get that set up and operating to get the thing off the ground.

[0:12:36.0] JM: The second cryptocurrency to gain serious traction was Ethereum. Ethereum is a platform for running decentralized applications. Why does the use case of decentralized applications — I can see why we would want a decentralized application for fault tolerance and so on. Why does that use case require a crypto currency?

[0:12:59.1] LX: Yeah. I think — Decentralized applications are really important because you just don't want a centralized source where they're the ones controlling everything that's coming in and out of it because they can get shut down. They could potentially be corrupt and be the middleman or take exorbitant fees.

With the cryptocurrency, you're able to have, like what Jordan mentioned, peer-to-peer exchange. People are able to exchange information between each other. You could have forms of decentralized governance where each person that owns part of the cryptocurrency, so they own digital currency, is able to vote on a piece of the decentralized application. I find that really important because how else would you be able to have an exchange of information like that in a decentralized manner?

[0:13:42.2] JM: Right. What's an example of an application that I want to run on Ethereum?

[0:13:48.8] LX: An application I find really interesting is Augur. Augur is a decentralized platform for prediction markets. The way Augur works is, essentially, you have people to hold their tokens rep and people to hold rep are able to vote on the outcome of the prediction markets, because you need to have a source of truth, like what was the outcome of the prediction market?

Otherwise, in the past, prediction markets have used centralized sources and they've said like, "Okay, we're going to pull from this database or we're going to just have someone arbitrarily say whether this event happened or not."

With Augur, you have these token holders essentially voting on the outcome of these events and actually determining what happens or not. In that sense, you know that there is not going to be some corrupt source whose cutting everyone off and saying, "This is what happens." In that sense, I think decentralization is really powerful for prediction market.

[0:14:42.3] JM: We jump forward there to tokens. Ethereum has Ether, which is a cryptocurrency, and then people build on top of Ethereum with tokens. They issue their own currency. Can one of you explain what's Ether used for or what's a token used for? I guess maybe we should define a token and define Ether separately.

[0:15:04.9] LX: Yes. Ether, you can just think of as the native currency within Ethereum, and that's what's used to essentially make these computations happen. Tokens are what's built on top of the Ethereum platform. You kind of think of it as just like — The way I think of it is like the App Store, so Apple has this App Store where they're able to make other people create applications on top of them. Within those applications, people then issue their own currencies which are used for arbitrary purposes.

In Ethereum, a token is just simply a smart contract that is used for a specific purpose within the decentralized application. The creators of these applications will pick what it's used for. It could be used for decentralized governance. It could be used for just sending a transaction fee. The reason a lot of these projects are doing tokens is because it creates network effects. Once you have this token, you're more likely to use their application and at the same time you're able to vote on potentially how the application itself should evolve over time without actually impacting Ethereum itself.

[SPONSOR MESSAGE]

[0:16:16.3] JM: Simplify continuous delivery GoCD, the on-premise open-source continuous delivery tool by ThoughtWorks. With GoCD, you can easily model complex deployment workflows using pipelines and you can visualize them end-to-end with its value stream map. You get complete visibility into and control of your company's deployments.

At gocd.io/sedaily, you can find out how to bring continuous delivery to your teams. Say goodbye to deployment panic and hello to consistent, predictable deliveries. Visit gocd.io/sedaily to learn more about GoCD. Commercial support and enterprise add-ons, including disaster recovery, are available.

Thank you to GoCD and thank you to ThoughtWorks. I'm a huge fan of ThoughtWorks and their products including GoCD, and we're fans of continuous delivery, so check out gocd.io/sedaily.

[INTERVIEW CONTINUED]

[0:17:27.0] JM: As I understand, Ether is the cryptocurrency that's you're awarded essentially for verifying transactions on the Ethereum blockchain similar to how Bitcoins are what you're awarded as a prize for memorializing transactions in Bitcoin. This is how we get a distributed ledgers, is we have all these people that are constantly verifying all the transactions, and occasionally they're going to be awarded Bitcoin for memorializing, for verifying those transactions.

Ethereum is on more rich development platform that you can build stuff on top of than Bitcoin. Is Ethereum just a superset of the functionality of Bitcoin? Why would you need Bitcoin if you've got Ethereum?

[0:18:22.1] JC: Bitcoin has a different philosophy on how it operates. First of all, Bitcoin doesn't have a leader. It doesn't have a centralized force under control. Not to say Ethereum technically does, but it's closer to centralized control with the Ethereum Foundation and Vitalik heading up development efforts. It's a lot easier to consensus on Ethereum protocol updates.

Whereas Bitcoin, is much slower to change. It's a lot more stable just because it's been around a lot longer. It's got a nine-year history now. It's got a much bigger community at the moment. Because of that, it has more stability which a lot of people like out of their money. They don't want a protocol that's going to be updating rapidly if they're being a bit more conservative about how they want to just have a better instrument or an assets to hold on to. Stability is nice property for money to have.

Really, they've just felt different value propositions. Ethereum is a much better platform to do smart contracts, to do decentralized applications, to do decentralized autonomous organizations, or DAWs, not to be confused with DDAW.

Ethereum has definite advantages over Bitcoin for certain use cases. If you really just want to be certain that you're buying something that's going to be around in two decades, Bitcoin probably is still the safer bet.

[0:19:45.0] JM: It's a safer bet mostly because of the governance? Is that basically what you're saying? Because the governance — My understanding of the governance is Vitalik and Ethereum are more move fast and break things and Bitcoin is more like holdback and be conservative in our changes to stuff.

[0:20:03.5] JC: Right. Core devs will often make analogies to rocket engineering or changing the the engine in flight, and that may or may not be apt. The truth is that Bitcoin does have a longer history, it does move a lot slower, and the protocol is a lot simpler. Bitcoin is a much simpler design. It basically relies on somebody having the unspent transaction outputs set. That

unspent transaction output set or, UTXO as you'll often hear them called, that is all there is to understanding this current state of affairs on Bitcoin. You have that set of unspent transaction outputs. Along with that will be addresses or kind of requirements to spend those Bitcoin, and that's it. It's a very simple design transactions, basically, are just modifications to that set of unspent transaction outputs and it's a very simple easy-to-understand design. Whereas Ethereum has an entire virtual machine built into it. It has a much broader scripting language on top of it. It's much more powerful and flexible and extensible, but it's also necessarily more complicated and it's going to take some time for it to mature.

[0:21:18.8] JM: We talked about tokens and any app built on Ethereum can issue a token, which is the currency that is used within the app. Can I go on Ethereum right now and just like make my own token and it's like I have control over all of that currency?

[0:21:35.8] LX: Yes, absolutely. There's are things like a token factory where you can actually go online and just create a token, name it a certain name. You can change the visibility of it, so you can say how many decimal places you want it to be and you can have full control over it and you can issue it to other people. It's just simply an ERC20 token.

[0:21:54.9] JM: How does that — What's preventing somebody from just dosing Ethereum and making a bajillion different tokens and do I have to pay Ether to run my application on the Ethereum blockchain?

[0:22:07.7] LX: Yeah. You do have to pay Ether, and they refer to it as gas that you have to pay to actually run an application. You can just DDoS the network without actually having to pay a cost.

[0:22:17.7] JM: Okay. What's the process for somebody who wanted to get started with a decentralized application, like do I have to just go buy enough Ether to get my application running?

[0:22:30.2] LX: Yeah, you only need a small amount of Ether honestly. It depends on how complex your smart contracts are, but you could just go online and learn how to start your first app. There's a lot of resources for that. There's some sites that teach you how to learn solidity,

which is what you need to write the smart contract. It's pretty simple. I don't have a really strong background in CS, but I was able to just write my simple smart contracts on that. There's also a test nets, so you could just write a smart contract on the test network without actually having to spend real Ether.

[0:23:04.0] JM: The topic around the Ethereum is often smart contracts, and now we're talking about tokens. Is there a mandatory relationship between tokens and — If I make a small contract, does there have to be token involved or are these just separate concepts each of which can be built on Ethereum?

[0:23:22.0] JC: They're definitely separately. There's many possible smart contracts that have no need for a token other than Ethereum itself. With a smart contractor, you can do things a crowd funding, you can do escrow and you can do plenty of applications that use nothing but Ethereum. It's not required to have an app token or another token on top of Ethereum.

[0:23:46.8] JM: I could I'd spin up my own token and then also spin up a smart contract that officiates some way that users will interact with me and that token.

[0:24:00.0] LX: Yes, you can pretty much do anything with a smart contract and a token is just arbitrary in whatever you want it to be smart.

[0:24:06.2] JM: Is smart contract — That's a type of decentralized application?

[0:24:09.3] JC: A smart contract is a special type of agreement that really codifies how a transaction should be handled. On Ethereum, there's two types of account you can have. You can have an account that's backed up by private keys, or you can have an account that's backed up by code. The second, the latter, where the account is backed up by code is often referred to as a smart contractor. That just means that it's code that is actually in charge of what happens with the balance of that account. You can invoke functions on the code. You can do almost anything. You can build tokens with the smart contract. Tokens are just something that grows out of a certain type of smart contract, the special case of a smart contract, but a smart contract is very broad. It just means logic is going to dictate what happens here.

[0:24:58.6] JM: When tokens or smart contracts get declared, can they ever be changed in the future or are they immutable?

[0:25:07.2] LX: You can definitely update smart contracts, but it's a matter of how often you want to update it and what you want to do with it. That's why a lot of these projects go the decentralized governance route and they're hoping that when you make updates to the smart contract that there's consensus around that update, because you don't want the developer to just update arbitrary pieces.

[0:25:24.9] JM: Of course. Now, these different features that we're talking about with Ethereum, these are not necessarily things that Coinbase really has to worry about, right? You guys are just storing Ether? What do users of Coinbase want out of an Ethereum Coinbase offering?

[0:25:42.4] JC: We primarily see ourselves as a brokerage and an exchange. Those are our two main products. In doing those two functions, we obviously need to be a custodian of other people's assets, of customers assets. I think what customers expect from us is really just relentless obsessing over the security of their funds, and that's something we do day-in, day-out, is obsess over the security of the funds. We put that above all else and then we just try to make it really easy to use. Exchanging fiat money or a government issued money for digital currencies is our primary business model and we just try to make that very easy, whether you want to use our brokerage Coinbase or our exchange GDAX. The point is to make it very easy to get up and running and to get your hands on some of this digital currency.

[0:26:28.2] JM: Was there anything significantly different that you had to do for supporting a Ethereum and Ether than you had to do for Bitcoin?

[0:26:35.2] JC: On the operations side, definitely, the legal and compliance aspects, because you go back to the regulators and law enforcement like, "Well, remember we told you about Bitcoin? There's something called Ethereum and there's something called smart contract." You basically have to have that conversation all over again, but it's even more difficult sometimes. At least there's a basis for understanding of what Bitcoin was, so that part was easier. Yeah, I think smart contracts is just like another level of understanding. Then on the technical side, maybe Jordan —

[0:27:04.4] JC: On the technical side, we have a specialized key storage solution for Bitcoin. That had to be re-implemented for Ethereum. That was a rather significant engineering effort just to create a new key management solution for Ethereum.

[0:27:20.6] JM: What's different?

[0:27:21.4] JC: It's completely different format for the private keys, the address format, the actual monitoring of incoming transactions. We have to basically monitor the blockchain for any transaction that could be going to one of our customer's accounts. It just throws a significant undertaking to launch a second digital currency just because the whole backend had to be reconstructed.

[0:27:44.8] JM: Laura, can you talk more about — Sorry. Linda. We've met today. Tell me more about the conversations with regulators and people who have no interest in the Ethereum from like a casual observer perspective.

[0:28:03.8] LX: The conversations generally go really well. We have a really strong team with a great background, so a lot of people actually come from that world or know how to talk to regulators. They're open to the idea. I think Bitcoin at the start kind of had this connotation of having been associated with darknet markets. Whereas Ethereum was just like this clean slate of just there a lot of developers that really want to just build applications that make it easier for people to use in a global sense. It's not just people in the U.S. who are able to access this.

I think the actual mission of Ethereum, a lot of regulators and law enforcement from my conversations have actually really liked it. They thought it was something ambitious and that it was — A few of them have a great — It's really going to change the world.

[0:28:49.8] JM: Was it hard in the initial conversations to explain what — Because, for example, I wouldn't be able to explain to my mom what a decentralized — Maybe I could. Probably if I spend an hour trying to explain to my mom what a decentralized application is, she would understand. I guess that's basically the conversation that you're having.

[0:29:07.0] LX: Yeah, it really is. I think people understand why something needs to be decentralized if you give them examples of things that have failed in the past. The conversations haven't been too bad, it's a step up from Bitcoin to Ethereum for people.

[0:29:23.7] JM: What's the state of — I don't know if you listen to Andreessen Horowitz podcast, but they've been doing a series of — They've done some recent shows about blockchain, trying to explain to congress or trying to get the upper levels of government to wake sort of like wake up to the blockchain or potentially use it or at least just be aware of it. Do you know kind of the status of is blockchain or, really, anything in this space? Is it starting to permeate areas of government? Are there advocates within government?

[0:29:57.3] LX: Yes, absolutely. I think the conversation has changed dramatically over the past three years that I've been at Coinbase. At the start, there are just a lot of questions, a lot of skepticism about blockchain and why anyone would need it. Now, when we have conversations, there are actually proponents within governments and law enforcement that are like, "Blockchain is really cool, guys. Listen to what these people have to say about it." The conversation has definitely really changed.

[0:30:22.2] JM: Do they have personal interest in it? What gets somebody in government to be a convert to being a fan of blockchain?

[0:30:31.0] LX: I think it's just like how any of us got into it. I think you start reading about it and being like, "Wow! This could change everything." I had a few law enforcement agents that came to me and said they actually use Coinbase as to other Bitcoin on a personal level. It's very cool.

[0:30:47.0] JM: Okay. The third cryptocurrency that Coinbase has decided offer is Litecoin. Litecoin is similar to Bitcoin but has faster transaction times. Why is that important?

[0:31:00.4] JC: Well, the jury is out on whether that's important, but the common sense would dictate that when somebody sends money, they want it to get there as quickly as possible. In that sense, it creates a better user experience. I guess I would say that Litecoin, because it has the faster block time — Litecoin is just a fork of Bitcoin. It's almost under the hood. They're almost exactly identical. You are pointing out one of the main differences, is the faster block

time. The other main difference being the scripts mining algorithm, which is supposedly or attempts to be basic resistant.

On the faster block time, Charlie thought that people get want their money to get there faster — Charlie, the creator of Litecoin. He basically made blocks four times as fast. Also, because it's fork of Bitcoin, it makes the capacity four time as large because the per block limit is the same. It ends up being slightly more capacity with faster throughput which results in a better user experience.

Now, I think one of the other main differences of Litecoin is the founders here and he's unknown person and he actually has a significant sway in the community. Bitcoin suffers from kind of a leaderless, no leader problem. There's plenty of voices in Bitcoin but none of them have control and none of them have enough influence to really swing the conversation. We've been in kind of a gridlock for the past three years and how to scale Bitcoin.

Whereas Litecoin, Charlie called a meeting and all of a sudden everybody's on the same page. We are kind of witnessing the differences in terms of the governance of the two systems. I think it's an interesting story that's going to play out overtime.

[SPONSOR MESSAGE]

[0:33:02.5] JM: VividCortex is the best way to improve your database performance, efficiency, and uptime. It's a cloud-hosted monitoring platform that eliminates your most critical visibility gap, providing insights at 1-second granularity into production database workload and query performance. It measures the execution and resource consumption of every statement and transaction, so you can proactively fix future database issues before they impact customers.

To learn more, visit vividcortex.com/sedaily and find out why companies like Github, DigitalOcean, and Yelp all use VividCortex to see deeper into their database performance. Learn more at vividcortex.com/sedaily, and get started today with VividCortex.

[INTERVIEW CONTINUED]

[0:34:06.0] JM: What are the engineering trade-offs that Charlie made when he said, “I’m going to make it faster.” Clearly, there must be some disadvantage relative to Bitcoin if you increase speed.

[0:34:18.8] JC: Yeah. The trade-offs that Charlie was weighing when he decided to make blocks come four times as fast with four times the capacity is kind of the — It’s a spillover of the Bitcoin block size debate in terms of decentralization. There’s a lot of people in the Bitcoin camp that think that increasing the throughput on chain with the block size increase is actually going to create a lot of centralizing pressure on the miners. It’s going to force miners to join pools to stay up-to-date. It’s going to shut a lot of small players out of the market because they just can’t keep up with the resource requirements of running of a heftier blockchain.

Charlie said, “Well, Bitcoin has already got the kind of decentralization as far as — It’s got way more decentralization than Litecoin. Let’s maybe not have to win on the decentralization. Let’s try to create a better user experience and maybe there will be little more centralization, but that’s okay because people really do care about faster confirmation times and cheaper fees which you get with more capacity.”

[0:35:23.1] JM: Is that what Bitcoin is doing with lightning networks? Like kind of you trade off — Because with lightning networks on Bitcoin, you get some more centralization but you get faster potential transactions, right?

[0:35:37.1] JC: Yeah. Whether you get more centralization or not is kind of up in the air because that really depends on the topology of your connections in your network graph. The idea of lightning is it’s really kind of a genius idea is rather than have every transaction be included on the blockchain proper, why don’t we batch transactions together and only once we really need to, let’s write to the blockchain?

It’s kind of a form of right-caching. When you are writing a lot of data to a spinning disk, you don’t just write it as it comes in. You wait till you have enough to just write it in one burst. This just creates a much better system, a more robust system. In the case of Bitcoin, the core developers really don’t think that Bitcoin can scale on chain, so they want to see layer two solutions of which lightning network is the main one that people are pinning their hopes on.

There's a lot of ways you can setup a lightning network. Lightning network just means that we're not writing everything to the blockchain. We're going to batch updates to the blockchain and serialize them all at once and we're going to save space that way.

The topology of the network is really going to tell us whether this is more or less decentralized. The naïve way to do a lightning network is to have a hub and spoke model. Coinbase maybe would even be a part of the genesis of this where Coinbase would spin up a hub and everybody else would connect to Coinbase and they would open up a payment channel with Coinbase. Then if people want to pay each other, they simply tell Coinbase to debit from their payment channel and credit the other guy's payment channel and this is all done off-chain.

That is obviously a very centralized way to setup a lightning network, but that's not the holy grail. That's not what people really want. What they really want is they want kind of decentralized routing where everybody connects to a dozen other people and through just large numbers, you can find a decentralized route from two points on the network. If I need to pay Linda, I might go to you and you might go to Jeff, and Jeff might go to Mark, and then Mark might go to Linda, and I can pay Linda without directly connected to Linda. That's kind of the real vision of lightning network, but it's still in the really phases of implementation.

Right now, because Charlie is leading Litecoin and because he's able to push for a consensus, Litecoin is actually stepped out front on the Bitcoin roadmap of scaling. The core devs, they've always said, "Let's implement segregated witness," which we can get into if you'd like. Then behind segregated witness, we have all these other improvements to scaling without actually increasing the block size. Signature aggregation is one example of that. Lightning network is the one that most people are very excited about.

Litecoin now is going and they're actually running the test in real life with real value for Bitcoin. Litecoin is kind of stepped out of the shadows of Bitcoin as a Bitcoin fork and kind of taking charge of, "Hey, you guys think this is the way? Well, we're going to trail-blaze and show Bitcoin how this can be done."

A lot of Bitcoin core developers have actually migrated to working on Litecoin because it's just a much more harmonious environment because Charlie leads there to create a community, and it's a smaller community. It's a nice testing grounds for Bitcoin.

[0:39:13.5] JM: The difference there being, I guess, that Litecoin, essentially, you get the best of Bitcoin coin and the best — Well, you get some of the best of Bitcoin and some of the best of Ethereum because you get the unified leadership in Charlie and you get moving faster and you also have, basically, the same fundamental simplicity of Bitcoin. You're not adding in the whole decentralized app ecosystem.

In that world, is there analogous — I guess Bitcoin still has value there just by the nature of its conservatism and its oldness. I guess Bitcoin will continue to have value in that conservative world because a lot of people want that. A lot of people don't want to let's move fast even if it seems objectively good other than the fact that it's not conservative.

[0:40:09.6] JC: Right. Litecoin does have the best of some worlds. I guess where Litecoin is still catching up is infrastructure and user accounts, exchange volume. Kind of some people get really excited about the technology with these digital currencies. Personally, I get much more excited about the money and the transfer of money and wealth and how that's much better facilitated in the new world.

Bitcoin has the biggest market cap. It has the most liquidity currently. Litecoin is playing catch-up quite a bit there. Litecoin is, I think, about a 20th of Bitcoin's market cap, and its exchange volume, some around there as well.

[0:40:52.7] JM: Linda, can you tell me what can people build out of multiple cryptocurrencies? When you have like multiple cryptocurrencies involved, are there some synergies and stuff I can do?

[0:41:05.9] LX: Yeah. Right now, honestly, I don't think there's good enough infrastructure to be building on multiple different cryptocurrencies, but what we are seeing is people building — Needing exchange of the different Ethereum tokens, and so there are some infrastructure behind that that's already existing and I'm actually advising one of those projects. It's called OX.

They envision a world where people are going to be needing to exchange multiple Ethereum tokens as they start using different decentralized applications. Behind the scenes, people would be exchanging that through smart contracts.

I think that as infrastructure gets better for multi-blockchain exchange, I think people will start doing that also. If they want to access a decentralized application on Ethereum but then they later want a privacy coin as they start doing day-to-day transactions, they might switch that. To be honest, the infrastructure just doesn't exist right now, but it will in the future.

[0:41:58.6] JM: Okay. That's an interesting use case, the idea of trading coins. I guess we could imagine that if you could build an Airbnb where people have to pay you in your coin or maybe they can trade you their coin for your coin and you can stay at their place next time you're in their area. That would be an example where you could just trade personal tokens.

[0:42:25.2] LX: Absolutely. Yeah. I personally envision a world where people have hundreds of different tokens but they might not actually realize they have it because it's being stored on maybe an exchange for them or it's just being exchanged in the background.

[0:42:42.3] JM: I want to talk about this article that your CEO; Brian Armstrong, wrote earlier this month. It's just basically about Coinbase's strategy. I'm just curious how I guess each of you see it. The strategy has four steps. The first step of the strategy is to make it easy for consumers to invest in digital currency by building a retail exchange. What is a retail exchange? What will be involved in building that?

[0:43:13.7] LX: Yes. Retail exchange is just, to us, different than institutional investors, so retail would just be people like you and me who want access to digital currencies. Also people like maybe merchants who want to accept Bitcoin or Ether as payments. Whereas the institutional side would be like high-frequency traders. These are the ones that need access to something like what we have GDAX. They're trading on a daily basis whereas fees are really important to them and it's important to have really fast transactions. Whereas like Coinbase, it's just like maybe a regular person and she's going to just buy Bitcoin, store it for weeks and then maybe use it every once in a while to pay merchant. It's not like — We don't see retail investors as like active traders.

[0:43:59.4] JM: The second step of the strategy will be to enable professional traders and institutions to trade digital currency. This means higher volume trading. If you're like — Correct me if I'm wrong, but today, most of Coinbase's consumers are — Most of Coinbase's users are like individuals who just want a place to store their Bitcoin, but you want to go to a place where you've got like professional traders, institutions. It seems like a big change. What will be involved in making that change?

[0:44:30.5] LX: We already have that. T that's our separate product; GDAX. That's where we're trying to split out those platforms and have it be its own brand. Coinbase is that retail person where they're just getting access to digital currencies through their bank account, and then we have the professional traders right now that are on GDAX that are trading Bitcoin and Ether and Litecoin.

[0:44:51.9] JM: What's the life of a professional trader on Bitcoin? What's a professional cryptocurrency trader?

[0:44:59.9] LX: I wouldn't know because I don't day trade well in Coinbase, but it is definitely, from people I've talked to, following a lot of the news that's going on. Cryptocurrency is obviously a really new area. There's a lot of developing going on in the space. Constantly, every signal day I feel like there's new news coming out that affects the price and so people have to be on top of hearing about developments and news going on in the space.

[0:45:22.9] JM: Are there sharding instruments and derivatives and they like backed by a legitimate legalese or is it just like —

[0:45:31.3] LX: Yes. We went through a lot of legal process with our margin trading.

[0:45:35.4] JM: Okay. Coinbase offers. This is in GDAX.

[0:45:38.5] LX: GDAX offers this. Yes. Yeah, separate product.

[0:45:41.3] JM: Okay. Is it separate engineering teams?

[0:45:44.6] LX: Yes, we have a separate engineering team, but some of the code base is still with Coinbase, so we're trying our best to separate that out overtime.

[0:45:54.8] JM: We're you involved in getting these derivatives okayed by regulators or anything?

[0:46:00.3] LX: I wasn't. I later switched over to a different team, but we have a really awesome legal and compliance team who worked on that.

[0:46:08.8] JM: Okay. Interesting. The third step of the strategy, and this is the one that starts to get really exciting is create mass-market consumer interfaces to normalize cryptocurrency usage. When I think about this, I think of like Apple Pay but for cryptocurrencies, like Apple Pay level of convenience, hopefully more market penetration than Apple Pay has today. What does that look like? What would you have to build to get that mass-market consumer interface?

[0:46:38.6] LX: Yeah. We have a version of that right now called Token, and you actually go to the App Store and download it. What that looks like this is just, honestly, like a WeChat, but your payments are in Ethereum so that anyone in the world can actually use it. WeChat for Ethereum is now able to access decentralized applications, and now you can interact directly with them.

We have a product for that already and the problem is trying to get people to build on that right. We recently had a hackathon where we gave out prizes for people who built the best apps for that and it was really cool to see the things coming out of that. We saw something like an app called EarnChinese, where people had to stake some of their Ether on the app and say, "Okay, I'm going to lock up this amount of Ether and if I don't practice each day then I lose some of that Ether. You can come up with all kinds of really interesting applications on top of this. We have all a lot on Token already that you can take a look at.

[0:47:36.0] JM: Okay. Then fourth is the expansion in the number of ideas tried. What kinds of things are going to happen? What are we going to see when the mass-market starts to get involved in cryptocurrencies?

[0:47:50.0] LX: I mean I think you're just going to see Ethereum and other digital currencies disrupt every single industry you can imagine, honestly. I think that there is so many middlemen right now that are just taking fees and all they're really doing is kind of like an if-then condition. They're saying like, "If this event happens, then I'm going to do this."

When you have all these cryptocurrencies being able to take over in that sense, you can cut out a lot of the middlemen. One of the problems that you have is identity and reputation, like how can you trust someone. I think that that problem really needs to be solved first before we see a takeoff of all these different applications. I think that, honestly, every single industry will be disrupted by this.

[0:48:31.6] JM: Okay. I guess just to wrap up, how do you both keep up with this industry, because there's a lot of information to consume? Do you have any tips for keeping up or just — I don't know, strategies?

[0:48:44.8] LX: Yeah. I think Reddit, honestly, is a very good resource. The Ethereum community is really active on Reddit, and so you can just go to our Ethereum and EthTrader trader for people that are more focused on trading. I found all kinds of really interesting things. There's projects talking about their crowd source structures, talking about what they're trying to do. There's people debating whether or not projects even need a token. The whole community pretty much is there.

Then I also go to Slack groups of these projects themselves. There's often hundreds of people in these Slack groups and they're talking about the project themselves, so you can ask questions there.

[0:49:24.9] JC: Reddit. I like RBTC, Bitcoin markets, markets even our Bitcoin on occasion to keep up with the latest Bitcoin news. Although, to be honest, I think a lot of the more interesting stuff happens even in just the lunch halls here at Coinbase and just various conversations with other enthusiasts when we get a chance to talk to them.

Also, I'm a part of the Bitcoin Core Slack. I do sometimes read the Bitcoin Dev mailing list because that's where a lot of the developer dialogue and debate occurs. It's just a good place to keep tabs on the Bitcoin scaling drama. Yeah.

[0:50:00.5] JM: What's the status of that; the scaling drama?

[0:50:04.2] JC: Yeah. Changes every day right now. I think today was what? The 20th, Wednesday. 80% of the hash rate is now signaling for the New York Agreement, which is also known as the Silbert Accord. This guy, he's one of our investors, Barry Silbert. He got together all of his crypto investments and invited the miners and the core he developers, the developers, the client and the client implication.

In New York, a few weeks back, they all kind of sat around the table and agreed to do Segwit first and then two megabyte hard fork. It sounds a lot like the Hong Kong agreement from a year and a half ago. This time it's looking a lot more promising. More than 80% of the hash rate is signaling for it. This is also known as Segwit2x. Segwit2x looks like it's gaining moment. Jeff Garzik is in charge of the BTC1 project which is implementing the Silbert Accord or the New York Agreement, and they have an Alpha released.

The idea is to start signaling and get Segwit activated before August 1st, which is the flag date for the user-activated sort folk. If you've seen any of those camo hats on Twitter with UASF, that's what that is. That's a movement from within the core supporters to say, "To hell with it. We really want to get Segwit activated. The miners are messing this up. Let's activate Segwit with or without their support and hopefully they'll join us. This could have been a very disruptive event, but it looks like sanity will prevail and Segwit2x will get adopted by the miners. We will get Segwit activated in a compatible with the UASF people. Fingers crossed, Bitcoin scaling drama may be paused for a couple of years. We'll actually see if that goes through in the next coming months.

[0:51:59.9JM: Okay. I need to do a show really devoted to that topic. Too many show where I like tangentially talked about segregated witness and the scaling drama and I'm like, "Cool. I'm out of my comfort zone instantly and don't know what I'm talking about."

[0:52:16.0] JC: Happy to do it.

[0:52:17.1] JM: Yeah. Okay, well. Great talking to both of you. Thanks Linda and Jordan.

[0:52:21.2] JC: Thank you.

[0:52:21.6] LX: Thank you.

[0:52:22.2] JM: Okay.

[END OF INTERVIEW]

[0:52:26.1] JM: Artificial intelligence is dramatically evolving the way that our world works, and to make AI easier and faster, we need new kinds of hardware and software, which is why Intel acquired Nervana Systems and its platform for deep learning.

Intel Nervana is hiring engineers to help develop a full stack for AI from chip design to software frameworks. Go to softwareengineeringdaily.com/intel to apply for an opening on the team. To learn more about the company, check out the interviews that I've conducted with its engineers. Those are also available at softwareengineeringdaily.com/intel. Come build the future with Intel Nervana. Go to softwareengineeringdaily.com/intel to apply now.

[END]