**EPISODE 325**

[INTRODUCTION]

**[0:00:00.4] JM:** Cryptocurrencies are not only a financial instrument. They're a new platform for building applications. The blockchain allows for new solutions to digital property management, micropayments, hedge fund incentives, and advertising fraud.

The cryptocurrency platforms with the most traction are Bitcoin and Ethereum. Bitcoin is no central leaders, and it's going through some growing pains with governance issues. Ethereum is led by the charismatic Vitalic Buterin, so there's more momentum when it comes to trying to resolve governance issues.

Bitcoin and Ethereum are not competing instruments. They fulfill different technical purposes. Under current conditions of algorithm development and network infrastructure, neither Bitcoin nor Ethereum can accomplish the dreams that one day will be realized, because of the problems of distributing transaction information across nodes in the system. If we compared cryptocurrencies to the internet, we would not even be in the days of dial-up yet.

Consensus is a venture production studio that is working on several projects within the blockchain space. Mike Golden is a software developer with Consensus and he joins the show to talk about blockchain application today, in 2017, where we are and where we're going? It was a wide range of conversation. I hope to have Mike back in the future so we can go deeper on some of the topics that glossed over, and I think you're going to enjoy it.

[SPONSOR MESSAGE]

**[0:00:00.4] JM:** Spring is a season of growth and change. Have you been thinking you'd be happier at a new job? If you're dreaming about a new job and have been waiting for the right time to make a move, go to hire.com/sedaily today. Hired makes finding work enjoyable. Hired uses an algorithmic job-matching tool in combination with a talent advocate who will walk you through the process of finding a better job.

 

Maybe you want more flexible hours, or more money, or remote work. Maybe you work at Zillow, or Squarespace, or Postmates, or some of the other top technology companies that are desperately looking for engineers on Hired. You and your skills are in high demand. You listen to a software engineering podcast in your spare time, so you're clearly passionate about technology.

Check out hired.com/sedaily to get a special offer for Software Engineering Daily listeners. A $600 signing bonus from Hired when you find that great job that gives you the respect and the salary that you deserve as a talented engineer. I love Hired because it puts you in charge. Go to hired.com/sedaily, and thanks to Hired for being a continued long-running sponsor of Software Engineering Daily.

[INTERVIEW]

**[0:03:07.4] JM:** Mike Golden is a software developer with Consensus. Mike, welcome to Software Engineering Daily.

**[0:03:11.7] MG:** Thank you very much for having me.

**[0:03:13.3] JM:** We've done a bunch of shows on the architecture of Bitcoin, and Ethereum, and other blockchain technologies. We're starting to get into some shows about the applications of cryptocurrencies, and what I mean by that is, as I'm sure you knew all along when you've been working on these things, these cryptocurrencies are not just tokens to be spent and speculated like normal currencies. They're actually entire applications platforms. Explain why Cryptocurrencies are not just a financial tool, but they're actually a primitive to build entire computer systems with.

**[0:03:48.8] MG:** Yeah, definitely. I actually did to get into crypto until I got into Ethereum. I had heard about Bitcoin. I knew what Bitcoin was, but I was just never that interested in it. I had plenty of ways to send money around to my friends. Then, what happened was my crypto story was I was applying for a summer job with the NSA, but I failed my polygraph for reasons we don't need to get into. Then, I was just looking for work, there was this random company called Consensus which happened to a few blocks from my apartment. They were looking for people

to write these things called smart contracts. At that time, there was nobody who really how to do that, so the fact that I was unqualified was okay. They thought that I could learn. I learned about blockchains in the context of Ethereum, which means in the context of decentralized applications.

What was interesting about it to me from the outset was that you could write applications which don't run on servers. You can write applications which nobody owns, or controls. That was very interesting to me at the outset. You could have these unstoppable, uncensorable applications.

The way this works kind of at a very high-level — If you understand Bitcoin to be a ledger which keeps track of accounts and their balances, you can abstract Bitcoin into being a spreadsheet that the miners maintain a state of consensus over the state of that spreadsheet.

What Ethereum is, which is a programmable blockchain, the thing that the miners are maintaining Consensus over, instead of a spreadsheet, it's a virtual computer. We have this thing called the EVM, the Ethereum virtual machine. It's like the JVM, for example, the Java Virtual Machine, just a lot simpler. Just like in Bitcoin, miners keep track of the spreadsheet. In Ethereum, we keep track of this virtual computer and transactions that go into the system, our inputs to programs on the computer.

**[0:05:38.6] JM:** This is a decentralized application platform, and much like the JVM, it's running multiple applications at any given time, except it's a much bigger computer than any single JVM that we would think about.

**[0:05:55.1] MG:** Yeah, arguably — Not even arguably. That's less performant than the JVM. One thing that's still not solved in blockchains is scalability. We have this world computer, but it's single-threated, which eventually we are going to have to solve if blockchains are going to get serious.

**[0:06:12.8] JM:** Now, before we get into that kind of stuff, at a higher level, this idea of the internet as a failed peer-to-peer system, the traditional internet, we discussed this on a show about Urbit a while ago. Basically, the sensation I got from that show was that there are certain traditionalists who have been around a while who, basically, believed that the internet doesn't

live up to its expectations. The original expectations where this is a peer-to-peer system where I transact with you and you transact with me, and we don't have broker our relationship through some centralized agency, like Google, or Amazon Web Services, or Comcast. Is that accurate?

**[0:06:12.8] MG:** You can use the internet as a peer-to-peer system. We've built blockchains on the existing internet. Those are peer-to-peer systems. The underlying infrastructure of the internet, arguably, is fine. Not perfect in terms of being decentralized. Eventually, we want to move towards mesh networking. The internet, its physical infrastructure is kind of okay. The web, however, which is the application that my grandma uses, which everybody uses, the web tends towards centralization in a big way. Everybody knows this. This is not novel to say. It's like Google knows absolutely everything about you, because you touch Google services 100 times a day even without knowing about it. Just by being on a page that servers ads through Google's ad network, Google is learning more about you constantly.

Then, we see things — Last year, in 2016, I think it was in the fall. There were these attacks on the DNS system. DNS is not a commercial system, but it is a centralized system. It's a hierarchical system, which eventually you can get to the top of, they are the root DNS servers, and there were DOS attacks against the DNS servers.

I think we are realizing as the web becomes more critical infrastructure in our daily lives, we are realizing that its centralized tendencies are brittle. If you take down the root node, or the central server, everything breaks, every other edge in that graph becomes useless. Yeah, I think we're just realizing that the centralized tendency is brittle and perhaps not ideal for a system as important as the web.

**[0:08:35.0] JM:** I agree that it would be great to have this decentralized application platform where there are things that do not get brokered by a centralized entity. With Bitcoin, as you said, the blockchain is just used for financial transactions. Even on Bitcoin, we've gotten to a point where the transaction volume that is able to be processed is pretty bottlenecked and this is leading to some problems, leading to some arguments for a fork. As you were saying earlier, on Ethereum, we have similar throughput issues. Why is there a canonical issue of throughput or multithread ability when it comes to these blockchain platforms?

**[0:09:24.1] MG:** Sure. First, I would say that Bitcoin and Ethereum's scaling issues are different. The share some scaling issues, but the one that Bitcoin is hitting right now is not one that Ethereum would hit where it's subject to the same traffic, or transaction volume as Bitcoin.

In Bitcoin, when the system was originally designed, there a one megabyte cap on the total size of transactions which can be validated in a block. These blocks come along every 10 minutes. Every 10 minutes, we have new state that is written to the Bitcoin database essentially. You can think of it as a database. It's a decentralized database.

When the system was designed, there was a one megabyte cap on that. Satoshi Nakamoto disappeared in either 2012, 2013, and there's a huge amount of debate in Bitcoin whether this one megabyte cap is important, whether it matters. There are valid arguments on both sides. Some people say, "We need to keep the block size at one megabyte." Some people say, "We need to increase the block size to 2, or 4, or 8 megabytes, or we need some sort of dynamic block size." There are some people who even say that the block size should be smaller.

Bitcoin's scaling problem, like the present problem that they're facing, which is really bad for the network — I love Bitcoin. I'm an Ethereum developer, but Bitcoin is great. I'm a pretty savvy user of Bitcoin given my day job, but Bitcoin is hard to use, because you can wait hours, even days now for transactions to get verified through the traffic. They have this issue with their block size.

On Ethereum, we have a dynamic block size. Miners can vote on what they want the block — We call it the gas limit, to be. We could have, in theory, higher transaction volume than Bitcoin does. However, we would eventually hit a limit, because there is a requirement in all block chains — There's a requirement in Ethereum — We won't get into the subtle argument of whether transaction ordering is actually necessary in Bitcoin.

In Ethereum, all transactions have to be run in a certain order. Now, the miner, the person who validates the transactions and wins the block, they can decide what order those transactions get run in. As soon as they've won that block and they broadcast it to everyone, all the other miners have to replay those transactions in the exact same order. If they don't do that, they're going to

wind up with a different system state than the original miner and the system goes out of consensus.

Just the fact that all of these transactions need to be run in order after they're mined means that the system is essentially single-threaded. Even we had in the EVM facility for multiple threads, because threads run in non-deterministic ways, two miners could get different outputs.

That is a problem which longer term — There is a roadmap for solving it. It's still all in the theoretical stages, and I would guess that we're years away from a scalable blockchain. What the solution will be is not threading. The solution is going to be something called sharding. We'll have a blockchain that we split into shards. All these shards will still be single-threaded, but there will basically be like a blockchain of blockchains just keeps the shards in sync with one another.

**[0:12:31.8] JM:** The reflex here is to go towards centralization, basically, because — I talked to the Blockstream people about a year ago. I don't remember my conversation super well, although it's a podcast episode. I should probably re-listen to it. If I recall, what they were saying was in order to — Whether or not we're going to keep the Bitcoin block size at one megabyte, you can use these side chains, or lightning networks I think they're called, where you could have people who are validating transactions on the side at a higher rate than the core Bitcoin protocol can do.

Then, maybe you get a bucket of transactions that have all been validated on the side, and they get rubberstamped by somebody like Blockstream, or whoever else is the rubber-stamper of that bucket of transactions which takes up less bandwidth than it would be if everybody just stamping every transaction.

Assuming I'm right about what I just explained, that creates centralization points. Now, it's a more granular subtle amount of centralization certainly than we have on the modern internet today, but it is a tendency towards centralization. You could see the same thing happening Ethereum, where you say, "Okay. We're going to shard this virtual machine into some points of centralization, some points of decentralization. Maybe some of the shards are paid for with anonymous payments, and we have no idea who's supporting the compute them. Nonetheless,

the compute payment is decentralized. You could see some shards that are controlled by Amazon web services, some shards that are controlled by Google, some shards that are controlled by the CIA maybe." Am I portraying the world that we are going towards where it's more of a mix of centralization and decentralization accurately?

**[0:14:26.5] MG:** First of all, the CIA does control all blockchains. Yeah, we already live in that world. That's a joke. They don't, actually. I hope. There were many interesting points that you hit on in your preface to this question. There are five things we could address. One, the tendency towards centralization even in the context of blockchains. Any blockchain engineer will tell you that you can do things more efficiently in terms of throughput in any kind of application using a centralized architecture. Even 10 years from now, I think it's going to be a long time, if ever, before we get to a place where decentralized systems can perform the way that centralized systems can.

The project that I'm working on right now is related to solving various issues in web advertisement technology in a decentralized way. Programmatic advertising is hugely scaled, millions of messages per second, trillions of messages per day. Ethereum would just die if we naively shoved all that on the blockchain.

Bitcoin has this notion of payment channels. In Ethereum, we have a notion of state channels. They're essentially the same — In a way, they're the same thing. The way these work in essence — We have some virtual machine, whether it's the Bitcoin virtual machine or the Ethereum virtual machine. We know the state of that virtual machine on the public network. Say, we have the Bicoin blockchain. We know what the Bitcoin blockchain looks like, because it's public. We can run our own nodes.

If you and I are going to engage in a large in a large number of transactions together, whether at a high volume, or just like a large number over a long period of time. It might make sense if I'm buying coffee from you every day to just put down, say, $100 in escrow on the Bitcoin blockchain and then set up a state channel, or a payment channel between the two of us where I sign messages to you. These are valid Bitcoin or Ethereum transactions. I sign these messages, they have my signature on them. I send them to you. you hold on to these things knowing that you can push the to the blockchain at any time.

At any time, you can take the amount of money which I've signed to you off-chain, out of the escrow that I've put down on chain. At any time, you can do that. You don't have to trust me for the duration of our engagement together.

This allows us, for example, overtime to not pay transaction fees every single time I buy a cup of coffee. On Bitcoin, for example, where transactions fees are getting rather high, like to 10 to 20 cents, and maybe even more than that. If I'm buying a coffee for a buck-50, I don't want to pay the 10 or 20 cent transaction every time. We should just settle. Once I've bought $100 worth of coffee from you, net that out. Pay 10 or 20 cents to net-out that entire $100 thing.

It's useful for saving money on network fees. In the context of you needing to do things with extremely high throughput, in any application, whether adTech or high frequency trading, people need to be exchanging messages at much faster than a 15-second block interval. The same thing applies. We sign messages back and forth to one another. Either one of us knows that we can go to chain at any time, and we don't really need to trust one another.

As soon as either of us misbehaves, either refuses to send a message back, or sends a message back which his malformed in some way, the other can go to chain. There are a lot of different ways you can influence this. In Bitcoin, there's the lightning network, and then there are also other federated side chain proposals. In Ethereum, we have a network called Raiden, which isn't out yet, but it's basically a lightning network for exchanging tokens.

Then, there are generalized state channels that you can write. I'm working at some state channel stuff right now. We're still waiting for the super generic API that you can just be like, "Hey, turn my application to a state channel." That doesn't quite exist yet. You have to kind of design your application such that they can be channelized.

This is technology that works today. It's early technology, but at least in Ethereum world. In Bitcoin, they're waiting for SegWit to do certain types of state channels. In Ethereum world, we're not waiting for anything. We can do state channels today. I feel like I took that question — I don't know. I feel I rambled a bit on that question.

 

[SPONSOR MESSAGE]

**[0:18:41.3] JM:** Software engineers know that saving time means saving money. Save time on your accounting solution. Use FreshBooks Cloud Accounting Software. FreshBooks makes easy accounting software with a friendly UI that transforms how entrepreneurs and small business owners deal with a day-to-day paperwork. Get ready for the simplest way to be more productive and organized. Most importantly, get paid quickly.

FreshBooks is not only easy to use, it's also packed full of powerful features. From the visually appealing dashboard, you can see outstanding revenue, spending, reports, a notification center, and action items at a glance. Create and send invoices in less than 30 seconds. Set up online payments with just a couple of clicks. Your clients can pay by credit card straight from their invoice. If you send an invoice, you can see when the client has received and opened that invoice.

FreshBooks is also known for award-winning customer service and a real live person usually answers the phone in three rings or less. FreshBooks is offering a 30-day unrestricted free trial to Software Engineering Daily listeners. To claim it, just go to freshbooks.com/sed and enter Software Engineering Daily in the How Did You Hear About Us section. Again, that's freshbooks.com/sed.

Thanks to FreshBooks for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

**[0:20:22.4] JM:** No. That's fine. I think I threw a lot at you in you did a good job of fielding as many questions as you could. Bitcoin versus Ethereum is not a question of like which is better, but a question of where are the synergies. How did the organizational structures compare? One interesting observation I always like to engage with people about is the fact that Ethereum has a leader in Vitalic Buterin. He's a kind of strange unconventional leader who has some really hilarious tweets. Bitcoin does not have a clear leader today. What are the pros and cons of these governance strategies, or governance states?

**[0:21:04.9] MG:** Yeah, okay. Like I said at the beginning, I love Bitcoin. Bitcoin is the mother of all blockchains. Every blockchain descends from Bitcoin. I never want to seem as though I'm speaking ill of Bitcoin. Bitcoin is in a tough spot with their governance, because they're running up against this very practical and very real issue of the network being congested and transaction fees going way up.

Kind of the dream of Bitcoin enabling micropayments at this time is on hold. It's possible that in the future they'll implement SegWit and side chains and lightning networks going, but we don't know. The community is split. There is the Bitcoin unlimited crowd, and there's the Bitcoin core crowd. There are some large mining pool, I forgot which one, which is now mining Bitcoin unlimited blocks.

It actually seems possible that Bitcoin could fork, which, for me, as an Ethereum developer, doesn't bother me that much. I think forks are okay. For a lot of Bitcoin people, a fork would be a disaster. A fork, meaning that there's one version of reality, essentially, which believes the network works one way and a separate version of reality, which believes the network works a different way, and they go out of consensus with one another. They're in a tough spot. It's very toxic, politically. I think even a Bitcoiner would tell you that their politics are toxic.

What's interesting about developing for blockchains, is because these are serverless applications, you don't own the server yourself. You can't just choose to upgrade it unilaterally. You have to get consensus from the community, and particularly the people who are mining the blockchain if you want to make upgrades to the system. Development does have a political element. The other thing about Bitcoin is Satoshi Nakamoto disappeared in 2013. They did have a leader once upon a time.

**[0:22:53.0] JM:** If he was ever a singular human being at all.

**[0:22:55.2] MG:** Yeah, it may have been a group. Yeah. But that voice disappeared. We have Vitalic Buterin who's an awesome, awesome human being. Not only is he super smart. We're just very lucky that he is a good, likable, and reasonable person that he is. Vitalic doesn't get mad. He stays calm in all situations.

**[0:23:17.1] JM:** Clearly, not motivated by money.

**[0:23:19.0] MG:** Yeah. No, not at all.

**[0:23:22.8] JM:** Other than as an intellectual pursuit.

**[0:23:25.0] MG:** Yeah. Yeah, definitely. Vitalic is not — This is not a get-rich-quick scheme for Vitalic.

**[0:23:30.0] JM:** In fact, he probably has the most abstract view of what money even is. Probably more abstract than probably anybody else on the planet.

**[0:23:38.9] MG:** If there's anyone who understands what happiness is, I have to think it's Vitalic, because he knows it's not money. We have Vitalic. We also have a guy named Vlad Zamfir, who's a super bright researcher. I consider him a leader anyway. We have this organization called the Ethereum Foundation, which provides direction for the ecosystem.

Now, if you're a hardcore crypto-anarchist, you may not be into this idea. For my part, and I think for the part of a lot of Ethereum enthusiasts, we knew when Ethereum launched in July of 2015, that the Ethereum we have is not the Ethereum that we want. Like I said, all of this is, it's kind of fun, but it won't really matter if we don't eventually get blockchains, which are both scalable and safe, and I would say that proof of work is not sufficiently safe consensus mechanism for truly global and systemically important blockchain. We know in Ethereum world that the Ethereum that we have is not the Ethereum that we want, and we knew this from the outset.

I think our community has a different mindset in that way. We've always known that we're going to have to do a bunch of hard forks to get where we want to go. One worry that I have right now is that the price of Ether has gone up recently, and as more people become attracted to this ecosystem, as the ecosystem becomes more systemically important in its current state, I worry that it's going to be harder to make the breaking changes that we need to make for Ethereum to be important in the long-term.

If you have a $1 billion blockchain, yes, that is a lot of money, but you can play with it more than if you have a $20 billion blockchain. Say, people get more skidding when that much money is locked up inside. I think we'll be able to push through it. Our community is great right now. We have a really, really great community. Our community is going to get a lot bigger as Ethereum continuous to grow, and I hope that we're able to continue to be brave and make the breaking changes that we need to make.

**[0:25:37.5] JM:** I would draw a comparison between the governance of the cryptocurrency world and the governance of our current American democracy, where — There are a number of comparisons to be drawn. You look at Trump, and he's arguably hard-forking the government. He's saying, "Look. We've been doing this certain consensus-driven long lead time to some bureaucratic motion system of government for a long time, and I'm hard-forking it. I'm going to just throw out executive orders. I'm going to throw out my own version of the truth on Twitter in an atomic, 140-character bombshell, and the establishment sits by in horror.

I sit by in horror sometimes. Certainly, this is not an excuse of Trump, but it is a — I'm curious about how it's going to turn out too, because if we survive it, if everything is fine, then it's like, "How will I stop worrying and learn to love the hard fork?" Whether we're talking about government, or Ethereum blockchains, or anything. Maybe it turns out we're just more resilient to extreme change than we thought. If we are, then I think it's a good judgment on how dynamic our U.S. government could be, and how dynamic our blockchains could be.

**[0:27:07.2] MG:** Yeah, I understand the point you're making. I would say it is important to note that Vitalic and the Ethereum Foundation are much less powerful relative to the Ethereum community even, than the U.S. government is relative to the population. The reason is we have this dynamic with the miners who — Vitalic has zero executive power. Zero. Trump has executive power, which he can exercise and, ultimately, he controls the intelligence agencies, and the military and all of that. Vitalic has zero executive power. The miners are the executives. Vitalic always has to convince the miners and convince the community that what he proposes are good ideas.

Vitalic advocated for the Dow hard fork, but the Dow hard fork was a hard fought political process, and emotionally draining for everybody in the community. This notion that the

foundation forced a hard fork on the community is completely false. It was a hard thought political process. One in which, which was like kind of beautiful in the end, because you had people who had long and serious conversations, and by the end of it, would change their minds.

People were willing to listen to the other side and change their minds as they came to new understandings of the facts. That kind of thing I think is going to be harder in the future, just because our community, like I said, is getting bigger. Yeah, I would make the important distinction that Vitalic and the foundation have zero executive power. Ethereum is not at all centralized in that way.

**[0:28:44.9] JM:** You are working on adChain right now. We had a show recently about adChain. You're working for Consensus, and Consensus is working on adChain, I guess I should say. Consensus is this venture studio. Maybe we'll talk about Consensus a little bit later, but let's talk about adChain, because we did a show about it recently. The motivation for adChain is to have a shared ledger for advertising transactions.

For people who are unfamiliar with this problem, it's basically because when somebody gets shown an ad on the internet, often times, that display of advertisement has been brokered through a number of exchanges based on information that is shared among different people, and there's a question over, sometimes, "Okay. What price was this paid for at time-X? Was this actually shown to a human being? Was it shown to a bot?"

Having a shared system of record where the different participants in the advertising auction ecosystem, which by the way, powers the internet, there's a question as to the validity of these transactions, and can we come to a conclusion about fair market value of advertising on the internet, which by the way, powers how humanity thinks. It's an important problem.

Correct me if I'm wrong about anything, and tell me what is motivating to you about adChain, and what are you working on within the project right now?

**[0:30:10.6] MG:** Yeah, sure. I can talk a little bit about adChain. I can't tell you everything. We're going to have a big public announcement, I think, the end of this month, or maybe the beginning of April. What I do on adChain is I am — Consensus is working with a company called MetaX

out here in Los Angeles. MetaX is a web advertising company. They work on the supply side. You embed one of their video players in your webpage and they serve videos for you and you get paid.

They realized — Independently. We had never met them. They realized like a year, a year and a half go, that they could solve a bunch of outstanding problems in the adTech ecosystem using something like a blockchain. They just realized this independently. We got hooked up with them through a mutual friend at Microsoft. We were very intrigued that this was an area where blockchains had applicability, which we hadn't thought about. Consensus is a pretty sprawling company, and we like to think that we touch everything.

What I'm doing on this project is I am — Consensus is like embedded engineer kind of. I work with the VidRoll engineers and with VidRoll's CTO. Right now, we've designing what the system is going to look like and prototyping use cases and applications for the system. What we're really looking to solve, at least with this first iteration of the system that we're going to come out with, is fraud in adTech.

Programmatic web advertising is like a $200 billion a year industry, approximately. The IAB, the something Advertising Bureau. I forgot what that actually stands for. They're a major industry —

**[0:31:44.7] JM:** Interactive. I believe it's interactive.

**[0:31:46.0] MG:** The Interactive Advertising Bureau, yeah. Their own estimate for the amount of fraud in $200 billion industry is that it's at $10 billion, and this is the conservative estimate, very conservative estimate from the industry zone advocacy group.

If you ask operators in the space in practice what they think the percent of fraud actually is, you will hear numbers between 10% and 50%. The way we see it, it's like a $20 billion bounty, essentially, on figuring out how to mitigate fraud in the programmatic advertising industry. AdChain is focused on solving that; creating more transparent supply chains such that advertisers, for example, can be sure that its real humans who are viewing their ads and publishers can be sure inversely that ads which they are serving, one; they're not malware,

which happens in adTech. Two; that they'll actually be paid for them, because there are all sorts of cases where publishers who are doing all the right things don't get paid when they should.

One interesting thing which I've learned about since beginning to work on this project in regards to dis-intermediating all the middlemen in adTech, there is a technology called — It's referred to as header bidding. The way ad exchanging works is user loads page — Say, it's a video player. The video player itself is going to send out a bid request to an ad exchange. The ad exchange will collect bids from the demand side and then choose one of those bids and send that back to the player.

There's an existing technology which is nothing to do with blockchains, but which his really cool, called header bidding, which dis-intermediates the exchange. It allows the video player to send bid requests directly to demand. Demand sends bids back to the video player, and then the video player just selects the bid that it wants. This is super cool.

A problem with header bidding or one barrier to adoption that they've had is that one utility of an exchange is that in theory, at least, they vet the participants. Your exchange makes kind of a weak promise that if you're an advertiser, your ads aren't going to get served to bots, and if you're a publisher, you are not going to end up serving ads that contain malware, or maybe containing inappropriate content, or whatever.

These promises windup being really, really weak, because exchanges make deals with ad networks and those are arbitrarily deep trees, so they're not really auditing every member of the exchange. Anyway, this is in theory a utility that exchanges provide.

When we release our whitepaper, you can read about this. One interesting thing we've done is come up with a means for supply and demand to identity one another in a decentralized way without having to pay anybody for that privilege and conduct header bidding peer-to-peer. There's just no longer any need at all for an exchange, because we solved the identity and discovery problem, and we give it away for free, because we can do that on a blockchain.

Yeah, we're going to have a whitepaper coming out either at the end of this month, or the beginning of April, which will describe the system more in-depth.

[SPONSOR MESSAGE]

**[0:34:56.7] JM:** At Software Engineering Daily, we need to keep our metrics reliable. If a botnet started listening to all of our episodes and we had nothing to stop it, our statistics would be corrupted. We would have no way to know whether a listen came from a bot, or from a real user. That's why we use Encapsula to stop attackers and improve performance.

When a listener makes a request to play an episode of Software Engineering Daily, Encapsula checks that request before it reaches our servers and filters bot traffic preventing it from ever reaching us. Botnets and DDoS are not just a threat to podcasts. They can impact your application too. Encapsula can protect your API servers and your microservices from responding to unwanted requests.

To try Encapsula for yourself, got o encapsula.comsedaily and get a month of Encapsula for free. Encapsula's API gives you control over the security and performance of your application. Whether you have a complex microservices architecture, or a WordPress site, like Software Engineering Daily.

Encapsula has a global network of over 30 data centers that optimize routing and cacher content. The same network of data centers that is filtering your content for attackers is operating as a CDN and speeding up your application.

To try Encapsula today, go to encapsula.com/sedaily and check it out. Thanks again Encapsula.

[INTERVIEW CONTINUED]

**[0:36:41.5] JM:** Okay, so let me give you some counter arguments to why I think adChain has maybe some conceptual work to do, or maybe I just don't understand it properly. Google and Facebook control advertising on the internet. Neither of them are really willing to talk about ad fraud. I know this because I've repeatedly tried to get people from those companies on the show to discuss online advertising and online advertising problems. They don't really seem to care. The executives don't really care.

Furthermore, the only people who would have a vested interest in solving ad fraud are basically the brand — The people who'd have the most interest in solving this would be the brand advertisers, or basically people who are spraying and praying with their advertising budgets where you have — Brand advertisers like — I hesitate to name names, but I'll name names anyway, like Coca-Cola, or McDonalds, or Procter & Gamble, or Ford, these companies that probably don't have a great understanding of how much of their advertising budget is going to bots and bot fraud. By the way, nobody knows. There's no convincing audit that I have come across.

I've talked to, basically, the most scientific auditors, or most of them. If there are more, I'd love to have you on the show. If you're an expert in this and you're listening to this episode. Nobody can audit this. The Procter & Gambles, and Fords, and McDonalds of the world don't really care about this, because they don't know about it, and because their advertising budgets are controlled by people who would rather just sign the check and get on with their day, then tackle what advertising fraud is.

Then, you have these solutions that come out that sort of try to thread a little bit of the needle for publishers, for example. If you're a publisher, you want to be able to tell your advertisers, or your advertising networks that, "Yeah, we filter some of the bad traffic." You get one of these little JavaScript tags on your page that supposedly filters a lot of the bad traffic. Except, there's actually plenty of markets that will give you fake bot traffic that can make it past these little things. This is something I really don't want to name any names on, because I've had one or two of these companies on the show to discuss, "Yeah, how do you block bot traffic?" They're like, "Oh! We do this thing with machine learning." I'm like, "Okay. How does it work?" They're like, "Well, it works this way." I'm like, "Okay. That doesn't work. Why are you selling these to people?" They're like, "No, but it works, and it doesn't work."

**[0:39:11.3] MG:** It's interesting. These are safety vendors is what you're referring to in the existing web ad ecosystem. What's kind of interesting about the incentives of safety vendors is that they depend on the continued existence of fraud for their business to exist. In a sense, they're only incentivized to mitigate fraud to the extent that their competitors are, and it becomes a slow race to the bottom.

A lot of safety vendors — I think most safety vendors, think it's like standard practice, I believe. I hope I'm not misspeaking. I've been told. They do get paid on a CPM basis. If there's 10,000 impressions and they identify 9,000 of them as fraud, they're only getting paid for a thousand impressions. Safety vendors have kind of like weird incentives in the system, and I think for that reason, kind of a fundamentally imperfect solution. They're a band-aid.

**[0:40:02.6] JM:** I completely agree. Where I'm going with this is what will keep adChain from being yet another safety vendor band-aid that a publisher can slap on their website and say, "Hey, we're adChain-protected," when in fact, unless you get buy-in from Google and Facebook, it doesn't really matter how many layers of safety vending you have on your website. You're still going to be obfuscated from the truth according to Google and Facebook.

**[0:40:29.0] MG:** There's going to be multiple stages to adChain. What we launched with this is not what we eventually want to be doing. At time zero, when the system launches. In the current game, if you think of this in the context of very basic game theory; in the current game of web advertising technology, fraudsters can win, and honest actors can lose. These are both possible outcomes in the game.

What we're doing with adChain in the initial iteration is we are providing cryptographically provable guarantees of remuneration in instances of fraud. What this essentially amounts to is an insurance pool for the advertising industry. It depends. You may end up paying some small premium for the guarantee that if you get hit by some significant fraud event, you can get paid back for that. You can see on yourself of the funds to do so are locked up on the block chain.

The way that changes the game is that fraudsters, because to participate in adChain, they will have to be putting up some money upfront. They can't win as much. Publishers who are the people who end up not getting paid in the industry, they will not lose as much. We improve the dynamics of the game a little bit.

Longer term — This isn't even probably medium-term, not even long-term. What we want to do is allow all actors in the system to rationally assess what their risk is by participating in a given,

what we call an ad market. There will be multiple ad market in the adChain ecosystem and it's open, anyone can create an ad market. It's totally a free market.

Ad markets essentially set rules by which publishers and advertisers have to play to exchange ads with one another. One rule set that an ad market may propose, for example, is that every participant in the system has to use the same bot detection technology. It's like an open source JavaScript thing that runs in all the web ads.

If you are a publisher — This is an open source program. You can vet it yourself. You say, "Okay. This thing says that I'm serving bot traffic 20% of the time when I know, because I'm me, and I trust myself, 5% of my traffic is bots." You can know that apparently and then adjust the prices that you charge for your impressions on that basis. Similarly, or the other side of that coin is we can enforce in an ad market, or an ad market can enforce that demand advertisers have to pay. They may have to lock up funds. They have to pay for impressions which are cleared as payable by this open source JavaScript bot detection engine.

In the happy path, that all works. Publishers are rationally pricing their impressions on the basis of how many payments they expect not to receive based on how this JavaScript engine performs, and advertisers are not paying for bot traffic. If they believe in this open source JavaScript engine, they feel good about that.

Of course, we always believe that things will grow wrong. There will be some new bot that comes out, which evades detection before the engine is patched. In that case, whoever side of the engagement got the short end of the stick due to this fraud, the can make a claim with their ad market. We have all sorts of stuff, which the whitepaper describes, which enforces logging for impressions events. They can provide their logs to their ad market, their ad market can make a decision as to whether or not fraud occurred. If so, they can pay these people out of this collateral pool. That's phase two.

Longer term, we'll have things like uPort identities where that's when fraud just totally goes away, because we'll have these on-chain reputation systems like very strong KYC, that just exists in the fabric of the Internet.

**[0:44:30.5] JM:** Now, I respect that road map. It makes sense, if you can get an open source bot detection system that actually works. My criticism —

**[0:44:42.0] MG:** Yes. I'll make the point just real quick.

**[0:44:44.1] JM:** Okay. Sure. Yeah.

**[0:44:44.4] MG:** This open source bot section system that I talked about, not something that the adChain protocol cares about. Like I said, ad markets, it's an open competitive market. We hope that someone would come up with something cool like that.

**[0:44:55.0 ] JM:** I understand, but you would need it though, right?

**[0:44:58.1] MG:** Not necessarily. I think there're all sorts of improvements that ad markets can make short of that.

**[0:45:04.7] JM:** Fundamentally, the biggest problem is the bots.

**[0:45:07.9] MG:** Yeah, for sure. That's the biggest issue in that aspect.

**[0:45:10.4] JM:** If you can't detect the bot, then you can only really make incremental improvements on the ecosystem. Maybe you could do some stuff around auctions, or that stuff. Mostly, the fraud is based on can you detect if this user is a bot or not. Is that right?

**[0:45:29.6] MG:** Yes. Essentially, yes.

**[0:45:31.1] JM:** Okay. The thing I think that is going to be a shortcoming is that, ultimately, the way that a human operates — The way that something that is close enough to the average human operates a computer browser like going to Facebook, making a Facebook account, going to Twitter, making a Twitter account, going to Gmail, making a Gmail account, going through the Internet, clicking on tweets like, "Oh, Donald Trump tweet. I'm going to tweet on that. I'll click on that, respond to it maybe."

It's systematic enough that it's just a touring test that you cannot solve. You cannot make a bot detection system that is going to be good enough unless, basically — Back to our centralization versus decentralization question. Unless you are Google and Facebook, and you can develop a really, really rich identity system, or maybe that's that version three of the road map that you were talking about, this KYC thing. Then, you have a decentralization of your privacy or your identity or whatever.

You kind of need this homomorphic encryption thing where some broker out there is collecting your private information, because the private information is what's, I think, is the unique hashed stamp of are you a bot or not. I think the public information is replicable enough to be always subject to a replay attack. Maybe I'm wrong, maybe I'm mistaken.

One way or another, if you're somebody out there who actually cares about stopping bot traffic from stopping advertising fraud — By the way, I think what adChain is doing is noble. It's a great business idea, a great long-term, long lead time business idea. I think it'll be very profitable for the people working on it, but if you're actually interested in the noble pursuit, and I do think it is noble, of stopping advertising fraud or at least minimizing it.

I think you have to speak out really loudly and get people at Google and Facebook to notice. For the conceivable future, these are the brokers of whether advertising fraud is stoppable or not, and they are doing nothing.

**[0:47:40.0] MG:** Yeah. A few things. One, I'll say, in regard to the detection of bots and our ability to detect them. I definitely agree that it's a hard problem certainly not a solved problem, but bot systems do get detected not always expediently. You may have heard about Methbot a few months ago, is this bot farm that was pulling in $5 million a day in elicit revenue. Methbot eventually was detected. I think it was White Ops who came out with that report.

In a system like adChain, which has cryptographically-guaranteed remunerations in instances of fraud, this would allow people who were hit by Methbot to recoup at least some of their loses, which I think would be cool. Then, in regards to needing to bring Facebook and Google aboard.

One thing that's interesting in using blockchains in ad tech — What is the reason that Google and Facebook control 85% or 90%, whatever it is of web advertising revenue? A big part of it is because they have control over their entire web advertising staff. They don't have this complex and opaque supply chains. It's like there's the advertiser, and then it's Google all the way down. Because of that, they are able to make much stronger assurances that they're not serving ads to bots or whatever.

**[0:49:00.5] JM:** For sure.

**[0:49:01.4] MG:** Yeah. When you bring a block chain into play, when you have this single shared database that multiple parties can interact with, as though it were, it's logically a centralized database even though, in fact, it's a decentralized database. When you can bring it together multiple parties and have them all play by the same rules and see into that supply chain transparently, I believe we can empower them to essentially have the same super powers, if you will, that Facebook and Google have in having these full stack monolithic integrated supply chains.

I agree here, centralization is efficient. It works. Facebook and Google are able to root out fraud in their ecosystem, because they control their whole stacks. You sell your soul to them and you also pay them a premium in exchange for that privilege. Bringing programmable blockchains into play, I think we can give this away essentially for free. We can make it a public utility. Let everybody have control of a logically monolithic advertising stack the same way that Facebook and Google do, but nobody is going to extract a rent from you for that.

**[0:50:06.6] JM:** The thing is the reason Google and Facebook can build these monolithic advertising stacks is because they have an incentive structure in place where they say, "Okay, we're going to collect tons and tons of information about you, but we're going to keep it under top secret like confidential encryption and whatnot, because that is what our business rests upon." If the information about you leaks, that's really horrible for our core business. Then, people are going to stop giving us identifying information. Whereas if you're talking about a decentralized identity format, what is that incentive of the decentralized database to keep that private?

**[0:50:49.4] MG:** This is important to know. The adChain project is going to be run by an organization called the adChain Foundation, which will be a not-for-profit. The adChain Foundation will have some operating costs, but this is not a for-profit entity.

Presently in the web advertising ecosystem, the collection of personally identifying information is perhaps the only thing in the ecosystem that is at all regulated compliance with these PII laws is scattered and not really enforced. At present, the adChain protocols don't describe anything in regards to dealing with personally identifying information. That gets pushed down to the ad market level, and they will need to follow regulations on that right now.

What the adChain protocols are concerned with are allowing demand and supply to exchange with one another in a peer-to-peer way and in a way that they can trust one another. The problem with these peer-to-peer transactions right now is you don't know who you're dealing with. We want to provide strong guarantees that if you are a victim of fraud, that's not going to be a huge hit to your business. Presently, we may in the future, but at present, we're not actually dealing with the issues of user data and personally identifying information.

We would love it if people built businesses and built services on the adChain protocols that handled information in useful ways, but it's not something that the protocol themselves express an opinion on.

**[0:52:12.6] JM:** Do you think that a publicly funded foundation, the adChain Foundation — Do you think that they can secure data and have the right granularity of exposure of personal data versus keeping the right amount of it private that a Facebook or a Google has the resources to do?

**[0:52:37.1] MG:** All the adChain Foundation is concerned with essentially is keeping these collateral pools locked up. What the adChain Foundation does, what it concerns itself with, is making sure that what we call — In the system, they're called registrars. They sit below the adChain Foundation and above the ad markets. They need to make sure that the registrars are properly collateralizing their pools on the basis of the total balance of disputable payments in their subtree in the system. That's the adChain Foundation's concern.

If those collateral pools are not properly funded, setting flags in that subtree of the system, saying that, “Okay, if you do business in this subtree, all bets are off. The protocols are not going to guarantee that you can be paid out if you’re a victim of fraud.” The adChain Foundation is providing that signal, is what it’s doing. At least at times, what the future holds. Who knows?

**[0:53:30.1] JM:** Yeah. I like the idea of that chain. I’m going to be very interested to see how it plays out. I like the idea of the status quo of online advertising, which is not very old, by the way. I’m sure this will be “disrupted”. I’m sure the incumbents will be assailed over the coming years. I’m sure that Procter & Gamble, and Ford, and American Express will all wake up to this at some point.

**[0:53:59.4] MG:** Advertising is advertising, but also, advertising is media, and advertising is culture. It’s a part of the reality that we experience. I don’t want to live in a world where Facebook and Google control all of the advertising that I see.

**[0:54:15.0] JM:** Yeah. I’ve done a bunch of shows, and the reason I keep reporting out is because it upfronts me in so many ways. Intellectually, it’s an upfront, because I’m like, “Okay. Google and Facebook, these companies that are technology companies.” I’m like, “Actually, a lot of their money is just made off of ads that are being served to bots,” and I don’t know how much, so I can’t totally pass judgment on them, but they’re certainly not disclosing how much.

It’s also an upfront, because the advertising content, most of it is just awful, and I’m like, “Why am I seeing this garbage all over the internet? Why is it 2017 and half of the images that I see on a page are just garbage, and they’re forgettable, and I don’t even — My mind doesn’t even process them.”

I have to imagine, a lot of other people are like that. Then, there’s the third problem. Some people call this the fake news problem, or whatever. I’ll just call it the horrible link-baby and sometimes hoxy-content across the internet that is driven by this botnets and by this advertising flow that’s hard to control and hard to regulate. That’s why you see 10 ways that acai berry will clear up your acne on a random webpage on the internet.

It's just personally upfronts me in so many ways that I'm just like, "I'm so done with this advertising problems. I just want it to go away and be fixed."

**[0:55:37.1] MG:** What we fundamentally want to do is empower the remaining 15% of the industry that isn't under the thumb of Facebook and Google. We want to empower them to compete the way that Facebook and Google do. Then, make sure that as advancements happen in web advertising, they happen publicly, and open-source, and outside of the Google and Facebook stack.

**[0:56:00.0] JM:** This duopoly, the Facebook-Google duopoly it's not going to last. There is no way it's going to last, because there are enough engineers in the world who just don't really like this state of affairs. I think, probably, even people within Facebook and Google, maybe even Mark Zuckerberg and Larry Page and are like, "We don't want this duopoly." Maybe it's people at Amazon, or whatever. It doesn't feel right. It doesn't feel productive, and I think there are going to be more flowers blooming in the near future. At least, I'm optimistic. Are you optimistic?

**[0:56:32.4] MG:** We're getting this garden ready, and hopefully a lot of web advertising flowers bloom in it.

**[0:56:37.4] JM:** Yeah. Okay, there's a ton of stuff we didn't get to. I had two pages of questions and I asked barely any of them. Mike, thanks for coming on the show. It's been really great talking to you. I really enjoyed this conversation.

**[0:56:47.2] MG:** Yeah, sure thing. Thanks for having me on.

[END OF INTERVIEW]

**[0:56:53.2] JM:** Thanks to Symphono for sponsoring Software Engineering Daily. Symphono is a custom engineering shop where senior engineers tackle big tech challenges while learning from each other. Check it out at symphono.com/sedaily. Thanks again Symphono.

[END]