

Demetri Kofinas: 00:00:00 Today's episode of Hidden Forces is made possible by listeners like you. For more information about this week's episode or for easy access to related programming, visit our website at hiddenforces.io, and subscribe to our free email list. If you listen to this show on your Apple Podcast app, remember you can give us a review, each review helps more people find the show and join our amazing community. And with that, please enjoy this week's episode.

Demetri Kofinas: 00:00:48 What's up, everybody? My guest on this episode of Hidden Forces is Muneeb Ali. Dr. Ali is the co-founder of Blockstack, a full stack, decentralized computing platform and application ecosystem that puts users in control of their identity and data. We recorded this conversation on Sunday morning, July 19th, four days after Twitter social media platform was compromised in what could have become one of the most catastrophic attacks in US history. I say could have, because the attackers didn't just compromise the individual accounts of people like candidate Joe Biden, former President Barack Obama, and CEO Elon Musk, but they actually hacked into the network itself and were able to take full control of almost any account on the platform, which means that they could have theoretically used any one of those accounts to broadcast anything.

Demetri Kofinas: 00:01:48 What they ended up doing with this godlike access was to broadcast a juvenile scam that brought in only about a \$100,000 in Bitcoin from roughly 300 accounts. Now, this raises a lot of questions, primarily "why would an attacker go to such lengths to gain access to the accounts of the world's most powerful people and all of their private data only to conduct a six-figure scam?" It just doesn't make sense, and it doesn't have to.

Demetri Kofinas: 00:02:23 We can still draw conclusions and learn lessons from this attack even before all the details have emerged. And this is exactly what today's conversation is all about. Dr. Ali, after all is in the trust business and at its heart this attack is a result of our willingness to trust companies like Twitter with immense amounts of power, not just over our data but over our very identities.

Demetri Kofinas: 00:02:49 Imagine if these attackers had managed to commandeer the account of the president of the United States, who has used his account to threaten nuclear war with North Korea, punished China with new tariffs and barriers, and announced the assassination of an Iranian general.

Demetri Kofinas: 00:03:05 Imagine what they could have accomplished with that level of access had they chosen to use it. And now, imagine if these attackers had compromised multiple platforms and systems and used each and every one of them in a coordinated attack against the United States. And you begin to appreciate the scope and scale of the security challenge that confronts us today.

Demetri Kofinas: 00:03:30 This is not the first episode that we've devoted to the subject of cybersecurity, and I encourage anyone who is new to the podcast to check out our past coverage. Most notably episode 60 with Bruce Schneier, and episode 8 with Josh Corman, both dealing with the subject of cybersecurity and terrorism.

Demetri Kofinas: 00:03:50 In this conversation, we spend the first half dealing with the Twitter hack itself and the rest of the episode including the overtime on Blockstack, and how systems like it are part of the solution. As a reminder, and for those who are new to the program, Hidden Forces is listener supported. We don't take

commercial sponsors and I don't interrupt the podcast with advertisements or product pitches.

- Demetri Kofinas:** 00:04:15 The entire show is funded from top to bottom by listeners like you. If you're interested in supporting the program, which also gives you access to the episode overtimes, including the rest of my conversation with Dr. Ali, the transcripts and the show rundowns, which are elaborate show documents full of images and graphics relevant to the topics we cover each week, head over to patreon.com/hiddenforces and subscribe to one of our three content tiers. There's also a scholar tier for those who are interested in spending time with me each month, reviewing content from the show or just about anything else you want to discuss.
- Demetri Kofinas:** 00:04:55 There's a limit of five per month and there are still two spots remaining for the month of July. Remember, if you like the podcast, if you're a regular listener or if even just one of our episodes inspired you to learn more or fed your curiosity about any one of the innumerable topics we've covered over the last three years, there are many things that you can do to support the show, including rating us on every single podcast platform you can find and subscribing to our mailing list at hiddenforces.io/subscribe.
- Demetri Kofinas:** 00:05:31 And with that, please enjoy this timely episode with my guest, Dr. Muneeb Ali. Dr. Muneeb Ali, welcome to Hidden Forces.
- Muneeb Ali:** 00:05:46 Thanks for having me.
- Demetri Kofinas:** 00:05:48 Congratulations.
- Muneeb Ali:** 00:05:50 Thank you.
- Demetri Kofinas:** 00:05:50 Do you know why I'm congratulating you?
- Muneeb Ali:** 00:05:52 I have a hunch that it might be related to the recent Twitter hack.
- Demetri Kofinas:** 00:05:56 Yeah. You just got your account back. So, you literally got it, what back like 10 minutes ago?
- Muneeb Ali:** 00:06:00 Yes, 10 minutes ago. And I think basically what happened was I think my account was also compromised during the hack and I actually saw that happen in real-time because when I was seeing other accounts being compromised, one of my first reactions was to go and change my password. And I changed the password and after changing it, somebody turned off my two-factor authentication, which to me was a pretty clear indicator that the hackers have access to the internal Twitter systems, because otherwise nobody else knows the password that had just rotated, right?
- Demetri Kofinas:** 00:06:35 Yeah.
- Muneeb Ali:** 00:06:35 And at that point it was pretty clear to me that someone has access to the internal Twitter systems and Twitter itself has hacked right now.
- Demetri Kofinas:** 00:06:42 There's absolutely nothing you can do in those types of circumstances.

Muneeb Ali: 00:06:46 No, that's what's called in the computer science circles as a "God mode," so someone has God level access to Twitter; they can do anything.

Demetri Kofinas: 00:06:56 Yeah. I mean, have you been hacked before?

Muneeb Ali: 00:07:01 Like small instances, nothing measured. I'm in the business of like trying to secure our software, so I'm a paranoid person with all sorts of security setups.

Demetri Kofinas: 00:07:10 Yeah. We're going to get into the details of the Twitter hack for those who don't know what happened or haven't followed up on the details. Of course we all don't know much, there's not much to know. I reached out to the reporter of the motherboard story Joseph Cox, and I also read up on it a bit. One of our previous guests Bruce Schneier has been contacted by the press as well to give comment, but he's made the same point that we don't know much, but before we even get into that and into Blockstack, why don't you give our listeners an introduction into your background? Who are you and what do you do?

Muneeb Ali: 00:07:49 Yep, absolutely. So, my background is mostly in computer science. I did a PhD in computer science from Princeton University, mostly focusing on computer networks and internet protocols. So,, think of that as a sub area of computer science where you're kind of like specializing in computer networks.

Muneeb Ali: 00:08:08 And I grew up in Pakistan; it was very interesting like growing up in the late '90s. I was the only kid on the block who had access to a computer or an internet connection. And that pretty much like shaped my life. Like imagine that I had a single stage run television channel that was our source of news. And I was the only person who has access to this other information channel: the internet. And sometimes I'll notice how the information being fed to us by the state is actually incorrect.

Muneeb Ali: 00:08:41 And that really shaped a lot of my teenage years and then I just really got deep into the computer science aspects, like studied that during my undergrad, started doing research work and basically that's been my life ever since.

Demetri Kofinas: 00:08:56 So, you knew early on that this was something that you wanted to do. When did your focus turn to distributed systems and cryptography?

Muneeb Ali: 00:09:05 Yeah, I think I was around 19 I believe, I took a course in computer networking. The textbook that we were using was by this Princeton professor, Larry Peterson. It's a very interesting story in the sense of I fell in love with that particular area by reading that book, and later in life ended up actually working with Larry Peterson, and some of her students are also, they join our project Blockstack as well.

Muneeb Ali: 00:09:31 And now the latest version of that book that textbook actually has a chapter on Blockstack itself. So,, we kind of like came back full circle over more than a decade where, how I got introduced to computer networking and then basically wanted to look under the hood and figure out, because like R&D is all about kind of like pushing the edges and coming up with better ways of doing things.

Muneeb Ali: 00:09:57 So, that was pretty much the thing that fascinated me that the internet is not an alien technology that aliens came and gave us like it's something invented by

humans. And most of those people are still alive and still with us, like most of the original designers of the internet, most of the founding fathers. And a lot of them actually agree on the shortcomings of the internet and they even agree on the kind of research proposals that what can be done to fix kind of like the foundations of the internet. And that's the work I like took on as a startup after Princeton.

- Demetri Kofinas:** 00:10:32 How many people in the blockchain crypto space would you say either have a strong academic background in these types of systems, or are familiar with the literature on what's been done before?
- Muneeb Ali:** 00:10:49 So I think it was pretty rare earlier in the industry. So, I started around in 2013, one way to look at this as Bitcoin was kind of like 80 or \$90 at that point, so that's how early we are talking about. At that time, I don't think there were a lot of people with deep backgrounds in distributed systems or applied cryptography. And that was something that I felt that is missing from the industry.
- Muneeb Ali:** 00:11:16 And it actually remained like that for a while, so a lot of the early projects, they come from people who don't have a deep domain expertise and they're kind of like trying like very experimental very much like, "Hey, it will be great if a system like this can exist without really thinking deeply about the technical implications of those things."
- Muneeb Ali:** 00:11:40 In the last two years or two or maximum three years, the things have changed a bit, I am seeing a lot more sophisticated teams entering the industry. People like Silvio McCauley, he's a MIT professor who started the Algren project and we actually collaborate with them on some of the smart contracts stuff.
- Demetri Kofinas:** 00:11:58 On Clarity, right? I think.
- Muneeb Ali:** 00:11:59 On Clarity. Yes. So, I think in the last two years, I would say there is a drastic change in which the broader, like more well-establish distributed systems community have started looking into blockchains and a subset of those people are now actively working in the area.
- Demetri Kofinas:** 00:12:15 So you mentioned before I asked you this question, you said something along the lines, or you mentioned the shortcomings of the internet. What were you referring to when you talk about shortcomings?
- Muneeb Ali:** 00:12:28 Yeah, so I think basically I'll give you one example. There are several kind of like different angles and different lens you can take on this but I'll give you one example. So, there's this researcher very famous in disability systems his name is David Clark, he is from MIT. And he was effectively the chief protocol architect of the internet in the '80s.
- Muneeb Ali:** 00:12:53 So if you can imagine like someone from a systems design perspective who's actually kind of like deciding on these protocols and working with the community, that's David Clark, and he gets a lot of credit for it. And he has worked on like several design principles for how the internet should function. And independently, he realized like in 2000s that there were certain shortcomings in those design principles. More specifically, basically they wanted

to design the internet in a way that the core of the network is very simple, like the core protocols do a very simple thing. They just take data packets from one point and deliver it to another point, and they don't care about what's inside the data.

- Muneeb Ali:** 00:13:35 And what David Clark and others kind of like realized is that, that vertical of design aspect works really well. It's called the end to end design principle, but it should have been more specific about security and trust that you should not trust anyone in the middle of the network as well, which is not how the current internet works. Like you implicitly, like even when you open a website, people don't realize this, that you're implicitly trusting like six, seven different parties that you don't even know who they are.
- Muneeb Ali:** 00:14:07 And you're just blindly trusting them even when you're opening a simple thing as a website on the internet. So, that's the shift.
- Demetri Kofinas:** 00:14:14 Is that because these communication protocols were built with the objective of survivability and not trust because they were already presuming that they trusted the parties that were participating in the network because it was built by DARPA and for military purposes?
- Muneeb Ali:** 00:14:29 Yeah. I do think that the core focus was that you should be able to communicate, so they were trying to optimize that if there was some disaster scenario, like a nuclear war or something like that, the core focus was more about like this should be able to function, this should be able to self-heal and still be able to work. And they weren't explicitly thinking about security. But I think like DARPA would have been worried about security, I think it was just a different time, it's a little bit, I think the analogy that comes to my mind is kind of like 9/11 and what happened with airport security afterwards.
- Muneeb Ali:** 00:15:09 Like before nobody really thought about there should be higher security checks when people are boarding a plane, like you would just like walk up to a plane pretty much and boarded and offer 9/11, it completely changed. So, it's a little bit like that, that we were living in the early days of the internet where people were just friendly online, we weren't like really kind of like spending a lot of brain cycles worrying about hacks and security and whatnot.
- Muneeb Ali:** 00:15:37 And people just didn't realize how important security is going to be down the road.
- Demetri Kofinas:** 00:15:42 How much also is this a matter of scale that as the internet has grown, there has been a level of centralization that wasn't prevalent in the early days?
- Muneeb Ali:** 00:15:54 Yeah, so I think there are two trends going on here. One is that the internet is growing and a lot more people are coming online and usually like, imagine almost like a small town where everyone knows each other and people are friendly, and then you suddenly move to a big city where a subset of the population is you don't know them, you don't trust them and the internet is kind of like that.
- Muneeb Ali:** 00:16:19 Like now there are so many people on it that obviously bad act, there are more bad actors in absolute numbers and all sorts of like different types of

demographics are just online now. So, it's just a different world from late '80s, like the late '80s internet like it's hard to imagine like what the internet was at that time.

- Muneeb Ali:** 00:16:37 And the second thing is that with centralization and this will connect back to the recent Twitter hack, centralization basically means that there are a few companies that are extremely powerful on the internet now which wasn't the case early on. And there are a few companies that basically are big prime targets that if they get hacked like millions and millions of people can get hacked just because of that one party being compromised.
- Muneeb Ali:** 00:17:04 Whereas earlier on, like you would really have to hack a lot of small parties to be able to compromise like millions of users.
- Demetri Kofinas:** 00:17:12 So let's pivot to the conversation about Twitter because that sort of relies on some of what we just discussed and then we'll expound on it. For those who don't know, kind of quick summary is that Wednesday around I think 8:00 PM GMT, I think it was 4:00 PM Eastern Standard Time, Twitter was hacked. And from what we know, it wasn't the individual accounts that were hacked as you mentioned and you sort of assume this based on the fact that they turned off your two-factor authentication after you changed your password, they hacked Twitter itself, the network. And it's not clear exactly how that happened but I'm curious what you understand about the hack, what you've learned, and what you think we know so far and what we're still waiting to learn?
- Muneeb Ali:** 00:17:58 So I was first notified of this in our kind of like company's Slack channel and people are like, "Oh, something big is happening on Twitter." And we are in the crypto industry, so there's almost like for the last two years, we have seen some version of this like potential scam on Twitter where people would try to like... So, many times like under my tweets, there would be fake accounts that are trying to impersonate me and asking people to send Bitcoin to a certain address.
- Muneeb Ali:** 00:18:29 Actually, these attacks aren't very sophisticated, and especially in our community like in the crypto industry, they've seen so many such attacks that nobody really takes them seriously anymore. But what was interesting about this attack was that really famous people like Elon Musk or-
- Demetri Kofinas:** 00:18:48 Barack Obama, Joe Biden.
- Muneeb Ali:** 00:18:50 Yeah, Joe Biden.
- Demetri Kofinas:** 00:18:51 Bill Gates.
- Muneeb Ali:** 00:18:52 Bill Gates, exactly, like they were posting about it so just the scale of this was really large. And secondly, the kind of following that Barack Obama would have is very different from a leader in the crypto industry, right? Because so many people who are not familiar with cryptocurrencies are people who have never seen such kind of like scams before might fall for them. But at the same time, those people are also very unlikely to hold any bitcoin. So, that's why like, I wasn't like that concerned about the hack, the hack actually didn't come across as like very sophisticated.

Muneeb Ali: 00:19:28 What was really scary was this God mode thing, right? Like there was this early indication that it really seems like someone has access to internal Twitter systems, which is scary as hell, because they can do anything, they can read your private messages. Imagine like instead of posting these crypto scam type messages, they were trying to create some sort of a civil disturbance, maybe, they were trying to get people to rile up against... I'm just thinking from the top of my head, but against like a black lives matter type of a movement or police brutality, like faking an incident that didn't happen and riling people up about it. Those things can actually be a lot more damaging, like this type of misinformation than a cryptocurrency type of, "Hey, I want to make a quick buck," that was cam.

Demetri Kofinas: 00:20:21 Yeah. What's also noteworthy about this is that the sophistication of the attack, and I can only rely on the opinions of people who know much more than I do. And so from what I understand, it was fairly sophisticated or at least more sophisticated than the types of attacks that would bring in only \$110,000. But also that the data that was compromised and the access was worth much more than what was generated.

Demetri Kofinas: 00:20:49 And as you say, the attackers could not have expected to generate, it's not that they could have expected to generate a million or a billion dollars with this hack worth this strategy. They couldn't have expected to collect much, and in fact, they only collected something like a 100 or 110 or \$120,000, which is nothing. You sort of wonder who would have even given their money in the first place? I think it was like 300 transactions. So, that seems suspicious, I don't know what your thoughts are on that.

Muneeb Ali: 00:21:18 Yeah. I think you're absolutely right there, it's very suspicious. And I think it's suspicious in the sense that it just doesn't add up because the attack itself and from what I know at least from the public statements of Twitter is that they are admitting that some of their employees who had access to internal systems got hacked, and they are at least from the public statements. What they're saying is it was some sort of like a sophisticated social engineering type of a hack.

Muneeb Ali: 00:21:48 But imagine like Twitter is a very sophisticated company, and if you are one of those employees that have access to internal Twitter systems, like you're very paranoid about your own security. And if these hackers were able to compromise such computer experts, I think like the level of sophistication just has to be very high there. I would assume even without really knowing them, like they wouldn't fall for something very obvious.

Muneeb Ali: 00:22:19 So this would have to be some sort of a new type of a very sophisticated attack, and you combine that with how unsophisticated the send me Bitcoin type of messages were. So, it's almost like it just doesn't add up, I can give you an example. If you have access to pretty much like the Twitter account of anyone in the world and you actually want to make money, like I'm not recommending that someone does that but you could actually build up a position for a public company stock and potentially move the markets.

Muneeb Ali: 00:22:52 And this happens like if a big celebrity, for example, I think it was one of the Kardashians who were tweeting about Snapchat and the Snapchat stock started moving. Like you can actually have an impact like that on public markets if you

have access to all the influencers in the world, but they didn't try to do that, they tried like some sort of a very unsophisticated, even the way the messages were composed, you could easily tell that something odd is going on and this is not normal Joe Biden.

Demetri Kofinas: 00:23:23 Yeah, so it kind of raises the question if this is really what the attack was about, was it really about making money? And another thing is that you make the point about taking a position in the market and then using this attack to generate some kind of price action in the market.

Demetri Kofinas: 00:23:41 It might be more difficult to exit that position but regardless, there are two types of ways in which you can take advantage of such an attack. One is monetarily and the other one is non-monetarily. And if you're a government having access to Joe Biden's account can be devastating to the US government and certainly if it were during election time.

Muneeb Ali: 00:24:04 Absolutely.

Demetri Kofinas: 00:24:04 So given that, given the implications of this, what did we learn about the internal security practices of Twitter? Is there any information that's come out about that?

Muneeb Ali: 00:24:14 So that's the area that we know least about, right? Obviously Twitter is taking it very seriously, they're doing internal investigations and I have not seen any information come out, but for me this is a little bit like, I think this is where it starts connecting to the work that we have been doing and kind of like decentralized protocols.

Muneeb Ali: 00:24:33 It's like, no matter how good the security practices of Twitter are, I think there's a fundamental problem here where a single company getting hacked can compromise like national security, as you mentioned.

Demetri Kofinas: 00:24:53 Yeah, and further to that point, and then this is a good opportunity to pivot into decentralization, what Blockstack is doing. There's kind of a buzz word decentralization. I hate to use it. But one of the things I want to note is that even separating whether or not we need to have alternative solutions like blockchain implementations or decentralized Twitter, Twitter wasn't even doing end to end encryption for its direct messages.

Demetri Kofinas: 00:25:21 So even there they could have done things, so these attackers compromise people's private messages, which didn't have to happen if they had taken certain measures. And that speaks to a larger issue as well, which is that a lot of these companies have immense power and they're simply not incentivized. It was a parallel issue maybe, but I think there's an argument for regulation as well. And at some point I want to ask you what your thoughts are on that regulation, as well as perhaps antitrust.

Demetri Kofinas: 00:25:49 And if such regulation can actually be beneficial for blockchain technologies, distributed ledgers, public ledgers and things like this. So, what is Blockstack for those who don't know, you're the CEO of Blockstack? What is Blockstack?

Muneeb Ali: 00:26:05 Yeah. So, Blockstack is an open source project, it got started at Princeton University in 2013. And the interesting thing over here is that we're basically building next generation internet protocols. And I get introduced as the CEO of Blockstack many times and-

Demetri Kofinas: 00:26:25 I'm sorry, CEO of Blockstack PBC, I should've said co-founder of Blockstack.

Muneeb Ali: 00:26:30 Yeah, no, that's fine. And I think I could see the confusion there and we might actually change the name of the company to avoid that confusion. So, there's a company called Blockstack PBC, and then there is Blockstack The Project. And the project is all about open source code and these next generation internet protocols that no single company or individual really controls. It's a little bit like what a future internet can look like and here are the protocols that basically fix the problems with that current version of the internet.

Muneeb Ali: 00:27:03 So as you can imagine, it's extremely ambitious project and what we did is especially given my background in academia, that I just wanted to make sure that this technology gets commercialized and it doesn't remain academic exercise, because I've seen like many such efforts before like there was this clean slate internet design project out of Stanford.

Muneeb Ali: 00:27:27 Like what would eventually happen is that researchers would write papers, publish them, you would have some sort of a prototype implementation of a different internet, but it would never lead the research lab, it would never get commercialized.

Demetri Kofinas: 00:27:41 Why was that?

Muneeb Ali: 00:27:42 It's an extremely hard problem, like imagine how many people use the internet and you want them to switch over to something new, there are network effects and because the user base is so large it becomes very hard to change the underlying technology there. Because the internet interestingly is valuable because everyone connects to the same network.

Muneeb Ali: 00:28:07 And in the early days of the internet, like imagine AOL, for example, it was a single company trying to build something like the internet.

Demetri Kofinas: 00:28:13 Walled garden.

Muneeb Ali: 00:28:14 Exactly, that was a walled garden and everyone who was connecting to AOL could just talk to people who are on AOL.

Demetri Kofinas: 00:28:20 Yeah, it was the internet but it wasn't the web.

Muneeb Ali: 00:28:22 Yeah. It wasn't the web and then the internet took off because it was permissionless, it was open, anyone can connect to it but still you're all connecting to the same network. Now imagine almost like a smaller island, a smaller internet, and there are fewer people there it's entirely possible from a technical perspective. In many ways in the '90s, there were some efforts like that. And if you're connecting to that internet, you're not on the main internet and there's very little incentive for anyone to be on a different network.

Muneeb Ali: 00:28:50 So it's almost like you need a collective upgrade across like hundreds of millions or billions of people and it's very hard to pull off. And there are several layers of technical complexity and whatnot. But also I think in academia, there is a little bit, that's the reason that I personally left academia and started building a company is because there's an incentive structure of a research publication is the finish line. You just put your ideas out there with the prototype implementation and your work is done.

Muneeb Ali: 00:29:25 And that's how the incentive structure in academia works because you are incentivized to put out a lot of, kind of like ideas and algorithms out there. You aren't really incentivized to go deep on one single paper idea and really see it through for decades.

Demetri Kofinas: 00:29:45 What do you think accounts for the fact that the internet and the web protocols were commercialized in the form of these web applications and browsers and everything that we've grown up with since, since the '90s really?

Muneeb Ali: 00:29:58 Yeah, so I think the DARPA deserves a lot of credit for this, like they funded a lot of the early research and then I think it's also like we have to keep the timeframes in mind, like it was decades of work even before we got to a position of like Amazon coming online. And there was like, basically a very interesting kind of like worldwide collaboration mostly at universities.

Muneeb Ali: 00:30:25 So a lot of these universities where the hub for different types of the research, like for example, some people are looking more at the hardware side, some people are building core protocols, and some people who are trying to look at chat type or email type applications And so, on. And they were competing protocols as well, and it all got resolved in a picture kind of like started emerging for universal internet. And still like, I think commercial entities like Netscape.

Demetri Kofinas: 00:30:52 Mosaic, exactly, Urbana Champagne.

Muneeb Ali: 00:30:55 Yup. Like Marc Andreessen, he deserves a lot of credit because he was, I think in a somewhat of a similar position that a lot of these crypto startups are at where to be able to deliver a certain experience to the end user, Netscape had to invent a lot of the underlying technology. They had to invent like browsers, they had to invent JavaScript like the programming language, they had to invent like cookies and this idea of keeping state at servers so that users can actually resume their sessions and so on. And interestingly, like this is where a lot of the crypto industry is right now for this next generation internet, where for a fairly simple user experience, like the 90% of the work is in the background and it's in the infrastructure and you'd really have to invent new things and new protocols and new ways of doing things to deliver that experience.

Muneeb Ali: 00:31:50 And I would give a lot of credit to Marc Andreessen and Netscape for filling that gap, like whatever was not there from the pure academic type of a research, he really commercialize things like back in the '90s.

Demetri Kofinas: 00:32:04 Yeah, and another thing that he did and his team did with Mosaic, which actually is something I want to discuss to Blockstack because I've checked out some of your applications and they also seem to have really functional really

user-friendly UIs. And so, similarly, like Mosaic was really innovative in bringing images into the browser.

- Demetri Kofinas:** 00:32:26 So that might be an interesting sort of parallel to discuss, but let's actually get down to the core functionality of Blockstack. What is it and how does it work?
- Muneeb Ali:** 00:32:37 Yes, so as I said, that it's a next generation internet, and we have built the core protocols and think of that as almost like public infrastructure, that developers can use to build applications that are user owned. And let me define that a little bit. So, the main thing that we are trying to do over here is over time the internet became more and more centralized in the sense that like imagine desktops where you own the computer, you install a desktop application, and then basically use it locally.
- Muneeb Ali:** 00:33:15 And you are supposed to keep a backup of your data on your hard drive, or a backup hard drive and so on. And with cloud computing and kind of like web 2.0 companies like Facebook and Google, basically what started happening was that your computers became a little bit like dumb screens, you're always connected to the cloud and some company is storing the data. So, some companies actually running the application, like imagine that you are working in Google Docs, that software is not installed on your computer, it's running in a Google data center and all of the data is sitting with Google.
- Demetri Kofinas:** 00:33:53 So the computer becomes almost like a dumb client and the server is Google.
- Muneeb Ali:** 00:33:58 Exactly, right. So, now we are like completely dependent on this third party the company and users are really not in control, but people were kind of like fine with it because all these products were free. And the big difference between let's call it web 1.0 and 2.0, was this advertising model where companies realized that by offering free products like Facebook or Google products, you can actually make more money by selling the user data.
- Muneeb Ali:** 00:34:30 And that's effectively what we've been seeing for the last 15 years or so. Like we have these giant companies and they offer free products and we are becoming more and more reliant on these large companies. And then we started seeing the backlash, I would say, in the last five to seven years. I think the last election 2016 was the first time when people, it really hit home that how much power a company like Facebook has on even the kind of information you get are, you can dig an even influence your moods or even elections in a certain way.
- Demetri Kofinas:** 00:35:06 So the fact that for example, payments were never enabled in the browser, the natural default was to rely on advertising which meant trafficking and user data.
- Muneeb Ali:** 00:35:19 Yup, so I think basically I would say that the dominant business model on the internet is advertising, like that's how most of the websites make money. And even that started getting consolidated a lot more like people actually don't even realize how much information companies like Google get, like because like Google has this analytics type of a service for websites where they're like, "Hey, install this piece of software on your website and Google will help you analyze your traffic."

Muneeb Ali: 00:35:52 But what's really happening is Google is now getting data from millions and millions of different websites on who the person is, and then they're using that data in their search and in their advertising and so on. And I think there recently people have started just getting a feeling of that, it starts becoming really creepy when they started doing the same stuff with voice.

Muneeb Ali: 00:36:15 So Google was actually recording people without people even realizing it, and it became like a mini scandal recently. So, imagine like people start noticing this when they go like, "Hey, I was just having a conversation with my partner about buying something and the next day I started seeing ads about it."

Demetri Kofinas: 00:36:30 Yeah. I had a similar experience just a few days ago, I went out in an area outside of New York and we were having a very, very brief conversation about Lyme disease because takes out here carry Lyme disease. And literally within hours on my Twitter feed, I see a post that's being promoted to me, dealing with an athlete who developed Lyme disease and hadn't been dealing with it for years. And I had never looked up a single thing about Lyme disease, it's not something I even talk about.

Demetri Kofinas: 00:36:58 So it's totally freaky and for people that are new to the show, I've mentioned Shoshana Zuboff's episode on Surveillance Capitalism many, many times, but it's a great episode for anyone that's interested in understanding not just the history of this type of economic logic, but the logic itself. Also, we did a great episode with, I'm blanking on the name of the person, but it was on the history of the early web which is fascinating and so, much fun.

Demetri Kofinas: 00:37:26 So let's get back to Blockstack the way I understand how block stack works. You guys have something called Proof of Transfer, so there's like, we all know about Proof of Work, a lot of people are familiar with Proof of Stake it's something that we've talked about on the show on multiple occasions, including with Vitalik Buterin and Vlad Zamfir where they tried to explain their roadmap and their vision for creating, for moving from PoW to PoS. What is Proof of Transfer and how does it work?

Muneeb Ali: 00:37:55 Yup. Let me finish one thought on the kind of like core difference, so what Blockstack is introducing is that it's basically introducing like ownership or property rights for the users. So, users can directly register their username on this next generation internet, they can directly own their profiles, their information, and they have kind of like these private encrypted drives where apps that are apps are more similar to desktop apps, like you just download them and they're writing data to your encrypted drive.

Muneeb Ali: 00:38:34 And for most part, like, only the user has the data and it basically is a complete inverse off what we see on web 2.0. So, with that in mind that this is about a user owned internet, I'll get into kind of like Proof of Transfer and the technology stack. So, basically I think for people who are familiar with Ethereum and Metalics work, we are the exact inverse of that. So, we go back to the early days when in 2013, 2014, even metallic was trying to introduce this new type of functionality of registering new types of assets or smart contracts on the Bitcoin blockchain itself.

- Muneeb Ali:** 00:39:18 And he very quickly realized that this would never be acceptable to Bitcoin developers or as against the design principles of Bitcoin. Bitcoin wants to keep the base blockchain like simple and just focus on security and payments. And he went off to basically start a different blockchain Ethereum. I and Blockstack are in the school of thought that Bitcoin is by far the most secure blockchain and you can actually build these types of decentralized applications and smart contract functionality connected to Bitcoin.
- Muneeb Ali:** 00:39:54 So I think that's the fork where metallic and Ethereum, they're basically trying to build a different network and we are still connected to Bitcoin. And the way we do this is we have this idea of Proof of Transfer. And what Proof of Transfer says is that the world needs one really, really secure blockchain and a reserve cryptocurrency, which is Bitcoin. And once you have that, right, so for people who are familiar with Proof of Work, in Proof of Work, you're effectively destroying electricity by doing this work to secure the network.
- Muneeb Ali:** 00:40:30 And you are getting newly minted cryptocurrency Bitcoins as a reward. So, once you have that, what we say is you no longer have to basically reinvent the wheel and then destroy electricity to secure a blockchain again, but you can actually use the Bitcoin itself to start new blockchains that are connected to Bitcoin, that benefit from the security of Bitcoin. So, I think the mental image is a little bit like imagine a very secure Bitcoin blockchain, and then imagine independent chain right next to it that connects to Bitcoin and benefits from the security of Bitcoin.
- Muneeb Ali:** 00:41:08 So in that sense, I think it goes a little bit back to how we were talking about in the early days of the internet, there were all these different types of networks and people didn't really know that which network is going to be the internet. And our thesis says, that it's actually going to be Bitcoin. So, anything that connects to Bitcoin down the road that is going to be the universal network that basically upgrades us from intranet where people don't have property rights and they don't have cryptocurrencies and they can't own things to a world where they can.
- Demetri Kofinas:** 00:41:42 So how does that work? So,, you guys have what you call, I think it's called the Stacks Token?
- Muneeb Ali:** 00:41:47 Yup, so that's the native cryptocurrency for the new blockchain, the stacks blockchain that connects to Bitcoin. And the way this works is the stacks cryptocurrency is what gets consumed when people are running smart contracts or they are registering intranet assets. So, imagine like let's take Twitter, for example, let's say that Twitter decides that this hack was really bad and they want to move to a more decentralized model.
- Muneeb Ali:** 00:42:17 What would happen is you cannot resist your 300 million users directly on Bitcoin. Bitcoins network does not have the bandwidth for that type of scale. But you can register 300 million users on the stacks chain because thousands of registrations on the stacks chain only result in a single hash on the Bitcoin chain. But this blockchain is designed for smart contracts and decentralized applications, but it benefits from the security of Bitcoin.
- Demetri Kofinas:** 00:42:49 So from what I understand how it works and I might have this totally wrong, the way that people mine, the mining operation is basically by transferring Bitcoin

to what is like the reward set from which stakeholders collect some amount of Bitcoin. And so, like, can you go through that process a little bit? Because I want to make sure I understand and I don't want to actually confuse my listeners, but I think it's important because I haven't seen you kind of explain this process anywhere that I've been able to find.

- Muneeb Ali:** 00:43:18 Yup, I think in the grand scheme of things is very recent, our Proof of Transfer full paper came out just a few months ago, so I'm not surprised.
- Demetri Kofinas:** 00:43:26 I mean, what I do understand is that you're using Bitcoin in order to bootstrap STX, and eventually STX could theoretically have enough value that you don't need to actually "transfer Bitcoin" and you can just use STX on its own to run these applications.
- Muneeb Ali:** 00:43:46 Yeah. Let me clarify some of those things. So, I think the bootstrapping problem is a little bit different, like it's basically... The problem there is, if you start any new blockchain network like in the early days there isn't a lot of like hash power or participation in the network and it can be easily attacked. So, the way Proof of Transfer works is that you're piggybacking on Bitcoin security, so you avoid this bootstrapping problem. And we can go into more details there.
- Demetri Kofinas:** 00:44:17 Yeah, I'd love to.
- Muneeb Ali:** 00:44:18 But let me step back a bit and explain the process because I know there are a lot of details there and can be a little bit complex. So, I think at the heart of it, first of all, it's all about incentives. In a network, that is not owned by a single company what you're effectively trying to design is who is going to operate the network? Like why would those parties have a financial interest to actually operate nodes and run the network?
- Muneeb Ali:** 00:44:47 So in our blockchain, there are two types of basically nodes or parties, one are the stacks miners. So, the miners, they're actually doing a lot of the heavy lifting, because they are processing kind of like new transactions coming in, they're collecting fees from those transactions, they are running the smart contracts in a block, they're collecting the fees from the smart contracts as well, and they are incentivized by newly minted stack tokens per block, similar to how Bitcoin or other blockchains work where the main incentive for these operators are called miners is to collect the newly-minted cryptocurrency, and the transaction fees, and the smart contract fees.
- Muneeb Ali:** 00:45:32 So our miners are a little bit special in the sense that they basically run, they have the state of both the Bitcoin blockchain and the stacks blockchain. The miners are the parties that are connecting these two blockchains together. So, these miners, they need to effectively participate in almost like a leader election process where, because we can't rely on any single party and this needs to be an open system. Anyone can become a miner and anyone can try to become the leader of the next round.
- Muneeb Ali:** 00:46:07 So all of that selection process for a leader happens on the Bitcoin blockchain. So, these miners are actually sending transactions on Bitcoin to participate in leader election, there's a verifiable random function that picks up a leader for a block, and that leader writes a block on the stacks chain.

Demetri Kofinas: 00:46:28 Wait, when you're saying it happens on the Bitcoin blockchain, you're saying the same people that win the leader elections in Bitcoin are the ones that are proposing new blocks in Blockstack?

Muneeb Ali: 00:46:39 No. So, Bitcoin miners are different, right? So,, you completely separate out the other Bitcoin infrastructure, that's for Bitcoin. These miners are just parties who are sending transactions on Bitcoin, and they're effectively, it's a use case for Bitcoin that we can use the existing Bitcoin network.

Demetri Kofinas: 00:46:55 You're taking the value of Bitcoin and they're sending them as transactions, and that's how that increases, the more they send in terms of Bitcoin, the higher, the likelihood that they will win the leader election and proposing you block on Blockstack, is that right?

Muneeb Ali: 00:47:08 Yeah. So, basically what happens is that there is almost like a bidding happening on using the Bitcoin layer, where miners are competing by bidding more Bitcoin, that I want to be the leader on the stacks chain. And then there's a random function that some probability, if you're willing to kind of like spend more Bitcoin you have more of a probability of winning a round for the stacks chain.

Muneeb Ali: 00:47:35 It's basically think of that as a process that is in theory, very similar to how Bitcoin miners are kind of like calculating hashes, and there's some probability that someone will get selected as a leader on the Bitcoin chain. And that leader has incentives to get newly-minted Bitcoin cryptocurrency.

Muneeb Ali: 00:47:57 So it's a similar process, but over here, instead of wasting compute cycles, people are just bidding using Bitcoin itself. So, their cost factor is described like you calculate your costs not as electricity or your computer hardware then that you had to purchase, but your cost is expressing the Bitcoin cryptocurrency.

Demetri Kofinas: 00:48:17 That seems to share some things in common with Proof of Stake.

Muneeb Ali: 00:48:21 Yes, so I'll get to that. So, basically Proof of Stake, I think in some ways is fundamentally different because the security of the network depends on the economic stake that these parties are willing to kind of like lock up and there can be basically bad behavior is disincentivized by slashing funds. The protocol can actually take away your fund, and that's a scary thing and I wouldn't go into the details of it but we wanted to avoid that.

Muneeb Ali: 00:48:50 Because the protocol actually can tell if someone's being malicious or-

Demetri Kofinas: 00:48:54 Right, or they're hijacked and compromised.

Muneeb Ali: 00:48:56 ... or even if there's a network partition or something, but it's an honest party but they're giving you information that is incorrect. So, we want to stay away from those problems and we fundamentally believe that Proof of Work is extremely important for certain security properties of blockchain.

Muneeb Ali: 00:49:12 So our blockchain is gives you security properties that are in the Proof of Work philosophy, to attack the chain someone will have to go and basically attack the Bitcoin's Proof of Work. So, good luck with that, that's the most secure network on the planet and we benefit from that.

Demetri Kofinas: 00:49:33 Can you explain that a little bit because don't you just need to accumulate enough Bitcoin in order to attack the chain in this case?

Muneeb Ali: 00:49:40 That's a different type of attack. If you have to change the history of our blockchain, you will have to go and attack Bitcoin and change Bitcoin's history.

Demetri Kofinas: 00:49:50 So if you were to let's say accumulate enough Bitcoin to participate in leader elections, that your probability of a victory is one that only allows you to fork the chain, it doesn't allow you to go back and rewrite previous blocks is your point.

Muneeb Ali: 00:50:05 Yes, exactly. Right, so that's an attack on the current block that some party is trying to, for certain malicious information in the current block but then there are protocol rules as well. So, you cannot do anything outside of the protocol rules because the other nodes would just ignore that as not valid.

Demetri Kofinas: 00:50:22 So Blockstacks chain is actually stored on a Bitcoin blockchain?

Muneeb Ali: 00:50:27 No, and I feel like we're getting very deep on the technical side.

Demetri Kofinas: 00:50:31 Yeah. So, sorry if I'm, yeah. I don't mean to, I'm sure this is probably a little frustrating for you because you have conversations with people they're much more experienced in this stuff than I am. It's just, I'm infinitely curious these are unique opportunities for me to learn, but I do not want to stray too far. But anyway, go-

Muneeb Ali: 00:50:48 Yeah. Let me answer that, I think I was trying to optimize for the audience, like at some point, like if it's a very technical audience I'm more than happy to take a much deeper dive. In general, like let me answer the question that the state of the blockchain is not stored on Bitcoin, it's a separate blockchain and that would be a scalability problem if the state of the blockchain was stored on Bitcoin. Because then going back to the Twitter example, those 300 million user illustrations, that data would have to live on Bitcoin, which cannot happen, because of scalability.

Muneeb Ali: 00:51:19 So the state of the blockchain is separate. And let me rewind back to when I was talking about incentives, and so, there are the stacks miners who are, think of them as somewhat similar to a miner on a traditional Proof of Work chain. Like it's just that their cost is expressed in Bitcoin and they're writing blocks on the stacks chain. Like they basically have to keep two different types of states in mind and they are doing leader election on Bitcoin but writing blocks on the independent stacks chain.

Muneeb Ali: 00:51:50 And then there are the stacks holders who are incentivized to actively participate in the network, run full nodes and periodically broadcast certain useful information on the network. And these people are rewarded in Bitcoin and then there's a ratio, like for example, if you're basically locking up a certain number of stacks, you can calculate what percent rewards you can earn from Bitcoin. And that property is similar to sticking where...

Muneeb Ali: 00:52:22 But I think the underlying algorithms are extremely different, so you can never lose your funds, you're not actually doing any validation or mining and you're

not writing blocks. These are just active participants on the network who are locking up their stacks earning Bitcoin and providing some services to the network, but the miners, the stacks miners are doing the actual heavy lifting.

- Demetri Kofinas:** 00:52:47 Right. To be clear, I should've been more specific, I didn't mean that the entire Blockstack blockchain was stored on the Bitcoin blockchain, but rather a hash of it or some sort of snapshot of the chain that would basically secure it so that you couldn't go back and rewrite it.
- Demetri Kofinas:** 00:53:01 I don't know if that's even accurate, but this is super interesting though. I mean, I looked at this point about bootstrapping because that's kind of how you bootstrap it, right? The fact that STX holders get paid in Bitcoin and the fact that the miners that win the elections get paid in STX, which allows them to then generate a return in Bitcoin solves a problem at the very beginning, which is why would anyone want to hold STX?
- Muneeb Ali:** 00:53:24 Yeah, so I think the problem in my mind that the high level of problem that it solves is, it solves the problem where you want to start a new blockchain, and it could be any reason, right? That you want to focus on a certain application and it doesn't make sense to write that state of that application directly on Bitcoin. And right now there is a problem where A) if you are starting another Proof of Work chain, in some ways you're trying to compete with existing Proof of Work chains including Bitcoin.
- Muneeb Ali:** 00:53:55 And it's not a very great position to be, and Bitcoin is this like 800 pound gorilla in the space, and if you're trying to get attention from people who can be miners or Proof of Work miners like that, it's a very kind of like hard thing to do. Instead, what we are proposing with Proof of Transfer is you accept Bitcoin as the kind of like the vendor in the Proof of Work space. And you reuse that by connecting to Bitcoin. So, that's a key difference where you are no longer trying to compete at the Proof of Work layer, and you are accepting who the winner is in that category and then you're connecting to it and benefiting from that.
- Demetri Kofinas:** 00:54:36 Theoretically, would you even need to use Bitcoin if STX is value sort of grew exponentially?
- Muneeb Ali:** 00:54:43 So I think it's basically this one comes down to, can you build secure blockchains without Proof of Work? And we are in the category that you cannot, we can get into like what types of problems are there with Proof of Stake. And there are some interesting work like Algren and others. But in general, I am personally in the camp that without Proof of Work, you actually lose many benefits of a blockchain.
- Muneeb Ali:** 00:55:09 Like for example, like with Proof of Work, any new node can independently verify that are you on the correct version of the blockchain. But Proof of Stake, you actually need some trusted nodes to bootstrap and then verify that am I on the right version or not? And which is, I think a little bit of a circular problem, like if I'm trusting these nodes to bootstrap like that's the exact problem that blockchains try to solve anyway.
- Muneeb Ali:** 00:55:36 And then there are other types of attacks where if someone is giving a different version of the history to you, in Proof of Work we're required a lot of work to

give you like even 10 or 100 different versions of history, whereas in Proof of Stake, an attacker can potentially give you millions or billions of versions very quickly because they don't need to do any work to produce these versions.

- Muneeb Ali:** 00:56:00 So you can actually like confuse people a lot by giving them several different versions of history, whereas in Proof of Work, that attack is very limited because an attacker has to do a lot of work to produce long versions of history.
- Demetri Kofinas:** 00:56:13 By nodes, do you mean people that are independently running the Bitcoin software but not actually participating in Proof of Work?
- Muneeb Ali:** 00:56:20 No, I mean miners.
- Demetri Kofinas:** 00:56:21 You mean miners. So, could you see a point at which you guys transition from Proof of Transfer to Proof of Work?
- Muneeb Ali:** 00:56:29 So I think in general, we don't want to transition away from either Bitcoin to some other Proof of Work chain or to our native Proof of Work chain. Because I think there are very interesting economic incentives here because, like forgetting the technical aspects a little bit, the model of the world in my mind is Bitcoin becomes a reserve cryptocurrency, everyone wants to kind of like, we already see signs of that where people want to hold Bitcoin.
- Muneeb Ali:** 00:56:56 They treat that as digital gold and stacks is a crypto asset where if you lock it up in consensus, you're earning Bitcoin, so you can model, let's say that 50 or 60% of the liquid supply of stacks is actually locked up for this use case, is being used in consensus. And people are basically modeling it as a, I get a Bitcoin yield on this asset if I participate in consensus.
- Muneeb Ali:** 00:57:25 And that's a good property, if we move away from Bitcoin, if you have our own Proof of Work that goes away, because there are no longer any Bitcoin that can actually flow to the holders who are participating in consensus. And then the other interesting thing is that for the liquid portion of stacks that are being used in smart contracts and to register assets. Again, the connection to Bitcoin is very important because for the internet assets like domain names or Twitter usernames. The ownership, as you mentioned, that there is a hash of a stacks block in a Bitcoin block.
- Muneeb Ali:** 00:58:01 So your ownership is actually ultimately defined in Bitcoin. And if you ask the question that which blockchain will be around 10 years from now, the answer would be, "We don't know, but Bitcoin would probably be around." So if you're paying for an asset, if you're purchasing a domain name like a blockchain backed domain name, or you're purchasing a username that is blockchain back, I would argue that ownership defined on Bitcoin is a hundred X better than ownership defined on anything else because that's something else may not be around down the road.
- Muneeb Ali:** 00:58:32 So that's why like I would, I think our default model is that Bitcoin stays there and we stay connected to Bitcoin in the exact same scenario. But technically speaking, yes, there could be some other blockchain or we could just incorporate our own Proof of Work thing if we need to. But I think it's a small probability and who would much rather not do it.

Demetri Kofinas: 00:58:53 But it also gives you a lot of flexibility and also this particular model of bootstrapping, the way you guys have done it, it's pretty ingenious. I've never seen it done any... it's not done anywhere else. I mean, in any kind of manifestation, I haven't seen anything like this.

Muneeb Ali: 00:59:08 No, it's not, it's completely unique. I think what's happening here is actually there's Proof of Work, there's Proof of Stake, and we're defining a third category Proof of Transfer. But what we're really saying is what Proof of Transfer really does is it enhances Proof of Work. Like if Proof of Transfer takes off, it's entirely possible that other types of Proof of Work networks let's take Monero for example. That there's no reason why Monero cannot use Proof of Transfer and just connect to Bitcoin versus doing its own Proof of Work.

Muneeb Ali: 00:59:45 If that is a more secure way of doing it and Monero holders are now earning Bitcoin, like why wouldn't you want to do that? So, what it does is, it's a little bit like it takes the really good security properties of Bitcoin has a more sustainable solution around Bitcoin. Like right now we're in a phase where lots of different experiments are happening.

Muneeb Ali: 01:00:07 If Proof of Transfer starts taking off, you will actually see a little bit of a consolidation that Proof of Work, we have a winner it's Bitcoin for a reserved cryptocurrency, we have a winner it's called Bitcoin. And then other use cases are connecting to it, and because they're connecting to it, we start a picture emerge for a future internet. Instead of having these disconnected small islands that we are currently noticing in the crypto space.

Demetri Kofinas: 01:00:34 That's interesting. So, I want to move the rest of our conversation into the overtime, Dr. Ali. And I want to start that conversation with a discussion about your smart contract layer and how that works. And then also into a conversation about distributed applications that are being built on Blockstack, because some of them are really beautiful. I played around with them, one of them I actually experimented with was the kind of the WeTransfer analog.

Demetri Kofinas: 01:01:00 So they're really, really well done, they're very user-friendly and I'm curious about that as well. That's what I was hinting at with the reference to Mosaic and images in the browser. For regular listeners, you know the drill, if you're new to the program, Hidden Forces is listener supported, we don't accept advertisers or commercial sponsors. The entire show is funded from top to bottom by listeners like you.

Demetri Kofinas: 01:01:24 If you want access to our premium content, which includes transcripts of every conversation we've ever had on the program, copies of my rundown which are elaborate show documents created by me ahead of every episode, or if you just can't get enough of the podcast and you want to hear more from my guests, including my overtime conversation with Muneeb, head over to patreon.com/hiddenforces and subscribe.

Demetri Kofinas: 01:01:49 Not only is the content worth it but it's a great way to show your support for the show and the work we do. Muneeb stick around, we're going to move the second half of our conversation into the overtime.

Muneeb Ali: 01:02:01 It sounds great.

- Demetri Kofinas:** 01:02:03 Today's episode of Hidden Forces was recorded in New York City. For more information about this week's episode or if you want easy access to related programming, visit our website at hiddenforces.io, and subscribe to our free email list.
- Demetri Kofinas:** 01:02:19 If you want access to overtime segments, episode, transcripts, and show rundowns, full of links and detailed information related to each and every episode, check out our premium subscription available through the Hidden Forces website or through our Patreon page at patreon.com/hiddenforces.
- Demetri Kofinas:** 01:02:40 Today's episode was produced by me and edited by Stylianos Nicolaou. For more episodes, you can check out our website at hiddenforces.io. Join the conversation at Facebook, Twitter, and Instagram @HiddenForcesPod, or send me an email. As always, thanks for listening, we'll see you next week.