Barefoot Podcast with Jai Ramaswamy

Jo Ann Barefoot:	Today's show is really going to be a treat for all of our listeners because my guest is Jai Ramaswamy, the Chief Legal Officer of Andreesen Horowitz. Jai, I'm so excited to have you on the show today.
Jai Ramaswamy:	I'm thrilled to be here today, Jo Ann. Thank you.
Jo Ann Barefoot:	We have a great lineup of topics to talk about. I think I first got to know you when you worked with us on the text print we did a few years ago on child sexual abuse material and cryptocurrency, and you were one of the experts on the money laundering issues there. And then since then, you've come to this role at A16Z. So, I want to start by asking you to tell the listeners about your background. So, let's start there.
Jai Ramaswamy:	Sure, happy to. My background has varied in a number of different areas. I tended to focus a lot on regulation, risk, and areas of financial crime. So, when I started my career after law school, I joined the US Attorney's Office in the Southern District of New York and there was a general white-collar prosecutor focused on different types of frauds, tax fraud, investment fraud, other things like that, but also ended up focusing on cybercrime. It was an interest of mine early on and was interested in pursuing those cases.
	After several years in the US Attorney's office, I ended up transitioning to the main headquarters, DOJ in Washington, D.C., where I joined the cybercrime section and really focused on a wide variety of cyber threats that were occurring at that time, which tends to be the case with Washington components of DOJ, also on some policy matters that were arising. One of the things that was clear at the time is that cybercrime was going to become as much of a national security issue as it was a pure criminal law or criminal prosecution issue. So, I had really an opportunity to delve into a number of different areas of cybercrime. One of the areas that was rising at the time was virtual currencies. Some of them were precursors or centralized versions of what eventually became cryptocurrency.
	There were ledgers such as e-gold or later on in case they had in a subsequent era of my career, Liberty Reserve that were centralized ledgers attempting to bring value into internet transactions. But it was a fascinating time and I was in that section for several years until I was asked to join the Asset Forfeiture & Money Laundering Section first as principal deputy chief under Jen Shasky, who subsequently went on to become the director of FinCEN, but she was chief at the time of AFMLS or the Asset Forfeiture & Money Laundering Section. The name to confuse things has changed even further today, and it's known as the Money Laundering and Asset Recovery Section or MLARS.
	But after she went on to become the director of FinCEN, I was asked to become the chief of AFMLS at the time. It was a wonderful experience, really focused on a number of different areas. One of the areas was enforcement against financial institutions for Bank Secrecy Act, Patriot Act, and sanctions violations in their compliance programs. We brought a number of pretty large cases at the time through my tenure there, including HSBC and BNP Paribas were probably two of

the biggest ones that we had at the time. But also, as I said, we're starting to focus on the nascent emergence of cryptocurrencies and other digital forms of value as I said.

Liberty Reserve was another case that we brought, but I was enjoying myself and really had a phenomenal run at the Justice Department over a decade by the end of my tenure at AFMLS. I started to think about what could come next. I wasn't really ready to jump, but out of the blue, I got a call from Bank of America. I hadn't really expected or anticipated to go into compliance, but Bill Fox, who I had met and is a big figure in the AML space. He was in the Treasury Department, the first director of FinCEN. It was a pretty unique opportunity to work with somebody that I really respected and trusted and learn a little bit more how things work in the financial services industry, because as a prosecutor, you don't really have as good a sense.

You construct things after the fact, but you don't understand the operations and how a financial institution works. So, I took a leap of faith, ended up there, and it was phenomenal as I anticipated. Working both at Bank of America as well as for Bill were just fantastic experiences and I learned a ton. Subsequent to that, an opportunity came to broaden my role in the financial services industry and to become the Head of Enterprise Risk Management at Capital One and that's here in the DC area. It was again a phenomenal opportunity to really understand the business and the risks associated with financial service at a much broader level. Capital One at the time was also very tech forward and currently is a tech forward bank.

So, it was an opportunity to work at the cutting edge, if you will, of financial services, which I also found incredibly attractive. After I think a total of about six, seven years in financial services, as I was getting more involved in a tech forward part of the finance service industry, I started thinking to myself, "Where else are there opportunities where I could really start to delve more deeply into what was happening in the technological landscape?" Honestly, I took a leap of faith and ended up in crypto thanks to another good friend of mine, Katie Hahn, who asked me to talk to some founders at Celo, which is a layer one blockchain protocol and really fell in love with the project, fell in love with the founders, and really believed in their mission.

That was my first entree over the past several years into crypto and Web 3.0. In a sense, I tell people I've been red pilled a little bit. The issues are so interesting in this space and unique for a lawyer to be able to contribute strategically to this space that I really haven't looked back. When the opportunity came to come over to Andreessen Horowitz or A16Z, for me, it was a bit of a no brainer. It's a great institution that's deeply involved in these issues, and obviously, more broadly in the venture capital space and in the fostering of new and innovative technologies. So, that's how I ended up in my current role and also interested more broadly in the Web 3.0 and crypto space.

Jo Ann Barefoot: That's a fascinating journey. When did you start at A16Z?

Jai Ramaswamy: It's going on for about a year, so I started in October of last year. So, yeah, I'm coming on my year anniversary.

Jo Ann Barefoot: I'm sure most of our listeners know about the firm, one of the great almost original venture firms in Silicon Valley, but just give us a quick profile of Andreessen Horowitz.

Jai Ramaswamy: Yeah, I mean it's a full-service venture capital firm, meaning that we invest in a number of different portfolios across the range of companies. So, that includes obviously a very large presence in Web 3.0 and crypto, but we also have traditional investments in traditional technology companies, infrastructure companies, consumer companies, and even have a very active and robust practice in biotech. So, it really is a full-service venture capital firm. It was started in 2009 by Ben Horowitz and Mark Andreessen, both of whom were entrepreneurs in the early days of the internet and wanted to bring an operational mindset to venture capital investing.

So, one of the hallmarks of our model is we really do see ourselves as partners with the entrepreneurs that we invest in and try to provide them as much as possible with operational guidance and expertise so that they know how to run and scale their businesses. We see that as a differentiator between what we provide and what some of the other folks out there provide. I think everybody tries to really help entrepreneurs, but we try to take it to the next level and have operating teams that are really there to assist these companies develop.

Jo Ann Barefoot: Great. So, the firm has really taken a leading role in popularizing or telling the story of where we may be headed with Web 3.0. Let me start by asking you to define Web 3.0 point for our listeners.

Jai Ramaswamy: Sure. So, Web 3.0 is supposed to connote a new evolution of the internet. If you go back in time and I'm going to be paraphrasing or simplifying things a bit, but I think it's a really good heuristic or mental model to have. When you think of what the web originally was, Web 1.0, if you will, it was a way for users globally to acquire information really for the first time in a comprehensive way. It started off as a peer-to-peer network. Obviously, the history of its inception through DARPA and through government involvement is well known, but the private sector obviously really took a lead in developing what it was.

Those original applications if you will or web browsers and search engines and Google being the most well-known of them, that really allowed us to access information on a global scale for the first time. If you think of it in computer terms, it was read-only, meaning you acquired information as a user. Fast forward to developments in broadband technology, mobile computing, cloud computing, and you had the rise of a new paradigm of the web which allowed not only the consumption of information but the publishing of information and by users. So, the rise of blogs, the rise of Facebook, of Twitter, of these platforms that allowed content generation and publication by users on a global scale. So, the web turned from read in computer science terms to read and write.

That's the world we live in today if you think about it. But one of the hallmarks of that is that our experience with the internet is really intermediated by these platforms. We have Facebook accounts or we have other types of accounts or we purchase things through Amazon or apps through the Google Play Store or the Apple App store. But in many ways, we have extensive, if you will, licensing rights to information through these platforms but don't truly own our content. That comes across in a number of ways. For example, at times, if you have purchased a book or a piece of music, you have extensive light-sensing rights with the platforms that you belong to. But if they want to take back those goods, they can and that's happened in a couple of instances.

But the idea is that the platforms mediate your relationship to the web. They really own, if you will, the content. In order to publish on these various platforms, the charges that are accrued can be high, sometimes as high as 30%, even higher in order to enjoy the fruits, if you will, of your labor on these platforms. What Web 3.0 is, is the potential and I should emphasize here that we're talking about really the early days of Web 3.0, roughly akin to the 1997 period of the web. If you remember, it was a very different internet back in 1997 that we enjoy today, so early days here.

But the potential here and the promise here is for something that will allow not just for reading and writing or information consumption, information publication, but actual ownership of content and information by individuals. That's really what the blockchain and decentralized blockchains provide is that they provide for the first time for users to one, own content and information through Web 3.0 through tokenization, which is a concept we can discuss a little bit later, and also, to participate actively in the communities that run these blockchains and have a voice in how the future of a particular blockchain that you are a part of that community develops. That can be done through what are called CodeCommit.

So, if I'm a member of a particular community that's responsible for a blockchain, I can commit software code that can then be voted on by the community to change the course of that blockchain and other types of proposals that come forward on how that community wants to be organized. So, you've now shifted to a model of read, write, and own, which is different than what we have today and which promises to potentially disintermediate some of these platforms and centralized entities that have been responsible for driving the development of the internet. That's a fundamental interesting shift, interesting development that I think could have profound implications for the way digital content and the digital economy develops.

As part of this and this is the last thing I'll highlight, it provides for the first time digital native property rights because what the blockchain does is it adds to an information layer, which is really what the internet was. It was way of communicating information, a settlement layer, meaning a way of recording who owns what, a way of recording who interacts with particular parts of Web 3.0. That settlement layer really is something unique. The fact that you can do it in a distributed way that doesn't rely on a central server is something that's unique

and allows a new version, if you will, of the internet to potentially come into being.

Jo Ann Barefoot: So say more about what the technology is and how it does that, the blockchain design and the tokenization. Maybe you can walk us through an example of how this works.

Jai Ramaswamy: Sure. To back up for a second, I'm going to caveat all this by saying that I am not a computer scientist. I've learned a lot of these things through the years, but I'm venture-

Jo Ann Barefoot: That might help you explaining it for us. Yeah.

Jai Ramaswamy: I'll try, what I think technical people have discovered. The important recognition, or if you will, that the important thing that Bitcoin actually created in computer science was the ability to essentially overcome the traditional architecture of the internet, which required trusted parties. If you think about the way communication and computer technology works, computers operate by something called state. When you are on a computer, it logs interactions of who you are and what you're doing on the computer, and that allows you to effectively program the computer.

The internet was a collection of computers that communicated with each other, but that state, the log of interactions between users and the computer was maintained on each of the individual computers or in a macro sense on servers, which are really large computers on the internet that communicate with each other. What the Bitcoin protocol in a sense published for the first time was the possibility that state could be maintained not on individual servers on the internet, but if you will, on a protocol layer of the internet itself, on a distributed layer of the internet itself.

So, you could now program natively on a distributed set of computers, because for the first time, you could maintain state at the protocol level because there was a way of recording information in a trustless and distributed way. In a crude way, what the blockchain does is it takes information and propagates it to all the computers connected to the network. So, that every single computer that's connected to a particular blockchain network, whether it's Bitcoin or Ethereum or whichever one you choose, maintains a copy of the ledger, if you will, the thing that you're trying to record, which is the single source of truth on every computer that exists.

There's a mechanism for coming to a consensus as to how and which pieces of information are recorded and get added to a chain of data blocks. That could only happen on a single computer before and then it was shared with other computers, but that single computer was a source of truth. Now, the network becomes a source of truth. Ethereum took that one step further and said, "Hey, if I can record who owns what, I could also program natively on the internet." That's what this notion of smart contracts that you sometimes hear about is

really about. It's about creating a distributed computer network. In some ways, that is what Ethereum did.

It created a distributed computer, a network computer that is comprised of individual computers connected to it, but is in fact bigger than any of them and uses the resources of all of them. The reason cryptocurrency is important is that digital tokens and there are unique ones for each of these networks are the way that you incentivize a distributed set of people contributing resources to this network and for people who use the network to pay those people who are providing those resources for the use of computing resources on the network.

So, the token becomes the economic value, if you will, that allows a distributed set of people who don't know each other, who have no reason to trust each other, to nonetheless engage in a community activity of maintaining a network, which before now was really maintained by private companies. Microsoft had its own network. Google has its set of computers and networks that it connects to the internet. For the first time, you can now have communities of people who own tokens, who participate in these communities through the economic exchange using these tokens. That is a new construct. We really haven't seen that before. That's what allows us to take it to the next level.

Jo Ann Barefoot: How do you distinguish Web 3.0 from DeFi, decentralized finance?

Jai Ramaswamy: Decentralized finance is one application of Web 3.0. In the same way, as I've described that more broadly, the tendency of Web 3.0 is to disintermediate platforms to introduce onto a distributed network information that was previously maintained on individual servers, the same thing is true with financial services. When you think of the way a bank is constructed, each of the banks have their own individual servers that they maintain private accounting ledgers on, that they maintain computer systems on. That's maintained and run by a financial institution, a bank, a brokerage house, et cetera.

In the same way that algorithms and a network computer can "replace" other types of digital services, it can also serve to replace what we traditionally consider the aggregation and settlement functions provided by financial institutions. So, if you take some of the protocols that have arisen, what they allow is for things like market making, which traditionally required a central book of business that was then mediated by a financial institution that maintained account ledgers by lines of code that essentially accomplished the same thing without human beings.

So, the idea is if you can program these networks, they can do some of the things that human beings and manual controls or even automated controls that had required human interaction and those could be replaced by automated functions. So, that's effectively what DeFi represents is the replacement of some functions that are performed in the banking system by human beings, by code, and if you will, the automation of certain financial services and the efficiencies and potentially the elimination of certain types of risks that come along with human beings in control of it.

Now, of course, you then introduce another set of risks when computer programs are in control of something and therein lies that regulatory issue. What do we gain by moving to a world that's disintermediate by computer programs and what potential risks do we have to address if that world arises? Again, with all of these things, these are relatively new and novel and therefore they're still in the early days.

Jo Ann Barefoot: Before we move to that, A16Z is investing in startups in this space. Can you share any examples of the kinds of use cases that are starting to emerge at the level of the entrepreneur?

Jai Ramaswamy: The first thing I'll say is and I should have said this at the outset, nothing I say is or should be construed as investment advice. Obviously, A16Z is in this business. I don't have investment discretion. I advise the company on legal aspects of the business, but I just want to make clear that that's the case.

Jo Ann Barefoot: You can also share other examples that aren't yours if you want, but bring it down to Earth.

Jai Ramaswamy: Look, here's the idea. There are a number of companies that are doing really interesting things, some of which we're invested in, some of which we may not be. But if you look at companies like a Filecoin for example, that's like Dropbox but in a distributed way, where the individual content owners have more control over the content they pose to a distributed network. That's an example of how a centralized service could be provided in a decentralized way. We're seeing the rise of, for example, decentralized social media where rather than content potentially being curated by a single company, it's mediated by a community of people who run that particular network.

We're seeing potential disintermediation of internet service providers in the form of decentralized ISPs. So, those are a couple of areas where we're seeing some interesting developments. As I said, I think that's an area where we'll likely see more. Obviously, DeFi has been something that there's been quite a bit of activity over the past few years, and now, we're also seeing other applications outside of the pure financial applications. The ones I mentioned are a couple of salient examples that I think those in the Web 3.0 ecosystem would recognize.

Jo Ann Barefoot: So one thing that has really been striking to me since this whole discussion emerged is that there's a very strong utopian dimension to it and a lot of people really arguing that Web 3.0 may be able to make things possible that have never been possible before. Part of that would be coming from the efficiency that you're describing, the ability to bring costs down, and therefore make all kinds of services more affordable and accessible, and then some of it also being driven by this notion of community control, decentralized control.

So, I'm a believer there's no utopia ahead per se, but also, that technology really can solve problems that you couldn't solve before you had the technology. Talk about that upside potential a little bit more. What might the world look like 15 years down the road if this vision really materializes?

Jai Ramaswamy: Sure. To be clear and I think this is our approach as a company as well, we try not to be utopians in the sense that the solutions we propose, and as you know, we've also been out there proposing regulatory solutions, are practical. We recognize that in this area, there needs to be practical things like regulation, which we'll get to in a moment, and that the kind of pure vision may or may not transpire. There will probably be steps along the way to get us there where what we know today is changed, but it may not be a utopian vision. It may be something that that's a practical intermediary from where we are today to where we end up tomorrow. That said, look, the internet has always been a space for inventors and dreamers.

On some level, if you had proposed to people that with a computer in your pocket, you'd be able to talk to anybody across the globe for free, that you'd be able to buy things that were only available in small flea markets pretty much anywhere you wanted to on the internet, critics may have described this as a bit utopian. They may have said that's dreaming and it seems not really practical. So, I just say that to say that the things that we think of as impossible sometimes become real life in terms of what we do today. I think that's the way we're thinking of it. The things that we can't imagine today all of a sudden in the future become possible. Let me throw out some simple ideas.

What I think we haven't talked about yet are things like self-sovereign identity, the notion that one can actually own their identity on the internet and own your own content on the internet in a way that others can't take it away from you. They seem like trivial examples today, but I'll give you some examples of those. Imagine a world where your identity could be tokenized. So, rather than what we do today, which is we all have to think about crazy passwords and ways of interacting with the internet that are vulnerable and insecure, we give that information over to these platforms. If they get compromised, then all of a sudden, all of our information, our passwords, and other information associated with it can be exploited.

But in a world where you could potentially tokenize that identity and only selectively disclose it based on what our program smart contracts and you have more control over the content that you have in your identity, that's a very different internet than we have today and arguably a more secure and consumer-friendly one than we have today. A world where an artist can produce something and it could be a piece of physical like a drawing, but it could also be music, it can also be books. People who produce things can produce them and gain direct access to the communities that support them, so their fan base or the people who read their books.

They can buy them directly from them and they can monetize that without having to pay intermediaries for it. It becomes actually viable for people to make a living out of this, where today, that's a little bit more difficult given the intermediaries who mediate that ability and who take part of the profits from it. These are a little bit further in the future, but to think about DAOs and these things called decentralized autonomous organizations, which are still in their infancy. But if you remember not too long ago, the ability of a community to

mobilize to purchase a copy of the Constitution wasn't successful. Obviously, there were some complications that arose, but the rapidity, the quickness with which that community was able to organize and raise money was eye-opening.

If you think about it, the ability to raise that amount of money to purchase something with a distributed community all over the globe hadn't really happened before in a way that we can think about it. So, these are just glimpses of what's possible. I hesitate to portray a picture partially because I don't know that it's possible. I don't know that anybody would've imagined that the web we have today would be a social media-dominated web if you were asking them in 1994 because a number of things had to fall into place for that to be the case. So, I think that there's just too much uncertainty to be able to go into it. So, that's why I like to give people glimpses of the world without being too prescriptive because I want to be humble about this. We don't know.

That can be a difficult argument to make to people to say, "Well, if you don't know, then how do you know it's going to happen?" My response to that is because we've actually seen it happen historically in the way that the computers and the internet have developed that this happens over and over again where you have a new technology, but you need other enabling technologies in order for it to achieve its full promise. So, without broadband, the internet probably would've been still borne in some senses.

Without cloud computing and what that allows and without the development of AI, a lot of what we think about today is probably something that couldn't have happened. So, there are some things that engineers still need to work out before this achieves that level of maturity and then the product market fit for the different types of things become apparent to people. So, that's why I'm a little bit loath to give you too much detail because I think that it's hard to say right now.

Jo Ann Barefoot: Yeah, I couldn't agree more. No one has the answers to this. One thing we do know is that talent and capital are both flowing into this section and there's a lot of very smart people who believe in the potential, even if they can't totally see where we're going. On the ownership issue and example that has stayed in my mind, I may have mentioned it on the show before, was the Economist article on DeFi from about a year and a half ago talked about the potential for a fashion model to keep some tokenized ownership in her likeness.

If you imagine that flexibility that the blockchain making it possible to lower the cost of information and records to a point where we could all have massive numbers of these kinds of financial arrangements without having to put our human hands on them to manage them all the time. The utopian side of this includes an argument that it might move us toward a more egalitarian society where people had more opportunity to own the fruits of their labor and be rewarded for it over time.

Jai Ramaswamy: I think that's right. I mean that's one of the promises here is that it potentially promises to increase competition, to increase consumer ownership, if you will,

and consumer protection. The one thing that still needs to be solved and I throw this out there because it's not fully appreciated yet, but privacy is a big issue that does need to be solved on these blockchains today. Although there's an undercurrent of hey, criminals use the blockchain, and therefore, it's bad. What I think law enforcement, what regulators have come to recognize that in their first incarnations, blockchains are actually transparent and you can track and trace whole hosts of economic transactions to their ultimate source. Is it perfect? It's not.

Are there other ways of upskirting identity? We've learned I think that there are. Nonetheless, it's a very powerful tool that doesn't exist when information is essentially privacy by default, which is what we have today. For better or for worse, your information is kept on private servers owned by private companies and it's a disaggregated. Therefore, it's harder for people to get access to who want to get access to it and they have to hack multiple servers in order to do that. But on a blockchain, if I can see everything transparently and I have your wallet address, I may not know your name, but companies have become very good at figuring out who people are based on their activity.

That's actually a world where you can see some of this as we go more mainstream becoming a problem. It can create cyber security concerns. It can create consumer protection concerns. So, for that world that you've laid out to exist, we do need more protections, if you will, for individuals, or else they won't have the trust to go out there and actually put their likeness out on the blockchain if they know that people are going to be able to know exactly who they are and what they do. So, there's some infrastructure things that do need to be built out and matured for that world to take place. Privacy is a very important part of this equation.

Jo Ann Barefoot: That's such an interesting insight because part of the argument for Web 3.0 is the potential to enhance privacy because as you said before, people could have more individual control as opposed to giving all your information to the big intermediaries and having it sold. But are you aware of emerging legal and regulatory thinking about how to solve the privacy problem in a Web 3.0 world?

Jai Ramaswamy: I think it's emerging, but I think it's actually something that needs a lot of development. I think that this will become an issue that regulators do really need to focus on because I think the principle control that regulators have been looking to in managing the risks of the blockchain and the industry as well has been blockchain transparency. That is the thing that has enabled law enforcement to actually have some fairly successful measures against even national security threats like the Lazarus Group or to trace and forfeit assets that were associated with major hacks. It has not been perfect, but it has been an important tool in the tool chest to allow the mitigation of the risks to a much more reasonable level that was thought possible.

But that said, that world creates problems for individual consumers and there are companies and technologies out there right now that are trying to solve this problem by creating tokenized identity, by creating the ability for selective

disclosure of your identity information as necessary through concepts like zero-knowledge proofs, where I can publish to the world that I satisfy a particular policy, say that I'm 21 years old and that I can go in and buy a beer at a shop or at a pub without disclosing my birthdate, my name, where I live, which is what happens today. You have to show your ID and it contains all that information.

This notion of selective disclosure is important because it could be that you could create mechanisms where regulators could get the information they want with the appropriate process while to the world at large, the transactions and the identity of individuals is private. So, that it can't be exploited by malicious third parties or by just puritan interests or even by corporations that want to exploit that data. But they'd first have to have a more robust way of getting my permission than they do today. That ability to square this circle that we've been trying to do for years is something that's technologically feasible. Companies are working on this. I will say that I think regulators have to catch up a little bit to the fact that there may be technical solutions to these problems.

Whereas before, the way we solve these problems was to impose an obligation on an institution to maintain information private and then allow that disclosure through the use of human controls and through the use of operational type of processes. We've seen that those processes and those controls have become porous over time as malicious third parties have become very good at exploiting them.

So, this potentially provides a better way, but some of our frameworks are going to have to adjust in order to accommodate the fact that there could be a technical solution to a problem that previously was a question of human controls and activity. I don't think that our regulatory frameworks have fully adjusted to it. There's a recognition of that, but I think they do have to adjust over time to permit some of these solutions to really start to occupy this space.

Jo Ann Barefoot: So let's really turn to that. I know we're going to start to run short on time here and it's so interesting to listen to you. Maybe recap for us what the primary risks are that we should be concerned about, and then let's talk about regulatory strategy and regulatory readiness to get the regulatory community to the point where they're going to do a good job with it. Recap for me what you think the primary risk areas are.

Jai Ramaswamy: Look, I think it's ones that the regulators have been focused on and it'll come as no surprise to anybody. Regulators are focused on the use of these technologies for illicit financial purposes. We're worried about consumer protection. How do we make sure that as this maintains or achieves more widespread distribution, that consumers have the information that they need in order to do this? There's been increasingly a worry of potential systematic risk if these tools and especially versions of them such as stable coins become more incorporated into our banking system. Although I think as Jerome Powell will even say either yesterday or the day before, this is an emergent risk.

We haven't yet seen that contagion, and in fact, we've seen the opposite that there seems to be cabins around where crypto is. So, it's an emerging risk as opposed to an existential risk at this point, but an important one. So, those three are the most important ones, I think, that are being debated around. It won't come as any surprise to anybody who's in this space. To me, one of the critical things that we do need to crack and I spent a career looking at some of these issues, are the issues surrounding AML controls, identity, and where we go there. That's where I think that there's some real potential if regulators are willing to engage in a really robust way with this technology where we can solve some of these problems.

Jo Ann Barefoot: A key, as you said before, is for regulators to think about the fact that there could be a technology solution as opposed to a traditional regulatory solution as part of the needs.

Jai Ramaswamy: That's right. Let me give you a specific example that's worth discussing and debating. Today, when you think about the way the traditional banking system works and the way we collect customer identity information and perform customer due diligence, every institution has an obligation to do that independently. If I'm Bank of America or if I'm Capital One, I have to go out, collect my customer information, and maintain it. If that same customer opens an account somewhere else, they have to go through that exact same process and provide all the same underlying documentation.

That has over time created potential risks to all of us because there's a bunch of information about us, redundant information that's protected by controls that have in a sense become porous increasingly, but creates what I think in the industry we call honeypots of information. It's a very attractive target whether you're a nation-state actor or whether you're just a criminal organization to obtain all that identity information in order to monetize it through phishing, through identity theft, through a whole host of other things, or to conduct espionage as we know that some state actors have done by obtaining this information on various people. The question is, is that really the way that we should go thinking about things like customer identity, and is there a better way?

One better solution would be to say, "Hey, what if there was a way of me providing all of that information and on a periodic basis to one institution and that institution was able to take that information and tokenize it in a way that it's not disclosed to the whole world?" But that if I then went to open an account at Capital One, they could say, "Hey, we know you opened an account at Bank of America. You have all this stuff available, and therefore, we can open an account for you knowing that your identity has been approved." That was always very difficult in the traditional financial system because of these siloed systems.

Move to Web 3.0 where let's say you're a crypto exchange and you do this, you can now send along with the transaction that tokenized identity in a way that the receiving party could know that you had passed through in a sense the gauntlet of this identity process with an institution. They could make a determination as to whether they trusted that process, whether they needed a

little bit more information, how they want to do. But in that way, your information is protected cryptographically. It is in a single place, but it's not available everywhere. That would be a better system. But in order to do that, we have to be willing to have a regulatory regime that recognizes the ability to share conclusions about your due diligence.

There's nothing, for example, in the Bank Secrecy Act that says you can't do it, but I think regulators have generally taken the view that that's not acceptable, that every institution has to perform their own. But if there was an ability to have a regulatory regime which was transparent in permitting that, that would be a much better, much more secure, much more beneficial to consumers, and it would allow potentially regulation to also accomplish what it needs to.

So, that's one example where this new architecture allows something that really wasn't possible in a previous architecture in the same way that it is possible today that could mitigate some of the risks while at the same time allowing the technology to develop natively. It's one small example and you can see other ways that technology could address risks, but that's a specific example.

Jo Ann Barefoot: Yeah, there's potential in this for win-win outcomes that make and knowing your customer rules do have impacts globally on financial inclusion where they normally do exclude people because it's too difficult or costly to do the whole process on them. It's an example of an area where we might be able to let more honest, hardworking people into the financial system than we do today-

Jai Ramaswamy: That's right.

Jo Ann Barefoot: ... if the compliance costs weren't so high. What other advice or thoughts do you have for regulators? Our listeners have heard me say a thousand times, regulators have the toughest job here. They have such a challenge in keeping up with all this technology change and walking the knife edge of allowing innovation but not allowing anything bad to happen. It's almost an impossible job. If you were sitting in a regulatory seat, what would be the main things that you would be trying to work on?

Jai Ramaswamy: The first thing would be to make sure that I have a granular understanding of the technology because it is shifting very rapidly. Even if you had knowledge of the way these protocols and where these networks existed three years ago and how they worked, a lot has changed a lot, and having real-time knowledge of those developments is really important. One of the things I worry a little bit about and others have spoken about this too, is that we have some rules in the federal government that make it hard for employees to actually understand these technologies.

For example, there was that recent ethics ruling that came out that if you own any crypto or digital tokens, you can't be involved in policy matters associated with it, which would be the rough equivalent of saying that nobody could own stocks in the government. That's not the right way to approach it. We have controls around how we think about some of these things, and there just needs

to be a more forward-leaning way of allowing people to experiment with these technologies so they understand what they're dealing with.

So, the number one thing is hands-on knowledge in real time because these technologies are increasing rapidly. The second thing and I would actually say this for the industry as well as for regulators, which is a certain amount of humility. We don't know where this is going. So, it's really important and regulators do have a tremendously hard job to monitor and understand the risks that are associated with these new technologies. They can't not do that. But I think it's important to distinguish between risks that are emerging and those have manifested themselves. Traditional risk management will tell you, you monitor emerging risks, you address existing risks, and then you look and see where you stand.

So, for many of these things, and I think again, just reiterating what I think a Chair Powell said of the Fed, we have some time to get this right. There's no reason to presuppose some of these things. Let's take the time to think about regulation that might be able to leverage some of these technologies that are inherent in Web 3.0 to come up with a better regulatory system, provide some concrete guidance to companies that they can start innovating in this area, and potentially be willing to be a little bit flexible in terms of their application in the current environment.

I know in the US, we don't like the notion of sandboxes. I think they can be very difficult for regulators, but I think regulatory regimes that have done this well and I include among them places like Singapore, places like the UK that have taken a little bit more of a forward-leaning approach and allowed a little bit of innovation to take place in reg tech will see huge benefits in the long term because they'll see entrepreneurs coming to this space and developing solutions. Whereas if you don't provide that space, you might find that there isn't a lot of incentive for people to try to build in this space, because they just don't know whether it's going to be accepted by supervisors, by regulators. So, that would be my general thing.

I tend not to give specific advice about specific policies because there's a vibrant debate going on there about all of that. I think that there's a whole host of good ideas on both sides about how to achieve this. I would let that take its way. But those are the areas I would focus on. The last thing I'd want to segue in before we stop is to just recognize that there's something bigger at stake here than each regulator's particular risk that they're managing. Each of which is really important. The SEC and the CFTC have to look at market integrity. FinCEN and OFAC need to look at financial integrity from a systemic perspective. Treasury and the Fed need to worry about systemic risks. These are all very important issues.

The overlying thing that I think we all have to recognize is that if the theory is correct and this represents another iteration of the internet, there's a geopolitical aspect of this to which all of this has to be balanced. I don't think it can be overstated, the extent to which the United States benefited by having

development of the original internet be shaped by US entrepreneurs, be shaped by US institutions, including government institutions, and the benefits that accrue to us economically. But also when you think about managing risks, the fact that we have internet companies in the United States means that law enforcement has people to go to obtain information when it's necessary.

What we want to avoid is the creation of this new iteration of the internet taking place largely outside of the United States. I think that brings an enormous economic but also candidly national security and national competitiveness concerns. I know some people poo-poo that and say, "Well, that won't happen," or "How can that happen?" But we're starting to see some of this. There was an interesting analysis produced by Electric Capital, another firm in this space that showed that software development in this area, while it used to be predominantly in the United States, is in fact taking place increasingly abroad and a minority of it is taking place in the United States right now.

That's an enormous shift, particularly for open-source protocol, which can be done pretty much anywhere. We need to be a little bit worried about that. The importance of the US in this area is not for ordained. It takes thoughtful, long-thought-out policy to do that. The consequences of it not happening means it's not just a question of money. I think that's what sometimes people think, but think about how many US values were embodied in that original internet. Are there problems with it? Sure. But freedom of expression, freedom of association, other types of values that are important for free and open societies came along with that internet.

The new internet that adversaries want to create, whether it's Russia and China on the one hand or others out there, is a much more closed version of the internet. You see some of this going on recently. There's an interesting battle going on in the UN's International Telecom Union, ITU, between the new president who could be an American or who could be a Russian, and who have very different views of what internet architecture should look like. That will lead to very different ways. I think we just need to recognize that many of those countries felt like they lost out in the battle for the first internet and they're positioning themselves not to lose out in the battle for this next iteration of the internet.

That's what's at stake and I think people should just recognize that there's a much broader thing here at stake that requires a balancing of all these different equities. So, if I'm a policymaker, I would say lift up the conversational level. Absolutely, every single one of these things, whether it's consumer protection, illicit finance risk, stability risk, all important, but there's an innovation risk that's here as well. We also have to think about inclusion. We also have to think about imbuing this new version with values that we care about and that our allies care about that are good for open societies.

I would put that into the mix and elevate the conversation so that it's a holistic conversation. We're not just focused on narrow applications of pieces of law to it. Ultimately, Congress and the administration are the right place for that, but I

think that that conversation needs to take place with a little bit more urgency than it's taking place now.

Jo Ann Barefoot: That is a wonderful note to end on. I was going to ask you about this and what you've shared I think is eloquent and thought-provoking. Where can people get more information about Andreessen Horowitz?

Jai Ramaswamy: Our website has a lot of information about us. I think that's probably the best place to go. I want to be careful. This is, again, not marketing to investors. I think you'll find a lot of interesting information about technologies. We have different content up there that can talk about not just Web 3.0, but across our portfolio companies as well as the things that excite us in the technology arena.

Jo Ann Barefoot: So I'm going to predict that this is going to be an instant favorite episode for our listeners. I have really enjoyed listening to you. I've learned a lot. So, Jai Ramaswamy, thank you for being our guest today.

Jai Ramaswamy: Well, thank you so much for inviting me. It was a real pleasure to speak with you today.