ICANN81 | AGM – How it Works: Blockchain Name Technologies
Sunday, November 10, 2024 – 13:15 to 14:30 TRT

YAZID AKANHO: Hello, everyone, and welcome to the How It Works: Blockchain Name Technologies session. My name is Yazid Akanho, and I'm the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions and comments will only be read aloud if submitted within the Q&A pod, mostly for the online participants. Interpretation for this session will include English, French, Spanish, Arabic, Russian, and Turkish. If you would like to speak during this session, please raise your hand in the Zoom, and when called upon, virtual participants will be given permission to unmute in Zoom. Onsite participants will use a physical microphone to speak. Please state your name for the record the language you will speak if speaking a language other than English and speak at a reasonable pace. I will now hand the floor over to Paul Hoffman. Paul, over to you.

PAUL HOFFMAN: Thank you, Yazid. Hopefully, you're all here for what's on the screen. If not, there might be something either more attractive or less attractive in a different room. So welcome. I want to start off by acknowledging many people here in the room because this is How It Works are here.

This is their first dipping their toe into the stream of blockchain name systems and blockchains maybe in general. This presentation is going to be—it's short on purpose so that there's plenty of time for questions at the end. This presentation covers two topics: blockchains and blockchain name systems. And the idea here is most people in the ICANN community who care about blockchain name systems also need to understand blockchains. So we're going to cover blockchains first and then cover how blockchain name systems sort of work and do that. But again, the focus is going to be for me to do this with brevity so that you can have plenty of time for the Q&A.

So let me start with some recent ICANN publications. Many of you know this, some of you may not, but because there is so much interest right now on blockchain name systems and people are hearing very different opinions and promotions for various name systems, there's been a lot of questions within the ICANN community about it. So the questions sort of come in two flavors. One is what are these name systems? People are used to the DNS. That's what we're doing in this building. But how are these name systems different? But then also, why are these name systems called blockchain name systems? So what are the blockchains?

So because of this, a couple of weeks ago, we published two documents. I'm the author of both of them, and the documents are in the OCTO document series. There are links here, if you get the slides, or if you just look in the OCTO document series, links on the ICANN website, you will find these are the two most recent publications. OCTO-039 is on Blockchain Name System Technologies and OCTO-040 is on blockchains. You can read them in either order. By the way, there

might be plenty of people who actually don't care about blockchain name systems but want to know more about blockchains. These documents are explicitly technical and neutral. So there's no promotion in them. And quite frankly, a lot of people don't like blockchain. So there's no disparagement either. They are meant to be technical and neutral. And the reason for this is both blockchains and blockchain name systems are constantly evolving, and so if you like something today, you may dislike it later when it transmortifies into something worse. Or the opposite might be true. You might say these aren't ready for real use yet but they may become so in the future. So these two documents, I totally would understand if you hadn't read them in preparation for this meeting. Feel free to read them during the week and such like that.

One thing I didn't put on this slide is I'm the primary author of both of them. The source material that I had for these documents was the documentation in the blockchain community and the blockchain name system community. That documentation from those communities is terrible, inconsistent, and things like that. So I put disclaimers in both of these documents saying I might have gotten it wrong. I mean, there might be facts in there that are wrong. So we're going to do a Version 2 of each of the documents in six months. I am eagerly looking forward to hearing if I made mistakes. I'm doing pretty well. It's been two weeks and so far no one has come at me with a pitchfork. But the reason why I'm saying that here is please also take a look again in six months. It will still be called OCTO-039 and OCTO-040. But I already know of some additions that people are wanting to help them understand, and I did find one terminology difference that just came to me the other day.

So with that, I'm first going to cover blockchains, and then I'm going to cover blockchain name systems. One of the funny things that I've discovered in doing this research on blockchains is that I come across people who say, "Oh, I know what a blockchain is. It's just a ledger. It's a database. It's got cryptography and such like that." Most of those opinions are wrong. And the reason that they're wrong is the blockchain ecosystem, very purposely, is trying to be as confusing as possible. And they're not doing that to hurt you. They're doing that to help themselves make more money. Totally understandable. This has happened in lots of parts of the Internet ecosystem in the past. For those of you who are as old as I am and remember the mid '90s, the exact same thing happened with web technologies around 1995. As a typical example, many people think, "Oh, blockchains are just a database." That's not true, and I'll go into that in the coming slides. Blockchains are much more than a database at the same time as being much less than a database.

The purpose of this session, the session that we'll be having on Wednesday, which I talk about later in the presentation and certainly the purpose of the two documents, is to try to reduce the buzzwords, and in doing so we're going to use different words than what the people in the blockchain communities are using. That's for two reasons. One is a lot of the terminology in the blockchain communities is purposely self-promotional. Fine. Again, those of us who remember the mid '90s remember the information superhighway. It wasn't a superhighway. In fact, it was a lot of barely paved roads. The same with a lot of the terminology they're using. But the other is, because it's not a well coordinated community, they use the same term to mean very different

things. So I sometimes picked one, sometimes I made up my own and said, “This is what it’s covering.” And to be super, super clear, most of the interest in blockchains is about finance, coins, and loans and such like that. I’m not covering that at all. That’s not what is of interest to the ICANN community. I’m sorry. That’s not what’s of interest to the domain name part of the ICANN community. It’s a wonderfully addictive topic. The more you get into it, the more you can get sucked into it. That’s not what we’re covering here.

The next few slides are on sort of the most important parts, technical parts of the blockchains. And the first is the ledger. We all know what a ledger is, even if we’ve never used one. We know that banks keep ledgers. It’s a sequential list of transactions. You can’t rewrite things. You can’t cut them out. Blockchains are based on the idea of a ledger. If you think of a bank’s ledger, normally it is this account moved $50 to this account, or this account took $50 away. That’s true for a lot of blockchain transactions as well. But some blockchains, notably ethereum, in fact, allow the transactions to be programs, and I mean like full blown computer programs, that involve things like, well, if this person who’s transferring this has too little money or too much money, do this, but if not this, write out this information over here. Things that are much more complicated that are in a bank ledger. But again, if you think about the ledger, even in the bank ledger world, you can’t look in the middle of the ledger and know how much someone has. You have to look through the whole ledger to figure this out. And in normal bank ledgers, an entry is not “Paul moved $50 to Yazid. Therefore, Paul’s account has this.” It’s just that Paul moved $50 to Yazid, and then you have to run through the whole ledger, keeping track of Paul and keeping

track of Yazid. So because of that, you don't just have a ledger, you also have a database.

This is even more important in the blockchain world, because all of these transactions might be complicated. For example, one of the typical transactions that you don't think about in a bank is someone opened an account with no money in it, and yet that happens all the time in the blockchain world. This account appears out of thin air. That is a transaction.

The nice thing about the way they do things in the blockchain world, as compared to looking at a paper ledger, is the rules are extremely specific and that if you take a copy of the ledger and you take a copy of the ledger and you run them through the same rule set, which is how you would do it, you will, will, will get exactly the same result. At that point, you can say, "What is Paul's balance?" And both of you, even though you did it on different computers, as long as you ran the blockchain to the same point, you absolutely will have the same answers. Having said that, some of these blockchains are giant, hundreds of millions of transactions. So getting the ledger takes a lot of time over the Internet. Running the ledger especially takes a lot of time. Remember on the last slide, I said some of these transactions are not simply move this number over here, but in fact, run this program. Now, all of the programs are deterministic. The programs don't have any random numbers in them. So again, 2 or 50 people looking at the same blockchain using the same transaction configuration machines will always come to the same answer. Their databases will look the same. That's super important because you don't want somebody saying, "I am

going to give this money to this person when I don't have that much money." Just like in the banks. But the blockchain people, because they were inventing this ledger 200 years after banks invented ledgers, were able to figure this out better. I just turned myself off instead of advancing the slides.

The next thing in blockchain technology—and this underlies everything and no one likes to admit this—is that the trust models between different blockchains are radically different. In a bank, when you look at the ledger, you trust that the bank wrote everything incorrectly and that it was only bank people writing things in. In blockchains, you have to trust who gets to write into the ledger, and once they've written into the ledger, did it really go in? So you might propose a transaction saying, "I transfer a bunch of my coins over to Yazid," but if you don't have those coins, you also are trusting that everybody who's processing the ledger is going to say at the same time, "You don't have enough coins to give them to Yazid so I'm going to reject that transaction."

In some blockchains, there are centralized authorities. But as you've heard, "Oh, blockchains are decentralized" is a very big word. Any acronym you hear in blockchain world that starts with a D, that's decentralized. You'll notice I didn't define decentralized here. That's because either there are no definitions of decentralized or they're 14 or 140. Different blockchains have different trust models for how decentralized it is. For example, some blockchains will let anybody offer, but to get into the database, there are certain rules. Others are very restrictive about who offers a transaction. Therefore, they don't have to be as restrictive on how to turn that into the database. This can

have a huge effect on how quickly the blockchain can be updated and how much literal energy—we're talking electricity here. These are all computers—it takes to add a transaction. And the sort of most common example of this is bitcoin, the one that sort of started all of this, has a very, very, very high electricity cost and entering transactions goes very slowly. Ethereum has a very low cost, and therefore the transactions can go faster. That doesn't inherently mean ethereum is better than bitcoin. It might to some people, especially those of us who care about future generations and climate change, but for the reasons that they exist, the trust models that they work on, each one has considered at the beginning of the blockchain how should they arrange this trust? Who should be trusted? Who shouldn't be trusted? How long does it take to be trusted?

For example, again, using the two that I just gave, let's say that a block of transaction comes into the bitcoin world, they don't trust that the people who are putting together the database don't trust that until nine more blocks have come and no one has said, "Get rid of that bad block." In ethereum, that list is much shorter. They will trust after five or six. Again, it's often the same people who are dealing in ethereum and bitcoin, but they are holding two different trust models in their mind. Now, as we go to talk about blockchain name systems, those are even different models. None of us want to wait an hour after someone has registered a name for it to appear. I'm sorry I can't say which ones are better or worse. It depends on why you're here and what you care about.

So this is a really brief description of the fact that not all blockchains are alike. Not only do they have different trust models, they're actually organized in different way. We're familiar with some of the big ones, like bitcoin, ethereum, those are called Layer 1. And that's not like actually a layer in the stack, it's how important are they. Layer 2 blockchains are much less important, but often much more flexible, and you will find that many of the proposals for blockchain name systems actually are using Layer 2 blockchains. And these Layer 2 blockchains to become more trusted, sort of send status information into the Layer 1s, so that you can be sure that as you're watching the Layer 2 blockchain, that it is aligned with the Layer 1 blockchain. And there might be data in layer. It gets crazy very quickly.

Then sidechains, which are actually better called independent blockchains stand-alone, are completely unrelated to anything. You can run your own sidechain, and we're seeing that some of the blockchain name systems are choosing to do either a Layer 2 or a sidechain, again, for different trust reasons. If you're a sidechain or if you're running a sidechain, you only need to trust you. Now, all of your users also need to trust you. And again, going back to the bank example, I bank at a bank that nobody here has heard of because it only has five branches where I live. I shouldn't say nobody. Some of you might actually be from the area that I live in. But I could easily have banked instead at a bank that many of you had heard of, many of you Americans had heard of, and I could even bank at a bank that many people across the world had. Very different trust model if I say to you, "Please send money to me at this thing you've never heard of" versus "Please send money this thing that you might have heard of and you might find

somewhere" versus "Please send me money to my account at this thing that you have heard of." So the types of blockchains are also sort of related to that idea where different trust models mean different things to how well do you believe this is going to exist in the future. The data in blockchains, because they're ledgers and because they're public, are always available forever. The trust model is do we really trust that all of the transactions that might have gone in could go in, and do we trust the transactions were processed successfully so that no one is cheating?

And then this is the last one. Many people have heard, "Oh, blockchains, they use advanced cryptography." Ignore that. Okay? Sorry, I'm going to get on sort of a little high horse here. But because my background is in cryptography, the cryptography that they're using is just fine, but it's also really not that interesting. It's no different than the cryptography we've been using for the last 25 years. Again, a lot of blockchain promotion is to people who don't understand what's going on. Again, if they were using bad cryptography, I would certainly be here telling you that they're not. They're using perfectly good cryptography. It's fine, but it's really not interesting. Now, having said that, because there's just so much money getting poured into the blockchain ecosystem, there are a bunch of very good cryptographers who are trying to work on new stuff that might differentiate one blockchain from another. It hasn't come to fruition yet. They've got some interesting ideas, but they either take an immense amount of memory or time to run. They might get better in the future, but for the blockchains you're talking about today—and it's fine if you don't understand cryptography, by the way. I totally understand that. If you want to learn about cryptography, come on talk

to me afterwards. There's some really good books on it. But if someone says to you blockchains are better than such and such because they have better cryptography, not the case at all.

So now let's switch out of blockchains so that we can get into—now that you have a basis for understanding, what are these name systems being on? Let's talk about the technologies themselves. Because every blockchain name system gets to make its own rules, it's impossible to say this blockchain compared to this blockchain has this advantage or disadvantage. They get to make their own rules at the beginning, but they get to change the rules at any time, just like you open up a restaurant that says Chinese food, you can sort of transform that into Chinese and Thai food, if that's what it seems like your customers want. You don't even have to change your name. Or you can change your name and still serve Chinese food. That's all just fine. Blockchain name systems can make these rule changes whenever they want, and it's even easier for them to do it than, say, the global DNS, which is the global DNS is changing the rules very slowly. All the old rules apply. We're coming up with new ones. But because the blockchain name systems are self documenting, it's really hard to find out at any given moment what are the rules in this blockchain name system, in this blockchain name system. So, because the blockchain technologies that they're using are also not well documented, if a name system says, "We are using this blockchain," and it's one that you've never heard of, that's like again me saying to you, "Send me money at this bank you've never heard of." It might be fine, but you might even have a hard time finding which bank I'm talking about because my bank, unfortunately, has different banks in different states in the United States. Last time I

checked, five different states have banks called Bay Area Credit Union. I mean, there's Bays in a lot of states in the United States. So that's a very common name. The same is true with blockchains. Because you don't know what is the trust model of this blockchain, you don't know how trustworthy is the underlying, much less and as we get into the actual technologies that you care about.

So everything I've talked about so far is just how do you trust it? Now let's talk about how blockchain name systems actually deal with names. Again, that's why we're here at an ICANN meeting. So the first thing that we think about in the global DNS is what gets resolved when I look up a name? And for those of you who've taken the DNS 101 classes, and there are more today, the How It Works for DNS, the normal thing that you resolve when you say icann.org is you want an address of a host, like an IPv4 address or IPv6 address, the normal thing that you get when you resolve a blockchain name, they call it a wallet address. It's not a wallet and it's not an address, it's an account identifier, and it is the account identifier of the blockchain account that created the name. It makes perfect sense. That's what is most useful in the blockchain world. When you say to somebody, "I want you to transfer me money," instead of having to remember a very long string of digits, which is the hex value of my public key and such, you can just give a name. That's very different than the global DNS where you can get an address, you can get a text, all of these things what you've probably heard. So at the very start, blockchain name systems are quite different with what is the primary use case. The primary use case for blockchain name systems is blockchain addresses.

Now, note that I've been saying that there are lots of blockchains. There are literally thousands of blockchains. Your address on one blockchain is going to be different than your address on another. So when you resolve a name, you also need to know which of my many addresses, if I happen to have, say, for example, an ethereum wallet and a bitcoin wallet and some other odd name wallet, which one is going to come to my name? And that's something that the blockchain name systems are still grappling with.

The other feature that many blockchain name systems promote as one of their big advantages over the global DNS is that all of the transactions that went into that name are public. They're stored permanently in the blockchain. So if you want to know who created this name? When was it transferred to this other person? When did it expire? Does it expire? Some blockchain name systems never expire. Others do. How did data change in it? That's all public information that is easy to find. It's not easy to digest, but it is easy to find, and that's something that we don't have in the global DNS. We have the opportunity to do it. That is any registry, any registrar, can make a ledger and make it public. There just hasn't been much demand for it. Within the blockchain world, because ledgers are so important, so central to decentralization—sorry, that sounded funny—so important to decentralization that this is a very, very prominent feature for them.

And wait, there's more. So one of the other features that is considered a big positive in the blockchain name systems is that you can buy your blockchains and such with the native coins, with ethereum, with bitcoin. And that's somewhat inherent because, again, your account ID,

your wallet address, is simply the thing you paid with. It's almost like saying that somehow if you, for example, bought a second level domain under a common gTLD with a credit card, that your credit card number was not only public but it was permanently associated with your name. People in this room might have a hard time understanding that totally, whereas people in the blockchain community, that's what they want. They want to know that somebody purchased this with this and maybe maintain it. And again, some blockchain name systems are buy once and own forever because that's the way that the blockchain works. Let's say that you create an account in bitcoin. You create a bitcoin account, you somehow use normal money and get some bitcoins and it's in that account. Again, that account is a public key, and you are holding the private key, and you lose the private key. Tough. Not only do you not have access to the account, that account lives forever with your final balance in it. And it is hard to measure exactly, but recent research shows that over 70% of the accounts in bitcoin are dead. Some of them have more money than I have in them, but even ones that have a small amount, someone said, "You know what? I don't care about this anymore." But that account is still alive. So if there's a blockchain name associated with that account, that name will always point to that account forever. In some name systems, in other name systems, they act like the global DNS, you have to renew every year.

Okay. The last two bullet points here are probably what's going to cause a lot of the questions, the mic line. A lot of the blockchain name systems—if it's a name system, it has to have some names. What do you base the names in? Some of them are using alt TLDs that are strings that are not currently delegated. So eth is a popular one, wallet, crypto. Lots

of names that seem associated. Those are not currently in the global DNS, and there are big questions about how to do that. So if you have a name such as under .eth, I have phoffman.eth, just because there aren't that many Paul Hoffmans in the world or who care about this. You, in order to find out the data associated with it, have to ask a resolver that knows what eth is. And there's just one resolver that's run by that name system. For .wallet, there are two different name systems with different names under .wallet. So if I had phoffman.wallet, I might have one over here and one over here. In fact, they might point to different addresses and such like that.

So many blockchain name systems use these alt TLDs, and then that opens up plenty of questions about what will happen in the future. What if they're allocated? What if they're not allocated? What if there are two or four or seven blockchain name systems with the same name? How does someone know how to resolve? So very messy. And that's part of the interest in these is because the global DNS has been so well organized. I mean, really, we're talking like no problems at all for well over 35 years. Sorry. I see people in the audience who are younger than that. But because we are so used to the stability, the blockchain name systems are like, "We don't need that. We want decentralization," which might include a lot of chaos, but there will be some value to the chaos in their minds.

Then the last bullet point here talks about how some of the blockchain name systems, in fact, want to coordinate or integrate or affiliate all sorts of verbs here with the global DNS by using names that are, in fact, already in the global DNS. They might do that by linking an actual global

DNS name into their blockchain. They might sell them over here first, then move them here first, here first, then there first. That's a smaller market now, but it's also very interesting because now we're taking names that we are familiar with and also having an alternative resolution somewhere else.

Right now, we're used to all global Domain Name System. When you say, "Please resolve this for me," you know how to find a resolver. Now, different resolvers have different capabilities. Some of them do DNSSEC validation. Some of them don't. Some of them purposely lie to you. There are plenty of resolvers out there that, for example, if you give them a name that is to a site or an address that you don't want to hear about for various political or gender or whatever reasons, they'll lie to you. You've asked them to lie to you. That kind of thing also exists in the blockchain name world because names are names, right? If you can register something here, you might be able to register it there. They also allow names that aren't in the global DNS. How does that work? All of these are quite open questions.

I think I hit the timing pretty much exactly right. Okay, very good. So we've got time for questions and comments. Yazid will be doing this. We have a mic line here, and you will remind them how to do this. But I want to point out, if you say, "How do blockchain name systems work with such and such?" I've got to warn you, they'll do it differently. I cannot speak definitively about any of them. And even if I could, they would make me wrong a few months from now.

Also remember that the blockchains themselves are very different. The trust models are very different. So if you have a question about

blockchains, why does someone do something like this? I can't answer why questions. For one thing, I'm not active in those communities. But also, those communities purposely change what's going on. Again, we're used to a nice, stable, global DNS with slow changes. Some of the changes are originated here in ICANN. So if you ask a question about the global DNS today versus 10 years ago—many of you have been coming to ICANN meetings for 10 years or more—those answers might be different but there would be an evolution. Within the blockchain world and within the blockchain name world, anything 10 years ago to now would be wildly different for various reasons. So with that, Yazid?

YAZID AKANHO: Thank you, Paul, for this nice presentation. I think we have enough time for questions, almost 40 minutes, which is quite fine. So as a reminder for those who are in the room, please, we have the mic which is in the center of the room. If you are not going to speak in English, please state your language. Of course, remind all of us your name before starting your intervention. And for those who are attending remotely, please use the Q&A for the questions. So far, we have three questions online, but I will probably hand over to the room first if there is anyone who would like to go on.

PAUL HOFFMAN: Someone sat closer to the mic, so you get to go first.

SAM YILMAZ: Thank you, Paul. I appreciate the presentation. Sam Yilmaz here, investor in blockchain space. OCTO-039 and 40 are trying to be neutral and informative. But if you were to say, "Here is how the standards that are proposed by and endorsed by ICANN could leverage blockchain," in your opinion, if you had your way, how would you like to leverage this new technology for maintaining better transparency, for intermediating transactions? I'd love to hear your vision for it.

PAUL HOFFMAN: Thank you for that question, but I'm going to disappoint you. I'm part of ICANN staff. My opinion doesn't count. It's the opinion of the community that counts. There are certainly things that the community might pick that would make me cry a little bit, but it doesn't really matter. Seriously, these are community questions of how things will—and this is one of the reasons that I wrote OCTO-039 and 40, it wasn't for staff. I mean, part of it was for staff because staff also needs to understand these things coming, but they're for the community to be making these decisions. I don't know when community will make these decisions. And to go specifically your to your question of how can things maybe be integrated and such, we have 1300 current gTLDs under contract. Is that number right? 1250? Some number. Thank you. Everyone's going like this, so that's okay. Those may choose to start having some blockchain interactions. Some of them might radically switch to a blockchain. Some of them might want to just touch gently. Some of them might not want to. Then we have the Next Round, which there are plenty of other people talking about right now. How will these affect the Next Round? What does the community want for the Next

Round? And it may be that the Next Round is coming too soon to make the kind of policy decisions that you were asking about, and so maybe the folks in the Next Round will be just as affected by how does one be a gTLD and then switch into or switch toward some of these technologies?

I want to be honest here. This is an opinion. Well, it is an opinion. It's prediction. I'm terrible at predictions. I have a long stretch of bad predictions from the past, but my prediction now is what's going to actually lead the policies is you're going to see some ccTLDs, not under contract to ICANN, doing some things and there will be great research coming out of those ccTLDs. I hate to say it, but half that research will show how bad things are, and half the research might show how good things are. When I was writing my documents, when I was trying to be neutral, it wasn't like I could write straight down. Basically, I was trying to anger both sides in an equal amount. And I think that we will see some of that from the ccTLD community. Again, please don't ask staff for opinions on things like that. I have opinions. I'm not saying I don't have an opinion, but it's your opinions. It's the community's opinions and all sorts of the community's opinions that will drive this for ICANN.

YAZID AKANHO: Thank you, Paul. Let's have the second question from the room. Oscar, over to you.

OSCAR GIUDICE: My name is Oscar Giudice, Uruguay. I'm going to speak in Spanish. Thank you, Paul, for your presentation. It was a very enlightening

presentation. If I have a system working with ciphering A and B system, and I have two names, the same name registered in both systems, and I can also have the same name in the global DNS. Do we have to modify all the resolvers? I mean, we have to start from scratch.

PAUL HOFFMAN: Too confusing there. Thank you. I apologize for not speaking your language. I'm one of those Americans who speak English only, and I apologize for that. Very good question. We don't have to do anything. We are encouraged to be as wide as we can here, but we don't have to do anything. If someone comes with an alternative name system to us, it is up to them to show how it might improve the global DNS. It is up to them to show how it should stay separate from the global DNS, or be integrated. ICANN and most of the Internet already knows what it is doing, and then new ideas pop up. And so you said you have a resolver over here, Resolver A, Resolver B. That's your choice and we might find a way to make everything work together, we might not. So, as a very good example, you said you have a name over on Resolver A and a name over on Resolver B. We don't even know if A and B are working together correctly, much less with the global DNS. So I believe that the answer to your question of do we have to update everything is no. But it's followed with we really might want to. There may be things coming in these blockchain name systems that are attractive. Now, I say that, and remember I said there are numerous blockchain name systems already, you said you have one in A and one in B, some of those will be better than others. And when I say better, I mean better for the ICANN community, better for the global DNS as we know it. Hopefully, we only

spend our time in making those changes with the better ones, but that means we have to understand them well enough to know whether you're A or you're B, in fact, is the better one, or maybe A and B are both good, and C, D, and E are not ones that we want. There's a lot of work to be done here. But again, it's up to the blockchain name systems to come to us and say, "This is how we want to do things. This is how we're doing things ourselves. Does the ICANN community want to participate? Do they want to participate in the ICANN community?" And it's very early days for now. So thank you.

YAZID AKANHO: Thank you. Let's have the last question from the room and then head to the online participants. Over to you, please.

UNIDENTIFIED MALE: Thank you. Thank you for your presentation. I have to admit I haven't read OCTO-039 and 40, so I apologize if you already addressed what I'm about to raise. My name is [inaudible]. I represent the security community, in particular, law enforcement. Speaking English. Yes. I hope, I hope. Basically, part of my job is to think about future risks, security risks. And of course, when it comes to technology, a bit complex for the average person as this one. I also wonder. Because even the current system, what we have, there are some issues when finding out who's behind registration. So I would be curious to know in your in objective view this technology, do you believe it poses some risks in that regard, or is difficult to say at this stage? Thank you.

PAUL HOFFMAN: Yes. Next question. Oh, sorry. Thank you for your question but I'm going to change your question a little bit. Do I think that blockchain name systems propose different risks than the ones that we are already facing? And the answer is absolutely yes due to their decentralized nature, where, in this case, decentralized means no one takes responsibility. You can set up a blockchain name system very easily. You can make it free for people to register. That is, at least in ethereum, you can set up a contract that says, "I'm a blockchain name system. To register a name, you must pay your own fees for doing this." I'm going to run a resolver over here, or anyone can run a resolver, and then just walk away. A contract on a blockchain does not require anybody to do active work. So if someone has done that, or let's say they set up a legitimate blockchain name system, their venture capitalists abandon them. They run off the runways, the term we use in English for venture capital funded things that fail, that contract is still alive. So there is definitely much higher risk of name systems that even if they originally intended to do good things around preventing malicious names, preventing salacious names and such like that, they may go away and their contracts are still just running off into the future. So that does pose a lot more risk.

Also, any time that you try to integrate to systems of any sort, certainly two name systems, there is a difference. You can't have two things actually be identical. You can work at it but you can't actually have two things identical. That difference, even if it's small, causes more risk, in my opinion, is going to be huge because the global DNS has 30 years of norms. Blockchain name systems have three. And for all of the profit motive in the global Domain Name System, especially the ccTLDs, that

is balanced against the fact that we have registries and registrars, which there is no equivalent registries and registrars. So we are very familiar with one set of risks which you consider to be too high. That's fine. Adding in more that we don't understand, the fact that we don't understand the risks is a new risk itself. So yes, it is much higher. That doesn't mean everything is going to go to hell when we do it, but we don't know. And again, that's absolutely going back to the earlier question of what is my opinion of how do we put this together? I'm one person, my opinion would be to do it as simply as possible. You are a large community. You've thought about these questions over time so you are much better able to do that risk analysis than any individual.

YAZID AKANHO: Thank you, Paul. Let's switch now to the online questions. We have a couple of questions from Fouad Bajwa. Sorry for this. So let's start with the first one.

"A special thank you to Paul for putting these documents together. We do lack concrete documentation on the topic, and these are helpful. Has Paul considered about putting together a proposal for a community working group on Blockchain Name System Technologies?"

PAUL HOFFMAN: Thank you for the question. No. Again, it's not up to staff to start organizing these things. This is really a thing from the community. I can absolutely believe that there are members of the community who will want to have such a working group, and I can absolutely believe that three quarters of the people in the room after hearing my presentation

would run away screaming from such a working group. Because the topic is so fluid, it would be hard to have a working group that can fix something in time and such like that. Again, if the community wants that, great. Tell staff or go through the Board, however that goes. But no, we staff are not setting up anything like that at this time.

YAZID AKANHO: All right. Thank you, Paul. Next question, still from Fouad. "How do you deal with the alternate TLD names? How are they recognized across the DNS if they are not being managed through IANA?"

PAUL HOFFMAN: Excellent question. They're not. They are not because they are not managed by IANA. Because all of us use normal resolvers, we don't see them. Each alternative name system has its own set of resolvers, its own ability to have resolvers. Some of them have agreed on resolver, so two different alternative name systems might use one resolver, so someone asking question can get answer from to them. The solutions are all over the map. Again, we're used to the global DNS. We know how to spread out resolution. We know how to spread out the authority of name servers. But for all of these others, they don't appear in the DNS at all. So if you ask a global DNS resolver about them, you will get no reply. Having said that, some global DNS resolvers are also starting to answer for some of the name systems. So, in fact, you might send a query to a global DNS resolver and for one of these alternative names and actually get an answer back. But what kind of answer are you getting? If you asked a query to the global DNS, you probably wanted an IPv4, an IPv6

address back. What you're getting back is an account name, a wallet address. It has nothing to do with it. So balancing all of these, very, very difficult. Even if we come up with agreements between ICANN community, the global DNS, and some of these alternative name systems, resolution is going to be really, really difficult. We know how to resolve things in the global DNS. The standards for doing that come from the IETF. Everyone follows those standards. Those standards have not yet come from them.

YAZID AKANHO: Thank you, Paul.

PAUL HOFFMAN: We're getting a mic line again. However you want to do it.

YAZID AKANHO: Okay. Let's just get one more question from online and then get back to the room. So the next one to you, Paul, is "What is ICANN's position on blockchain based domain system and the integration with traditional DNS systems? Are there any initiatives or discussions within ICANN Org as well as community to address the compatibility or regulation of blockchain based domain names alongside the existing TLDs?" More or less the previous question.

PAUL HOFFMAN: Not only is it a bad idea to ask staff about policy, the last person you want to ask is a techie, right? I'm not in the Policy Team. I'm not in the

Legal Team. However, having said that, I feel somewhat comfortable in saying that ICANN currently has no policy. Okay. No one from the Legal Team jumped up so I'm good. Will we have a policy? Will a policy be developed? I don't know. One possible answer is, well, yes, of course, that the community is going to do work on this and such like that.

Another possible answer is, "Oh God, no, this is too difficult. We're already too busy on other things." Another possible answer is "Why bother?" The blockchain name systems have their own ecosystem already. They are doing things for their world. The global DNS is doing things for our world, which is significantly larger and more stable. But it may be that our answer is we're not going to bother to do that because it's just fine. And again, ICANN has no policy to criticize the existence of any name system, regardless if it's based on blockchains or whatever. We have an antique document called ICP-3. Did I get that right? Or is it IPC-3? ICP? Thank you. Thank you. Early in the week for me. Yes, right. That was developed in the early 2000s, like 2002 or whatever, which says that we don't have policies about other name systems. And that makes good sense because there's a million name systems. We're used to name systems that look hierarchical and have human names in them and such like that. Postal Codes are, in fact, a name system. They're sometimes depending on the country you're in. They're harder to read or easier to read, but those are name systems, and ICANN has no position on postal codes. ICANN has no position on how one names your children. And in fact, many countries do have rules about how you can name your children. Blockchain name systems fall into that extremely large category of things that we don't have a position or a policy on. That can change. The community can choose to change that.

You, the community, may or may not, depending on what you do, that will make my work harder or easier. Not hinting here. But we don't now, and I believe that if the community embraces this, it will take a while. Because, as we've seen today, it's a fairly steep educational curve before we get to start to talk about the meat of things. Sometimes, in that situation, people might get exhausted and walk away. Other times, people might say, "You know what, the global DNS is moving too slowly. They've got great ideas over here. Let's really work on this." But that's up to you all.

YAZID AKANHO: Thank you, Paul. So let's get back to the room now. But just a quick reminder for those attending remotely, questions and comments put in the chat will not be considered as such, so please put them in the Q&A. Thank you. Over to you.

BERTRAND DE LA CHAPELLE: Hi. My name is Bertrand de La Chapelle. I'm the executive director of the Internet and Jurisdiction Policy Network. Two things, basically. One, thank you very much for holding this session, for producing the document and for raising an issue that I think has been in the minds of a certain number of people in this community and at large. The compatibility and the articulation between different naming systems is an issue that is a recurring element. You're absolutely right to contrast the well-organized system that we are familiar with that has 30 years of existence that is very hierarchical with the very unruly.

PAUL HOFFMAN: Let me stop you right there. It's wonderful for us to say well-organized. I just spent the week at the IETF. Nobody other than the people in the DNS world would call what we have well-organized. So it's all relative.

BERTRAND DE LA CHAPELLE: It's absolutely relative. Yet it is a different space from as you described, the environment of the new naming systems. Yet, I'm a little bit… After the congratulations and I'm glad that this discussion is starting, and I hope it will continue in other ICANN meetings. I'm a little bit ill at ease with the position of extreme stepping back that you expressed because I think it points towards the real question of the role and the positive role that the ICANN staff can have. The alternative is not between we have a policy and we have no policy. The role of the staff and the helpful role of the staff is to help frame problems. And if you take people outside of this community, how we collectively going to explain in very simple term that "I don't know, a .xyz is the DNS but a .eth is something completely different." I'm sorry it looks the same, and we need to be very clear about the articulation.

So there are two tracks. One is what can ICANN provide to this community externally? Do we have lessons to share to the external community in terms of the way they will want or not to organize? Maybe some blockchain naming systems will want to not adopt the way we have done it, but some of the lessons or some of the dangers that they want to address and others won't. But vice versa, I think it is necessary at least to have a serious discussion on what are the potential impacts in particular in terms of confusion for the users. I mean, we spent a lot of time in the New gTLD Program about confusing names in the DNS

and we wouldn't address the risk of confusion in the other? That makes no sense for me. So I just would like to encourage us to not be in a 01 type of thing where it is either just the community or just the staff, or it is just a policy or no policy. We need to work together in organizing the discussion on how to frame this. And I believe, personally, that the staff has a huge contribution to make on both the technical part and the policy part to say, "Without taking position, this is how to frame the problem. Where can we help and how can we be impacted?" So I would encourage not to set up a working group, that's not the tool, but to have a structural process so that at each meeting of the subsequent ICANN events, we have a dedicated structure. Let's not replicate what we've not done with the DNS abuse discussion.

PAUL HOFFMAN: Well, that was a bit of a zinger at the end. Fair points. And thank you. I work for the Office of the CTO. There's a big T right in the middle, or not in the middle, just to the right of the middle of that. Staff should be driven by the community, even to start the things that you said. Now, we don't need a lot of a push. So I did these two documents, pretty much because I had heard confusion in the community and such like that. It wasn't that the Board said, "Hey, staff, you need to do this." There are probably people on the policy side who feel similar to I do, but to, as you say, talk about the policy parts.

Framing is very important. Framing is almost impossible in this case because of the amorphousness of the fact that there are many blockchain name systems and such like that. I'm hoping that OCTO-039 helps frame questions that the community might ask an individual

blockchain name system saying, “Of these five or six features, where do you line up? Are you going to change in the future and such?” so that that kind of framing that you’re concerned about happens.

Now I’m going to go into opinion again. I don’t believe that the blockchain name systems care that much about this. They want to see what they can do, and if it takes too much work on their part, they aren’t interested. I would be thrilled to be wrong, and I believe that one of the differentiations we’re going to see in the blockchain name community is some of them will have better interactions and more consistent interactions with the ICANN community and others will be much more “That didn’t work. Oh, there’s a squirrel.” That’s fine. That’s how they get to do it. So if you want framing in the policy side, don’t ask the techies. Having said that, there are plenty of people, as you know, in the policy side of staff that can do that. I don’t know which communities would need to ask them and such like that, but I think that would be valuable, like you say, is to have those discussions.

YAZID AKANHO: Thank you, Paul. I must admit, some of those questions are quite hard to answer, but let’s move on. Welcome, Peter, and please go ahead.

PETER: Thank you so much. Peter for the record. I guess it hacks part of my question, and I still want to bring you back to the policy aspect and from your own opinion because you say that you cannot dictate and to tell the community what to do. But what do you think are the policy conversations that we need to have? If you think we cannot frame that

because we need to start discussing this, and how does that affect the ICANN, the trust environment, the multistakeholder environment? What are things that we need to start talking about?

The second question would be, when you talked about the trust model, the different blockchain has different trust model. From your own opinion, what are the trust models that you're considering? Because you're speaking as an expert here, and you're telling us these are the old things and all these blockchain technologies does not have the right cryptography. So what are the things that we need to start talking about here, and where do we need to start from?

PAUL HOFFMAN: Thank you for some very difficult questions. I'll start with the second one, which is, what would be my preferred trust model? I've been doing this for 30 years. I want a trust model that's like what I've been doing for 30 years, which is very centralized, very controlled, there's an IANA at the middle, and all of this flows out. Having said that, I started dealing with this before there was an ICANN. So once there was an ICANN, and all of a sudden there was a community dictating a lot of this, my first reactions in the early 2000s was, "Oh God, this is going to get more complicated." Later on, my reaction was, "Oh, good. This is going to get more complicated," meaning that there was a larger number of voices having a choice in the trust model. The trust model that I started with was Jon Postel. The trust model that I evolved into in the near term was—Jon's dead—there's this thing called ICANN coming. It's going to be chaotic. I'm very concerned. But the ICANN community, to me, proved that they could work through the chaos towards significant

policy procedures that came out to something, maybe it takes too long. Probably everyone here would agree that all policies take too long. But they come out with actual community policies.

So, to me, that's what I would want to see in a blockchain. And a few of the blockchains have that, but they're not the popular ones. Having said that, a blockchain name system gets to choose which blockchain they use. And again, some of them are picking their own blockchain. They're making their own rules. I would trust one that made rules that I already like more than I would trust one that is making rules from the "Let's throw all the cards in the air and see what happens." I want to give credence, though, to there's a lot of people who like the let's throw all the cards in the air and see what happens. Those are different communities than what we have here.

So then going back to your first question, and again, coming back to where you are at, when do we do this? I'm not the person you want telling you how you should spend your time. As you can see from the presentation today—and by the way, we have another presentation late in the week. The slide didn't get in the slide deck. I'm sorry. But on Wednesday morning, every year OCTO has a thing called Emerging Identifier Technologies, where I'll be going through some of this again. But we also have a representative of one of the blockchain name companies, and we also have a lot of time for Q&A. If you're interested in this topic, I would certainly come on Wednesday, not to hear me again, but to hear the Q&A line from all of you again. But I'll throw in a little kicker here. The blockchain name company that is being represented on Wednesday has a model that if you don't know it might

surprise you and might actually make you feel good. Policy evolves here better than in almost any other organization. Well, better than, I would say, any other organization that I'm in. Almost the IETF comes up to that standard. But again, you don't want somebody at the front of the room saying you should spend your time on this or you should spend your time on this. You all get to pick. I know you don't like to hear that because many people will then, as I say, run away, but that's true of all the policy decisions. So choose your battles, pick your time. If you choose to step in to the blockchain, name description, I assure you, you will be supported by ICANN staff, not just me.

YAZID AKANHO: Thank you, Paul. [Brad], let's make a quick deal, please. Can you keep your question for the coffee break? I will be happy to invite you. Let's just take the questions online. Okay? Okay. We still have like three minutes to go.

The first one is "Is there any mention or analysis in this report about the blockchain DNS query time and response time? If not, are there any such plans in the future? I believe that the DNS query performance is what we are more concerned about."

PAUL HOFFMAN: A technical question. My favorite. I'm going to disappoint you. No, there hasn't been. There's been very little research on this at all, and part of that is because of the way that resolution happens in these blockchain name systems. Even though they say decentralized, it's a very centralized name resolution. So any number that I give you from here

would be different than a number from here. I believe that will change over time and that they will get much better query response times. But no, we haven't done any measurements. Because the measurements I've seen so far, I didn't trust. Not that I didn't trust the researcher. I didn't trust the measurability.

YAZID AKANHO: Thank you, Paul. Another hard question. "Do you think it will be a good idea to shift from the current global DNS system to blockchain even if it's a slow progress, considering that the current global system took a long time to evolve and has systems in place?"

PAUL HOFFMAN: Thank you. That's a hard question. It's not hard because I know the answer. The answer is no, I don't want to see it. Apparently, someone else agrees with me. But there have been other technology shifts on the Internet, not in the DNS, which I also didn't want to see, that ended up actually being beneficial. So patience is a virtue. So if this shift that you're asking about actually happens, I may not want to see it, but I should be patient and see whether it turns out to be a good change or not. I'm not going to help but that also doesn't mean that I'm going to hinder.

YAZID AKANHO: Thank you, Paul. With the support of translation services, please let's get these last two questions. "Even at this early stage, do some innovations and components of blockchain naming systems that can

help the global Internet community or enhance the global DNS as overseen by ICANN even as a complete integration could be hard to picture at this stage?" I think the question is to you.

PAUL HOFFMAN: Again, thank you for the question, but I'm the wrong person to answer. That's for the community. I can certainly see it go either way, but it's the community who gets to choose here.

YAZID AKANHO: Thank you, Paul. And the last one, "Blockchain—is it about registry or DNS itself?"

PAUL HOFFMAN: Excellent question. We've run out of time. But again, thank you for good technical questions. When you have a name system that is so fundamentally different than what we're used to in the global DNS, questions like that, like what is a registry? Who does the resolution if it's not the registry? Where do you find that? That changes from blockchain name system to blockchain name system, and it will continue to change. If this community says to the blockchain name community, "We're willing to talk to you but we want you to act more like us," and they're interested, they will act more like us and they will make technical changes or policy changes around that. It's going to be a two-way conversation.

YAZID AKANHO: Thank you, Paul. I think we are done. Just as a reminder for those who are in the room, there is another session on Wednesday, which was mentioned by Paul already, Wednesday, 10:30 am. You can go through the scheduler and you can see them. Thank you, everyone, for your participation and your great questions. As a reminder, the presentation is also available on ICANN meeting schedule on this session page. With that said, we are the end of the session. And thank you, everyone. Bye.

[END OF TRANSCRIPTION]