KATHY SCHNITT: Welcome to the SSAC Evolution of the DNS Resolution Work Party teleconference on the 6th of July 2023. I'm not sure. Barry, Russ, or Andrew, over to you.

BARRY LEIBA: Yeah. Actually, I think Andrew here. So go ahead.

ANDREW MCCONACHIE: I think it's me. Yeah. I forgot to mention this on our earlier call, Barry and Russ, but I won't be here next week. So I just wanted to let you know that I'll find a replacement. It'll either be Steve or Danielle. But I wanted to let you know. I'm sorry forgetting to tell you earlier.

BARRY LEIBA: Yeah. And the week after that, we will be canceling because that's going to be IETF week. Do I have my weeks right, or are we off?

WARREN KUMARI: I think that you're off by a week.

BARRY LEIBA: I'm off by week but I will be—no, actually, I won't be traveling because it's San Francisco. So, some of us will be traveling. I don't know whether it's a good idea to can it for the 20th and the 27th or just for the 27th.

WARREN KUMARI: I will be gone early because I leave on the 15th because of NOC team.

BARRY LEIBA: Right. And I imagine Geoff will have to be traveling. Geoff, are you going to the IETF meeting?

GEOFF HUSTON: I am but I'm going to be traveling early. So I'll be actually around in the Bay Area across that period.

BARRY LEIBA: All right. Well, let's currently plan to keep the meeting for the 20th.

RUSS HOUSLEY: I will miss Barry on the 20th.

BARRY LEIBA: Okay.

[TARA WHALEN]: I will as well, but you should all go ahead.

BARRY LEIBA: Well, we might still cancel for the 20th. But let's not decide that yet. But we'll definitely cancel for the 27th.

ANDREW MCCONACHIE: Okay. Noted.

BARRY LEIBA: Okay, carry on.

ANDREW MCCONACHIE: Okay. So into the document. So we're starting off today in the Definition section, because one thing I've noticed writing Section 5 is that this definition we had of alternative naming systems as any naming system other than the global DNS used by computers to map from a name to an IP address is really not true. It's not how we're using the term. So we changed it to blah, blah, blah, mapping to from a name to a network service. And I just want to run that by the work party before I hit Merge. Going once, going twice. Okay.

BARRY LEIBA: So we were all ready to have Russ and me cut off rat holes, but glad we didn't have to.

ANDREW MCCONACHIE: The rat stayed above ground. So then on to Section 5 and this is where we're discussing the various animals in the zoo. We spent a lot of time talking about this paragraph last week. The consensus was that this paragraph should get deleted, and then there should be a little bit for each section on this kind of thing. Like, what is it dependent upon with the Internet and the DNS and that kind of stuff, and how is it different? So I left this paragraph here, but we'll just look at each individual

section. And then if we're happy with that, we can go ahead and delete this paragraph.

So first off on mDNS, I added this final sentence in green here. Going once, going twice, considered merged. Onto Tor.

I did a bit of research on how Tor works. I think we talked last time about how it uses the SOCKS proxy or SOCKS protocol. So it does use SOCKS for clients to connect to the Tor network, but then internally in the Tor network, it uses just TLS connections between Tor nodes. Besides the onion naming stuff, that's essentially its only dependency on the Internet. IP, obviously.

WARREN KUMARI: Yeah. I think that going down the rat hole of does it use IP is likely a false thing, right?

ANDREW MCCONACHIE: It does.

WARREN KUMARI: All computer system naming things rely on electricity as well, or computers or silicon. At what level does one decide where we're drawing a line?

ANDREW MCCONACHIE: Right. Atomic chemistry.

WARREN KUMARI: Indeed.

ANDREW MCCONACHIE: But I think it's important to point out it has no dependency on the DNS.

WARREN KUMARI: Yes. I agree. We appear to find agreement.

ANDREW MCCONACHIE: Is there anything wrong with these final three sentences?

WARREN KUMARI: I don't know because I'll have to have a look. I don't know what is used in the TLS protocol and the certificates that they present to each other if there's DNS names there. I don't think it matters. But I think that we need to be careful that people don't get the wrong impression.

GEOFF HUSTON: That was my question too. Because Tor, peel it all away is a bunch of point-to-point links running TLS, right?

ANDREW MCCONACHIE: That's the idea.

GEOFF HUSTON: And if you've got no dependency on the DNS, then the point-to-point links are based solely on manual configuration with IP addresses at either end. And I don't know what TLS does in terms of other party authentication, or it doesn't use any. If it doesn't use any, that's a problem. If it does, then it's IP address-based. Where do the certificates come from? I'm a bit confused at that point.

ANDREW MCCONACHIE: Yes, that's true. I guess there's no certificate authority in that sense. And I don't think there's any SNI included in the Client Hello message.

WARREN KUMARI: I do remember I read the Tor or .onion write-up where it came up, but I've managed to page it all out. Actually, we say both SOCKS v5 and TLS use IP addresses as their underlying identifiers. Is that strictly true? This seems like something that Russ might have a view on or knowledge thereof.

ANDREW MCCONACHIE: Having recently been forced to go read the SOCKS version 5 RFC 1928, I can tell you that SOCKS version 5 is the one that implemented IPv6.

WARREN KUMARI: Tor-spec.text. I guess—

ANDREW MCCONACHIE: Do you want to see if it requires … What do you want to know about—

WARREN KUMARI: What goes in the certificates that they use? I don't know.

RUSS HOUSLEY: I don't know either.

ANDREW MCCONACHIE: What you want to look for is Client Hello.

WARREN KUMARI: Components other than the common name is just sit in the identifier. Okay. So your self-signed certificates—

RUSS HOUSLEY: Okay. So you get no security.

WARREN KUMARI: Yeah. The common name of the subject or issue of the certificate ends with a suffix other than .net. Why other than .net?

RUSS HOUSLEY: It doesn't matter. If it's self-signed, we know where—

WARREN KUMARI: Yeah. Why is that one special? Weird. So yeah, this is going to require some more.

ANDREW MCCONACHIE: Okay. Should I leave this unmerged for now? Do you want to investigate this, Warren? To investigate if—

RUSS HOUSLEY: If you just want to say TLS with self-signed certificates, I think we're done.

ANDREW MCCONACHIE: Okay.

RUSS HOUSLEY: That means if you want to be a node, you can make yourself a certificate.

GEOFF HUSTON: Look, the point is it's not a name-based certificate. It's an address-based certificate. And everything else follows but it was just merely sanity checking your there is no relationship with the DNS at all assertion. And I think this bears it out.

ANDREW MCCONACHIE: Okay.

GEOFF HUSTON: Self side. Sorry.

RUSS HOUSLEY: The point of a certificate is to bind to public key and the name, you ain't got one.

WARREN KUMARI: Your name is the certificate, right?

RUSS HOUSLEY: Your name is the public key. Go.

WARREN KUMARI: But it does kind of question like how do nodes find and connect to each other? Anyway.

ANDREW MCCONACHIE: There are these so-called master nodes that know about all Tor nodes. When you fire up a Tor node, you have to contact one of these master nodes and tell them that you exist in your IP address.

WARREN KUMARI: Okay.

ANDREW MCCONACHIE: I don't know that much about it. But I know that's part of the deal.

GEOFF HUSTON: Oh, so random routing attack, here I come.

RUSS HOUSLEY: No, you have to convince the master.

ANDREW MCCONACHIE: Who runs the master?

GEOFF HUSTON: About my IP address.

RUSS HOUSLEY: Oh, right.

WARREN KUMARI: Let's not go down the hole. Well, you also have the certificate, the public key to be able to present. But anyway, sorry.

RUSS HOUSLEY: A self-signed one. Come on.

WARREN KUMARI: Well, no. But your identity that you're attesting to is the key, right? So when you say, "Hello, I am 27314856," you signed something with that key. And by definition then, you are 2347516, whatever number I just

made up. Your identity is what you present as your key and then you sign something to prove that. We might be talking past each other.

ANDREW MCCONACHIE: It doesn't matter for the paper. The Tor network is notoriously suffering from DDoS attacks probably for these kinds of reasons.

Anyway, on to ENS. So I switched ENs and unstoppable domains around it. Unstoppable domains used to come before ENS, but that didn't make any sense because unstoppable domains is based on ENS. So put ENS first and then copied a lot of the text from the Unstoppable section into the ENS section and probably change a bit. So please reread the section on ENS, Section 5.3.

WARREN KUMARI: I would put the second sentence first.

ANDREW MCCONACHIE: Yeah, it's what it is.

WARREN KUMARI: Yeah.

ANDREW MCCONACHIE: Yeah, that just works a lot better.

WARREN KUMARI: You might also want to move the second paragraph further up, right? Why does it exist? But anyway.

GEOFF HUSTON: I understand at this point, you're using a term called Ethereum address. What is an Ethereum address? If you're not going to explain it, why are you talking about it?

WARREN KUMARI: Yeah. I guess maybe we could solve that by simply saying, an Ethereum address is an identity.

ANDREW MCCONACHIE: Well, it's this but it's buried down here.

WARREN KUMARI: Yeah. But they're not just a string of hex digits. They're a hash of your key. So they are your name and identity.

GEOFF HUSTON: So stated but implied, an Ethereum address is—next paragraph—a cryptocurrency wallet address. Is that right?

WARREN KUMARI: An Ethereum address or an Ethereum name service address.

ANDREW MCCONACHIE: Ethereum name service. Maybe this sentence isn't actually true, because now I'm starting to wonder about Ethereum addresses as well. Because they definitely are cryptocurrency wallet addresses but ENS can also be used for IP identifiers.

WARREN KUMARI: Yeah. You can put whatever you would like.

ANDREW MCCONACHIE: In the Ethereum address.

WARREN KUMARI: Yeah.

ANDREW MCCONACHIE: So maybe we just need a sentence here saying what an Ethereum address is.

WARREN KUMARI: It seems like we should. An Ethereum address is a hexadecimal address derived from the last 20 bytes of the public key controlling the account is what the Ethereum address is. So it's an encoding of the last bit of the public key.

ANDREW MCCONACHIE: How do you explain that to our audience? Can we just say hexadecimal addresses that represent—

WARREN KUMARI: We can just say an Ethereum address is the cryptographically unique identifier of the—yeah, it's hard to put it—

RUSS HOUSLEY: In what? I'm waiting for this.

WARREN KUMARI: Yeah.

ANDREW MCCONACHIE: Unique identifier for an address on the blockchain?

WARREN KUMARI: No, because an address on the blockchain is a term that people often use to mean a particular block of the blockchain.

GEOFF HUSTON: Russ just said it was a portion of a public key.

WARREN KUMARI: Yeah, that's not bad. Do you think—

GEOFF HUSTON: Russ said it, not me.

WARREN KUMARI: Actually, maybe we should flip this around with Ethereum is a decentralized blockchain. Yeah, I keep starting sentences like knowing what I'm going to say. And then once I engage my mouth, my brain stops working. I should have that on a T-shirt.

GEOFF HUSTON: If I get this right—and I'm speaking informally from what I'm seeing here because I have not read Ethereum. Ethereum maps common use names into public keys or portions thereof and it uses a blockchain ledger system to effectively ensure verifiability and uniqueness. Is that's what's going on?

WARREN KUMARI: Sort of. The problem is that there's Ethereum and Ethereum name service, right? So Ethereum is a blockchain which allows smart contracts, or is specifically designed to allow contracts. One of the smart contracts that is implemented in Ethereum is a system that allows you to look up a human readable name into the output of the contract. And the output of the contract is often a public key, like your Ethereum public key, or an IPFS URI, or whatever else you want to put in it. Does that explain it?

GEOFF HUSTON: If I said I think so, I might have said more than I mean.

WARREN KUMARI: Okay.

GEOFF HUSTON: I can see kind of what you're getting at.

WARREN KUMARI: Think of Ethereum like Bitcoin, except that instead of the system representing currency, it represents a small program that can be executed. And one of the well-defined small programs that can be executed as a function that maps geoff.eth into a piece of data. And that piece of data is often used to store your wallet address or an IPFS link or a piece of text or whatever you like. So Ethereum is basically it's a distributed blockchain but the whole purpose of it is to run contracts, and the contracts can do many different things. One of the defined contracts, which I think is like 791 or something—I don't know the full name, but it's got like something, something dash 791—is a contract which will map human readable string like geoff to whatever you want to put in there. I want to see if I can find a—

GEOFF HUSTON: So many questions, but this is not the time nor the place.

WARREN KUMARI: So, so, so difficult to understand so much of the blockchain and ETH stuff because it doesn't seem to be written in a way that's easy for people to understand.

ANDREW MCCONACHIE: It's kind of half technical and half manifesto.

WARREN KUMARI: "The Ethereum name service is the distributed, open, and extensible naming system based on Ethereum. The job was to map human-readable names like alice.eth to machine-readable identifiers such as Ethereum addresses, other cryptocurrency addresses, content hashes, and metadata." So I will paste this into the chat.

ANDREW MCCONACHIE: Is that from their website?

WARREN KUMARI: It is indeed from their website, which is why it actually sounds sane. And it didn't have me being like, then the word and the thing. Yes, this is from docs.ens.domains.

ANDREW MCCONACHIE: Right. So I could just include that as a blockquote beneath this paragraph. I don't want to plagiarize their text without calling it out.

WARREN KUMARI: Yeah. Having it as a quote seems reasonable.

ANDREW MCCONACHIE: Okay.

WARREN KUMARI: But it seems like a good introduction, maybe towards the top.

ANDREW MCCONACHIE: I don't want to open this section with a—I mean, I'd like to have our own explanation, and then beneath that, the blockquote. I'm okay with that. I don't want to just use their explanation.

WARREN KUMARI: Okay. I thought we could expand upon their explanation. To me, their explanations much clearer than ours. But we can also—

ANDREW MCCONACHIE: Sure.

WARREN KUMARI: ENs has similar goals to DNS but different architecture blah, blah, blah, blah, blah. ENS Manager app. This is where they're going to want me to log in, and I've got no idea how I log in to any of my ENS names.

GEOFF HUSTON: Look, I think this resolves my issue of dangling unresolved references to terms, right? Because it all started with what's an Ethereum address. And I think this now resolves that.

WARREN KUMARI: I put a link to an example of an Ethereum name. There's a pretty webpage here which provides a friendly UI. But that's wkumari.eth, and you can put whatever the hell you like in it.

ANDREW MCCONACHIE: But it's just resolving the DNS.

WARREN KUMARI: Well, this is a webpage that speaks Ethereum on the back end, and DNS or not DNS on the front, HTTP on the front. I pasted it so you can read it.

ANDREW MCCONACHIE: Anything else? Let's see. So we'll skip down to here and folks can read the rest of this section.

WARREN KUMARI: Well, ENS maps names too that is not to Ethereum addresses. ENS maps names too like if you look at the link I put in. I've got a txt record and a description and a notice and a keyword and a telegram name.

ANDREW MCCONACHIE: Wow. Ah, okay. I see.

WARREN KUMARI: That's what I was trying to explain by.

ANDREW MCCONACHIE: So this sentence is just wrong, though.

WARREN KUMARI: Yeah. So ENS maps human-readable names to—I think technically it maps them to text. And if the text happens to start with URL colon, then they think that it's a URI. And if it starts with description, then it's just random text.

ANDREW MCCONACHIE: Let's try this.

WARREN KUMARI: Yeah. Even up above there, ENS's job is to map human-readable names to machine-readable identifiers such as Ethereum addresses, cryptocurrency addresses, blah, blah, blah.

ANDREW MCCONACHIE: So we can just delete this whole paragraph? Is that what you're saying?

WARREN KUMARI: I think you're the primary use seems like a reasonable one, because those are generally what it is used for. Also, once a user reserved a domain and ENS, it can be used to reference fairly much anything. We do say that it's often used for all addresses. A couple of attributes which I think are worth noting about ENs and many of these blockchain-based

domains is your—let me try this differently. With DNS or something else, your ability to manage the name is because you log in through a registrar web interface and then you can change things. With ENs and Bitcoin and a bunch of other things, your authentication is purely the fact that you have the private key.

So I have wkumari.eth because I bought that using a wallet. And that generated a key for me and sign stuff. I no longer know which wallet that is or where that wallet lives. So, unless I spent a bunch of time and effort, I have lost access to managing wkumari.eth and nobody else can really administer wkumari.eth realistically.

ANDREW MCCONACHIE: So, by that you mean you cannot change what—

WARREN KUMARI: Yes, I cannot sell it, I cannot transfer it, I cannot change any of the records in it. And neither, realistically, can anyone else. And at the moment, wallets are generally very, very, very hard to use. Over time, they might get better. But I tried really hard when I bought this name to make sure I didn't cock it up and I have cocked it up by not knowing which—

ANDREW MCCONACHIE: It's a bit like losing your password to your registrar account. But in that case, you could actually call a registrar.

WARREN KUMARI: You can click Forgot Password. Over here, I think that my password is in MetaMask. I mean, the other problem is your wallet lives on a device, generally. So my MetaMask wallet lives on my phone. If I lose my phone, I am screwed.

ANDREW MCCONACHIE: So I think this is an important distinction. So I should really add text on the differences between a user management, right, the difference between having a registrar and having a key that you have to keep in a wallet which is really easy to lose.

WARREN KUMARI: Yes. It just thinks I have a password, I have no idea what my password is. I can erase my current wallet and then I've lost everything that's tied to it. Seemed like everybody's heard the stories of people who mined 7000 bitcoin and put it on encrypted thumb drive thing and then forgot what the password to that is or had a bitcoin wallet and threw away the hard drive and can never access their money ever again. The other interesting thing about blockchain-based domains is you basically buy them. And once you bought it, it's yours forever. There's no—

ANDREW MCCONACHIE: There's no maintenance. There's no yearly fee.

WARREN KUMARI: Woo. I guessed the correct password for my wallet. I can now, in theory, administer that domain again, maybe. The usability aspect around all of the stuff is really bad at the moment, though.

ANDREW MCCONACHIE: There's no administrator that can help you. I mean, that's the key thing. There's no one actually in charge. It just sits there and it's just gone forever.

GEOFF HUSTON: That's the major point here. Once you remove the manual ledger keeper or the intermediary registry, registrar, etc., from the system, then the relationship between the identity space inside DNS and you is based on solely your knowledge of your private key. And no third party can alter that. Be they government, hacker, or anyone else.

WARREN KUMARI: I mean, that's kind of—

RUSS HOUSLEY: The group of seven, right?

WARREN KUMARI: Right.

GEOFF HUSTON: Except the group is seven.

WARREN KUMARI: Which I don't know if they have ever used that power.

RUSS HOUSLEY: Put something really illegal out there.

WARREN KUMARI: Somebody has actually embedded an incredibly—and when I say incredibly low resolution, it is nothing that you can actually make anything out from. But they have embedded what could be considered CSAM in the bitcoin blockchain system as a proof that this is an issue.

GEOFF HUSTON: You've lost me. CSAM?

WARREN KUMARI: The CSAM has a full copy of the Bitcoin chain potentially.

ANDREW MCCONACHIE: CSAM is Child Sexual Abuse Material.

GEOFF HUSTON: Okay. Because someone's been provocatively naughty and it's now unerasable.

WARREN KUMARI: Same like the patent lawyer who has a patent on fire and the wheel and the number.

RUSS HOUSLEY: Which proves something but not—

WARREN KUMARI: It proves that the patent system is busticated.

RUSS HOUSLEY: Right. It's a human invention. It's flawed.

ANDREW MCCONACHIE: Okay. Well, you've given me good writing prompts here. If I add that text about how big of a pain this is for users, but how some people like that because it proves that it's censorship resistant, are we mainly good with this section?

WARREN KUMARI: I think maybe there's some point that you can say something, something's Zooko's triangles something, something again because—

ANDREW MCCONACHIE: Well, I was thinking about that. Do we want to map all of these things on Zooko's triangle?

WARREN KUMARI: Maybe. I'm conflicted. I just made the suggestion. So yes, but also, there are some issues in that. Zooko's triangle talks like human-readable, and I think this is partly human-readable but also human-usable without—

ANDREW MCCONACHIE: The original paper on [inaudible] claims that they'd beaten Zooko's triangle.

WARREN KUMARI: I'm sorry. I clicked on a thing in my wallet app and it decided to go crazy and stop talking.

ANDREW MCCONACHIE: I think bringing up Zooko's strangle here, we'd have to bring it up for all of them. So I'm very hesitant to do that.

WARREN KUMARI: It seems like we could though, right? The DNS is human-readable but not decentralized.

ANDREW MCCONACHIE: Right. That's in the Zooko's triangle section. That's the example we give. DNS with DNSSEC validation and signing is human-readable and secure but not distributed.

WARREN KUMARI: Ethereum naming service is human-readable and distributed and censorship resistant. Does it solve all three? I don't know. Maybe we should because that would require thinking.

ANDREW MCCONACHIE: It's the mapping of the actual name, the string. It's the resolution process you go through, which determines whether or not it's secure or not. That's where these blockchain naming things break down.

WARREN KUMARI: But they are secure. ENS is the string wkumari.eth can only be controlled by a single private key. So the person who holds the private key is the only person who can make the changes to the record that you see there. It is signed with the private key.

ANDREW MCCONACHIE: Then they have all three. They've squared the triangle. That's the claim they make in the original paper.

WARREN KUMARI: Yeah. And somewhere actually, I've made—where do I have it? Somewhere I have a picture where I created Warren's square as a riff on—here we go. Warren's triangle. I knew I had it somewhere. Can I quickly share? It will just take a second.

ANDREW MCCONACHIE: Do we need to? I'd like to continue to move on. We've only got 20 minutes left. I mean, I think it's a larger question about whether or not we want to talk about Zooko's triangle in here at all.

WARREN KUMARI: I can e-mail it around. Basically, I added on policy acceptable because—

ANDREW MCCONACHIE: The question I have for the work party is how much faith do you guys want to put into Zooko's triangle? I mean, it's an interesting toyish way to think about this, but I don't know if it's really rigorous. But I'll leave that to you guys.

GEOFF HUSTON: I think it's a distraction to some extent. At this point, you're simply saying why these things are worth including here and what their property is. I thought their property, particularly in the case of ENS, and moving on to unstoppable is this removal of intermediaries that can remove or alter a client's relationship with the client's entry into this mapping world. ENS substitutes ledgers and bookkeeping and so on with you own the private key, it's yours forever until the group of seven don't like you. I thought that was the extraction of why this is worth mentioning. And it's a good point.

ANDREW MCCONACHIE: Gabriel, go ahead.

GABRIEL ANDREWS: I just have question, guys. Sorry. I'm mostly a lurker whenever I have the opportunity to join these calls. But I was just curious, has there been any discussion of what happens if the Ethereum servers that the ENS is built on were to again fork? I don't know if the CNS stuff came after the latest fork or if there's been one since or at least lay a significant fork. But I know that in Ethereum's history, there have been some rather prominent forks way back when. But I'm, by no means, an expert. I'm just curious whether or not if it were to occur again, what would the impact be?

ANDREW MCCONACHIE: We don't talk about forking. I mean, we say this as far as governance. But we could mention forking here as well. I mean, you can fork the codebase and suddenly you have a new blockchain, right?

RUSS HOUSLEY: That's the thing. It's a blockchain. Is it really a fork or is it just a different blockchain?

WARREN KUMARI: The thing that holds the name .eth, and whatever the other big one .eth uses, is specifically a smart contract on the Ethereum name service. So if somebody stands up something else based on Ethereum and there are actually a bunch of other Ethereum ones, there's some test blockchains so that you can put stuff on a test one without having to pay all the gas money, they don't have the smart contract for .eth. Someone else could

make another one and claim to be ETH, but then that's just a simple name collision. You get back to the—because ETH is registered virtually anywhere.

GABRIEL ANDREWS: So if I'm hearing you Warren, then the registrations made on ENS will stay with the original version of any potential future fork? There's no way to automatically replicate them over to whatever the new fork is?

WARREN KUMARI: I believe so.

ANDREW MCCONACHIE: If we define ENS as the smart contract, that's true.

WARREN KUMARI: Up to the top. Sorry, go ahead.

ANDREW MCCONACHIE: Do you want me to go back up? Well, I was just saying if we define ENS as the smart contract, then that's true. You can't fork that smart contract unless you are four of the seven people agreeing to do so.

RUSS HOUSLEY: Or you compromise your private key.

WARREN KUMARI: Yes.

ANDREW MCCONACHIE: Compromise four private keys, if there's seven.

RUSS HOUSLEY: No. If I get Warren's private key, I can go change this blockchain entry as long as I pay the gas, right?

WARREN KUMARI: Sure.

RUSS HOUSLEY: Okay. That's what I meant.

ANDREW MCCONACHIE: But I was thinking more systematically for the whole blockchain.

RUSS HOUSLEY: Now that I know Warren has a wallet, his becomes more interesting than the rest of you.

WARREN KUMARI: Not only do I have a wallet, I also have $26 of ETH, 26 whole dollars.

ANDREW MCCONACHIE: It may be worthwhile talking about forking. I don't know if it's—I'll think about that.

GEOFF HUSTON: Why? Part of this issue is that all these alternatives have strengths and weaknesses and so on and so forth. I thought the aim here was to highlight the fact that there are other ways of doing this and each of them focused on a particular aspect of the current system that they want to change. This is the paper about Ethereum. I mean, it's a paper about the evolution of name resolution and Ethereum does it in a certain way, full stop. I think that was all we needed to say. If you say much more, you get trapped up into saying the same detail about all of these and that's kind of turgid and I'm not sure it really makes the point we're trying to get to.

ANDREW MCCONACHIE: We're rabbit holing on ENS. So let's move on to Unstoppable which I've shortened because it's just based on the Polygon blockchain platform, which is inspired by Ethereum. In an effort to just not repeat a whole lot of text, I just say like ENS. So please read that single paragraph on Unstoppable.

WARREN KUMARI: Actually, I think you should say, "At the time of this publication, this list includes that." Because I believe they've got way, way, way, way, way more. I think that they're close to 100 at this point.

ANDREW MCCONACHIE: Those were the only ones on their website, but maybe it's changed. But I like includes, that's safer.

GEOFF HUSTON: I just added a clarification.

WARREN KUMARI: No, because they've also got .nft, .dow, .blockchain, .x—I don't know if those understood—.polygon.

ANDREW MCCONACHIE: Polygon is not listed.

WARREN KUMARI: .bitcoin, .nft. I mean, these things are basically free for them to create. So they're creating them like candy. Okay.

ANDREW MCCONACHIE: I mean, the implication of them using all these names is left to the reader, right?

WARREN KUMARI: Yes.

GEOFF HUSTON: Isn't your point they're not delegated in the root zone of the DNS?

ANDREW MCCONACHIE: But they're not anywhere in IANA.

GEOFF HUSTON: Right. But you all just said they're note in the special use registry.

ANDREW MCCONACHIE: Nor are they in the root zone? I could say that.

GEOFF HUSTON: Yes.

WARREN KUMARI: Okay. That's a good point.

GEOFF HUSTON: It is a matter of speculation, of course, were any of those names to be delegated into the root zone how a system that wants to straddle both would operate. But that's a dog of a different breed, it's a different problem.

ANDREW MCCONACHIE: We're going to resolve this. So we're happy with that. Onto GNS in our last 13 minutes. I think I have to admit, Geoff, that this sentence that I originally had an issue with, I think it's actually correct. And I had a good conversation with Russ and Barry about it earlier. The idea of a search

hierarchy does not really exist in GNS. After reading their Internet draft, I view it more as C structs with pointers in them. Because they can have one struct pointing to another struct, they can actually experience resolution loops. So in that sense, it's certainly not a hierarchy. I think that sentence is fine now.

WARREN KUMARI: Direct confrontation with the incumbent mode of names. The grammar, that feels weird. The sentence just after that.

ANDREW MCCONACHIE: It's rather confrontational.

WARREN KUMARI: But also it's really hard to parse. I'm guessing, Geoff, you wrote that, didn't you? Your brain is bigger than mine.

ANDREW MCCONACHIE: But this is different.

WARREN KUMARI: My brain, it hurts.

ANDREW MCCONACHIE: We could just incumbent mode of names. Can we just say the DNS?

GEOFF HUSTON: Yes, you could. Did you see what I'm trying to say?

WARREN KUMARI: Yes.

GEOFF HUSTON: The innovation is everyone said you can't do flat because it doesn't scale in the namespaces near [inaudible].

ANDREW MCCONACHIE: I went and read a bunch of stuff on GNS and tried to think about things that might be interesting that are also different. I think the big difference is to have this concept of a start zone where if you and I have a different start zone, we basically have different namespaces.

WARREN KUMARI: One of the things that they are very pleased with, or when I say they, I mean, Christian Grothoff, is he believes that what you resolve www.example.com to and what I resolve www.example.com2 can be different. And that that is a feature, not a bug. You and I are in complete control of how we think name should resolve and we should be able to have different understandings of names. He seems to view names as more like bookmarks or keywords or something similar and less of things that are inherent in the desire of the person running the content.

ANDREW MCCONACHIE: Another way to look at that is to just say, "Well, GNS describes a protocol and not a namespace." And if we have different start zones, we'll have different resolution for names. But if we have the same start zone, we'll have the same namespace. And then that's not true.

WARREN KUMARI: Except that they've also got their whole pet name concept which allows you to randomly overwrite parts of the tree with other parts if you think that that's something that floats your boat.

ANDREW MCCONACHIE: It's true. They're very proud of the fact that they do not support denial of existence. So there's nothing like NSEC. It's clear that they do not like the zone walking and they consider a zone walking to be a bug of DNSSEC. They've actively worked around that by just not ever denying existence cryptographically.

WARREN KUMARI: They're an interesting set of folks. I mean, some of them are more reasonable than others, right? I guess, I'm being unkind.

ANDREW MCCONACHIE: I found their discussion of portable governance model is really just lacking. I couldn't stomach it.

GEOFF HUSTON: Well, isn't the essential issue around that second aspect, depends on where you start from, that the other innovative part of GNS is to actually allow individual users to effectively shape the identity space that they wish to use independently of others? In other words, there's no coherency of the namespace that exists outside of individual users. Whether that's a bug or a feature, as Warren said, it's kind of—

WARREN KUMARI: Isn't that the same thing for any of the alternative roots that were created? You can choose the alternative root which includes .box but does not include—

ANDREW MCCONACHIE: It's exactly like using hyperlocal root with different root zones.

GEOFF HUSTON: I'm not claiming otherwise. I'm just saying that's another—whether you call it as an innovation or an aspect, it's certainly there. It does not try and impose a consistent view of the identity space inside it.

WARREN KUMARI: We are working with people who have an ideological view which appears to be different to our own. They view this as the desired outcome and I think many of us view it as like, "You need a consistent namespace so that we're all talking about the same thing." Their worldview and our worldview are different. I mean, they've also got

Richard Stallman involved so their worldview is definitely different. Wow. I'm snarky in things today, aren't I?

ANDREW MCCONACHIE: I guess my question here as the writer is is there anything else here I need to say? Or do these three paragraphs we have here, do these say everything we want to say about GNS?

WARREN KUMARI: That might be good enough. I mean, the one thing which feels might be polite to us to do is unlike, for example, unstoppable, the GNU naming people have tried quite hard to actually describe how their system works and to—

ANDREW MCCONACHIE: That's true. There's draft on it. I should say it is described in a draft.

WARREN KUMARI: Yes. And I believe will soon be an RFC. We should just make a note that before we publish, "Note to self, see if DNS is published as an RFC yet."

ANDREW MCCONACHIE: Okay. This other stuff we can just delete. So in the remaining five minutes, we have—I think this is new text from you, Geoff, in Section 8.

GEOFF HUSTON: Well, that's what somebody asked for in the last call and it was deliberately informal language that, Warren, don't we hash on it. But it was trying to sort of put some flesh around the concept that having broken the coherency of the identifier system and addresses, the consequences of ambiguous name resolution in the Internet is actually futzing around with the coherency of the Internet itself because addresses can't hold you out of this mess. And that's what it's trying to point out. It's not the best way of doing it. It was just to hang some text as a framework for us to work from.

ANDREW MCCONACHIE: Awesome. I suggest next time, we spend some—I'll go and clean this up. Maybe add a little bit more meat on the bone. We can discuss it next time.

WARREN KUMARI: I actually like Geoff's text and square brackets. I think we should try and keep that somehow.

ANDREW MCCONACHIE: Okay.

GEOFF HUSTON: If you only get one thing, you get what is in square brackets, the rest doesn't matter. It is true.

ANDREW MCCONACHIE: That makes a good opening paragraph then.

WARREN KUMARI: I put the Humpty Dumpty quote in the chat. I think having that somewhere in the beginning of the dot thing. “When I use the name, Humpty Dumpty said...” It means just what I choose it to mean, neither more nor less. Seems like a good way to open this document, maybe.

ANDREW MCCONACHIE: Sure.

GEOFF HUSTON: I think it’s true. And I think it does point out that once you start talking about evolution of name resolution, you’re also talking about the namespace itself, which brings in the Humpty Dumpty quote, and you can’t talk about one without the other. We can try but it doesn’t really work.

ANDREW MCCONACHIE: Then finally, in the last two minutes, and this is something else that we should talk about next week, is I wrote a new finding as I was asked to about motivations and interoperability. But that’s just to excite you to join the call next week. With that, Barry, Russ, I think we’re out of time. Do you have any closing remarks?

BARRY LEIBA: Nothing for me. Russ?

RUSS HOUSLEY: No. I look forward to digging into the text that Geoff's provided. Thank you for taking on that work.

GEOFF HUSTON: No problem. Thanks.

BARRY LEIBA: All right. Thank you, everyone.

WARREN KUMARI: Bye, y'all.

BARRY LEIBA: Thanks for coming.

ANDREW MCCONACHIE: Thanks a bunch.

UNIDENTIFIED MALE: Bye, y'all.

[END OF TRANSCRIPTION]