

**EPISODE 1322**

[INTRODUCTION]

**[00:00:00] ANNOUNCER:** When you want to visit a website, you enter its domain name in your URL's browser bar. When you want to purchase a domain name, after you've completed the transaction, that domain will be held by a custodian like Google domains. Blockchain domains, on the other hand, are similar to regular domain names, except they're stored and controlled in your cryptocurrency wallet. The company, Unstoppable Domains, provides blockchain domains that enable users to do things like keep a universal username across apps and websites, act as a website URL, acts as a payment address for wallets and much more. Using their solution, you can replace cryptocurrency addresses with human readable names. In this episode, we talk to Matthew Gould, founder and CEO of Unstoppable Domains.

[INTERVIEW]

**[00:00:52] JM:** Matthew Gould, welcome to the show.

**[00:00:54] MG:** Happy to be here.

**[00:00:55] JM:** Since you are a person who's familiar with the decentralized web, I have a very simple question to start with. It's 2021, why do we not have zero transactions cost payments on the Internet?

**[00:01:07] MG:** That's a good question. I think, actually, it just takes a long time for the financial system to update. If we were going to point our fingers at anyone, I would point them at the finance industry, and just say there's a lot of regulations there for, I guess, a lot of good reasons. But then there's also just a lot of antiquated software. I mean, it's one of the few places you can still get a job in COBOL is in the finance industry.

**[00:01:29] JM:** Yeah. But is there anything wrong with that? I mean, there's nothing wrong writing in COBOL, right? It's more like what are you writing?

**[00:01:34] MG:** Yes. But I would say there're probably better places or better ways to store your data inside of a database instead of storing it as text files and then processing it with Python scripts, which sounds crazy to anyone out there who's listening. But large financial institutions are still doing things like that today with their data. And I think, also, we just had a lack of technology. I really do think that we needed to have a new way to publicly track financial transactions. And that's something that has only happened recently since Bitcoin came around back in 2009. Actually make it so we have a safe way to track financial transactions in an open manner between unrelated parties. So I do think there was a bit of a technology holdup there. And we still have a lot of work to go, because as your listeners know, there's probably scaling issues with that.

**[00:02:19] JM:** But that spec that you just described, for what you need to have a good financial system, you actually don't need decentralization. You actually listed several qualities of software that the financial institutions need, and you did not include decentralization. Do we actually need full decentralization to have the kind of financial system that we're looking for?

**[00:02:37] MG:** I think what we want is a way to audit or feel very confident about the records that are being stored. So that is a property that you get from having a network that has lots of participants validating its accuracy. And so I think that's the part where people start talking about decentralization. And then when people say like full decentralization versus partial decentralization, it's a security quality of the network, and security qualities are always spectrums. So it's like how secure do you want your financial transaction network to be? You can have something that's very, very simple, in which case, there would only be one person verifying the transactions, and that would be superfast. But it also wouldn't be very secure if that one area got compromised. For instance, like Equifax got hacked, and a lot of people's credit records got exposed. These things happen all the time. So I would say it's a spectrum. You do want to have some level of – You want to have multiple parties participating to verify this data. So I don't think it's good to just have one person do that. And then I would question what is full decentralization. I would say full decentralization is a network where there's enough independent parties verifying the data that you can feel very confident, at least statistically speaking about the accuracy.

**[00:03:44] JM:** What about 10 people? If we decentralized only 10 people, is that enough?

**[00:03:47] MG:** This is a good question. If you were told to hold a gun to my head and ask me what's a good number? I would probably say somewhere in the low thousands is enough. And if you look at some of these decentralized networks out there, most of them already have achieved several thousand people. The reason why I say that is if you just look empirically at places like the Pirate Bay, or some of these organizations that have existed for a very long time, under very adverse conditions, having a lot of people try to shut them down from the outside. Once they achieved a node size of several thousand or tens of thousands of users, they were able to keep accurate networks up even under adverse conditions. So that's what we kind of see empirically. I'm sure there're a lot of researchers out there who would have something to say on that. I'm not an expert on that field, but would be my gut feel.

**[00:04:27] JM:** Wait. You're not an expert in that field? Aren't you like working in the decentralization business?

**[00:04:31] MG:** That's true, but I'm on the application layer. So we're actually working on building blockchain domain names, which is a small niche part of this decentralized movement, this Web3 movement of trying to give people new tools for interacting online digitally, and it's a really broad field. There's a lot going on behind the scenes.

**[00:04:50] JM:** So why would you decentralize among more than a thousand people? If it's enough decentralization among a thousand people to get a decentralized DNS, why would you go for more than a thousand?

**[00:05:00] MG:** So I means, if you look at it, there is a cap on the total number of nodes that are running on any of these networks. So I think Ethereum maybe has 100,000 or so. So what we're talking about here is just the differences of a couple of orders of magnitude. I would just say, as long as the cost is low, there's really not a disadvantage to having more nodes participating on the system than less. It's really a cost consideration. And you're going to see tradeoffs like that happen on apps. And I can give you an example with our application. There're multiple different types of interactions that you could have with blockchain domain names, like for instance, you could want to resolve a website, or maybe you want to resolve a cryptocurrency address. And depending on the level of security you want for the different types of information you're trying to

resolve, then you could actually have less security. And you could choose that. And that's something that you're going to be able to see as well on these networks. So yeah, I hope I didn't go too far into the weeds there, but I think it's going to be pretty complex on people's security choices in the future.

**[00:05:56] JM:** I get it. But like why do you need more than a thousand? Like why would you want decentralization among the more than a thousand nodes?

**[00:06:02] MG:** Well, I guess maybe the question is why would you want decentralization beyond the point at which you feel secure? And I would say that you probably don't. So once you feel secure with whatever that level is, and you can just pick any number in, right? It doesn't matter what it is. But beyond that level, you're right, you don't really need it, because what you're doing is you're paying more money for security that you don't really need. A good example here is actually the Ethereum blockchain and compared to the Bitcoin blockchain. So you can see that the Bitcoin blockchain has a very expensive proof of work algorithm where they have to mine a block every 10 minutes, and it costs a lot of electricity to do that. And then the Ethereum network is actually upgrading to a different security model called proof of stake, which they think will provide just as good or, if not, better level of security with using a lot less resources. So these are also not a fixed pig. What I'm trying to say is, it could be that today, the best technology has to offer says that you can get to about a thousand or maybe 10,000 nodes. And that's going to give you as much security as you can without getting too much cost. And if you fast forward another three or five years, there could be enhancements and technology where it's now easier to distribute that among 100,000 people. You get increased security for no additional cost. So it's kind of like asking, "Why would you want to pay for more security?" And it's just a cost benefit tradeoff. So if you don't need it, then there's no reason for you to pay for it past a certain point, and people won't.

**[00:07:20] JM:** But again, why do I even need it like among 10 people? Or why do I even need it on nine people? So what is N? Like what is N?

**[00:07:26] MG:** Yeah, and we're going to find out what it is. I tried to answer this earlier. So I'll give us another step. It is the point of time in which you feel that you have enough security on that network. And we haven't seen a lot of attacks on blockchain networks yet. But we've seen

at least some attempts. And we've also seen some peer-to-peer networks in the wild, like BitTorrent, or these other file sharing ones. And from what we've seen so far, we think that number is at least several 1000, if not tens of thousands. But again, I think it's a theoretical question. Like it doesn't really matter to build on top of these projects. You can build on these projects. You can try to get as much security as you want. Like you can optimize to get as much security as you can for reasonable costs. And then you kind of call it there. So you put your thumb up in the air and you try to get an idea of what you think is enough. And I think 10 is not enough. Personally, I would feel uncomfortable if there was a network and there are only 10 different places where the information could be overwritten, and then I would have the wrong info on my side.

**[00:08:18] JM:** But I have most of my domains, all of my domains hosted by services where there is essentially a proof of authority single point of failure kind of system. So if we just get to like three participants, it's still an order of magnitude more decentralized than the single participant system.

**[00:08:36] MG:** Yes. But there are some differences here. Like, yeah, I mean, I agree with you. Even anything more than one is going to be an improvement on the underlying system. But there's a lot more stuff that's happening on these decentralized networks, like financial software, that has much higher value. So I think that the level of security that you need is going to go up. I mean, you're not currently storing a million dollars in Bitcoin on your .com domain name, right? Or receiving payments in that size there. So there's a different level of security going to want for something that you could potentially receive like a million dollar payment then for something that you're going to be hosting a traditional website. So you don't want higher security, I think.

**[00:09:12] JM:** But why do I need that security at the DNS level?

**[00:09:15] MG:** So DNS, I think people need to wrap their head around that, actually, it should have been much more than it is today. And the way that DNS was constructed, it's not really able to do much more than resolve websites. And it seems a little bit silly that that's all DNS was built for, because it is a naming system to connect different computer networks. And these networks can have all sorts of information of data, financial information about you, etc. And I think that what we actually just need is an upgrade of the DNS system. So when people try to

compare what we're building on several domains with blockchain domain names, and maybe your.com domain name, I would just say that you do expand the vision a little bit to think about what would you do with a generalized naming service that you're not going to be doing with a traditional domain name service. And those things are sending and receiving money to each other. We think that's a super big part of this. We think that being able to attach data back to your blockchain domain name generalized forms of this data that other people could interact with by you permissioning them on SSO. These are all types of things that the traditional DNS system can't do, mainly because the domain name itself is owned on those servers instead of being used around and inside of your wallet. Basically, you don't have a private public key pair associated with your regular Verisign domain name that you can use to sign transactions or receive cryptocurrency or receive payment. And that's kind of like the thing that happened with these blockchain naming systems that we think is very innovative.

**[00:10:34] JM:** So you think that the like DNS should have like trigger based-functionality for like doing transactional stuff?

**[00:10:40] MG:** So there's an architecture problem. I think there's an architecture problem with DNS, if I'm just going to get right to it. And that architecture problem is that instead of having your digital endpoint for your website, like I have my website, matthewgould.com is just a personal website. Instead of having that owned by you and controlled by you and you're able to define all the different things that you point to, and you can do this on domain. And like you can have a text record or a DNS record or something like this, but you don't own and control that. And you don't have the ability to add a bunch of different functionality on it. It's defined by the spec for.com, the different records that you have there. So because you don't control it and you can't choose how it can interact from like your own personal wallet, there're just all sorts of things that can't be built on top. So let me try that one more time. The DNS system is basically like a walled garden. And it has a defined set of functions that can be built on top of it. Whereas blockchain-based DNS systems are open so the developers can come in, just look at the code, and then build their own applications on top. They can plug in to these blockchain domain names to do all sorts of things. You're like, "Okay, well, what things could I do with my blockchain domain name?" The most obvious one is sending and receiving cryptocurrency. Another one could be if someone sends money to you, it could convert it automatically to Bitcoin or Ethereum. Or it could go from Bitcoin or Ethereum back to USD. You could also use your

blockchain domain name to store a reference to generalize data. So you could store a reference to your healthcare records. And then when someone could do a look up, like using an authorization protocol, and you could them permission to pull data off of a resource server that's pulled from your blockchain domain name so that you can portably take your data on the Internet.

So the example that I give right now is, when you go online, you probably have 15 different accounts that you log into. If you use LastPass or something, you may have like 50 different websites that you log into. Every single website that you log into, you have a different digital identity. But you'll usually log in with your email and passcode, but they'll be creating a backend instance for you of your user account on each of those websites. And if you think about it, the reason why you have to create a new ID on every app that you interact with is because there's not a generalized digital ID service for you to plug into. And that's what naming services are at their core. Is there a way for you to do lookups about an individual?

So what I'm trying to say is, I imagine in the future, instead of having to create 50 different logins and pass codes across Facebook, LinkedIn, Reddit, all the sites that you sign into, you'll actually be able to sign into each of these sites with a name built on one of these blockchain-based naming services. And then that will be able to point to the information stored about you. So you'll have the same name across all these different applications. And this is where the term Web3 comes in, when people are talking about our space, is Web1 was a static website, Web2 was a static website connected to a server. And Web3 is a static website with a server that also allows the user to bring data to that application. And I think that blockchain domain names are going to be the pointers that people use to do lookups for bringing data about themselves to the apps that they interact with.

**[00:13:35] JM:** Are drawing an equivalency between decentralized identity and the decentralized DNS business?

**[00:13:44] MG:** I'm saying that I think, yes, and I think that DNS is a very good candidate. Like domain name services are a very good candidate for DIDs. And this is something that we're actively exploring along with several other people in the space. And it's actually interesting for people who may be less familiar with what's going on with the crypto market. A lot of people are

launching all of these like NFT's or pieces of artwork. And people are posting these pictures on their social profiles. These things have aspects of identity in them. Like I want to be associated with this picture, or I want to be associated with this particular project. And people are starting to get rewards based on those projects, which I think is pretty interesting. So it's kind of like if you have a CryptoKitty or one of these other famous projects, you can also get a hat for your CryptoKitty if you log into a different website. And then you can also log into one of these VR spaces like Decentraland, and people can see that you are this CryptoKitty. So you're starting to see this emerge in this space where you have some sort of blockchain token, and that's used as your identifier across multiple networks. If we just kind of step back a little bit, we think what would be a really good generalized blockchain token to use as an ID across different computer networks that you're interacting with, I think that naming systems are just a natural fit for that. It's very easy to remember my name. It's easy for me to share it verbally or visually. And people already have a hook in their minds for using domain names to look up records.

**[00:15:07] JM:** So you have a token?

**[00:15:08] MG:** So our project does not have a like ERC-20 token. So we haven't done anything like that. But when you buy a blockchain domain name, actually it is an NFT minted on the Ethereum blockchain. So if you were to go and you buy your name, jeffmeyerson.crypto, or .coin, or .bitcoin or any of the other blockchain-based extensions, you are minted in NFT on the blockchain, which it is a crypto token then you then own inside of your wallet. That's how that works.

**[00:15:35] JM:** So what happens if I have an NFT that entitles me to jeffmeyerson.eth on one chain, and then somebody else has jeffmeyerson.eth on another chain?

**[00:15:48] MG:** So far, we have not had those conflicts, and most people have been avoiding those. And I think that that would be – Like that would be a tough problem for people to crack, because then consumers may accidentally send money to two different places by accident. So likely, that's going to be figured out in the commercial space, like these companies are going to talk to each other. Just to give you some maybe inside baseball. We've talked to several other projects in the space who are also working on blockchain domains. And everyone is intentionally not building the same extension because of that conflict that you would run into. And I think that

each of these extensions are essentially representing different types of brands, right? And then people are representing these brands on their Twitter profiles. Like they could post their name like matthewcool.crypto. I also have like unstoppable dog crypto, and post that on your Twitter profile. So you're seeing people identify these already as ID endpoints. People are doing the same thing with art projects too. I'm not sure how familiar you are. But there're things like – There's CryptoPunks, which is also pretty famous. People are posting those as their picture on Twitter as well. So I think people are going to avoid these types of conflicts, at least legitimate businesses, because there's really not a legitimate reason to intentionally build a conflicting namespace with another registry.

**[00:16:57] JM:** I mean, you're literally describing the double spend problem and telling me that people aren't going to want to double spend.

**[00:17:03] MG:** This is different. So the double spend problem is being able to spin money twice. So this is actually just a problem of looking up at the wrong place. So it'd be like – I guess a better analogy, maybe be having your DNS settings configured incorrectly so that you're actually reading from like the wrong file in order to find a piece of information.

**[00:17:20] JM:** So if I register on unstoppable domains jeffmeyerson.eth and then I go to like Ethsimple, which is like another Ethereum related domain registrar that my friend Brian Soule runs, and then I have somebody else register jeffmeyerson.eth, and he says, “That's fine.” That's a double spend.

**[00:17:44] MG:** So you can't register .eth domains and ensemble. So you'd be registering actually a .crypto domain on our website. And that's always trying to get that earlier. So we wouldn't be issuing a domain name that somebody else offers. So maybe there are some people out there who want to do that. But that would just be like the same thing. Maybe a better analogy here is like if you want to make fake handbags and then you wanted to import them and sell them on the streets of San Francisco or wherever, you're welcome to do that. Like you could make a fake product handbag, or a Hermes, or something like that, and you could open a store. And people do set up shop and do that types of things. But they also eventually get shut down because the consumer harm there is quite high from basically just ripping off another person's brand and then putting that – Devaluing it right through that.

I mean, if you're asking me, like are humans going to always create – Or there are always going to be some people out there who's going to want to create problems? I think the answer is probably yes. But I think from a business standpoint, like there's not going to be any legitimate businesses out there trying to create that type of confusion for users.

**[00:18:39] JM:** What if that's on my roadmap already?

**[00:18:43] MG:** Jeffrey Meyerson, that's what you're building next? Yeah, I mean, that's great.

**[00:18:48] JM:** I mean, why wouldn't I, right? Sounds like a good business.

**[00:18:51] MG:** Yeah, yeah. I mean, this is probably something you should talk to with your own personal counsel. I would just advise that starting a business selling fake product handbags would probably in very poorly for you. And there's a reason for that, because people don't think it's okay for people to sell fake goods to unsuspecting consumers. So yeah, I think it's going to follow that same path.

**[00:19:11] JM:** But what if I literally set up my own domain registrar dominion? What if I just say, “Look, domain registration as a category is so broken. I just set up my entire blockchain. I'm setting up my entire Internet on my own DNS system. It's completely clean. Mine is the most pure of the DNS systems. I will sell .eth domains. I will sell .crypto domains. I don't care who else owns them on the traditional internet. I'm setting up my own internet.” Can you stop me from doing that?

**[00:19:40] MG:** I mean, I'm not in the business of stopping anybody from pursuing their dreams. Jeff, if you want to go out there and doing that, I think it would be a very poor use of your time. I mean, theoretically, I guess it's just not a question that we've run into in three and a half years of business. So I don't think it's actually like a thing that's going to happen. And I'm excited for you if you're going to try a domain project. I do think that there's a lot of innovation needs to happen here. And like I said, there are dozens of projects already operating in this space and have not run into this problem yet.

**[00:20:07] JM:** I mean, there also hasn't been like a double spend of Bitcoin, and people still want Bitcoin to be more decentralized than it is today, right? Like today, it's what? Centralized among like a few mining operations essentially? And people don't like that. You'd like the true decentralized potential of money. But my main contention is like do you need that for DNS? Like I know you want it for money, but do you really need it for DNS?

**[00:20:32] MG:** I think that whenever you have more competition in a market, you're going to get more innovation. So I think in this case, the monopoly that has been DNS for the past 35 years hasn't really innovated that much. At least I haven't seen a major change –

**[00:20:44] JM:** Wait. Wait. Who's the DNS monopoly?

**[00:20:46] MG:** I would say it's the current people who own those registry systems. So I would say probably the ICANN system, just in general, would be the monopoly –

**[00:20:54] JM:** ICANN? They're a monopoly?

**[00:20:56] MG:** I would think so, yeah. And if you look recently, they've been behaving very much like one. Are you familiar with what happened with.org recently?

**[00:21:03] JM:** Yeah, it got like commercialized, right?

**[00:21:05] MG:** Correct. There was a private equity hedge fund who tried to buy .org. And actually the hedge fund was founded by the former CEO of ICANN, right?

**[00:21:13] JM:** But like, that's because this is a problem that has to be a free market problem. It's like there's no other solution to it.

**[00:21:19] MG:** What do you mean?

**[00:21:20] JM:** The ICANN problem.

**[00:21:22] MG:** There's basically no other way to play it other than to be a monopoly, because it's an N of one problem. That's like saying that like SED, the command line tool SED, has a monopoly over being the streaming editor for Linux. Like it's kind of the only streaming editor on Linux that comes as a default, right? Like that's just the thing. It's just the same thing. Like you're making an ICANN-like system, it has to be a monopoly by definition, because it's an N of one thing.

**[00:21:47] MG:** Oh, I see. I think that was probably true maybe 30 years ago. Again, it comes back to this consensus problem, right? So 30 years ago, you really had a problem knowing if the records inside the DNS were accurate or not. Correct? And so the only way you could do that was by having a trusted authority. That's no longer the case if the information about the records is stored on an open network, right? So if you store this on a blockchain network, then anyone can verify the data. So yeah, ICANN was definitely necessary in 1992 or whenever, because they didn't have a way for people to have to write records on a public database that could be privately verified. And that's what you get from blockchain systems, is that you actually have exactly all those properties. So that happened in maybe 2015 when smart contract blockchain started coming out, is that you could build these complex systems where you could write information publicly. And then anyone could verify that privately. So Verisign don't have that ability, right? So for.com, there's no way for me to actually verify. I mean, yes, there's all these trusted DNS servers. They have like a really pretty good centralized system built to make those verifications. But for blockchain domain name systems, you can launch one, and then anyone actually can look and then see that it's accurate right out the gate. So that actually saves you a lot of time and a lot of resources, and enables you to have lots of these systems being launched, which is what you're saying.

**[00:23:10] JM:** So if I'm defining the business that you are in, it is decentralized domain name registration. Is that correct?

**[00:23:17] MG:** Yes.

**[00:23:18] JM:** Okay. What is the advantage over a centralized domain name registration system?

**[00:23:25] MG:** There are two primary advantages. One is that you don't have to trust the third-party for the security model. We talked about that earlier in this.

**[00:23:32] JM:** Wait. Let's zoom in on that for a sec. So you don't have to trust a third-party for security model? Is that what you said?

**[00:23:38] MG:** That's correct, because you can verify the data yourself on chain. So like when I look up a .com address, at some point, deep down to the bottom of everything, I'm trusting that Verisign is keeping the records accurate for .com. But actually, I think this is the smaller point. I think the bigger point –

**[00:23:52] JM:** Hold on. But let's just focus on that one for a second, okay? So has there been an instance where Verisign has done anything wrong like that?

**[00:24:01] MG:** So I think maybe it was france.com would be an example. So there was a guy who had france.com. And he owned it for like 20 years. And then they finally just decided that they would give it to France. And depending on your view on private property rights, you may feel differently about how that should result. And so because the user never actually owned it on a system where they could verify ownership and they weren't depending on a centralized system, the operator decentralized system, in this case, Verisign, could just update the records and then transfer it to another individual, which is what they did. And there're lots of cases like that that happened. Most of them are not publicized as widely as that one, but that's one famous case. And then the other thing that I want to talk about –

**[00:24:39] JM:** Wait. Wait. Hold on. Hold on. France.com, who does that hurt? Like who does that impact? Like what's the problem there?

**[00:24:46] MG:** Well, if you built a business for vacations, which is what I think this guy did for a decade, and then someone else can take that business from you. It's kind of like imminent domain.

**[00:24:54] JM:** Oh, I get it. So somebody built a france.com, like vacation in France business, and then Verisign decided that France, the country, deserves the domain.

**[00:25:04] MG:** Like eminent domain. Yeah.

**[00:25:05] JM:** That doesn't seem that bad. That doesn't seem that controversial. It's like it's France.com. Like France should own France.com. That's just like an emergent norm.

**[00:25:15] MG:** Well, they also have .fr, right? Like their own extension. And .com is supposed to be a commercial entity.

**[00:25:20] JM:** They should have both though. I mean, saying .com means it should be a commercial entity. That's like saying that if I own jeffmeyerson.eth, it should be an Ethereum-based entity.

**[00:25:32] MG:** I'm just pointing out that when those things were relaunched, that was the original intention for each of those extensions. Like that's what people thought –

**[00:25:38] MG:** But that's not true anymore. Like that's a norm. There are emergent norms and the internet, right? Like things change.

**[00:25:44] MG:** And they do. And I'm actually pretty excited about the changes we're seeing with blockchain domains. And I think that this is actually going to change the way that people view their information online. So like I was saying on the second part that I want to get to, I'm going to get there, is that once you have these open systems, then people can come in and innovate on these records. Sorry, innovate on blockchain domain names in a way that they can't do with standard ones. So if you want to start a company, for instance, that would take some action based on a domain name or store some data there. For instance, we'll just keep it easy. If you wanted to receive Bitcoin to your blockchain domain name and then have it automatically convert to Dogecoin, because you're a big Dogecoin person. If you want to do that on Verisign with a .com domain, that would be quite difficult. But if you wanted to build that functionality into one of these blockchain domain names and offer that as a service, that would actually be quite easy. Maybe a more obvious one would be something like if you wanted to have increased privacy on your transactions, you can actually build a system that would automatically update your payment address every time someone sends you a different payment so that you would

have a little bit more privacy on their transactions as you're receiving on these crypto networks. That's an application that a developer can build on top of a blockchain domain name.

And the reason why they can do that is they can actually just look at the smart contracts that's on the public blockchain system. They can read through it. Figure out how to interact with it. And then they can build their own applications on top. So it turns domain names from a walled garden, like you have with Verisign with.com, into more of an open platform for people to innovate on top of.

**[00:27:10] JM:** I mean, isn't the domain name kind of – It's like not really – I mean, I guess it is an open platform, right? Because it's just a domain name. Like the domain name is like just the entry point to whatever you're building on top of that. Like you have a Turing machine behind whatever domain name that you instantiate, right? Like you have all the freedom that you need within that Turing machine. It doesn't matter if it's a decentralized or centralized domain name, like unless decentralization adds something that is meaningful. I'm just trying to understand what decentralization of a domain name system really adds today and what that N is. How decentralized it really needs to be?

**[00:27:47] MG:** So yeah, I'll go back to this again. So for decentralization, again, I think that it's a security question. And all you're trying to get with decentralization is some level of security. So once you've achieved whatever that level of security is that you want for your application, let's say it's a few thousands nodes in this case, then that problem is solved. So you can put that done. And then what you want to look at is, “Okay, well, what's the advantage on having an open system where anyone can come in and inspect the code and then know how the system is built and how they can interact with it?” And that's the thing that you're not going to get with a regular traditional domain name, is the ability to plug in an app on top of it. So like if you wanted to create a new record type for regular domain names that enabled the sending or receiving a cryptocurrency, it would probably take you seven years, because you'd have to go through like eight different committees, right? And then they would have to be approved through like four different subcommittees. And then you would finally get there in 27 or something. Whereas if you want to do the exact same thing on a blockchain domain name, you actually can just look at the code base, deploy a smart contract, and users can start interacting with that next weekend if they want to. So that's what's happening here.

Again, because you're taking a database that's currently – Domain name databases today are in a server owned by a company, and they're not open access. What you're doing is you're taking all that information and you're publishing it on a blockchain, where anyone can read that data. And then they can also verify it so they know that the data is not corrupted. That means that they can then create all sorts of applications that can manipulate that data or add information to that data. And that's where the innovation is going to happen. So it's the transition from domain names as like a service, which is what you're getting when you buy a domain name from someone like a .com domain name. You pay an annual fee, right? You have a SaaS product, and you have to pay every year, because you're getting a service of that domain name. It's moving away from that to domain name as a platform where, you, the end user actually own it inside your own wallet. And then you can choose to add a bunch of applications on top to try new things to do with naming services.

**[00:29:41] JM:** But again, so the security properties of having a decentralized domain system or decentralized domain specifically, the security properties there that I'm hearing are basically that I've started a travel service with the name France.com, and I'm afraid that france.com is going to be coopted by France the country. That's the main security concern that I've heard thus far.

**[00:30:02] MG:** Well, so something that's common with new technology is it's actually not rehashing the use cases that you already have. It's more about the use cases for the things that people aren't doing yet. So if you start using blockchain domain names as identifiers across the Internet, and this is your representation of yourself on Twitter, or on Reddit, or any of these other social networks, for instance, then the loss is actually quite great if you were to lose it. And if you look at people's Twitter handles now, I mean, we had Donald Trump get kicked off of Twitter, right? There's some new famous person who gets kicked off of Twitter every week. And they don't just lose access to Twitter. They also lose all of the investment that they've made in building that personality behind that name, right? And that's the thing that you're losing. So I think that maybe the difference here is we're talking about blockchain domain names as user identifiers. And so it's a new market. It's not just for launching websites. It's one thing that you can do with it, because you can point to any kind of content.

But when I see them as user identifiers, then there is a lot more harm in having your user identifier revoked. And again, I would just point to Twitter. If you get kicked off of Twitter, it's actually quite bad for both your business and your brand. It can make it much harder for you to communicate with your followers. But in a future where you get to own that name across these different platforms and you can move it around because it's portable, and that naming system is actually an open naming system that works between these different applications. That means that you're much more protected on like the social networks. And we're seeing social networks much more common than france.com, right? Like Twitter handles get revoked every day.

**[00:31:35] JM:** Yeah. But if you're talking about a future situation, like shouldn't we be moving incrementally towards that future? So if we're some incrementally distant place from this future in which we are under constant attack from people that want to sort of run some kind of attack in the decentralized domain name system, or like somewhere before that bleak future, like shouldn't we have maybe like a two to three, or five, or maybe a hundred participants in the decentralized domain name system? Like do we really need to be locking on the entire blockchain every time we go to read or write the like decentralized domain name registrar? Like isn't that a little much?

**[00:32:15] MG:** So I think what you're trying to say is how we're going to have a lot of throughput on these blockchain domain systems. Is that what you're getting at? Like just how are we going to store that much data there? Or I'm trying to understand the question.

**[00:32:27] JM:** Well, there's a throughput trade off, right? The less decentralized you are, the higher throughput you are, the cheaper you are, the faster you are. So if decentralization is really not an important security property today, but you're saying that it's going to be important in the future, then you should be incrementally decentralizing. Not completely decentralizing.

**[00:32:46] MG:** Yeah. So I do think that it is important today. And like I just mentioned, the Twitter handles. I actually think this is a hair on fire problem for people on the social networks getting kicked off. And as far as your question on like how we should be moving towards decentralization, I actually agree. And I think that we should be very pragmatic about how we step towards a decentralized future. But I also have faith that the technology is getting better.

I'll just give you some examples where I'm already seeing improvements inside the space where there are already blockchains that exist that are significantly faster than eight or 10 years ago. And there are already different ways of working with blockchains. For instance, roll ups or other ways of storing data on them, ZK proofs. There're different types of technology that are advancing right now that make that tradeoff less of a tradeoff. So I like to tell people that I think we're in the dial-up phase of this blockchain adoption, but I think we're going to get to broadband. So I actually think we're going to have a thousand or 10,000 or 100,000X speed-ups. And part of getting us to that future is actually building some of these apps now. And we are a small, relatively small domain name register. So we have a million domains registered total. And if compared to .com, who has 150 million plus, we're still tiny. And for that size and that niche market, people who are interested in this technology, it works actually fine today.

**[00:34:00] JM:** So can you take me through the read and the write path of Unstoppable Domains?

**[00:34:05] MG:** Yes. So right now, at its most basic level, the read and write path is, when you want to write something, you can write it directly to the Ethereum L1 blockchain. And then when you want to read something, you can actually do that read directly from the Ethereum L1 blockchain. And then on your writes, you can also write a pointer. So if you want to store some data off-chain, for instance, a picture, which is very common, then you could also write that to the blockchain. And then when someone does a read, they can do a read, find that server where that picture lives and then go look that up. So it's not like you're storing video files on the blockchain or anything like that. You're actually just storing pointers. And pointers are actually reasonably-sized for blockchains today.

**[00:34:43] JM:** So you're writing pointers to the Ethereum blockchain.

**[00:34:45] MG:** So we're actually writing directly to the Ethereum of blockchain for things like cryptocurrency addresses. And then for other items, like if you want to store a website or something, you'll write the address of the file that the person wants to look up, like on IPFS, or could just be a simple server.

**[00:34:59] JM:** So when you do a write to the Ethereum blockchain, what does that cost these days?

**[00:35:03] MG:** A write to the Ethereum blockchain probably cost right around 25 cents as of today. And that is probably 25 times higher than it cost about 18 months ago. And we expect that writes to the Ethereum blockchain will get cheaper probably Q1 of next year as they start rolling out sharding and probably dropped that by a factor of 50. At least, that was my last conversation with the team over there. And so we can get those back to sub-penny prices. And I agree with you, longer term, these prices are going to have to be fractions of a penny for anyone to want to write this data up there. But I also think that that's going to happen over the next three to five years.

**[00:35:38] JM:** And what do you charge per register?

**[00:35:40] MG:** So domain names range in price from \$5 up to I think 50 is the average price. We have some domain names that are shorter characters that cost significantly more that have gone to auction in some cases. But the average domain name is right around, I think it's just under \$40 now. Again, we have some starting at five bucks. Their onetime fee, I think that's another important thing to point out. We don't have any renewal fees for these blockchain domain names. And you own them inside your wallet. That's part of the difference, because we actually think that the business here is not charging SaaS fees every year, but instead selling services to blockchain domains.

**[00:36:12] JM:** So you charge \$40 for an average domain. What's the cost of goods sold for that item?

**[00:36:17] MG:** Yeah, so it's a software product. So our margins are much like other software products. It's probably the same as Verisign's for their .com, right? So it's like 90% on that side. Yep.

**[00:36:28] JM:** But what goes into the cost of goods sold? I'd have to get my account on here to go through everything. But it's things like gas prices, right. So we pay for gas in a lot of use

cases for the Ethereum blockchain domain names. And then just the basic setup on the backend for writing these things.

**[00:36:42] MG:** So 25 cents?

**[00:36:44] MG:** It is more than that for creating a blockchain record than it is for writing a simple record.

**[00:36:49] JM:** So 25 cents, plus additional costs of what?

**[00:36:55] MG:** So whenever you make a transaction on a blockchain, and I don't know how often you've used blockchain products before, but you had to pay gas fees. And then depending on the thing that you're creating, it costs different amounts. So a basic transaction on Ethereum is somewhere around 20,000 gas. And then a more complex transaction, for instance, creating a domain name can be anywhere from 150 to 300,000 in gas depending on what it is that you're doing. So if you want to grind down to the nitty-gritty, then it's probably closer to a couple dollars for creating a domain name on these blockchain systems at the current state of technology.

**[00:37:26] JM:** So it's called a \$2 cost of goods sold. So if you make a 20x per \$2 cost of goods sold, it's a pretty good business. What kind of volume are you doing?

**[00:37:33] MG:** As I said earlier, we actually just crossed a million registered domains this year. Now, some of those were also given away and part of partnerships with wallets. But yeah, I think we're one of the first blockchain-based DNS products to actually cross a million registered domains ever. So that actually just happened this past June.

**[00:37:49] JM:** And what's your attention look like?

**[00:37:51] MG:** Hard to say, because it's still so early, right? We've only been around for three and a half years. And then the majority of our business has happened in the last six months, just because the growth has been pretty fast year over year. So we have maybe three or four times more customers this year than last year.

**[00:38:07] JM:** I mean, people don't really churn from DNS, right? Like very rarely. Like I think about the number of domain names, I bought so many bad domain names, and I pretty rarely churn. I'm kind of a squatter.

**[00:38:16] MG:** Well, I think that I also got stuck with a bunch of domain names. So I probably own around 100 traditional domain names myself. And I pay them every year. And every time that bill comes up, I just think to myself I can't believe I'm paying this again. But they've got you, because there're even people out there who wait for your domain registration to expire and immediately register it behind you and try to resell it. I don't know if you experienced that, but that's quite a jolt when you have that happen the first time.

**[00:38:39] JM:** Okay. So I buy an unstoppable domain. And remind me what I get from that unstoppable domain relative to a normal domain, like buying from Google domains.

**[00:38:52] MG:** Yep. So I would say the biggest benefits for blockchain domains are, one, there's no renewal fees. So it's pay once. You never have to worry about paying for it again. Two, it comes with cryptocurrency payment support out of the box. So if your friends use any one of the 50 supported wallet applications that we have, it'll be easier for them to send any type of cryptocurrency for you. This is a use case that makes a lot of sense to people who use crypto. Every single blockchain network has its own hex address, and they're all anywhere from 26 to 40 characters long. So instead of having to remember that, you can just remember to send money to matt.crypto or whatever your name is. And I would say those are the two like initial things that people are very excited about with blockchain domains. A lot of people see these like collectibles. They want to get one of these, hold on to it just like they do with a CryptoKitty or anything else. And then they're looking forward to having blockchain domain names be integrated into more of their apps.

**[00:39:43] JM:** So there's an impedance mismatch between a DNS system and an NFT. And the reason for that is because in an NFT system, you want to let the user define the properties of the collectable set. You want the user to be able to define rarity, essentially. With the domain name system, your rarity is always the same. You always have a rarity of one. Every domain is unique. It needs to be unique, otherwise the system doesn't work. So isn't this a system where you have to have N of one enforcement? You don't want NFT, right?

**[00:40:23] MG:** Well, there are lots of collectible NFT's that have unique – Each of their products are unique. And I do think that that's one of the special properties of domain names is that every single domain name is unique. So I think that maybe it's a type of sort of in that category.

**[00:40:37] JM:** Who charges the recurring fee on these domain systems. Like if I buy from Google domains, why am I paying \$12 a year?

**[00:40:43] MG:** Yeah. So because Google wants to charge you. And then also, every single one of the TLDs is actually owned by a company. So a lot of people don't know this, but like .com –

**[00:40:53] JM:** What about .com though?

**[00:40:54] MG:** Yeah, they're owned by Verisign. So Verisign is the company behind.com. They've owned it for 30 something years.

**[00:40:59] JM:** SO they lease it to Google? Or like I buy through Google, it's like I'm actually buying through Verisign. And like Verisign gets \$9. Google gets \$3 or something.

**[00:41:08] MG:** Yeah, and I don't have the exact numbers. But I think Verizon gets \$7 is the last thing that I've seen, but it's a basically reseller agreement. And so, yeah, that is Verisign that's collecting that fee on the back end.

**[00:41:18] JM:** Gotcha. Again, my issue here is sort of that like you actually want scarcity in the system. You actually want monopoly in the system. You actually want a monopolist in control of the system, because you don't want any kind of transactional conflict over domain name system. You don't want to have a hard fork over a domain name system, because that takes down the Internet. You don't want this to be decentralized.

**[00:41:42] MG:** So I would disagree. I think that as long as you have a system of record that everyone can reference in order to check the validity, then you're actually fine with having multiple competitors. And again, the only reason why we have a monopoly system is because

we didn't have a way to do that until very recently. So if you have a standard place where you can check to find out where these TLDs are, then you can verify the information validity, in which case, you don't have to have a single person saying this is right or this is wrong. And what you get by allowing to have multiple different people participate is you get competition in this space. And this is something that's been lacking for 30 something years. So you've had a lot more innovation in domain name systems over the past five years from all of these people inside of the crypto space working on this. Like the idea of being able to send a crypto payment with a domain name didn't exist prior to five years ago. The idea for using your domain name as personal SSO prior to two years ago did not exist. These are the types of things that I think are going to change the way that people interact online. And that's what I think is exciting about this.

So whenever you go from an area where you just had one monopoly provider, to now you can have several, you have a chance for people to come up with new and creative ways to interact with it. And I think that, again, the number of developers that are going to be able to build on top of these blockchain domain systems is going to be much higher, because you don't have to work for Verisign in order to build a product for a .crypto domain. Like you could build – I'll give you an example. There's a company called Ethereum Mail. I think it may be Ethmail for short, and they build a system where you can connect a blockchain domain name up to their email service. And they just basically launched an email provider for blockchain-based domain names. And we didn't have to do anything as the registry. And they didn't have to ask us permission to do that. And they just built this very simple system. Now, I know that seems very straightforward, because they're just doing something that exists. But there're a lot of different applications like that that now have the ability for one or two person dev teams to just start building apps to work with naming systems that haven't been tried before.

**[00:43:42] JM:** Cool. Well, unfortunately, I got to get going. Great talking to you. Very cool company. Yeah, I look forward to buying some .crypto domains from you.

**[00:43:48] MG:** Alright. Thank you, Jeff.

[END]