EPISODE 1289

[INTRODUCTION]

[00:00:00] JM: Our first book is coming soon. *Move Fast* is a book about how Facebook builds software. It comes out July 6, and it's something we're pretty proud of. We've spent about two and a half years on this book. And it's been a great exploration of how one of the most successful companies in the world builds software. In the process of writing *Move Fast*, I was reinforced with regard to the idea that I want to build a software company. And I have a new idea that I'm starting to build. The difference between this company and the previous software companies that I've started is I need to let go of some of the responsibilities of Software Engineering Daily. We're going to be starting to transition to having more voices on Software Engineering Daily. And in the long run, I think this will be much better for the business, because we'll have a deeper, more diverse voice about what the world of software entails.

If you are interested in becoming a host, please email me, jeff@softwareengineeringdaily.com. This is a paid opportunity. And it's also a great opportunity for learning, and access, and growing your personal brand. Speaking of personal brand, we are starting a YouTube channel as well. We'll start to air choice interviews that we've done in-person at a studio. And these are high-quality videos that we're going to be uploading to YouTube. And you can subscribe to those videos at YouTube and find the Software Daily YouTube channel.

Thank you for listening. Thank you for reading. I hope you check out Move Fast. And very soon, thanks for watching Software Daily.

[INTERVIEW]

[00:01:55] JM: John, welcome back.

[00:01:57] SL: Hey, Jeff, good to see you again.

[00:01:58] JM: Good to see you too. This is the first time meeting you in person, I think.

[00:02:03] SL: Yeah, I think the first time was through phone as well.

[00:02:06] SL: Okay. And we've done two previous interviews, I think.

[00:02:09] SL: Yeah, I think one was Docker and one before we changed the name to Magic.

[00:02:14] JM: Right. Okay. Yeah, the Formatic company. I want to talk about all that. First, I want to ask you – We're in San Francisco. I am finding as I come out of the pandemic that I actually still like this city. I forgot for a year that I liked the city. How are you feeling? Like coming out of pandemic, give me the entrepreneurial zeitgeist of Sean Li.

[00:02:40] SL: Well, before I moved to the city, I was in San Mateo. And during the pandemic, I realized I was where I needed to be. I actually really like San Mateo. I'm actually moving back next month. But yeah, when I started the company, we moved to SF to be closer with my co-founders. And now that the company has grown and then there's more of a remote cadence being built around the company. So everybody's just remote now. So I can live wherever I need to be.

[00:03:13] JM: Are you back in San Mateo?

[00:03:13] SL: Will be next month.

[00:03:14] JM: Great. So do you think there is an exodus, an entrepreneurial exodus, from San Francisco? Or has it been overstated?

[00:03:23] SL: I think I have my own perspective around it. I don't think there's like an exodus. I don't think people are fleeing here, because I believe Silicon Valley is really unique. It is the only place with art, tech spirituality. It's gotten really, really nice weather. Yeah, is the place with all of that combined. And I think, if anything, there's a really good chance that more inspired things will come out of Silicon Valley.

[00:03:51] JM: Yeah, I'm feeling the same way. I'm feeling definitely the energy in a way that you don't get in remote. I didn't get for the last year. Did you miss that energy? Did you kind of forget what made San Francisco San Francisco?

[00:04:07] SL: I'm personally pretty new to San Francisco, because I was only here for around two years. And that two years is all for my company. So I didn't really get much time to explore besides sort of like the downtown area, kind of the Westfield mall area. Besides there, I didn't explore as much. I do enjoy Golden Gate Park and Ocean Beach sort of on the on the west side of it.

[00:04:32] JM: Gotcha. Well, the reason I wanted to bring you on, you're the second person I'm doing a video interview with, is I like your entrepreneurial taste. So if I look at the three products that I've seen you build, first with – What was your pre-Docker company called?

[00:04:51] SL: Kitematic.

[00:04:52] JM: Kitematic was like – The way I think about that company is if you take Docker in its early days and then you add much better UX to it. That's what you get with Kitematic.

[00:05:02] SL: Yes.

[00:05:03] JM: And if you think about Docker, Docker is one of the most developer-friendly products in existence. Then you were attempting to do something similar with Fortmatic, which was kind of like – The way I understood your vision for that company was very UX friendly developer API's for crypto related activities, which is really appealing to me as a developer. So I'm like a longtime fan of Heroku. I think Heroku was like transformative, stripe, obviously, these things in developer UX that were milestones. And I see you as somebody who's really capable of thinking that way.

And then now where you're at with Magic, which we'll dive into pretty deeply, you're trying to introduce an easy way to build the kind of passwordless authentication that some people get from –The first thing that comes to mind, by the way, Slack. Is that right? They're kind of the first people to really productize that.

[00:06:01] SL: Right. Slack and medium, I would say, are sort of pioneers in using Magic link as login.

[00:06:07] JM: Right. Okay. So before we get to Magic, actually, do I understand your ethos correctly as a product developer?

[00:06:15] SL: Well, as a product, that makes sense. So we make sort of passwordless login. Basically plug and play. Super easy for developers to just put it in their application. And it works really well with modern tech stack, like Jamstack. And even also, it plugs seamlessly into the blockchain ecosystem, sort of additional bonus there. So it is a very future-proof oriented kind of authentication for developers.

[00:06:44] JM: Do I understand your overall – The through line in your products. Is it this ambient focus on developer experience?

[00:06:53] SL: Yes, like everything we do, it's developer focus. We want developer experience to be top notch.

[00:06:59] JM: Okay, gotcha. So of all the things you could focus on, why is passwordless authentication a meaningful product?

[00:07:10] SL: Mm-hmm. Well, in my opinion, passwords are already quite obsolete. So like there're so many breaches these days. Like, recently, there's the Facebook hack, and there's a hack recently that demanded ransom in Bitcoin. So, basically, it’s a huge problem, because a lot of people reuse their passwords. So about 59% of all recorded users reuse their passwords across different services. And sometimes I find myself reuse some passwords too for like one-off services. And imagine what happens when hackers crack these companies, expose the encrypted passwords, and sort of figure out the username to password hashes, right? And kind of reuse that to log-in and impersonate as users?

So right now, I think for people with like simpler passwords, if you go to haveIbeenpawned.com. Type in your email, you're going to see all the services that have had been compromised and has leaked out your information.

[00:08:16] JM: Isn't the solution to this to store all my passwords in the Chrome password manager?

[00:08:23] SL: Well, that's sort of – I would say the problem is all the passwords, it's not about where you store it. It's more about what password you're using, right? So let's say if you use the same password, another let's say in app A and then app B. Another hacker can just take the same password and login as you using the same password, even if your password is being secured in a Chrome browser.

[00:08:51] JM: Alright. So shouldn't my best practice be to generate entirely new passwords for every account using Google and stored in Google?

[00:09:00] SL: Yeah, yeah. So right now I think that's as close as to the mainstream solution, which in this case it's like, “Oh, hey. By the way, as an end user, you are responsible for your own security hygiene,” when companies can just prevent this issue from scratch from happening in the first place by not offering password-based authentication. So because in this case, the companies are still storing these passwords, right? So yeah, like a lot of users, more security sensitive users will generate password. But a majority of Internet users do not do that, and do not want to deal with extra tooling around security. The most ideal way to enforce security is for security to be invisible to the user instead of a user have to do like a nuclear launch code every time they access an application, right? So what we do here is sort of leveling up the base bar for security by not even deferring the responsibility to the users, but giving developers the tools to build passwordless in the first place so that users will not have to do that.

[00:10:15] JM: So if I'm building a food delivery app that's going to be used by people of all levels of technical skill, catering to the average consumer, I want to provide the most seamless password usage and recovery experience that also covers security as possible. Security, if I'm just trying to get my app off the ground, I'm probably not going to care that much about security

upfront. I'm probably not going to go with the most secure solutions up front. I'm building instacart from day one. I've got enough problems. I'm not going to use magic, right?

[00:10:59] SL: Well, that's why Magic exists actually, because companies don't want to build authentication themselves. Like every app needs authentication. And if a company ends up getting hacked, that's pretty bad. Over 40% of customers never comes back. There's also going to be liabilities around the damage caused by breaches. There's also necessary work around security compliance and privacy compliance, and also ensuring that your login system works reliably and scale, and would scale with your own growth.

So as someone building, let's say, like POC for new Instacart. They don't want to think about all this stuff, right? But you need authentication for users to interact with your app in the first place. So why not pick a solution that's really, really easy to use and give you that peace of mind to basically worry about what's core to your business rather than authentication?

[00:11:58] JM: So are you an authentication company?

[00:12:01] SL: Yeah, we are authentic. Right now we're very focused on authentication side of things.

[00:12:06] JM: Do you compete with Auth0?

[00:12:08] SL: Well, the space have so much surface area, right? I don't think we're a direct competitor. A lot of people in our authentication space does a lot of things, right. And for us, we want to do basically the developer friendly sort of customer identity side really, really well, whereas Auth0 and Okta does a lot like workspace identity.

[00:12:33] JM: Have you worked with Auth0 before? Have you used it?

[00:12:36] SL: I used it. I used it myself. I think as a company that provides so much functionality, I do believe that their content is quite good.

[00:12:47] JM: If we're imagining the listenership is somewhat familiar with Auth0 – Okay, short history of Auth0. It's developer friendly authentication as a service. Kind of the next generation of Okta, which is why Okta acquired them. How are you differentiating the product direction from Auth0?

[00:13:08] SL: Yeah. So like I mentioned earlier, Magic is a lot about being future-proof, right? So let's just make an example here. So the old guards in identity would be like Microsoft, Oracle, IBM, all these companies. And you have these newer companies like Okta, Auth0, ping.com, OneLogin. These companies are trying to shift the market into the next generation identity applications. But these applications, a lot of it are still based on technology that's decades old, whereas now a lot of things are happening around us, like decentralized identity, blockchain, further decentralizing sort of essential infrastructure for the Internet. And all of that depends on PKI, so public key infrastructure.

So without proper key management, the older providers of identity will not be able to plug seamlessly into the more future-proof eco systems, right? Like blockchain, decentralized infrastructure. But Magic, coming from the crypto and blockchain is those, we do a really good job in terms of managing the private keys, right? So with that in mind, Magic is going to be the one after Okta, Auth0. So we're sort of establishing our own category as sort of this future-proof, super, super developer friendly, and really compatible with modern tech stack sort of authentication solution.

[00:14:42] JM: If we think more expansively about this from the blockchain inclusive world of software, Auth0 is proof of authority. You want to be proof of what?

[00:14:57] SL: Well, basically what we do is we manage the private keys, or we sort of help user manage the private keys. And what that allows is that let's say if a user want to take hold of their identity, they can export the keys, right? So this way, the user is not vendor locked-in to Auth0. They can take their identity out. Move it somewhere else. It's going to be hyper-portable. And our goal is to eventually sort of – The vision is to be the passport of the Internet, right? So instead of just solving this for one of companies that need a quick authentication solution, we want Magic solution to be future-proof, to be scalable, to be very, very sustainable, rather than sort of this aggregation of huge amount of identity and expose ourselves as sort of this

honeypot. We want to be able to decentralize a lot of the things that we've been working on. How we manage keys? How we do identity? How we work with technologies like even IPFS to potentially even store user data in decentralized infrastructure, rather than sort of in our centralized warehouses.

[00:16:18] JM: So you're going after one of the biggest outstanding problems in the crypto space. If you go to a crypto conference and you polled the audience what startup in crypto they're working on. 5% of them will answer I'm working on decentralized identity.

[00:16:35] SL: Yeah.

[00:16:35] JM: Why are you the person who can solve decentralized identity?

[00:16:39] SL: Yeah. Well, you can't have identity without key management. Because to store this identity anywhere, it's really just data, right? Like what format is the data? And where do you store it? Do you store it on IPFS? It depends on what technology to use. But the more urgent problem at hand, nobody can really use crypto applications, because you need to download the browser extension to use it, or some other app, like a wallet app on your phone before you can even interact with the application itself. So there's a lot of barrier of entry for any user to interact with more decentralized applications.

So what Magic helps is that we are the alternative to MetaMask, which is like a popular browser extension that is very, very appealing to the mainstream user, because we make the whole blockchain experience invisible. You can just log in with your email, click Magic link, and boom! You're logged in. Automatically hooked up with a crypto key pair, right? So we make it super, super easy. And even if we don't end up owning the identity standard, we'll be the enablers for many of these identity formats to reach mainstream, right? Because we're right now securing the identity of over millions of users, and that is actually growing about 5% to 6% a week, right? So it's actually growing really, really quickly. And all of these users are now on a decentralized form of identity, whether they know it now or not.

[00:18:24] JM: The way I always describe MetaMask is that it is the jQuery of the crypto ecosystem. Everybody uses it. Nobody really wants to be using it to the extent that they're using it. You still want to use jQuery today sometimes.

[00:18:43] SL: For like a quick hack.

[00:18:44] JM: For a quick hack. And that's pretty much what MetaMask should be. It should be this transient place to store a little money so that you can engage with application, just like you store 80 bucks in your wallet. But I have spoken with people. And I asked them, “Hey, what crypto do you hold?” They'll say, “Oh, this and that. And this that prime?” Elon com rocket, whatever. And I say, “Where do you actually buy this stuff? And where do you keep it?” And they say, “I keep it all in MetaMask.” “Are you insane? You're keeping 20% of your net worth in your browser? You're nuts.”

[00:19:25] SL: Yeah. There could be like phishing scams. It is a reasonable solution for what it is. But it's really hard to use. It’s limit – Only about 10% users can actually convert through the onboarding experience. And also, it is still tied with the Chrome store, right? So there's likely going to be a lot of like phishing scams. And there're malicious applications that sort of trick the users into sending like a bad transaction, right?

[00:20:01] JM: We are maybe a decade beyond the days where you had to be afraid of what to click on the Internet because you thought it would download something that would force you to reinstall your operating system. And now we're storing 20% of our net worth in that same platform.

[00:20:21] SL: Mm-hmm. Yup. Yup.

[00:20:24] JM: Probably not a good idea.

[00:20:25] SL: Not at not a good idea. And we need to really start to think about like how the keys are managed, which is like the blockchain space, it's super distracting. There're a lot of crazy price movements. There's like insane projects coming out. A lot of people are only looking at one layer of the problem. And they sort of just assume the key management is what it needs

to be now. But it's nowhere near ideal in terms of how keys are managed these days. So I think as a fundamental issue that Magic aims to address to. Not only for like blockchain apps, but also for web 2.0, the more mainstream type of applications that would eventually benefit from a more decentralized form of identity.

[00:21:12] JM: If I look at your product evolution, I think you're asking the question, “What is MetaMask? And how can I make a better version of whatever that is?” Your first crack at that was Fortmatic. It looks like you realized that you could focus on actually a subset of what you were trying to do with Fortmatic and have a more focused and directional business.

[00:21:41] SL: Yeah, that's right. And Fortmatic was like v. zero of this exploration. It was really clear that a lot of users and developers were frustrated with a more traditional browser extension experience. So there's a lot of frustration that I picked up when I was in the space during 2017. And then, in 2018, I decided to start a Fortmatic to basically surgically tackle these problems for users and developers and sort of boost the conversion rate for blockchain applications specifically. And after a year, a year and a half in operation, we've on boarded about 30% of decentralized apps back then in all of Etherium. So that was kind of a revelation that, “Hey, maybe like the Ethereum space is still growing, right?” It's not going to be super viable if that's all we’re focused on.

There's new ecosystems popping up, other blockchain platforms, and also sort of passwordless authentication, which is sort of a natural transition from Fortmatic. Because, essentially, what Fortmatic was is authentication plus key management. It’s just packaged as a crypto-specific solution. But if we package that as Magic and make it more appealing to the mainstream developer audience, then Magic would be kind of seamlessly be the next generation from the old Fortmatic product, right? So it was kind of born naturally to sort of make the product simpler and more viable for more developers, because the end goal is we want to bridge the gap between the mainstream users and developers now with technology that is really good and sustainable for the future, right? In this case, decentralized identity and key management as a form of authentication.

[00:23:46] JM: Side note, what do you think Coinbase’s direction for authentication is?

[00:23:52] SL: I would say Coinbase's direction would be sort of maybe login with Coinbase. Similar to how you can do login with coin with Facebook, right? You can do login with Coinbase. And maybe you can grant permissions to these applications in terms of like crypto transactions and crypto signatures and different kinds of actions in the blockchain ecosystem. So I think that would make sense for Coinbase. But so will many other applications. Binance could do it. So it would make sense for, let's say, a wallet to provide login with Coinbase login with Binance sort of like as an Oauth provider.

[00:24:35] JM: Nobody's going to use a Binance wallet.

[00:24:39] SL: Well, only if they're holders of tokens that's listed on Binance. Yeah.

[00:24:45] SL: Okay. Right. B&B users, maybe? Yeah. Okay. So does anybody win the digital wallet space? Or is it a multi-winner thing?

[00:24:56] SL: I think winning is too early, right? So I would say if you're looking at the sort of decentralized technology timeline. With the Coinbase IPO, I would mark that as sort of the Netscape moment of blockchain, right? And it would mark the beginning of this movement. But that's not the end, right. And we're sort of just starting. Because, Netscape, nobody uses it now, right? But it's just to show that being the first is not always the winner of the space. And what ends up happening is different companies will specialize in different things. Even if both company could be providing wallet services, it could be for very different audiences, right? One wallet provider can be more for like enterprise and institutional asset storage. On one side, the wallet could be used for regular users on the Internet that's not storing as much money into their account. So I wouldn't say there's like a one size fits all solution, which is kind of the beauty for this space, right? It is very open and decentralized. And it actually encourages sort of like non-monopolistic behaviors from companies, but rather encourages collaboration, because it's very easy to work with another company if you are both built on the same blockchain. And in the future, even if it's on different blockchain, it will be really easy to work together too.

[00:26:34] JM: What are the subjective decisions you can make in designing a wallet?

[00:26:39] SL: Well, I would say security and UX. It's like a slider. If you go for too good of a UX, then it's really easy to log in, but introduces more single points of compromise, right? But if you move to the other side, then you may have like two or three steps before you can even interact with the wallet. You can have like multi-signature wallets. You can have social recovery and things like that. So I would say like my take on this is the ideal way to approach this is to start with the lowest common denominator, which is like in this case, email, for more like Western societies. Everybody uses email as like a verifier. But China aside, China uses phone numbers more and WeChat. So I would say for sort of email-based user base, starting with email is like a good first lowest common denominator.

And what we try to do is to make Magic more extensible, kind of like Lego pieces for authentication and security. Based on your own desire, you can add two factor authentication or add another social login mechanism to your application. So those are some of the next things that we're working on to extend beyond our basic authentication offering and add more composability in terms of like end user authentication.

[00:28:14] JM: I think you're Chinese, right?

[00:28:15] SL: Yeah.

[00:28:15] JM: Okay. Are you from China or were you born here?

[00:28:18] SL: I'm born in China.

[00:28:18] JM: You're born in China? How much time did you spend there?

[00:28:21] SL: About 12 years.

[00:28:22] JM: 12 years. Okay. And do you go back much?

[00:28:25] SL: No. I used to go once a year to visit my parents. Since COVID, I haven't gotten a chance to go back.

[00:28:32] JM: Okay. All right. But pre-COVID, you went a fair bit?

[00:28:37] SL: Yeah, like once every one year or two years?

[00:28:40] JM: What's the dynamic, the public dynamic of crypto there? Like how many people are using – Or a lot of people using crypto? Or have the government successfully crackdown on it? Is it kind of a fake crackdown where people still use it under the covers?

[00:28:56] SL: I wouldn't say people are necessarily using crypto. But I would say a lot of people are talking about it, and have bought Bitcoin. So I could be biased, because that's sort of like –

[00:29:08] JM: I hear it's a means for getting money out of China. That's the line I hear all the time.

[00:29:13] SL: I wouldn't conclusively say that without like firm evidence, but it would hypothetically make sense, right? Let's imagine like a very conspiracy sort of scenario is – But not factual. Just going crazy, right? Doing a thought experiment. So let's say if you're an investor, you can invest in sort of the mining operations in China. And then the Bitcoin that's being mined gets transferred out of China, right? So in a way, there's money, there's RMB going in, but there's crypto coming out, right? So as long as the money is coming out and exiting the system, then effectively the money is now free from China. So, I don't know. It's kind of strange how there's a lot of conversation about banning crypto. But people still are able to buy it. And so if China wants to ban something, they would ban it.

So yeah, I'm not sure. But it is really interesting to watch, because every time there has been a bull run, there are rumors and fud around China wanting to ban crypto. So it's happened many times already. But I do think that it may be a good thing to regulate it a little bit, because there are a lot of like crazy scams on there. So to protect people's investment, I think it's a good a good idea sometimes to have more supervision.

[00:30:52] JM: I don't think that's what China has in mind when they regulate crypto.

[00:30:56] SL: Yeah, no. If their intention is to ban it, I don't know. People still can buy it and own it these days.

[00:31:04] JM: When they do that, when they kind of do these fake bans, do you think they actually have the opposite effect where they make people kind of curious? Didn't they do this a year ago? Why hasn't it worked? I think people just think that and they start to wonder.

[00:31:20] SL: Yeah, for sure. I noticed this a lot, right? And this is like similar with like freedom of speech to. The more you want to ban something, the more people want to talk about it. Yeah. Yeah, it's very similar how the parallel is. The more you say, “Hey, don't look there.” People are going to look there, because I think a lot of people are genuinely very curious people. And want to learn more about the world.

[00:31:50] JM: How constrained do people actually feel in terms of expression of free speech in China?

[00:31:56] SL: I'm not very familiar with that. But as far as I know, it is definitely a very curated experience. Yeah, there's like less trolling, less vicious trolling compared to what we see on Twitter here. In a way, it is kind of nice. But in another way, that's kind of scary, because people aren't really sharing as much as – So you just don't know what's in people's head, because it's not okay to share certain things.

[00:32:28] JM: Do you think that stifles innovation in the tech sector?

[00:32:32] SL: Yeah, for sure. I think any kind of censorship sort of stifles innovation, right? I would say it's really up to the government and regulators to recognize these things and find the right balance for like startups and to innovate and being able to share their opinions.

[00:32:54] JM: The product cycle these days seems to be that you have wild innovation in the West. And then the Chinese can capture and refine whatever innovations the West creates in a way that 10X's whatever was created in the United States. And then the United States then borrows from that and productizes it. It’s kind of a copacetic relationship, but kind of horrifying at the same time, because it's going really fast.

[00:33:27] SL: Yeah, yeah. I'd say it's definitely accelerating. Now there's so much innovation and data that's accumulating. And there's definitely like a lot of really big areas of innovation. Like machine learning, AI, that's one part. But also, I think blockchain and sort of new form of infrastructure that's coming up as well, right? Like China's rolling out their own digital currency. And, yeah, there's like more talks about actually using blockchain as sort of essential piece of infrastructure that allows you to program trust into whatever you do, which was not really possible before the blockchain.

[00:34:11] JM: Consumerization of crypto, still extremely early days, right? When do we get beyond this primitive world where all we really do with crypto is like speculate? Generate pixelated avatars? And then you have this like alternate DeFi universe where you have inscrutable technology and insurance products that have no market, synthetic assets that nobody understands. Surely, there's something in the middle of these two worlds.

[00:34:50] SL: Yes. So that's a very good question. And with every technology, if the birth of every new sort of paradigm in tech, it always kind of starts a bit like troll. So the PC didn't have much functionalities when it was first introduced. It’s for kids to draw using like paint, right? And then eventually there's more program that was being built for it as it matured. The Internet too, in the beginning, people just use it for like random stuff and like message boards and all kinds of stuff, right? So I think with paradigm shifts like this, you always see a lot of noise in the beginning, right? And as the market consolidates and more entrepreneurs enter the space and actually try to find real use cases, you're going to see sort of a transition over more practical use cases, right? I think you see a lot of games on crypto these days, right?

So game, in many cases, are the drivers of like new technology even for like the more like mainstream Internet as we know today. Yeah. Also, we could we could see – My ideal vision is that users don't have to know that is backed by blockchain or cryptocurrency when they use a blockchain-based application. It's kind of like why we don't say that, “Hey, I use an app, a SQL app.” We just say we use an app, but the app could be using SQL, right? And I think the same is for blockchain.

So a blockchain companies shouldn't just be blockchain companies. They're just companies and applications. And blockchain is sort of an implementation detail that they use to implement certain level of trust in their services. For example, one really cool idea you can possibly do with crypto is making new business models. For example, imagine like WhatsApp. One way – Like a new WhatsApp with millions, millions of users. To use WhatsApp, each user can stake, let's say, $20 into their account, like 20 crypto, right? And then what they can do, this new WhatsApp can do is sort of accrue interest in decentralized finance with the deposit. And everything is transparent. For people to verify, there's a lot of trust involved there.

So then this new WhatsApp can generate revenue based on the interest. They'll take a piece. And then actually they can also redistribute the interest back to the users. So by using WhatsApp, you can actually make money by using it. And the company would make money as well, and not have to be more exploitative, and sort of sell people's information. So, hypothetically, new business models like this could emerge from the maturing like blockchain industry.

[00:38:00] JM: Okay, That's as a profound example. You got to give me a bigger example. Take it to Amazon. Give me the Amazon version. You gave me the WhatsApp version. I need to see the Amazon version.

[00:38:12] SL: I don't know. It's bit a bit hard, because Amazon touches both physical and digital –

[00:38:17] JM: Give me the AWS version.

[00:38:18] SL: Yeah.

[00:38:19] JM: Or maybe that's too much? Is that too much? Can you give me the Instacart version?

[00:38:23] SL: I can try the AWS one, because I thought about it a bit. So as scalability in blockchain improves, they would open us to more potential, like I would say Amazon competitors, right? Right now, the problem with AWS, it's great. It's good price for many

companies. But the issue is now you're relying everything on AWS. Like the essential infrastructure of your application is tied to Amazon, right. But that's sort of like privatized roads and basic infrastructure needs that we have, right?

So AWS is sort of owning all of that, like basically the essential infrastructure in the digital world. And I think that's a huge risk, right? So with crypto, you may be able to decentralize some of the infrastructure. Like, for example, storage is what people look at a lot, right? So how do you store data in a decentralized way? There're people who have been working on IPFS as a technology to store files this in a decentralized way.

[00:39:38] JM: Yeah. But can you spin this in a way where I'm making money off of my storage?

[00:39:41] SL: Yeah. So I would recommend taking a look at Filecoin, which is a pretty cool example. But, basically, imagine a situation where you can run a program and you can provide your data storage. You can stake a node with some coin. And then, basically, as long as you're providing this node service to let others store data on your servers, you can actually make money.

[00:40:10] JM: Okay. That's making money as a host though. That’s not like the WhatsApp example where I can use this service and also gain money from it.

[00:40:17] SL: Yeah. Yeah. I would say because infrastructure is such an important piece of the Internet, I think, ideally, they should be decentralized as much as it possibly can.

[00:40:27] JM: Alright. Centralized, but I probably still have to pay for it.

[00:40:30] SL: Yeah. Yeah. It'll be cheaper probably when more people provide the service.

[00:40:34] JM: Got it. Okay. All right. Let's get back to the present. So, Magic, what's your user base like these days? Like what kind of apps are using it? Do you have any flagship people you can talk about?

[00:40:43] SL: Yeah. So on the sort of mainstream application side, we have UserVoice, who is currently one of the customers of Magic.

[00:40:52] JM: UserVoice, that's a like customer feedback tool?

[00:40:56] SL: Yeah. Yeah, customer feedback. So a lot of customers go to their site and provide feedback. So they would like to improve the security and also make the authentication experience super slick, right. So the users have like almost zero friction to signing up.

[00:41:13] JM: Got it. So UserVoice is using it for all of their customer feedback integrations?

[00:41:19] SL: Yeah, yeah.

[00:41:20] JM: Wow! That's pretty big.

[00:41:22] SL: It's pretty good.

[00:41:23] JM: So that’s like an infrastructure provider basically adopting your solution to use for all of their infrastructure customers.

[00:41:30] SL: Right.

[00:41:30] JM: That's powerful.

[00:41:31] SL: Yeah. So a lot of our audience –

[00:41:34] JM: How did you get them to trust you?

[00:41:36] SL: Well, they kind of came into our website after we launched last year. And I just hopped on a call with them. And yeah, we had a good conversation with Matt, who is the CEO there. And yeah, they're willing to give it a shot. And we built out several features for them over the month. And that's how we kind of build a relationship and eventually launched with them earlier this year.

[00:42:03] JM: What was the vetting process like? You're essentially saying, “Hey, outsource the highest – One of the highest points of risk, or key point of security risk in your infrastructure. You’re outsourcing your password reset to me.” How do you convince somebody of that?

[00:42:24] SL: Well, it's a balance, right? In fact, most companies don't want to deal with it themselves. So people want to offload. There is an inherent drive to not manage authentication one’s self, right. So there's a drive to outsource that. And if we sort of prove that it's really simple to integrate, it's really secure, and we have really, really good customer support, which is really important for solutions like this, then we check all the boxes. Then we're just as competitive as other vendors that's more like mature. In fact, I would say, companies would actually prefer startups because they get better support, right?

[00:43:09] JM: What can you say about the implementation?

[00:43:12] SL: It's super, super easy. And like I mentioned, we want it to feel like Lego.

[00:43:16] JM: I don't mean how it feels. I mean, how it actually works behind the scenes.

[00:43:20] SL: To integrate the SDK, right?

[00:43:22] JM: I'm not talking about that. I'm talking what are you actually doing?

[00:43:25] SL: Well, we do different things, right? Yeah, I don't know how deep do you want to go. Yeah.

[00:43:30] JM: Okay. So I am logging in without my password. Give me the quick description of why I am doing this. What the actual use case? Like have I lost my password? Is that what's going on here? Is it my first time logging in? What exactly are you talking about? What are you solving? And then how is that actually implemented on the backend?

[00:43:48] SL: Gotcha. Gotcha. So let's go now versus Magic, right? So now what a lot of companies provide is email-based login with passwords.

[00:43:58] JM: Forgot your password. Send you an email. I click the email. I maybe get an SMS code also to do two-factor. I put the SMS thing in, and then I can reset my password.

[00:44:12] SL: Mm-hmm. Yeah. So that's sort of the flow these days, right? But in the end, the security really lies on your email already with forget your password, right? Assuming there's no two-factor that's added. So basically the whole security of your system is reliant on that email recovery anyway. So why ask for that redundant password field and offer two different flows for users to sign up, right?

[00:44:42] JM: Inherent in the status quo is that your email – Subject to two-factor authentication, your email is a point along the critical path here.

[00:44:58] SL: Yeah, so everything's dependent on an email. Even after you type in your password to login, you still have to verify your email in many cases. So there're just way too many steps to even get started with an application.

[00:45:14] JM: So what you're saying is you could imagine a world where you log in without password. You could even still do the SMS gateway. But you just don't require this norm of entering a password. And you basically say, “Okay, if you've verified that you have the rights to this email address, and you may or may not have verified your SMS, we can log you in, and then we can cookie you or whatever, and know that you're safe. You can log in from this device whenever you want. And you're not going to have to go through this again.

[00:45:48] SL: Yeah. So we don't provide that feature now. But because we're based on public private key pairs, as long as you have your key, you'll be able to log in even without email or SMS, right? Or it could be really easy for us to provide some kind of a guest mode where you can just get started without sign up on your device. And then eventually add permanence with your email and other sort of identifiers.

[00:46:14] JM: Okay, this is brilliant.

[00:46:17] SL: Yeah. Yeah. We're basically working on what people would be able to imagine now.

[00:46:23] JM: But you haven't convinced me that there is a significant point of friction in almost every product I use.

[00:46:31] SL: Yes, unnecessary friction that's not even good for security at all.

[00:46:36] JM: Yeah, it's arguably bad for security. It's actively bad for security.

[00:46:41] SL: Yes. Yes. Yeah. And, collectively, I think what the password industry feels like have been doing is, "Hey, user. It's your responsibility. It's not our responsibility." It's kind of like, yeah, taxes are hard to do. Let's make it hard so we can – Let's keep it hard.

[00:46:59] JM: But arguably, that's right posture, right? Because if you are ceding everything over to the email, which you pointed out. We're doing that whether we like it or not. But philosophically, we may be doing the wrong thing by seating – Or like at least the idea of the password represents that I'm in control. You know actually Google's in control, because Google has your email. Google controls your email. If you get taken off of Google, you might as well not exist. You're saying it's time for us to admit that. If we want to do something about that side of things, we can do something about that side of things. That's not in your scope. We need to admit that. We need to admit that the email provider has control over your identity.

And then, I guess, one thing you're kind of implying is that if you can create that acknowledgement that the email is the critical path of identity, you can make it clearer that, first of all, this is too much power to be in a centralized identity. And second of all, there can be a refactoring or a reframing of how we do identity. And it may not actually have to be that painful.

[00:48:04] SL: Yes. It will be a really smooth transition, because the goal is to get users on key-based authentication. As long as the user is on the key-based authentication, you're sort of separate from the centralized providers already, because all you need is the key to authenticate. In fact, it's actually very similar to username and passwords, right? As you know, PKI, public key infrastructure, is public and private keys, right? You keep the private key secure. And the public

key is sort of your username kind of thing. So it's the same as username, password, except it's better. It's generated by computers. But username and password is generated by the user, right, which is really prone to user errors and making like bad passwords. So the password is essentially an antiquated version of a private key, right? And the username is sort of your public identifier. So we're just doing the same thing, but with a different format that's more improved in terms of security. And we abstract away all the complexity using familiar authentication methods like email and Magic link.

But the goal eventually, like the dream is one click Login from a push notification on your device. And the challenge there would be sort of solving how do you recover like a lost device? So that's where it gets more fun.

[00:49:32] SL: Have you thought through that stuff yet?

[00:49:34] SL: Well, there's many – I think about that every day. I think figuring out how to effectively recover lost devices will be the future. And there's many ways that people are trying these days, like social recovery, I can add like five friends. And if three out of the five can vouch for me, then I get my identity back. I think like WeChat used to do this. It's is really cool. Sort of like, recognizing which one of these are your friends on your contact list. So like they'll show like 10 people, and you had to select all the people in your friend list kind of thing. I remember seeing that like years ago. Maybe it's changed these days.

[00:50:22] JM: Did you hear about how Vitalik maintains the keys for his cold wallet?

[00:50:30] SL: No. I have not heard of that.

[00:50:31] JM: Oh. So you know the whole Shiba Insu coin thing? How he got airdropped all these Shiba Inu coins and he his wealth like 10X'd or something? His wealth 10X'd from a billion to 10 billion or something like incredible like that during the crypto run up recently. And he had this this wallet, this cold wallet that everybody knew about. Everybody knew this wallet is his if you do Ether scan or whatever the tool is. Okay, this wallet is worth billions. But it's mostly Shiba Inu coin, which is obviously going to crash. So he wanted to donate it. He wanted to donate most of that wealth, liquidate it as soon as possible. So he's under this like time pressure. And

he's trying to figure out how to – He talked through this. His method of wallet security was he – I remember this correctly, he had a sheet of paper with one number, one really long number. His family had a sheet of paper with another really long number. If you add these two numbers together, that's his private key, I think. I think that was what it was.

[00:51:47] SL: That would make sense. A lot of this space one like does multi-signature.

[00:51:52] JM: And so, by the way, what he did was he bought a new computer. And then he bought a new computer, bought a new phone, called his parents for the number. Have them read the number over the phone, added the two numbers together. Logged into his wallet on the new computer and transfer the funds.

[00:52:12] SL: That's fun. Yeah, that's awesome.

[00:52:16] JM: So that's where we're at today. Can you better than that for identity? Maybe a little better for decentralized identity? Please?

[00:52:24] SL: Yeah. I think there's many like sort of I would say more innovative approaches to like managing key, where I don't know if that's what he did too. But there's sort of this multi-signature. They call it multi-party –

[00:52:39] JM: Yeah. He said there's actually more details that he couldn't talk about.

[00:52:42] SL: Yeah. It's probably. But you can basically generate a wallet signature, a transaction signature, without actually having a private key. And that's really cool. So this is like really new stuff that I think people have been looking at it, but it's only more popular since like late 2019. So what you can do is actually you can send the same payload, same transaction to multiple nodes, or multiple computers in this case, and have them sign a signature, and then get all of the signatures back. And if you have like a majority of the signature, then you can regenerate the actual transaction as if you have the private key. So in this model, you never have the private key to even begin with. I think that'd be really, really cool.

[00:53:35] JM: That's really similar to distributed systems research that was done probably 20 years ago. But that's a reimagining of it applied to this application.

[00:53:47] SL: Yeah. And, yeah, it's really exciting how there's so many paradigm shifts that's just happening in terms of infrastructure, right? And only because of crypto and blockchain, obviously a lot of noise here. But a lot of money and a lot of energy is being poured into this technology. So that now we're seeing more and more actual applications of this technology that maybe appeared decades ago, it's only seen the light of light of the day.

[00:54:21] JM: If you want to actually decentralized identity in a seamless way, do you ultimately have to do a federated proof of authority thing? Do I have to say, “Okay, I want to set up a decentralized identity system, where ultimately if I want to be seamless, I could issue a coin and I give 20% of the coin Amazon, 20% of Google, 20% to Stripe, 20% to Facebook, 20% to Microsoft. And I trust them to operate a semi-decentralized blockchain for federated decentralized identity. Do I have to do that? Or is there a way to do it that's like Bitcoin level decentralization?

[00:55:11] SL: Well, I would say like if I were to select the parties, I wouldn't sample all the big tech. You kind of mix and match a little bit. But –

[00:55:22] JM: 20% is controlled by Barack Obama.

[00:55:25] SL: Barack Obama. Yeah. So I think that's at least better than what we have today, right? So I would say that sort of intermediary step that's necessary to improve our current situation. And as technology improves, then we can look into what we can do to like fully decentralize it. But the issue with full decentralization is performance. So yeah, basically, the more decentralized something is, it's very likely that it’s slower, right? So, let's say to optimize performance, then there's change that's like proof of authority, right? And then that can go like a layer down to Ethereum, right? But on its own, it's much, much faster. So yeah, we're seeing more of this.

And I mentioned before about being able to program trust using blockchain. Is this decision between how decentralized you want something to be, right? And based on that, you can

choose different blockchains, or different blockchain related technology in your app to communicate different levels of trust. So yeah, like now we have a past there to decide, “Hey, if you want full decentralization, maybe you should use Bitcoin, or Etherium?” But let's say if you want a reasonable level of decentralization, and performance is really, really important if your application, then you can't use like a layer two solution, right? Like maybe Polygon, or a scale, or some other new layer two solutions out there.

[00:57:02] JM: How decentralized are those layer two solutions?

[00:57:05] SL: How centralize?

[00:57:05] JM: How decentralized are they?

[00:57:08] SL: My cofounder is someone who's more knowledgeable there.

[00:57:12] JM: My guess is not very.

[00:57:13] SL: It’s not as decentralized as the main chain, right? But a lot of these companies have really innovative ways to ensure that that is reasonably decentralized, right? That's why like making the right layer two solution is really, really hard, right?

[00:57:29] JM: I mean, we know where this is going. The layer two solution is fast and untrustworthy. The layer one solution is slow and trustworthy. So you route all your authentication through layer two, and you verify it later on layer one, Just like Have I Been Pwned is sort of like the, “Sorry, we can't let you know you've been pwned in real time. But we'll at least let you know that you've been pwned a year after you were pwned.”

[00:57:58] SL: Yeah. Yeah, it's kind of like the black box in airplane, right? Yeah. Yeah.

[00:58:05] JM: Yeah. There you go. Which can actually be okay, because if you – Let's say there's an SLA of a day. You got an SLA of a day knowing if your identity has been stolen from you. If you're operating on today's banking infrastructure, you've got a pretty big window to

recover transactions through the traditional banking system. Amazon's going to refund you for a day's worth of stuff. That's pretty good.

[00:58:38] SL: Yeah, that's like a step forward, right. And as someone with sort of a design background, like I would prefer things to be more like forgiveness-oriented rather than prevention-oriented, right? So instead of like I'm going to do 50 different things to make sure that I can do something. I'd rather be able to undo, right? Sort of have more forgiveness afterwards. And I think blockchain does a really good job with that, like forensics, and being able to have transparency into what actually happened. And the immutable nature makes it that really good audit log actually. So it doesn't have to be fully decentralized for some use cases. You could actually just have multiple parties, like 5 to 10 nodes that host like an audit log, right? So to make sure that there's some level of trust over the audit log instead of just one company storing in a database.

[00:59:36] JM: This is sort of the design of Ripple, right. That's like what Ripple did. It's kind of what Facebook Libra did.

[00:59:42] SL: Yeah, I think it's just different blockchains for different use cases, right? It's not that – Obviously, if there is the fully, fully decentralized blockchain with superfast performance, that will win for sure, right? But it just seems like that there're going to be compromises based on what your needs are.

[01:00:06] JM: So today, you're a fully centralized system, right?

[01:00:09] SL: Yeah. So the authentication side. Yeah.

[01:00:11] JM: Okay, got it. And I guess the most sensitive piece of infrastructure is that you're basically hosting private keys of everybody who's logging in through Magic.

[01:00:23] SL: So this is sort of the infrastructure that we use from Fortmatic. So we actually have a pattern around this. It's called delegated key management. So we're able to manage private keys without actually seeing the private key itself. So all of these private keys are generated directly –

[01:00:41] JM: Do you use zk-SNARKs?

[01:00:42] SL: Oh, no, we don't use zk-SNARKs.

[01:00:44] JM: Sorry. Sorry to interrupt you.

[01:00:45] SL: Yeah. No worries. So yeah, we generate these key pairs in the user's browser. We don't generate it in our system. So in any part of the flow, we never see the private key, right? So then the private key is sent through Amazon Cognito directly to Amazon's KMS, which is like their hardware, their hardware security module. So yeah, and then that encrypted private key is sent back to the user. And we store a copy of the encrypted private key. Not the actual private key. So what's cooler is we actually discovered this accidentally.

[01:01:23] JM: Wait. Sorry. How does the client, the user's client decrypt the encrypted private key?

[01:01:29] SL: So it uses Amazon Cognito as a middle layer to decrypt the private key.

[01:01:33] JM: Oh, okay. So they can hit – So they have the encrypted private key, and then they can hit Amazon Cognito to decrypt it?

[01:01:41] SL: Yeah. The cognito will give them access to the KMS. And then they can talk to the KMS directly to decrypt the keys.

[01:01:49] JM: Got it. Okay. So you are delegating. You are effectively Heroku for Amazon Cognito.

[01:01:59] SL: Yeah. Yeah.

[01:02:02] JM: Nice one.

[01:02:03] SL: Yeah. That's the sort of how it is now. We do have plans to reduce the platform risk on just basing it on Amazon.

[01:02:13] JM: Hey, man. I mean, you could pick a lot worse of a company to manage your platform.

[01:02:17] SL: Right, because they do they do really well in terms of like securing those hardware security modules, right. So we don't want to run our own data centers and store these hardware –

[01:02:27] JM: So Heroku margins are great. What kind of margins are we talking here? Can you share any of that?

[01:02:34] SL: Honestly, we don't have a really good idea on what that looks like now. But when we move off Amazon, it's going to be much better margins. I can say that.

[01:02:48] JM: Right, right, right. Do you think you'll move off of Amazon directly to a blockchain solution?

[01:02:55] SL: That's up in the air. That's up in the air. And I think it's really about what do we do in terms of the replacement for Amazon Cognito? And also, the replacement for Amazon KMS, right? So their key management system. So like where do we find the hardware security modules?

[01:03:16] JM: And more importantly, it wouldn't be delegated then. If you actually had your own security module, you have to delegate to somebody, right? In order to maintain what you're trying to do, you have to have somebody else.

[01:03:26] SL: Yes. Yeah. And it doesn't have to be one party. It could be many parties, right?

[01:03:32] JM: Oh, interesting.

[01:03:35] SL: So, yeah, I think that would also help with the price and further decentralization and de-risking the platform.

[01:03:41] JM: Interesting. So if let's say Google had comparable services, would you route the entire path of the key so that it's hidden from – Can you route it such that it's hidden from Amazon and Google and use both of them? Or would you use – How would you use that if you had an additional provider? Will it serve any purpose?

[01:04:08] SL: Well, if there's multiple providers, then you can do something more around like distributed key generations, right? So you don't have to generate the keys on one node. You can generate it on multiple nodes, right? So you don't have to generate a private key and send it to Amazon or Google directly. You can send a piece of it, right. So then when you are orchestrating the reconstruction of the keys, you can sort of use different nodes.

[01:04:39] JM: So nobody ends up with the complete key except the client.

[01:04:43] SL: Yes. Yeah. That's the dream.

[01:04:46] JM: Powerful. Okay. So if you did that with two cloud providers, you've proved the base case of doing that across the population.

[01:04:54] SL: Yeah. And you can even make it better. Like every time you use the key, you could refresh the keys on each of these nodes too. Basically, let's say even if Google, if one party gets hacked, then it will be irrelevant after a while, because the keys that's being – Part of the key that's being stored is rotating all the time, right? So even if a hacker, let's say, grabbed the stolen shares of the key, then there's also a chance that they would not be valid by the time they do something. So yeah, thinking about this makes me really excited. Because if we just solved the key management really, really well, then the applications will be endless, right? And if you combine that with some sort of more like continuous authentication that gets more secure the more you use it, that's going to be sort of the ultimate solution here.

[01:05:59] JM: switching up the conversation a little bit. We've just lived through this pandemic. You're working on a really innovative product. You've got how many people in your company at this point?

[01:06:13] SL: We're close to 30 now.

[01:06:14] JM: 30?

[01:06:15] SL: Yeah.

[01:06:16] JM: How many are engineering?

[01:06:18] SL: About 12 people are engineering.

[01:06:21] JM: 12 engineering. And what are the other 18 people doing?

[01:06:25] SL: We have marketing, we have developer advocates, we have customer success people, product people, designers.

[01:06:31] JM: Got it. How much did you grow during the pandemic? How many people did you go by?

[01:06:36] SL: During the pandemic, we went from around 11, I would say. 11 to 30.

[01:06:41] JM: 11 to 30?

[01:06:41] SL: Yeah.

[01:06:44] JM: How is the pandemic been across your workforce? How have people dealt with it? How have you dealt with it as a leader?

[01:06:51] SL: Yeah. I think not being able to go out and meet people. Definitely, it is challenging, because when you're home alone and you're dealing with a lot of stress, you have

to really like think about your life more holistically. So I feel like, for me personally, it's a very good like growth period. I was more focused on my own mental health and physical health, and trying to be more connected with people. I was like very, very introverted, before the pandemic. Now I'm much, much better. And I actually feel like I want to connect and socialize with people more.

And I will say, a lot of the team experienced this too themselves. And for the team, it really helped us grow in a way to be better communicators and more proactive communicators, because you have to in a remote environment. Yeah, and be more authentic and transparent about the things that we're discussing. I would say it sucks, for sure, during pandemic. But I think I think, overall, a lot of us got a lot out of it.

[01:08:12] JM: There's this breakdown of norms that occurred during the pandemic. First, it's we're all going to work remotely forever now, or have the choice to. Then there was, “Are you going to wear masks? Are you not going to wear a mask?” There were a bunch of these kinds of things that kind of got politicized. People say they were word politicized. But it's more like we all just had a bunch of identity crises happen at the same time. Should you have people over? Can you have a barbecue? Can you have barbecue if it's outside? Like even today? Can you have dinner parties? Can you have a 200-person outdoor party? There's a sign in my elevator in my building. And the elevator says you're not required to wear a mask, but it's neighborly. What does that mean? Does that mean you're a bad citizen in our apartment if you do not wear a mask? Does that mean that there's a social norm expected to wear a mask in the – And I'm not making a commentary on mask or no mask. We have a public identity crisis. We have a breakdown of social norms. Has that affected you?

[01:09:23] SL: Actually, I've been pretty secluded. Actually this is the first time I heard about that.

[01:09:27] JM: Do you agree with me on that though?

[01:09:29] SL: Yeah. I would say, lean into science. If, let's say, there's really good evidence that like most people, like 80% people got vaccinated in San Francisco, then maybe we should lean into sort of getting back to where we were, right? So that's sort of like my personal opinion.

[01:09:52] JM: What if I see a hyperlink with a scientist that says we've got vaccine resistant variants on their way.

[01:09:59] SL: That, we'll have to know –

[01:10:01] JM: Or there's a 50% chance that we have vaccine resistant variants on the way. It's like I have this like – It's like in my head I'm like writing numbers on a chalkboard and like the chalkboards gotten to – Like it's filled with all these numbers and these calculations and these probabilities, and I can no longer come to a conclusion of the expected value of wearing a mask.

Okay, I get it. It makes me a little bit incrementally safer. But it restricts my ability to have human to human casual interaction with the people I bump into in the building. Is that cost worth the benefit of being slightly healthier? I don't know. I'm trying to do the calculation. I can't do the calculation. And now I'm a pariah to society.

[01:10:48] SL: Yeah, yeah. Like, yeah, I don't really go to a lot of crowded areas.

[01:10:58] JM: But with your newly discovered extraversion, you're going to have to.

[01:11:01] SL: Not like crazy a lot of people. Like I think 30 people, that's like a reasonable amount. But if the company gets bigger, then obviously we'll have to have a separate conversation there to decide like what's the mask situation like. But I find the bigger part of the problem is there's a lot of like information out there. And some are true, some are misinformation. So it's like really hard to know what the actual percentages look like. And also this situation is kind of new to a lot of us.

[01:11:40] JM: That's an understatement.

[01:11:43] SL: Yeah. I think I have faith in people figuring it out as we go. And I think, yeah, being more open-minded and do more research on the things that we're reading. And it's good to be more cautious, in my opinion too. In any situation where it's like, “Okay, I'm not sure.” Then

maybe mask is a good idea. But let's say if it's like with people I know, with a smaller group, then maybe we can like relax that a little bit. So, yeah, I think it's very flexible. There's no like one or the other, right? Purely no mask, or all everyone masks. It's flexible, because where people, and situations are dynamic from person to person. So I think instead of like needing like one authority to say, “Okay, what we should do here?” Maybe people should think more for themselves and sort of adapt to their own situation.

[01:12:45] JM: Wrapping up. Any reflections on product development? So I see you as a very sticky, persistent entrepreneur. You had Fortmatic. You pivoted. The pivot looks awesome. There are people who are going to be giving up before they find the thing to pivot to. How do you advise people? And probably sometimes you should give up. I mean, in my career, I've built products that were going nowhere. I gave up, sometimes I regretted it. Sometimes I've really big regrets about giving up, because I think in retrospect, “Oh, if I only would have done this move, I could have done a little bit better. And maybe that would have worked.” Because you get really lost sometimes with your product. You're like, “What the hell am I doing? I've been working for two years on this thing, and it's terrible.” And then other times you wake up in the morning, you know exactly what to do. You have the week-long vision. You have the year-long vision. You have the minute to minute vision for what to be doing. So how do like navigate those different states of mind and keep yourself going?

[01:13:55] SL: Yeah. I think a lot of people don't see the projects that haven't worked.

[01:14:02] JM: I'm sure you have a lot of them. I’m sure you have a big graveyard.

[01:14:04] SL: Yeah, like insane, right? So those are all things that give up. And I just felt maybe there's no founder product fit, right? I think that's also really, really important. So, for me, when I decided to work on Fortmatic/Magic, I felt like I have to work on something that I perceive as almost art. It's not necessarily, “Okay, I need to make this company so that I can address this market and make money.” Obviously, like that's a standard. But that's sort of like a tiny piece of the equation.

What I want to build is something that is inherently good and is sustainable in the long run, right? Let's say if Magic worked out with decentralized identity, then the whole internet would

benefit from that, right? To me, working on projects like this gets me really excited every day. It's a huge and extremely difficult endeavor. But it gives me the energy. And even if, let's say, for any situation it doesn't work out, there's no regret, because I tried the biggest thing that I could do. And also there's a sort of like founder product fit to here. Like in terms of making good developer experience, it's really difficult to compete with like our team's intuition, right? I think we'll be able to build a following of developers and really kind of push this product and vision forward that actually is sustainable for the future, rather than at some point, we'll have to be more like exploitative, right?

Yeah, I think that gets me excited and almost approach it as like an art project that spans multiple years instead of, “Okay, let's cash out quick here.” I don't want to do that. If I wanted to do that, I would have launched a token like way earlier.

[01:16:09] JM: It’s never too late. I see the long con. The long con. It’s just waiting a little bit longer for the token.

[01:16:17] SL: Well, you need the network before any kind of token. I don't want to do the thing where I launch a token where it just wouldn't make sense just to raise money.

[01:16:27] JM: Yeah, I think you should do. I think, eventually, I hope you do a token or something token-like. That would be awesome. I think the token-driven economics are so powerful for a business like what you're building.

[01:16:41] SL: Yeah. I think when we get to a place where I'm satisfied with the decentralization that we're providing, then it would make sense, right? But right now we're very focused on the developer platform. Make sure that Magic is giving our customers what they need, and on the side to do research and improvement on the existing infrastructure continuously to eventually get to that place where we have a decentralized identity. It doesn't happen. Rome is not built overnight. So this is kind of our path forward. And it's the same with Docker. A lot of effort goes into the open source side. So for us, the open source is the research and improvement on decentralization. And around that, we have the company right? So as say as we grow and Magic is successful, then automatically it will be providing the more open and decentralized and more sustainable infrastructure for identity.

[01:17:44] JM: Sean, thanks for coming back on the show.

[01:17:45] SL: Yeah, thanks so much, Jeff.

[01:17:47] JM: Great talking.

[01:17:47] SL: Yeah.

[END]