EPISODE 1447

[INTRODUCTION]

[00:00:00] JM: Crypto companies have cemented themselves as a company category that is not going away anytime soon. Bitski is a company that makes web three tooling and infrastructure including a wallet and a collection of tools for creating and selling NFTs. Patrick Tescher joins the show to talk about the engineering behind crypto infrastructure and API's.

[INTERVIEW]

[00:00:19] JM: Patrick, welcome to the show.

[00:00:21] PT: Thank you.

[00:00:22] JM: NFTs, I think many people in the audience are hardcore software engineers, they probably work on infrastructure or enterprise applications. They may be skeptical of the concept of NFTs. Can you start off by describing why there is value in the idea of a non-fungible token?

[00:00:46] PT: Yeah, absolutely. So since as a technical audience, there's probably sort of two sides of NFTs. One is potentially the content behind them. We see this in digital art. We see this in potentially music, all sorts of things like that, that NFT's are tied to. And then of course, there's the underlying technology that controls NFT's mostly based on Ethereum blockchain. And so there's sort of two separate concerns there.

As far as the art, a lot of what we've seen there mimics the real world art market, and NFT's are just sort of a way for that real world art market to be sort of mirrored in the digital world, and for digital art to sort of get the same treatment that fine art does. You see a lot of complaints around this around, people limiting access to these markets, people spending a huge amount, those are all largely things that you also see in the real art market. And so, a lot of the NFT art space has really just sort of copied the playbook from the art market as a whole. So, there's pros and cons to that.

What we are seeing, though, is that there's sort of an emergence of artists who create digital art and really haven't had access to those fine art markets, because those markets only deal in specific kinds of art. So, those digital artists are all of a sudden being recognized the way that traditional artists have been. I think, there's only really a positive side to that, right? A lot of the younger artists these days are creating art online and art on computers, and they should have access to the same markets. And then, we're also seeing these sort of – it started with CryptoPunks, and we're starting seeing this evolution of sort of, it's basically generative art, a limited set of generative art pieces that are being collected, being issued as NFTs. This is sort of like how NFT started. So, a lot of it has to do with sort of being original and being unique. And that space is, it's a very interesting space, it's new, it's brand new, nothing really has existed like it before.

There's a lot of people trying to hop on and then scam people, and all the sort of things we see in an early digital market are sort of emerging there. On that side, there's a little bit of technology on the art generation side. But largely, these are being powered by the same NFT ecosystem, the same NFT technology. And then there's also like a third use case of NFTs which is things like music or digital real estate, sort of areas where other people have been unable to really create a great online marketplace and NFTs are providing that. All three are sort of being grouped together as NFTs even though NFTs as ethnology is really just like a database of who owns what.

[00:03:41] JM: So, the infrastructure needed for NFTs, s I can issue a smart contract that guarantees the uniqueness of a JPEG or an mp3 file or video file or anything and I can put that asset in my wallet. What are the engineering challenges around delivering and recording that transaction?

[00:04:18] PT: Yeah, so there's a few things involved there in ensuring uniqueness. For one, you can't really insure the uniqueness of an image or even of a video or anything like that, right? What you can ensure the uniqueness of isn't NFT. So, what a lot of these NFT projects are doing is actually saying, okay, the image is not unique. We're going to release the image in a creative commons way, and what we're going to do though, is basically point to the NFT and saying the NFT is actually the real representation of this piece of art or this image. And the NFT

is unique. It's represented by a 256 bit integer typically on a smart contract, usually an Ethereum. And you can sort of prove that only one of these copies exists, and you can sort of look up its owner. You can look up the history of its owners.

So, if someone is claiming, “Oh, this is the original, this is original.” You can sort of look at who owned it and tie it back and sort of prove beyond reasonable doubt that this is the unique instance of this. An interesting thing there is that this is not sort of unique to NFTs, right? This is basically the original problem that Bitcoin solved, which was in their case, a double spend attack. But the idea is, how do we keep track of a history of an item and who owns it without having any sort of central authority, and the NFT sort of standards that are out there provide that. But what some people have done is kind of sort of a step further there, and to say that, “Okay, well, we can't really ensure that the image is specifically unique”, but we can point NFT at like a hash of the image and add sort of an extra layer of uniqueness to that NFT, where the NFT is ID points at a specific hash, of a specific JPEG, and you already sort of know, “Okay, this JPEG is always going to generate that hash.” So, there's sort of two levels of uniqueness there.

But really, as far as uniqueness goes, it's not really saying there's only one person who owns this JPEG. It's really about saying this is the original version of this JPEG, here's when it was created. Here's all the people that owned it and here's where it ended up. And that's often what's more exciting with NFT projects is less about the actual, like visual representation, but more about the social dynamics of who's owned it, who minted it, who the other potential collectors are of similar pieces of digital art, or similar NFTs and how they're all related.

[00:06:46] JM: So, on your side, building wallet infrastructure for NFTs and API's for NFTs, can you describe the engineering challenges for delivering those tools at scale?

[00:07:00] PT: Yeah, absolutely. So because NFTs are built on the Ethereum blockchain or a similar blockchain, there's a whole sort of new set of tools that are needed to interact with NFTs and with the blockchain underneath. And I liken it a little bit to when computers were brand new, and people are sort of figuring things out, right? So, the Ethereum blockchain sort of gives you a CPU and a disk, and says, “Okay, build whatever you want.” And people have built up these applications that control these NFTs. But ultimately, one of the problems with it is that because you have these really low level primitive objects, there's no sort of API's on top of it. There's no

AWS built on top of it. All these sort of systems we rely on, these programming languages, middleware, all the stuff that exists in a traditional software stack, you sort of have to throw out and start from scratch.

One of our original challenges with that was how do we access a wallet? How do we access a blockchain? How to access NFT? And when we started Bitski, our idea was to launch just several fun projects, put them out there and sort of see what sticks. We quickly realized that it was almost impossible to build like a small fun project on Ethereum at the time, because all the tools that you'd expect weren't there. The wallet infrastructure was incredibly difficult to use. The token, basically indexing the blockchain was almost nonexistent at the time. And all these problems made it really difficult to launch anything. So, we ended up building our own sort of internal tech stack on top of the blockchain to build the types of products we want. And that internal tech stack is actually eventually what became Bitski. Some areas are API's. Some areas are user interfaces. It's sort of similar to the idea of like an operating system. Ethereum provides us computer, but it does not provide an operating system. So, it's hard for both developers and for end users to really access it. And Bitski tries to provide like a common set of tools for both developers and end users to interact with that computer, much like you might have in like a basic desktop operating system.

[00:09:25] JM: So, if I want to use Bitski to acquire an NFT, how is that different from other wallet infrastructure? There's plenty of other ways I can acquire an NFT. So how does it compare?

[00:09:48] PT: Yeah, so the standard way that you might get an NFT today, if it were to sort of the first time the NFT were created, is you would go find a project that's creating NFTs, and they would probably expose is a function on a contract somewhere that would let you mint an NFT. These days, they'd probably also whitelist that NFT and create a list of people who are allowed to mint it. And so, you try to get on the list, you'd install a wallet, typically say, MetaMask, where you would generate a private key. It would walk you through some steps to try to secure that private key. And then eventually, MetaMask would interface with the contract, sign a transaction on your behalf. You would need some Eth to pay gas in order to access the network in order to meet that NFT.

And then once that happened, the NFT would sort of show up within that contract under your name, you wouldn't necessarily see it unless you went to a third-party site that told you where those NFTs are. Or you could sort of manually add it to MetaMask, and it would sort of keep track of it for you. And then, most people would end up taking that to a site like OpenSea, which is sort of a digital marketplace for NFTs where it would show up with its image and its name and everything, and you'd have options there of buying and selling and that sort of thing.

That entire process, once you've done it, 5 or 10 times like a lot of people in our in a sort of NFT ecosystem have done, it gets relatively easy to do that. But as an initial user, the first time around, there's a huge sort of onboarding step that is quite difficult. And so on Bitski, what we've done is we've sort of abstracted that all away, and the first time you come to a Bitski NFT sale, you find something you like, you click buy, we have you sign up for an account, username and password, you can autofill that from your password generator, we ask for your credit card. And then we just charge your credit card both for the cost of the original NFT, if there is one, and of the gas to mint and everything about that for you, and we generate a wallet for you that we store that NFT in that wallet. We secure in a hardware device called a Hardware Security Module or HSM, so that it's still completely secure, and there's not a bunch of security risks there. And then we put that NFT into your wallet, and we show it to you in a nice easy to interface.

So, the experience for you as a user is that it feels a lot like using an Amazon or a Shopify store of buying something, and then it just shows up like you'd expect, with its image and its name in your wallet, and you can move it around and transfer it, that sort of thing.

[00:12:32] JM: So the added functionality of a Bitski wallet, and the ways that people transact with it, has that led to any NFT behavior or transactionality that has surprised you?

[00:12:53] PT: In some cases, yes. The NFT ecosystem, if you sort of look at it is relatively small, and there's a small number of buyers and sellers buying and selling most of NFTs. One thing that we were sort of expecting our products to appeal to, people want to buy NFTs, but also to people who don't know what NFTs are, and maybe see a mixture of that. For some projects, we've seen a huge number of people buying NFTs who've never owned an NFT before, who find an artist or some sort of project, they like, they want to support it, they buy an NFT from that project, and they're happy with it. They don't need to own other NFTs. They're not

really an NFT consumer. They don't even think about what they bought as an NFT. They just like to support a project or an artist and, they did that.

So, on some of these projects we're seeing, it completely moves around where 99% of the people buying these NFTs have probably never bought an NFT before, may not even know really what an Ethereum wallet is or what a blockchain is, and still got to participate in this ecosystem that is being built out.

[00:14:06] JM: You also have tools to allow for distribution and management of NFTs. If I'm an artist, I can distribute my NFTs on your platform. What's required? I mean, when I think about that, it sounds like almost like an email platform like a Mailchimp kind of thing. I can imagine entering a bunch of addresses and sending NFTs to all those addresses. Is that the kind of functionality they have to build?

[00:14:38] PT: Yeah, exactly. So, in the NFT world, everything is new. There aren't those tools exist. There's no Mailchimp, there's no Twilio, there's no Shopify. So one of our first projects was to build sort of a Shopify. Most of the NFTs at the time were being sort of bought, and so we wanted to build very simple e-commerce platform that just lets you bind NFT. Underlying that infrastructure is a simple API we built that will take an NFT, and put it into any wallet you want. You don't need to know about blockchain, you don't need to have a wallet. It's just a developer API REST endpoint. You can hit it and we process the rest for you.

That API we're exposing to developers today. But we're also building tools around it, like you said, to take a list of email addresses or list of phone numbers, or any sort of contact list you already have, and potentially distribute NFTs to all the people on your list. And that requires actually a bunch of steps. The first of course, is that you need to deploy the code to process your NFT. We would call it smart contract. The next bit is you need to potentially provide all the content, the names, and images and everything for NFTs. And that third bit is you need to then need to associate unique NFT IDs to that content, and put those in the wallets of the people you're distributing tokens to. And that process is relatively complicated. Most projects that are successful, have sort of blockchain developers on board, people building out really low level primitives and providing sort of bespoke solutions.

In our case, we've taken some of those solutions, sort of made a generic version of them and create an API that we think works for most developers, where they're able to treat the blockchain as more of like a traditional REST endpoint, and they don't need to know about any of the underlying fundamentals. That's helped both develop products internally. We have new products coming out around NFTs that are using those API's. But it's also helping third party developers who don't want to build that infrastructure themselves to still access NFTs, create NFTs just like they would accessing a Mailchimp API.

[00:17:02] JM: Can you tell me about the infrastructure in more detail for issuing NFTs? If I do a drop of a bunch of NFTs to a bunch of people, just give me a sense of your stack.

[00:17:14] PT: Yeah, sure. So anytime you interact with Ethereum network, you basically have to sign a transaction. In our case, we have an Ethereum wallet that has a bunch of Eth in it in order to pay gas on the Ethereum network. And whenever someone wants to interact with something, we end up establishing transactions on our end. So, the first sort of step of any of this process is making sure there's a wallet that has the funds necessary and the permissions necessary to create NFTs. We've been calling those enterprise wallets because they offer a shared wallet that a whole team can use. Traditionally, each action on the blockchain required a user to sort of manually go and sign a transaction. I'm using MetaMask. That's great for like individual projects. But for a company like ours with dozens of developers, we sort of need to have programmatic access to those wallets. So, it sort of starts there.

And then, sort of the next step would be, having all the content from the creator of the names, the images, all the sorts of things they want to attach NFT available, so that when we create this NFT for user, it's all there. That's mostly just a traditional database backed, CDN back system. And then sort of the third part, which is getting more user focused is that today, in the Ethereum system, when you want to send an NFT to someone you need to know their Ethereum address, or at least a way to look it up. As sort of a traditional developer, you don't necessarily have those access to that with your – you might have a mailing list to a bunch of contacts, bunch of app users. So, we do something what we call lazy minting, which is that all the NFTs are sort of created ahead of time. But in order to get them into a wallet, someone has to redeem them.

We create redemption codes for each of the NFTs that can be redeemed, and then users can be sent those redemption codes via text, via email or any sort of traditional system. And when they click on them, we go and ask for them to like connect a wallet, whether it's a Bitski wallet, or a different kind of wallet, and then that lets us look up the address, and then we can mint the token into their wallet once it's delivered. This means, of course, that if people don't redeem those tokens, they don't show up in their wallets, and the tokens essentially aren't even created at all. But for anyone who has redeemed one, it then appears in their wallet after they've sort of gone through that process. This sort of acts as a bridge between the Ethereum world and the blockchain world where everyone has a wallet with an address associated with it. The more traditional marketing and software world where you have a bunch of users with some amount of contact information for them, and no concept all about their connection to the blockchain, and it allows those companies to bring users in through this quite easy to use redeeming flow and get them connected with other NFTs.

Of course, if you do know the address of a bunch of wallet holders, we've seen this a bunch where a creator might create a sort of collection of entities and then another collection in the third collection, and they say, “Okay, anyone who owns one of each of my collections, one NFT of each of my collections, I'm going to go ahead and drop them a fourth NFT, that's just for people who've sort of supported me the entire year.” And those types of NFT drops are getting more and more common. In that case, you do know the address of other people, and you can sort of do a onetime bulk drop of all the NFTs at once.

[00:21:05] JM: Can you give me a sense of the volume that you're seeing across the NFT infrastructure?

[00:21:13] PT: Yeah, I mean, there are certainly thousands of NFTs sort of being created every hour, probably. Most of those NFTs are not sort of going anywhere. But the reporting we have shows billions and dollars of NFT volume trading hands every month, millions of active users involving in that ecosystem, either receiving or sending or transmitting or doing something with an NFT every day. That sort of growth continues and it's actually an interesting problem, because as NFTs grow, and as that sort of infrastructure grows, the dataset becomes more and more difficult to work with, and the scalability of NFTs becomes a problem.

So, we've already seen this on Ethereum main net, where NFTs can really become prohibitively expensive very quickly when multiple projects are happening at the same time. So, the larger sort of Ethereum project itself, is trying to solve this through a system they call sharding. But there's a larger sort of ecosystem where people are putting NFTs on Ethereum like chains all over the place, moving them around, and sort of expanding that system onto chains that are much cheaper, where the NFT minting is much cheaper, where the buying and selling is much cheaper. On some of those, the users don't actually have to provide any sort of like Ethereum payments or gas payments at all. So, the volume on those chains is probably, I think, we're going to see like exponential growth there pretty quickly, as those sort of barriers to entry sort of fade away.

We're also seeing more and more creators getting involved outside of this core crypto audience. In some cases, those creators sort of have the best intentions in mind. And in some cases, they don't. So we're seeing pushback from some industries there. But a lot of what excitement we're seeing on sort of the tech side is around the idea of connecting NFTs with other projects, making them more useful than just sort of a digital asset. That could be using them as like a ticket to get into a special event. It could be using them in a virtual world as a piece of clothing, like we're seeing fashion, potentially go into the NFTs. It could be art, can be music, and as the NFTs evolve, and the sort of the use cases expand, we're seeing people come in from industries that are expecting to be able to drop 10 million NFTs to other users. So, the entire infrastructure for NFT minting, for NFT ownership, for the middle layers, that sort of power NFTs, is all sort of expanding very quickly to capture that demand.

[00:24:09] JM: So, when you look at the current applications of NFTs, it's mostly things like art, and digital goods, and perhaps other kinds of collectibles. Is there a route to more – I guess there have been some experimental stuff like NFTs for real estate. How much of that practical application of NFTs has made it to production?

[00:24:38] PT: Yes, so most of these projects that want to put into production, it's a sort of an untested, unproven technology for them. And so, they've learned from technology adoption in the past that it's probably not best to just sort of adopt that immediately. We're seeing at the moment, I would say, it's a stage where companies that want to use NFTs for use cases are launching sort of small projects to sort of test the viability of NFTs as a solution. And we're

seeing that I think sort of in a bunch of different sectors. I would say that as far as like being in production, the best example would be sort of these open virtual world video games. There's one called Decentraland, which is sort of pure Ethereum. There's one that we like a lot called the Sandbox, which is sort of an open world sandbox building game where you can build assets. One of the use cases they're using for NFTs is sort of owning a plot of land in a large virtual world.

It's not adapting to real, real estate, but sort of virtual real estate. By adopting NFTs in like an area, like a virtual real estate game, you get access to not only the non-fungibility of NFTs, the transferability, the ownership later of NFTs, but also the sort of ability to bridge that with this sort of decentralized financial network that lets you trade currencies and things like that, and able to create like a real estate market pretty easily. That's an interesting thing that I think a lot of other companies are looking at as well, once you create NFTs, once you bring them in, you can bridge those to the other aspects of Ethereum, like defy and trading, and create marketplaces without really having to write any code yourself.

So, these games now have access to this giant digital marketplace, these digital trading grounds that exists through a bunch of different sites, through a bunch of different protocols and services, and it lets people create sort of their own aspects of the game as far as like trading and ownership goes.

[00:26:48] JM: So, when you look at the different blockchains, and how they implement NFTs, or I guess how NFT contracts are issued on top of them, can you draw comparisons between, for example, Solana and Ethereum?

[00:27:08] PT: Yeah, absolutely. So, when Ethereum first came out, there were almost no smart contract chains. The issues that come about when you're creating smart contracts, or creating these sort of distributed computers, weren't really known yet. Some of those involved throughputs. Some of those involve gas fees. Some of those involve programming languages. A big one, obviously, that we've been seeing, it was the sort of reliance on sort of a proof of work mechanism, basically taken pretty much directly from Bitcoin, to power, the sort of underlying network and the underlying economy of Ethereum. All those have various solutions from various people that sort of solve them, right? So, each one of these other chains is saying, “Okay, here's

a problem with Ethereum. Here's a list of solutions. I'm going to pick one, and launch a new chain on it."

So, there's pros and cons to each chains answer to all the problems of Ethereum. One, for instance, is the idea of how do you execute transactions? How do you mine transactions, without sort of a proof of work system that's potentially very energy intensive and expensive. So, some chains are somewhat more centralized, some chains have adopted more complicated consensus systems. A lot of chains, including Ethereum themselves, their idea is to move to what they call proof of stake, where instead of doing a bunch of intensive computation in order to get rewards and participate in the network, you would lock up some of your Ethereum and put it in a smart contract or something somewhere, and then you would get access to that. Now, the network of people who are involved in sort of the mining and running of the chain becomes much smaller, because it's only the people who can put up a certain amount of Eth.

All those systems have their different tradeoffs, and so most of the chains out there, there's no like sort of silver bullet yet. There's no one chain that's done everything right. Most of the chains are basically taking some of those little knobs and adjusting in one way or the other. Even with something like proof of stake, which is most likely going to be the future of Ethereum, if you were to launch a new chain, you have the problem of how do you distribute the coins in the first place. So Ethereum sort of distribute a lot of coins to various ways, one of them was proof of work. Now, they can switch to like a proof of stake system because a large group of individuals have their tokens in their wallets already. But a new chain launching tomorrow, it's very difficult to use proof of stake because the original creators of the chain essentially have all the coins in their wallet, and they're the only ones who can sort of stake anything.

So, building up a new network from the ground up there is quite difficult. There's another type of network, we're sort of referring to L2, and L2 networks use Ethereum as sort of a way of – they basically write the state and read their state back from the Ethereum main net, and they're able to partially secure the network by relying on Ethereum itself. They're also able to potentially have their gas tokens bridge to Ethereum, and there's some pros and cons there. So, there's a lot of tools that you sort of get for free when you bridge to Ethereum. The downside, of course, is that you're still tied to Ethereum main net in some way. You're still relying on what's currently proof of work. You're still relying on a chain that has sort of slow throughput, but we're definitely

seeing a rise of L2 products. The L2 solutions generally have much faster throughput. The transaction minting fees are much cheaper. Bitski is evaluating a bunch of other chains like L1s like Solana, as potential future replacements for Ethereum. But currently, Bitski is focused on Ethereum or Ethereum compatible chains.

So, we announced a partnership with Polygon recently, where we include Polygon tokens in our wallet. We're going to announce the ability for creators to use polygon as well, in the near future. And on both the creator side and on the user side, Polygon gives them the ability to mint for a tiny fraction of the cost on Ethereum. It allows tokens to be transferred much quicker, and in a lot of cases, it allows on the user side for gasless transactions where the users don't need to have a bunch of gas in their wallet, to move NFTs around. And that is lowering the barrier to entry for NFTs, which is great for certain projects. It's also creating an opportunity for spammers and scammers to dump all sorts of NFTs into people's wallets. So, as we move to those cheaper chains, and as we move to those projects that are enabling that, we need to focus on, how do we make sure that there's better spam control? How do we make sure that people aren't dropping like inappropriate NFTs in the chain, and that we're showing them in various wallets? All those sorts of things.

[00:32:28] JM: Something I don't understand is why it's expensive to mint NFTs, and why you couldn't just, for example, maintain a database of all the NFTs that you wanted to, in IPFS.

[00:32:47] PT: Yes, so there have been digital assets created before. NFTs, aren't the first digital asset, right? Traditional assets in the past that are stored in some sort of database, rely on someone to maintain that database. I think when a lot of people think about NFTs, they think about sort of the end result of them, which is on the user side of NFTs, which sort of is important. But what's really interesting about NFTs and where they deviate from the idea of just a bunch of assets in a database, is the rules around NFTs and how they're created. So, an NFT, for instance, that is minted on chain often cannot be taken back by its own creator. It is permanently in the hands of the person who's bought it and received it, sort of in the way that if you, as an artist sold a painting to someone, you can't just take that painting back whenever you want, you can't just destroy that painting whenever you want.

This is allowed sort of these digital creators to build on top of the chain in a way that respects both them as creators, and the consumers and users of their products. We've seen time and time again with digital content, whether it be on YouTube or on Facebook, where people build a business based on a platform that's effective for them. And then the platform goes and changes the rules underneath them. It changes the algorithm. It changes the types of content it's hosting. And suddenly, that entire business is gone overnight.

What the blockchain allows us to do is to create that database of users in a way that neither the original creator nor the user of the database can change the rules fundamentally. This allows you to not only sort of build a business on top of it, right? There are people who professionally buy and sell NFTs. There are people who buy NFTs on behalf of a large group, sort of an investment fund and issue like currencies to that group. Each one of these businesses knows that the platform underneath it, that NFT platform, that Ethereum platform is not going to change underneath them. It makes it so that they can invest potential and draw out some money in those projects in those companies they're building.

I think, this is sort of – what we at Bitski see is the future of NFTs and the future of blockchain is not necessarily someone minting NFT and selling it to one person and having that be the interaction. It's potentially layers of different service writers, layered on top of each other, using each other's API', using smart contracts, and building out solutions for users that might involve multiple NFTs, that might involve other digital currencies, that might involve smart contracts around real estate, and combine them all into a single project in a single product. That's something that you can't really do today on any API's. There are certainly API providers like Amazon, who are very trusted, or Twilio or SendGrid. But for various reasons, even on those providers, the underlying infrastructure could disappear tomorrow. If your long term business is built on the idea that that infrastructure will exist forever, then you're in a very risky position as those change as you try to adapt.

[00:36:16] JM: Right I see. So really, there's just been something about the universality of the Ethereum centric NFT contract.

[00:36:27] PT: Yeah. So, when computers were originally coming around, most people interact with computers via some sort of mainframe. Those mainframes were centralized, they never

had to deal with the issue of multiple people interacting in different ways. They never had to deal with spammers and things like that, because they sort of controlled access very strictly, and it was very simple. When you wanted to like send someone an email, you just basically wrote an email file into their folder, and then they send you an email, they wrote you an email file in your folder. Those mainframe systems were much easier to code for, but really hard to access. So, as you all got personal computers, they became much easier to access. But we had to trust these sort of third-party API's in order to use them.

Ethereum is sort of like a mainframe again. And it's a mainframe that has access control in a way where no single person controls it. This is allowing us to sort of write a whole new type of software that isn't owned by anyone in particular, but where everyone can kind of see how the code works and how the underlying protocols work.

So, NFTs actually evolved out of – the reason that an NFT exists, is because of a standard called EIP 71, or EIP 721. And EIP 721 came out of this Ethereum proposals project, and there's this idea of creating standards on Ethereum that many contracts can implement, right? The reason that one NFT can behave the same way as another NFTs because they both belong to the same standard. They both implement the same standard API Interfaces. I can verify that both NFTs implement the standards, I can sort of trust that and I can build layers on top of that. That sort of shared computer, even on IPFS doesn't really exist, right? IPFS can have shared data, and a lot of the Ethereum contracts use that sort of shared data. But there are no rules around it. There's no logic around it.

So, essentially, if you want to change the data, you have to tell everyone, “Hey, I'm the source of authority here, and the new data is over here.” When you do that, you have complete control over that API, over that protocol that you're building. If you change the rules, everyone who's built anything on top of your IPFS database has to go with this new set of rules. There are still mainframes in use today, in areas where the sort of distributed computing doesn't work. A lot of them are in banks, or places like the Nasdaq Stock Exchange, right? They're basically still using a mainframe to do day trading everywhere.

Those were sort of the first software, the first applications that were developed on Ethereum, were essentially re-implementations of these sort of mainframe pieces of software because we

suddenly had access to a mainframe like system that can be used by anyone anywhere. You see stock trading applications. You see stock trading, smart contracts. You see currency trading, smart contract. You see banking, sort of smart contracts. Those are all the obvious first use cases for the sort of Ethereum computer. Now, uou're seeing NFTs which are sort of somewhat new, right? They didn't really exist before. But they're using that same idea as the stock trading applications say, “Okay, this is just an edger. This is who owns everything. Here's sort of the history of it. Here's the current balances. And if you try to move an NFT around that you don't control, you're not allowed to.”

But I think that as we’re moving forward with Ethereum, we're seeing more applications come into play, more types of applications. I imagine there are other areas, especially any area using like mainframes today, there's pi logistics companies that can be on blockchain. Once you put all those technologies, all those smart contracts all the standards in one computer, you can build applications on top of it, that execute essentially atomic transactions across all those applications, and it opens up a ton of possibilities for all sorts of new use cases. And NFTs can be sitting on top of that. NFTS can be part of it, sitting underneath it, and I think the types of technologies and the types of solutions we're seeing that use NFTs, we haven't even really like begun to scratch the surface there.

[00:40:47] JM: Give me a little bit more of a window into what your engineering stack looks like, in terms of difficulty. So, what are the hardest problems you have to solve?

[00:40:57] PT: Yeah, so one of the issues we have with our stack is that we're dealing with what we would call unsigned transactions, and then transaction signing. There’s like a chain of trust between the user and the interface we provide for them. And then, they hit yes, I want to approve this transaction. And it goes through a series of steps where it reaches our hardware security modules and get signed, and then relayed back to the network. Once a transaction signed, it's public information, it's available to everyone.

But up until that point, at any given step, if someone could manipulate that data, if someone could create a transaction and sign on behalf of another user, or if someone could modify a transaction the user signing to be to point at something else, that's a huge security risk for us. So from the ground up, when we were building our system, we decided to build it on Rust, which

it gives us two advantages. One is it avoids a certain type of bug, buffer overflows and things like that, largely memory safety issues, that basically lets us sort of ignore a certain type of attack on our system.

The other thing it does is give us very good performance for all over low level infrastructure. And so because of that most of our level infrastructure is written on top of Rust. Rust is also used somewhat extensively throughout various blockchain projects. So there's some tooling available around blockchain that wouldn't be in other languages. And Rust has been great for us internally, it's been a really fun language to work in. It's a fun ecosystem, but it is somewhat new, and there are challenges around the fact that Rust is just changing constantly and evolving, and we have to sort of keep up with that.

The next step up that was a challenge for us is probably the fact that we need to secure these keys. And so securing keys, we haven't seen a way of doing it, where the keys are in any way ever, in like a standard computer's memory that works in a really secure way. We've opted to secure all our keys in hardware security modules, those hybrid security modules are – they've been used by banking industries and other industries for decades. They're incredibly good at securing private keys, and letting us still sign messages with those private keys.

But the security modules that are available in the cloud are relatively difficult to use. So, they don't essentially provide all the features that we would need. We've ended up having to run our own datacenters to house their security modules, and at a company, as a startup size company, running your own datacenter is really not really a thing anymore. So, we've dealt with the fact that running a datacenter a very small company, is somewhat difficult process.

Lastly, we've dealt with the fact that the larger software ecosystem written on top of Ethereum is relatively new, and relatively incomplete. There's a lot of cases where we would ideally like to not write a piece of software, but as a service that we'd ideally like someone else to offer. And in a traditional like software environment, there'd be dozens of vendors competing for our business. In the blockchain space, there are none, or there are one or two, and neither one provides a complete solution for us. So, we've had to sort of build our own tools and our own infrastructure in areas where it really normally wouldn't make sense for a company our size, or a business our size.

[00:44:38] JM: To close off, what are the other tools that you're planning to build in the near future?

[00:44:46] PT: Yeah. So, one of the challenges of NFTs is that they feel like a common web technology, right? They have data associated with them, names and things like that. But the standard they adhere to are brand new, and the data sets that are available are brand new. So, for a lot of providers, the data that they need is not available on the blockchain today.

For instance, we would love to have digital wearables. NFTs, you could buy, say, a pair of Adidas sneakers that were like limited edition, one of a kind sneakers, and wear them when you're on Snapchat filter, wear them in a virtual game you're playing. And to do that the sort of metadata associated NFT needs to represent the state of the NFT in each of those worlds, right? We need 3d models, we need potentially, like 2d images and those sorts of things. Right now, NFTs as a standard can sort of have a model or an image attached to them, but not multiple. If you were a game or a Snapchat filter, and you sort of want to say, "Hey, show me all the NFTs that are compatible with my game", there's almost no way of doing that.

So, we're trying to create a lot more API's around NFTs, around finding NFTs, discovering NFTs, sort of slicing and dicing that data in ways that makes sense for the types of projects we're working with. We are also looking at launching tools that make it easier to sort of go from never having created a wallet ever, and scaling up to having complete access to the Ethereum world and ecosystem. Right now, our solution is basically when you sign up, we'll create a wallet for you. But as you get deeper into crypto, and you might want to control your own keys in a different way, and you might want to use a hardware wallet, you want to be able to have the tools that we develop evolve with you. We're looking at supporting more types of wallets in addition to ours. We're looking at building out tools around seeing all the things that are in not just your Bitski wallet, but in all the wallets that you control and manage. And then we're also looking at trying to figure out how to show you all the information that's happening in the ecosystem that's related to your NFTs, even if they're not sort of on chain.

So, a lot of what – there's a lot of people saying, "Okay, if you have access to these NFTs, you can go install this app or get into this discord." But none of that data is available on chain. It's

hard to find what discord you have access to. It's hard to find what places you can use as NFT, and we want to make sure that's all accessible to the users. So, when they buy something, or when they put something in their wallet, they can see all the different places they can use it, they can see all the different things it gives them access to, and potentially if there are other NFTs that it unlocks, they know where to find those and where to get those.

And then lastly, for creators, we want to give them a lot more tools around distributing NFTs and getting access to who owns those NFTs, what's happening with them, where they're being traded. All that sort of data is often sort of lost once the NFT goes beyond like the initial stage of sale. So, for creators, especially, they really need access to all those analytics they might get from a traditional analytics product on a traditional tech stack.

[00:48:10] JM: Great. Well, Patrick, it has been a real pleasure talking to you, and I wish you the best on Bitski.

[00:48:13] PT: Thank you so much.

[END]