Demystifying NFTs Episode 4

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, Demystifying NFTs. We would like to remind everyone that the information and opinions expressed by our speakers today are their own, and do not necessarily represent the views of their employers, or of PLUS. The contents of these materials may not be relied upon as legal or financial advice.

And now I'd like to turn it over to our host, Alice Budge.

Alice Budge: Thanks so much, Tyla. Hi everyone, welcome back. I'm Alice Budge from Specialist Risk Group. Thank you for joining us again for our fourth episode of Demystifying NFTs. We had a bit of a hiatus, but we are very pleased to bring you today's episode, which focuses on NFTs and cybersecurity.

I am joined by the usual co-hosts, Jenni Stivrins and Vito Marzano of KSW. And I'm very happy to be joined by our NFT cybersecurity guru for this episode, Dave Sigmundson of Kroll, welcome Dave.

Dave Sigmundson: Thanks, Alice. Happy to be here.

Jennifer Stivrins: Yeah, welcome Dave and for our regular listeners, and we did learn that we have regular listeners on a [00:01:00] recent visit to London, so that was exciting.

We've had a bit of a break, like Alice said, while we searched high and low for a cybersecurity whisperer who had some firsthand experience, specifically with cybersecurity issues inherent with NFTs. And so, we're pleased to have met Dave Sigmundson at Kroll. Vito and I have had the opportunity to have a couple initial conversations with Dave, and we think you'll really enjoy this chat today.

Vito John Marzano: That's right. One of our favorite things about Dave is that he breaks down this incredibly complex topic with easy to relate to examples like sock puppets. And with that, we'll let Dave take it away.

David Sigmundson: Thanks so much, all. To give a bit of roadmap for today, we're going to start by discussing cybersecurity for digital assets, including NFTs.

We will then turn to some common cybersecurity risks for NFTs, and then we'll have a few words at the end where we can dive into the threat of quantum computing as well as the imminent threat, which I believe to be AI assisted cyber-crime.

Alice Budge: We do love a good teaser, Dave. Everyone wanting to hear the AI impact has to stay to the end of the episode, though.

David Sigmundson: That's right. So, let's [00:02:00] jump in. In the field of cybersecurity, we use all these weird, exciting terms. You got red teams, kill chains, ransomware, nation-state threat actors. But the secret of it all is that it boils down to risk management. Identifying risks, understanding those risks, quantifying them. You mitigate, you remove, you transfer, you accept those risks.

So, with that, let's step into the world of NFTs. I actually won one recently. I ended up with a V-IRL token. This NFT, is I believe to be a sock-puppet. And there's some very interesting games being developed to be fully resident on the blockchain, which is super cool. This was actually from Structs.so, but this NFT, it was supported by the Secret Network, a privacy preserving blockchain network.

But the gimmick of this NFT is that the NFTs were redeemable for actual, physical socks. But let's put a pause on that topic and we'll come back to it a little later on.

Alice Budge: A cliff hangover for the sock-puppets then.

David Sigmundson: Indeed, you'll have to wait on that. But, the [00:03:00] bottom line when it comes to cybersecurity is that we think that blockchain is hard, and the premise here is simple.

Information security is difficult. It's a process, it's a practice. This is a constantly moving target. And two, cryptographic assets and blockchains are an information system. So, with that, we can arrive at: blockchains are difficult. And really, the first issue that comes into play when we talk about security of and securing digital assets is education.

This is one of the most important topics we talk about in computer security. A critical line of defense is always going to be the end user. It is you, your coworkers, anyone interacting with these systems. So, thinking about your

organization running phishing training, phishing simulations, or your periodic security training telling you never to plug in USBs that you find on the ground.

Jennifer Stivrins: I'm always telling Vito not to plug in random USBs that he finds on the ground.

Vito John Marzano: It's not fun.

David Sigmundson: One of the first and best things you can do is educate yourself about the risks [00:04:00] and pitfalls involving cryptographic assets, and just keeping this discussion to an end user key holder perspective, we do want to inform you about controls and practices that have a reasonable influence over the outcomes, which is here, being secure.

Practical advice that you can implement right now. And slight segue as we move through the day, I tend to avoid using the term wallet. It's a bit ambiguous, so we prefer key or key chain. And thinking about these as keys, physical or otherwise, just conveys the sensitivity. A wallet on the other hand, that's got my ID, it's got a pack of gum, odds and ends.

A key though, that actions something. It opens something, it grants access, it signs transactions. And being utterly scrupulous about handling and using those keys is really the foundation of securing cryptographic assets.

Alice Budge: That's a really helpful way of framing it, but is there any way we can go back to you winning a smelly sock?

David Sigmundson: Just can't get over the socks, but yes. Yes, absolutely. And we'll talk socks. We'll get through a little bit of discussion about on-chain versus off-chain. And some of this [00:05:00] is really that “what is an NFT” type discussion that was covered in the first episode, but it is a good refresher overall to get us talking about cybersecurity and really the security mindset.

So back to the important discussion, it's the socks. We talk about these socks, and fundamentally, it's really an interesting thing to consider if they are on-chain or off-chain. We have to talk really about what an NFT represents, how it may be implemented, and I'm really hoping to convince you that there is a practical and meaningful difference even to the end user.

So, when we look at how NFTs exist on a blockchain, they come in really two main flavors. The first would be an on-chain NFT. Succinctly, this is where the metadata, the contracts, that tokenized element itself, exists entirely on your

chosen blockchain. That data, and therefore the existence of the NFT is immutably part of this ledger.

Long story short, storing data in bulk on the blockchain is expensive and kind of a pain. But comparatively now, if we contrast off-chain NFTs exist in two [00:06:00] parts, the blockchain resident data, the smart contracts, interactions and so on, and then this external reference. In most cases, this blockchain has now a pointer which points to some external source, and let's say it's a website.

And now this is exactly where the potential issue could reside: your lovely decentralized trustless NFT now relies on the continued hosting of that external reference. That asset can only exist as long as that reference data is available. So, if your NFT market goes insolvent, if they lose a domain name, if the organization maintaining that reference changes, moves, or deletes it, it's gone. And perhaps with it, its previous value.

But anyways, sidetracked briefly, going back to the socks. I can at any time redeem this NFT for a physical sock. And this is just part of the system they've developed. But clearly in this as well, there are dependencies in this system that should be considered. I would still need this service to exist, and I'll come right back to education.

End users [00:07:00] should be able to discern if their NFTs or socks are on-chain or off-chain. So, if their providers go out of business, if they're insolvent and with them, your access to the underlying asset could disappear. So NFTs overall, just to summarize here, can represent and rely on more than just that blockchain resident data.

There are issuers, there are maintainers, technological dependencies.

Vito John Marzano: So, I realized we maybe should have called this episode Dave’s Socks. But so anyway, okay. So off-chain NFTs present that inherent risk that something could go wrong outside of the blockchain and poof, no more NFT. Without getting too far into the weeds, which is not something I always like doing, and while recognizing that none of us on this show are cybersecurity practitioners, could you explain what types of standards are in place for securing digital assets.

David Sigmundson: You know what, Vito? This is a fun topic for me. So how do you go about securing an organization's digital assets?

You start with a standard. If you look at the automotive industry, food safety industry, drug [00:08:00] safety, there's regulation and enforced standards that must be adhered to. This is really the foundation of trust and reduction of risk in those products. These are often hard learned lessons codified into written rule.

In the cybersecurity realm, we have frameworks and standards, and my second point today was really that cryptographic assets are an information system. So, when we are securing an organization's handling and operations with cryptographic assets, we want to see that a robust, well-managed information security program is in place.

The usual suspects being third party independent audit to standards like the NIST Cybersecurity Framework or the ISO27001:2013, but...

Jennifer Stivrins: No worries, Dave. We love--we love an acronym word salad on this show.

So, for those who don't know, can you tell us who NIST is?

David Sigmundson: Sure. N-I-S-T or NIST is the National Institute of Standards and Technology, which is an agency that is part of the US Department of Commerce. So, on top of [00:09:00] something like NIST standards, you can also bring in an additional layer to address the complexities of handling cryptographic assets.

Specifically, we look to a nonprofit organization called C4, or the Cryptocurrency Certification Consortium, and four more letters to throw at you - they maintain a standard called the CCSS, the Cryptocurrency Security Standard, and this is a set of criteria and requirements that controls processes, methodologies that are intended to help securely handle cryptographic assets.

And this can also be third party audited and certified. And the details of the standard get into the really nitty gritty about how keys are generated, stored, used, assigned, backed up, revoked. But overall, it's really just build trust, have that verification that these controls are in place and that assets are safe.

And overall, if you look at the standard, it's pretty clear that this was essentially built by running postmortems against the series of incidents and working backwards to determine what kind of controls would have eliminated those vectors of attack or provide more direct indicators for something like complicit insiders.[00:10:00]

Alice Budge: So that's very cybersecurity-y indeed. But what are the common risks for NFTs and crypto assets? Are they some of the same risks we see in the more traditional Web2 sphere?

David Sigmundson: You're exactly right. There are common risks and the first couple that we'll talk about affect regular non-blockchain-based companies and assets as well as crypto assets and NFTs.

Vito John Marzano: So, okay, let's start with social engineering and scams. That's one area where you see a lot of issues, right?

David Sigmundson: It's right now probably your number one threat that you can actively sort of protect yourself against. And without a doubt, it's not really a technical problem. It's people, specifically those that intend to separate you from your assets via deception, coercion, tricks of all sorts.

And I know I tend to make them sound like cartoon villains. But social engineering attacks are incredibly convincing. These are often professional cons. They will and can do everything they can to part you with your assets. In the end, you may hand them over willingly. This can [00:11:00] get into investment scams, tech support scams, romance schemes, and business email compromise.

And I can tell you that the FBI will agree that a substantial amount of these cases just go unreported. And the defense here is really knowing when something sounds too good to be true. We must be defensive. You must trust, but also verify. Do everything you can to validate your counterparties. If you're out there, looking for reputable organizations, check to see if there is that third party attestation of their business practices.

Does this business have an online presence? Do they have a physical location? Is there registered business investment or charity information? These are all indicators you can use to start to really suss out if this is a trustworthy party.

Jennifer Stivrins: Okay. And so, beyond scammers or bad guys trying to part you from your assets, you actually run into a lot of folks who manage to part themselves from their own assets because of lack of backup or issues with key handling, right?

David Sigmundson: Losing keys or key chains is obviously huge, very impactful. [00:12:00] Some people can have millions of dollars of assets existing on a single hardware wallet or key chain.

With no backup solution, that's an incredible single point of failure that can irreversibly fail, and with it you may lose access to those assets.

And best practice for using backups of your keys is the 3, 2, 1, 0 rule. The zero is an additional criteria for key storage, but let's walk through it. You have three copies of your key. You have it across two mediums, and you have it on one offsite location and zero, absolutely zero, copies of those keys are stored unencrypted.

Alice Budge: I absolutely love this rule and think it's a great data point for underwriters to have when considering a risk and whether or not they want to touch NFTs or digital assets in any way. How are your keys stored and how are they backed up?

David Sigmundson: Yes, and I absolutely support the notion that the protection of keys should be proportional to the assets custodied.

The higher the value, the more you should be scrutinizing the key storage and protection systems in place. I can tell you that your [00:13:00] local bank is not going to use a dollar store padlock on their bank wealth.

Jennifer Stivrins: Right. So, what do we do when people are just awful at creating strong keys or keeping track of them?

David Sigmundson: Yeah, we should talk about the risks of key handling. Regardless of any legal ownership, any entity that has control of your private keys can authorize transactions with it and move or use the assets. And, in whole, the security of cryptographic assets is only guaranteed by the secrecy of the private keys.

And I really hope that's a point that we can drive home here, so we have a few stories to go with it. And the first, as it relates to key generation, no matter how creative people think they are, we are a terrible source of entropy. Creating strong cryptographic keys requires an entirely un-guessable sequence of random data, and this has been proven time and time again.

The number of possible Bitcoin addresses, for example, is an incomprehensibly large number using a strong key [00:14:00] generation function that's built into something like a hardware wallet, or at least if it includes some proven cryptographically secure pseudo random number generator. That's pretty much mandatory for generating a strong key.

And just to provide a little bit more example, as far as the technology goes, anyone who generates a key with the same input will get the same private key. And with that, you can effectively arrive at ownership of the address. Probably the most stunning example of this is a DEFCON 23 talk. This is a hacker conference in Las Vegas each year by Ryan Castellucci, where he discusses how trivial it was to actually guess phrases from literature as source input and generate the key pair, and then surprise to him he found those addresses already had funds.

So, unless you really know what you're doing, using a proven system that can generate keys for you is really the only thing you can do. If somebody else can reasonably arrive at your same input, it's not secure. [00:15:00] And this applies to the passwords anywhere else on the internet, mind you. So, in whole, we should treat private keys like the world's greatest secret.

If you can, make it as random as possible, and we make sure that key is secret as it is called a secret key.

So interestingly enough, I was brought into a room full of insurers last year as part of a panel on this topic and midway through, as part of, just to get the discussion moving along, I asked everybody in the room if they wanted to be a part of Dave's Holding Co. Not a real thing, mind you, just an illustrative example. And I proceeded to read off to the group a BIP39, 12-word seed phrase that could be used to generate or technically restore a private key and super useful if this backup is used correctly.

But for this example, I then proceeded to ask the group who owned this wallet, making abundantly clear that no less than, let's call it the 50 or so people could have potentially recorded, memorized, written down this seed phrase. Everyone there was forcibly part of my fictional [00:16:00] organization and they now had access to the key.

So, following the morning's sessions, which was introducing blockchains and cryptographic assets. Having discussions, making people think critically about safely handling those assets now was really the next step. And through our discussions, everyone arrived very quickly to the conclusion that reading out this seed phrase was an awful idea.

Anyone could have heard it and with it, exposed the key. This is very true. We must be incredibly careful about writing out keys, key pieces, reading out any information that could even partially compromise a key. And after we all agreed

that my actions were highly irresponsible, I motioned to shamefully resign from my fictitious position as a key holder.

And with this, I turned my sheet of card stock where I had written the seed phrase down over to my fellow panelist and I said, “that's it. I'm out.” And the immediate question then I threw back to the group is that, how does one revoke a key? There's no guarantee that I haven't copied, disseminated the key.

Further, the only safe option we came to was that the assets need to be moved [00:17:00] to an address where this secrecy of the private key is guaranteed, right back to that tenet. So, this process is what we call a Key Compromise Policy. Having a plan in place that can be enacted if you believe that a secret key is or potentially compromised.

So, the final point that we arrived at being that, even if the key was safe in this room, is that if those assets moved before we left today, there's nothing to indicate which of the 50 of us actually signed that transaction.

Vito John Marzano: And so, what do you do about that? How do you make sure that there's some way to more fully secure the keys and in turn the assets?

David Sigmundson: Yeah. Vito, I'm glad you asked. We use multisignature. Very early on today, I discussed why we wanted to call wallets keys or key chains.

The cryptographic key, much like a key to your house or car, is intended to operate or action a certain lock. These are one-to-one, really, but you can copy a key and hand it to somebody, and now they can effectively use it in the same manner that you do. Similar to me sharing that key earlier in that example with the group.

However, in cryptography, [00:18:00] we can enforce something called multisignature or multisig, multiple keys required to do one thing. In practical examples, think of an extremely high security facility where two people, three people across a room, must each turn their keys at the same time to authorize something - launch a missile, open vault.

That's effectively what we can do with multisig, and what we call an M of N scheme, which I promise isn’t candy. Meaning M of N people. Let's say three of five people. Three of any five of them must then sign a transaction with their respected keys to actually have that transaction executed. And that group, three of five, it would be called a quorum.

And this is huge. I can't understate how powerful this is. Instantly, thinking back to that last example, we can now have added the following assurances. 1) No one key or even one person can independently move the assets. This now requires that quorum to actually confirm. 2) Each person or role can have a unique key all to themselves.

This is now [00:19:00] full accountability. A transaction signature is tied to an individual. 3) Destruction of up to two of those key pieces in this three of five scheme won't impact our ability to use the assets - we have built in redundancy. And the last point, is that this can actually introduce organizational distribution.

This is technologically enforced separation of duty. Accountants, rejoice. So even for an individual, using a two or three system, you can have a signing key at your house, one in a safety deposit box, one with your lawyer. This is incredibly powerful, even for something like estate planning, key backup.

Jennifer Stivrins: That's great. So, it's multisig that saves the day. This might feel like a little bit of a jump, but I think one thing that we discussed previously with my partner, Merri, and you on the line in one of our initial calls, was what your thoughts were on the threat of quantum computing. Particularly where we're hearing that such computing may make the current key and password systems subject to challenge or collapse entirely.[00:20:00]

And again, recognizing we're not cybersecurity practitioners on this podcast, we would appreciate you simplifying your thoughts on that for us.

David Sigmundson: You know what, this is always a big topic to really tackle, but happy to jump into it. A fairly famous quote in the space is if you think you understand quantum mechanics, you don't understand quantum mechanics.

And to that extent, I do think it is important to take heed to the true experts in the space, and this is where we should absolutely defer to those with their PhDs in cryptography or quantum mechanics that is applied to computing technologies. And thankfully, there are those individuals that have come together as part of our, NIST, our good friends at the National Institute of Standards Technology, Post-Quantum Cryptography Standardization Group.

And a bit of history briefly, the AES Standard, Advanced Encryption Standard. This is an algorithm which underpins a truly wild amount of your everyday computing. It actually came from a NIST contest, where the cryptographic community submitted and evaluated how to replace the then vulnerable DES algorithm, and this was about 20 years ago [00:21:00] now.

But since then, the algorithm is now so prevalent, that many of your computers actually have been designed to be efficient with this algorithm. It's hardware accelerated by design to be good at AES. Regardless, this process is happening again right now to identify a replacement for AES. It's identifying quantum resistant algorithms.

And I should put out here that right now there is currently no known quantum computer to me with sufficient capability to put established cryptographic keys at risk. NIST estimates that this could take years to decades until this capability actually is out there.

Alice Budge: Don't want to scare you. But what happens when these computers do have that capability? What happens then?

David Sigmundson: That's where the discussion gets a little bit more difficult. If such quantum computer actually becomes feasible, a number of current public key systems such as RSA, are extremely vulnerable. This impacts a number of technologies including digital signatures, [00:22:00] signing certificates, among others.

The potential damage of a cryptographic weakness or breaks theorized to be possible with quantum computing is substantial. The theoretical effectiveness of something like Shores algorithm is proven. What we don't have is, again, those quantum computers that are large enough and stable enough to crack those keys at scale.

So private key systems like AES are theorized to have their affected key links halved. Even still, symmetric encryption schemes like AES 256 should still be considered highly resistant for the near future, and this is where, again, I will directly quote those experts.

It's actually not the time to panic. It is time to plan wisely.

Jennifer Stivrins: Well, we love planning. This definitely speaks to my Virgo energy.

David Sigmundson: Yes, planning is underway. Those quantum persistent algorithms are being explored and intended to be rolled out by NIST in 2024, next year. The change to quantum persistent algorithms does not really protect against what we call a "store now, decrypt later" attack.

This [00:23:00] is essentially hoarding data with the expectation that those encryption schemes being used will eventually become weakened or broken. And NIST recommends that you keep encrypting data per your currently established standards, for now, but build in processes to really understand where keys exist in your organization, what will need to be replaced as those rollouts continue.

So, one last thing I'll leave off with in the topic in the quantum space is Scott Aaronson, an academic. He has a blog where he often muses about quantum computing, and the header reads something like, if you take nothing else from this blog, quantum computers won't solve hard problems instantly just by trying all the solutions in parallel.

And I think that's as good a takeaway as any.

Vito John Marzano: So, stop the presses, Jenni revealed that she's a Virgo. Um…

Jennifer Stivrins: Shocked, you're shocked.

Vito John Marzano: I'm shook to my core. I'll reveal that I'm a Leo, as if anybody couldn't tell, or by my innate need to tell you that I'm a Leo. So anyway, if we aren't spiraling out over quantum computing, tell us where we should be worried.[00:24:00]

David Sigmundson: Right now, in my opinion, at least, the greatest imminent threat I think is actually going to be AI. And I want to quickly say it's not in any singularity end of the world kind of way. It goes right back to that first topic of ordinary people driving these risks. The advances in Chat GPT, image generation, deep fakes, and the availability of that tooling is concerning to me.

We've barely scratched the surface on that tech, but threat actors with relatively low sophistication, now have a horrifyingly convincing battery of tools built to essentially deceive, extort, coerce, and cause harm to their victims. And just for some examples here, a language model like Chat GPT can certainly be trained to emulate the speech patterns of individuals.

We can generate extremely human appearing text in a convincing fashion. I fear that we're going to start to see scams being somewhat automated or aided by AI tooling. A single threat actor could now effectively increase the number of campaigns, remove language barriers, automate their processes, [00:25:00]

perhaps starting to get into multimedia tactics with great effect - full digital impersonation is now very accessible.

And we have seen cases where people have been social engineered out of payments for posing as their friends, as their family, using AI generated voices, using deep fakes to pose as celebrities as part of romance scams. It's everywhere. And this is what scares me, and I'll keep calling back to our earlier points that we've identified these risks, now we need to address how we move forward.

Alice Budge: Thank you, and move forward we must. I would note I went to a wedding last weekend, and the best man thanked Chat GPT for helping him with his speech. So, it's used widely. But Dave, we want to thank you so much for coming on to our show and podcast. It's been incredibly insightful for all of us here and I'm certain that our colleagues in insurance in the States and the UK market will find it similarly helpful.

David Sigmundson: Of course. Thank you for having me on.

Alice Budge: With that, we look forward to speaking to our listeners [00:26:00] again on our next episode, which will be purely focused on underwriting the NFT risk, and we have some pretty great guests lined up for that. Don't forget to submit your questions for our Q&A episode at the end of the series.

PLUS Staff: Thank you to our speakers for sharing their insights with PLUS, and thank you to our listeners for listening to this PLUS Podcast. If you have ideas for a Future PLUS Podcast, you can share those by completing the Content Idea Form on the PLUS website.