Non-Fungible Tokens and Cyber Insurance

A Supplement to OMG's Discussion Paper on the State and Future of Cyber Insurance

Version 1.0

A Discussion Paper from the OMG Cloud Working Group

Document mars/21-09-07

September 2021

This page intentionally left blank

Table of Contents

Copyright Notice

Acknowledgements

The development of this discussion paper has been a collaborative effort, bringing together diverse customer-focused experiences and perspectives. The following participants contributed significant expertise and time to this effort:

- Tim Cavanaugh (Maiden Global Servicing Company)
- David Harris (The Boeing Corporation)
- Janice Reese (Network PDF Cloud Solutions)
- Steven Schwartz (Periculus)

In addition, Claude Baudoin (cébé IT & Knowledge Management) reviewed and edited the paper.

Introduction and Executive Summary

The virtualization of resources that resulted from the emergence of cloud computing has challenged our old models of ownership and possession, resulting in new risks and a need to mitigate them. OMG's Cloud Working Group started addressing this problem in 2020 through its discussion paper entitled *The State of Future of Cyber Insurance* [1].

The premise of that document was that since we increasingly entrust the custody of enterprise (as well as personal) information to Cloud Service Providers (CSPs), to whom we grant great latitude in deciding where and how to store that information, and who strive to reduce their own risk and liability through exclusions and limitations contained in their Cloud Service Agreements (CSAs), Cloud Service Customers (CSCs) are left "holding the bag." A particular concern for a CSC who uses cloud resources in customer-facing activities is that if the CSP fails – whether it is for several hours, due to an outage or cyberattack, or permanently, due to a sudden cessation of operations – the business consequences can be devastating and the CSP is only liable for a refund of the cost of the service that was not provided, not for the considerably higher business loss suffered by their customer.

As we explained in the paper referenced above, insuring against such risks has been a new challenge for the insurance industry, largely because of the difficulty in calculating the value of intangible assets such as data [2]. Insurers has come up with some interesting innovations to address it, in particular a new form of policies called *parametric insurance*. Our previous paper explained this and provided cloud customers with ways to understand how to take advantage of these new offerings.

Lest we become too comfortable with this new situation, the virtualization of what used to be physical possession – monetary instruments that are not guaranteed by national banks, or rights to artistic and intellectual property that are not embodied in physical objects – is further complicating the situation. In this Supplement to our original paper on Cyber Insurance, we address the impact of Non-Fungible Tokens – in essence, a form of "property in the cloud" – on insurance mechanisms. We alert our readers to the risks related to such virtual ownership, and what to expect in terms of protection against loss of those tokens of ownership.

Non-Fungible Tokens Defined

A Non-Fungible Token (NFT, sometimes pronounced "niftie") is a digital token that is associated with a specific physical or digital asset that has a unique form and value [3]. The adjective "fungible," used in law and economics, refers to goods whose parts are indistinguishable from each other and can easily replace each other. Traditional currencies, or cryptocurrencies such as Bitcoin, Ethereum, are fungible: a bitcoin or euro is interchangeable with any other Bitcoin or euro. By contrast, and even though NFTs are leveraging the same underlying distributed ledger technology (DLT, more commonly called "blockchain" even though blockchains are only one kind of DLTs) as cryptocurrencies, each NFT is typically linked to a unique asset: it can be a physical object such as a diamond, or a digital asset such as an online concert ticket or a certificate of ownership of a piece of digital art.

NFTs come in all shapes and sizes, but they have two key linked properties:

- They represent unique actual assets – whether physical or digital. Effectively, an NFT is an advanced digital version of a "certificate of ownership," cryptographically encoded in a blockchain.
- As a result, the record of ownership is tamper-proof and the ownership history is always verifiable.

As in the case of cryptocurrencies, a user who owns an NFT actually holds a private key that points to the token stored on a blockchain. When an NFT transaction is recorded on the decentralized ledger, the token is assigned to a different private key and no one can reverse nor repudiate the transaction. "Not your key, not your NFT."

The Rise of NFTs

The launch of the Ethereum-based CryptoKitties game in November 2017 ("Collect and breed digital cats!") took the so-called "crypto world" by storm, with some digital cats selling for up to $300,000 and transactions from players slowing down the entire Ethereum network. While this initially seemed like a frivolous application of blockchain technology (the nerd version of Pokemon cards), the potential to apply this model to other kinds of digital assets was recognized.

The growth of crypto collectibles was then fueled by the emergence of standards to control the creation and management of NFTs:

- ERC (Ethereum Request for Comments) 721 is the basic set of rules to be followed to create an NFT so that it is different – and therefore can have a different value – from another NFT.
- ERC 1155 was added to resolve the proliferation of token types and associated smart contracts that would result from the previous standard [4].

The Value Proposition of NFTs

Today, NFTs are enabling creators to revolutionize the art market, and they also enable additional use cases, including support for many types of unique physical and digital goods, such as concert tickets, identity documents, and more [5]. Since NFTs use blockchain technology, they can be tracked as they are transferred or sold to other people. In addition, NFTs can be programmed so that when they are sold on the secondary market, a portion of the proceeds can automatically be sent to the creator of the underlying artifact (such as a song, a painting, etc.), thus creating a new motivational value chain for the creator economy. While NFTs are designed to give you something that cannot be copied (ownership of the work), the artist can still retain the copyright and reproduction rights. To put it in terms of physical art collecting: anyone can buy a Monet print – but only one person can own the original.

Beyond gaming and digital art collection, other applications of NFTs to the management of digital assets are barely emerging and are likely to affect the global financial ecosystem. Leonard Nakamura, an

economist at the Federal Reserve Bank of Philadelphia, estimated in 2014 that there was more than $8 trillion in non-valued intangible assets on the balance sheets of publicly traded corporations. One can only extrapolate what that number might have grown to by this time.

Potential applications of NFTs are nearly limitless: trustless transfers, trading, fractional ownership, security tokens, and more.

Risks Associated with NFTs

Investors buy NFTs believing them to be permanent and immutable records of ownership, this is not always the case – fundamental flaws in the construction of many tokens threaten the long-term integrity of the asset.

The security of the private key that controls access to the tokens is central to any cryptocurrency or NFT use – especially since a transaction cannot be reversed. For investors, who may have bought myriad NFTs, all proof of ownership revolves around protecting those keys.

Various hardware and software technologies have been developed to help secure the private keys and the tokens they control. Trusted hot wallets[1] (such as Metamask) typically use two-factor authentication (2FA) or even multi- factor authentication. Hardware wallets (such as Ledger Nano) rely on hardware security modules (HSMs) with tamper-proof chips so that the private key is kept away from the Internet. The two solutions can be used in combination: every time you initiate a transaction, the hot wallet will send a request to the hardware one, asking your permission to approve it.

Clearly, one risk associated with NFTs is the loss of the private key, which makes the tokens impossible to retrieve or sell.

A second risk is the failure of the server that holds the actual digital asset. The link from the NFT to that asset will become useless of the target of that link has become unavailable. As a result, the purchaser might be left without recourse due to the fact that NFT's are unique and cannot be replicated.

Mitigating those two risks is mostly achieved by backing up the wallet that is holding the keys to your NFTs. Additionally, one can use replicated, distributed and content-addressable data storage mechanisms such as the InterPlanetary File System (IPFS), but no system can be 100% safe [6].

In addition to accidental loss, criminal activity must be considered [7] [8] [9]. The growth in popularity of crypto assets (cryptocurrencies as well as NFTs) has outpaced the infrastructure built to support them. In terms of security, electronic exchanges that serve both as marketplaces and as stores for digital assets have become a hacker's favorite targets. While bad actors initially focused on stealing cryptocurrencies (whose total market capitalization is on its way to surpass $1 trillion), the NFT market is increasingly alluring too, with over $2.5 billion in transactions in just the first half of 2021 [10].

[1] "A hot wallet is a tool that allows a cryptocurrency owner to receive and send tokens. The difference between a hot wallet and a cold wallet is that hot wallets are connected to the internet, while cold wallets are not" (Investopedia)

Parametric Insurance for NFTs

Given these risks, there is a nascent demand for insurance products covering digital assets. Historically, insurance has been something everybody needs but nobody likes. Today, blockchain technology and oracles have the potential to transform insurance into a life-changing tool that helps businesses around the world grow and prosper, unencumbered by the fear of catastrophic external risk.

Insurance that covers the theft of NFTs is critical for this new market to thrive as intended. Insurance not only helps to legitimize this new asset class itself but forces the entire ecosystem to enhance its security controls. For example, insurance against theft and loss would likely only be offered for NFTs that are:

- purchased from approved exchanges with full KYC/AML (Know Your Customer / Anti-Money Laundering) Compliance [11] and adequate evidence of the exchange's security audit and business continuity plan; and
- owned and stored in approved wallets where multi-factor authentication is required.

Insuring NFTs can fall within the domains of *crime, fidelity and species* insurance products:

- "Fidelity and Crime insurance coverage addresses the most common threats to organizations, including losses due to employee dishonesty, credit card forgery, computer fraud and theft, and the disappearance or destruction of property." [12]
- "Specie insurance is a niche product that covers high-value, portable items. It's a specialized coverage form that protects valuable goods, like cash, bullion, diamonds, fine art, valuable documents, and even cryptocurrency, when they're on location, at a third-party location or in transit." [13]

However, when it comes in particular to the digital art market, "underwriters still need more understanding as to where collectors, galleries and auction houses are actually custodying their NFTs, and they want some familiarity with the vendors that are being utilized." [14]

In a previous discussion paper, OMG's Cloud Working Group explained the challenges posed by the evaluation and protection of intangible assets, and presented the definition and usefulness of parametric insurance, a relatively new mechanism particularly well suited to this kind of assets. [1]

Parametric insurance achieves its ideal form when it leverages blockchain and artificial intelligence (AI) to make coverage simple, transparent, and accessible. Advanced parametric insurance solutions use AI to assess the risk and ensure that claims are only triggered if it is proved that an event actually happened, as verified by an independent source. In the specific case of NFTs, such parameters may include the validated ownership of an NFT, the presence of security controls such as multi-factor authentication, and analysis of on-chain and off-chain data to validate claim payment.

Due to the nature of the NFT digital asset class, a parametric insurance policy offers significant added value and certainty – for both the insured and insurer – compared to traditional indemnity-based insurance policies. The owner purchased an NFT based on its market value, which is often speculative and volatile. A parametric insurance policy offers a construct wherein the policy limit can be based on the market value paid for the NFT.

Beyond the theft or loss of the NFTs themselves, the policy would provide coverage for proven third-party hacks or theft of private keys through cyberattacks, phishing, malware, and device theft. The loss of wallet keys may also be covered if the insurer, or a third-party partner of the insurer, stores a back-up of those keys.

If an NFT were stolen due to of any of the perils listed above, the insurance policy would pay the insured the agreed-upon policy limit in *fiat* currency[2] upon validating the occurrence of the adverse event. The power of blockchain, machine learning and AI enable the insurer to have real-time insights into these events such that the claim can be paid in less than two days from the time the insurer receives the First Notice of Loss (FNOL). After events such as device theft or a malware attack, smart contracts trigger a rapid payout to policyholders. This eliminates the subjectivity and uncertainty inherent to the traditional claims process of indemnity insurance policies by tying payouts to objective data, while making insurance inclusive and readily accessible to investors in digital assets who do not currently have a financial instrument to protect them.

Understanding exclusions and limitations is always a critical step when considering an insurance policy. With respect to the theft of NFTs, the following types of losses would typically not be covered:

- Theft of NFTs owned and stored in wallets that have not been approved by the insurer
- Theft of NFTs from a wallet that did not have multi-factor authentication in force at the time of the loss
- Theft of NFTs purchased and traded on exchanges not explicitly approved about the insurer
- Failure, breakdown, or disruption of the NFT Blockchain
- Direct physical loss of or damage to any hardware if the NFTs are held in a cold wallet
- Deliberate sending of an NFT by the owner or someone authorized by the owner
- Failure to identify NFT ownership on the blockchain.

Conclusion

Cloud computing started with a fairly simple reference model offering three types of services: infrastructure (IaaS), platform (PaaS), and software (SaaS). In less than two decades, we have seen a proliferation of “XaaS” – sometimes pronounced “anything as a service” – including voice services, collaboration environments, disaster recovery, and even “malware as a service” and its latest ugly offspring, “ransomware as a service.” As everything under the sun gets virtualized and offered over the Internet, customers need to concern themselves with how to protect those resources and holdings. Because NFTs are expanding so rapidly, and the property they represent can fetch enormous values (tens of millions of dollars), the worlds and technologies of cloud computing, blockchain, and insurance need to come together to provide solutions for the protection of virtual assets. May this paper help the reader make safe choices.

[2] Currency issued by a central bank (dollar, euro, etc.), whose value is based on an agreement or government decree rather than on an intrinsically valuable commodity such as gold.

References

[1] Object Management Group: *The State and Future of Cyber Insurance.* December 2019. www.omg.org/cloud/deliverables/the-state-and-future-of-cyber-insurance.htm

[2] Wall Street Journal: *Accounting's 21st Century Challenge: How to Value Intangible Assets.* March 2016. www.wsj.com/articles/accountings-21st-century-challenge-how-to-value-intangible-assets-1458605126

[3] Conti, Robyn, and John Schmidt: *What You Need to Know About Non-Fungible Tokens (NFTs).* Forbes, May 2021. www.forbes.com/advisor/investing/nft-non-fungible-token/.

[4] Numbrs Deep Tech: *Ethereum's Standards for Non-Fungible Tokens: ERC-721 and ERC-1155.* www.numbrs.com/tech/2021/04/28/ethereums-standards-for-non-fungible-tokens-erc-721-and-erc-1155/

[5] Binance Academy: *Top 7 NFT Use Cases.* August 2021. https://academy.binance.com/en/articles/top-7-nft-use-cases

[6] Barker, M. Ridway: *Non-Fungible Tokens: Legal Issues to be Considered.* Martindale Legal Library, June 2021. www.martindale.com/legal-news/article_withers-bergman-llp_2546974.htm

[7] Pickett, David: *Are NFTs Safe?* HelpNetSecurity, May 2021. www.helpnetsecurity.com/2021/05/06/are-nfts-safe/

[8] Bonderud, Douglas: *Token Resistance: Tackling the New NFT Threat Landscape.* Security Intelligence, May 2021. https://securityintelligence.com/articles/new-threat-landscape-nfts/

[9] Anderson Kill: *A Hacker Was Selling a Cybersecurity Exploit as an NFT. Then OpenSea Stepped In.* March 2021. www.andersonkill.com/News/A-Hacker-Was-Selling-a-Cybersecurity-Exploit-as-an-NFT-Then-OpenSea-Stepped-In

[10] Howcroft, Elizabeth: *NFT sales volume surges to $2.5 billion in 2021 first half.* Reuters, July 2021. www.reuters.com/article/us-fintech-nft-data-idCAKCN2EB1I8

[11] ComplyAdvantage: *KYC vs AML – What Is the Difference?* https://complyadvantage.com/knowledgebase/kyc-aml-know-your-customer-vs-anti-money-laundering/

[12] Traveler's: *What is Fidelity and Crime Insurance?* www.travelers.com/professional-liability-insurance/fidelity-crime

[13] Insurance Business Magazine: *What is specie insurance?* www.insurancebusinessmag.com/us/guides/what-is-specie-insurance-214564.aspx

[14] Insurance Business Magazine: *How can we insure NFTs?* www.insurancebusinessmag.com/us/news/breaking-news/how-can-we-insure-nfts-260576.aspx

