J Inf Process Syst, Vol.20, No.2, pp.273~283, April 2024
https://doi.org/10.3745/JIPS.03.0196

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

QNFT: A Post-Quantum Non-fungible Tokens for Secure Metaverse Environment

Abir El Azzaoui and JaeSoo Kim*

Abstract

The digital domain has witnessed unprecedented growth, reshaping the way we interact, work, and even perceive reality. The internet has evolved into a vast ecosystem of interconnected virtual worlds, giving birth to the concept of the Metaverse. The Metaverse, often envisioned as a collective virtual shared space, is created by the convergence of virtually enhanced physical reality and interactive digital spaces. Within this Metaverse space, the concept of ownership, identity, and authenticity takes on new dimensions, necessitating innovative solutions to safeguard individual rights. The digital transformation through Metaverse has also brought forth challenges, especially in copyright protection. As the lines between the virtual and physical blur, the traditional notions of ownership and rights are being tested. The Metaverse, with its multitude of user-generated content, poses unique challenges. The primary objective of this research is multifaceted. Firstly, there's a pressing need to understand the strategies employed by non-fungible token (NFT) marketplaces within the Metaverse to strengthen security and prevent copyright violations. As these platforms become centers for digital transactions, ensuring the authenticity and security of each trade becomes paramount. Secondly, the study aims to delve deep into the foundational technologies underpinning NFTs, from the workings of blockchain to the mechanics of smart contracts, to understand how they collectively ensure copyright protection. Thus, in this paper, we propose a quantum based NFT solution that can secure Metaverse and copyright contents in an advanced manner.

Keywords

Copyrights Protection, Metaverse, NFT, Quantum NTF

1. Introduction

With the Metaverse rapidly evolving, it's crucial to stay abreast of market dynamics, both domestically and internationally. This research seeks to chart the growth trajectory of Metaverse technologies, identifying trends, challenges, and opportunities. The need for this research stems from the digital domain's rapid evolution [1]. As Metaverse expands and non-fungible tokens (NFTs) become more mainstream, there's an urgent requirement to ensure that digital rights are protected, transactions are secure, and users can navigate these virtual worlds with confidence [2].

The primary focus is on the Metaverse and NFTs, particularly emphasizing copyright protection mechanisms. While the study will touch upon the broader digital landscape, the primary lens will be

Manuscript received November 6, 2023, first revision December 28, 2023; accepted December 31, 2023.

***Corresponding Author:** JaeSoo Kim (jskim@seoultech.ac.kr)

Dept. of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Korea (abir.el@seoultech.ac.kr, jskim@seoultech.ac.kr)

through these two intertwined domains [3-5]. Moreover, while the study will examine the technological underpinnings of NFTs and the Metaverse, it ventures deep into the technical details of blockchain and smart contracts. The emphasis is on understanding the broader implications of these technologies, their impact on digital rights, and their potential future trajectories.

This study constitutes a comprehensive investigation into the realm of NFTs with a primary focus on safeguarding against copyright infringement within various NFT marketplaces in the Metaverse environment [6]. Its core objective is to meticulously scrutinize the strategies and methodologies adopted by these platforms to bolster security, inhibit copyright violations, and cultivate an environment that respects intellectual property rights [8]. The report first analyzes the foundational technologies used to prevent copyright infringement using NFT technology. Overall, the report provides a comprehensive analysis of the security and technological landscape of NFTs, covering various aspects such as blockchain technology, smart contracts, NFT marketplaces, and measures to prevent copyright infringement [9]. It aims to contribute to the understanding and development of a secure and reliable systems for the South Korean industry to manage and trade NFTs without compromising of copyrights of user generated digital goods [10].

The Metaverse, by its very nature, is a vast, interconnected space, hosting numerous activities ranging from social interactions to economic transactions [11]. Such a vast expanse necessitates robust security measures to protect user data, digital assets, and the very integrity of the Metaverse itself. Furthermore, as the Metaverse becomes a hotbed for creativity and innovation, the importance of copyright technology becomes paramount [12]. Protecting the rights of creators, developers, and users is not just a legal imperative but also essential for fostering innovation and trust within the Metaverse ecosystem. This section provides a comprehensive overview of the current state of security measures and copyright technologies associated with the Metaverse. Drawing from both domestic and international perspectives, we explore the challenges faced, the solutions proposed, and the advancements made in ensuring that the Metaverse remains a secure and rights-respecting environment. From understanding the vulnerabilities that threaten the Metaverse to the cutting-edge technologies designed to counteract them, this section offers a holistic view of the ongoing efforts to make the Metaverse a safe and equitable space for all its users worldwide. As the Metaverse usage expands, so does the complexity of ensuring its security and the protection of intellectual properties within. As the Metaverse expands, the intertwining of its security vulnerabilities with copyright concerns becomes more pronounced. Addressing these challenges requires a multi-faceted approach, combining technological solutions with legal frameworks to ensure that the digital rights of creators and users are upheld. Below is a summary of the primary technologies and strategies dedicated to this cause [13].

A NFT constitutes a record of ownership that resides on a blockchain, with Ethereum's blockchain being a prominent example. While NFTs are primarily associated with digital assets like images and videos, there is a growing trend in the trade of physical assets, including items like postage stamps, jewelry, precious stones, real estate, and artworks. Within the realm of cryptocurrencies, NFTs serve as the digital equivalent of traditional sales documents, such as physical bills/invoices and electronic proceeds. NFTs offer several appealing features, including verifiability and trustless transfer. Verifiability stems from the fact that transactions involving NFTs are securely recorded on the blockchain, enabling a transparent record of ownership changes. Furthermore, the NFT framework facilitates the exchange of digital assets between parties who may not fully trust each other, as both the

cryptocurrency payment and the asset transfer occur seamlessly in a single, atomic transaction [14].

The foundational technology empowering the NFT technology consists of the blockchain technology based on a peer-to-peer decentralized platform, smart contracts for minting and assigning ownership of NFT and tokens which represent proof of authorization to access digital data. These technologies are the main components that form the NFT marketplace where tokens are traded, which are as follows:

Blockchain: The most widely used platform for managing NFTs is based on the Ethereum blockchain technology powering the Ether digital currency and serves additionally as the building block for several decentralized applications. In September 2023, the Ethereum blockchain network transitioned to the Proof of Stake consensus protocol due to it being more energy efficient and more secure than the previous Proof of Work protocol. Each user part of the network is assigned an account represented by a unique blockchain address which is used to perform transactions on the network. There are two types of accounts, an externally owned account (EOA) managed by any user in possession of its assigned private key and a Contract account which enables creation of smart contracts. Both accounts allow users to receive, hold and send NFT tokens and Ethereum cryptocurrency. Exchange of NFTs is processed on smart contracts using transactions for transfer of funds between two accounts [15].

Smart contracts: Smart contracts are an important element for NFT transfer of ownership between two parties. Each smart contract contains a code and a set of defined parameters behaving as a set of instructions, are sent to a defined address in the blockchain network. Each contract executes its functions automatically without user intervention, such as automatic transfers of NFT ownership when the seller, the owner of the NFT receives the requested amount of Ethereum. Further royalties can also be placed in effect as part of a legal agreement if a buyer of an NFT from its original designer decides to resell to a third party. In such events, the smart contract created by the original designer of the NFT can stipulate that in each instance the NFT is resold, the designer is required to receive a part of the sale value as royalties. The transfer ship of funds are automatic using smart contracts and do not require any manual interaction. A smart contract in terms of copyright management serves as a software responsible for the execution, control and documentation of buying and selling of NFTs [16].

Non-fungible token: In the Ethereum blockchain network, each NFT design and the execution of smart contracts are based on the ERC-721 standard. The standard enforces that each NFT is required to possess a unique token ID, which is assigned during the creation of the token. NFTs are represented as digital assets that are developed on the blockchain network using smart contracts. Each token represents a user's ownership of a particular digital asset, such as artwork, jewelry, sale deeds, etc. A unique token ID represented as _tokenId is assigned to an NFT to keep track of its transfer and ownership. The management of NFT in the ERC-721 standard is assigned to a manager, termed as an operator or controller, responsible to act as an authority on behalf of the NFT's owner. The management of the owner's NFT assets are based on a parameter set in the _approved argument. If the owner set the parameter as setApprovalForAll(), the operator is assigned as the manager on behalf of all tokens. If however, the owner decides to delegate authority of a particular token instead of all, a controller is assigned to manage that single entity. A function is executed, approve() along with the unique _tokenId assigning the operator the authority to manage the particular token. Transfer of ownership by either the owner of the NFT, its designated controller or operator are executed using the transferFrom() function along with the NFT's unique _tokenId, its owners _from blockchain address and the buyers _to blockchain address [17].

2. Related Work

A NFT marketplace is designed on the Ethereum blockchain network as a distributed application where NFTs are listed to be bought and sold. The marketplace is developed with a front-end, behaving as a web app with which general users interact for trading. A back-end component of the marketplace employs smart contracts which are responsible for interacting with the blockchain network. A general user provides general buy/sell instructions on the front-end web app which sends instructions to the smart contracts on the back-end [18-22]. These instructions to the smart contract include marketplace protocols responsible for the sale of tokens and token contracts, which manage the tokens. The NFT market allows the following functions to each user:

Authentication: Each user is required to initially register themselves on the marketplace for further service interactions. Authentication processes are based either using basic username/password-based credentials or a more secure method, termed as the signature method is implemented. A user is required to sign using their private key a challenge string. The Ethereum based blockchain network verifies the signature by recovering the public key of the user and verifies the integrity of the message. The public and private keys are designed based on the elliptic-curve signature cryptography for secure authentication. Traditional credential-based authentications are prone to brute-force attacks, thus exposing a user's marketplace account and all NFTs to a malicious user.

NFT minting: Each token is created using the ERC-721 standard where a single contract manages the ownership of individual tokens. A unique integer-based ID is assigned to each token, termed as _tokenId, is paired with its unique token_contract_address. These pair identifiers are stored on the ethereum blockchain to establish ownership to its appropriate user. NFT minting is possible based on three methods, default contract, replica contract, and an external contract. A default contract is designed/minted by NFT marketplace when the content creator does not provide their custom contract. Several marketplaces employ default contracts such as OpenSea, SuperRare, and Foundation. A replica contract used by marketplaces such as Nifty and Rarible, are implemented by the marketplace on content creator's behalf to manage the NFT collection sharing similar bytecode but are customizable during the initialization parameters. Lastly, the external contract requires a content creator to independently implement a custom contract for their NFT collection and upload it to the marketplace. Each customized token minting requires that it follows an established token standard such as ERC-721.

NFT listing: A content creator or seller are required to list their tokens on the NFT marketplace once the NFT collection and its seller are authenticated as the valid owners. Verified owners are provided a trusted badge on the web marketplace as a sign of trust that the NFT is offered on sale by its authorized owner. Several NFT marketplaces prevent listing of unverified collections to prevent deterioration in their buyer's confidence. Trusted sellers and content creators are boosted in the marketplace, thus increasing the likelihood of being sold.

NFT trading: NFT marketplaces support auction based selling formats to trade tokens. Buyers are required to place their bids on the NFTs and once the offer is selected, the token is sold, and all token assets are transferred to the seller to the buyer. This auction process, followed by OpenSea and Foundation, requires a minimum price set to be by the NFT owner and based on subsequent bids by interest buyers, the token is sold to the highest bidder. As gas is expensive, several marketplaces such as OpenSea provide storage of bids on off-chain for gas efficiency. This process requires the marketplace to crypto-

graphically verify the buy order and the sell order to prevent a malicious buyer from purchasing unauthorized or not on sale NFTs. All NFT transfers are required to be processed on on-chain environment. As part of copyright, each buyer of an NFT from its creator is required to pay a royalty fee for each secondary sale. The royalty fee is decided by the creator during its initial sale to the buyer. In each secondary sale, the royalty fee is automatically transferred to the creator. The marketplace undertakes the responsibility to track the secondary sales of the NFT and manage the royalty sale proceeds to the original owner. If the sale is processed on-chain, the marketplace deducts the royalty fee for its creator, otherwise the marketplace keeps track of all royalties accumulated from all secondary sales on the off-chain environment.

3. Quantum NFT for Secure Metaverse Environment

The NFT marketplace is illustrated in Fig. 1 describing the interaction between the underlying technologies, which include the authentication of ownership, minting/creation of tokens, its listing and trading. The associated actors of the ecosystem include the users, i.e., the buyer, seller, and the content creator of the marketplace.

3.1 System Overview

The detailed step by step process of interaction between the users and the underlying technology is described as follows:

Step 1 (Upload): The unique content, for example an artwork, is uploaded on an external database for public visibility, such as an online art gallery or a hosting service. As not every content creator has the skills to mint the NFT by themselves, the task is assigned to an external actor to convert the art into an NFT and store it in the blockchain network.

Step 2 (Authorization): The owner authorizes a seller on the marketplace to mint the NFT to offer it in the NFT marketplace. Alternatively, the creator may decide to behave as the seller during the listing.

Step 3 (Token listing): Once the NFT is listed on the marketplace by the designated seller/creator, the token is open to the auction process where buyers place bids on the NFT to purchase.

Step 4 (Fetch NFT): Once a buyer whose bid is selected at the auction, the marketplace seller fetches the token from the external hosting service such as Amazon Web Services (AWS) cloud storage or from the Interplanetary File System.

Step 5 (Transfer ownership): The ownership is transferred using a transferFrom() function to establish the new owner of the NFT.

Step 6 (Transaction): The marketplace on behalf of the seller who accesses the marketplace through the front-end web application, sends transactions using smart contracts in the back end to perform the sale. At this stage, the creator-buyer rules are agreed upon where the buyer is allowed to mint the NFT and offer it on the marketplace with the accepted royalty charge for all subsequent secondary sales. Furthermore, the marketplace places a nominal fee as part of the sales services provided by the platform.

Step 7 (Secondary sale): The new owner of the NFT is established as the owner/seller of the NFT and

is allowed to mint the token and offer it for further bidding and sales on the marketplace. As part of the initial agreement, the secondary seller is required to transfer royalty fees to the creator.

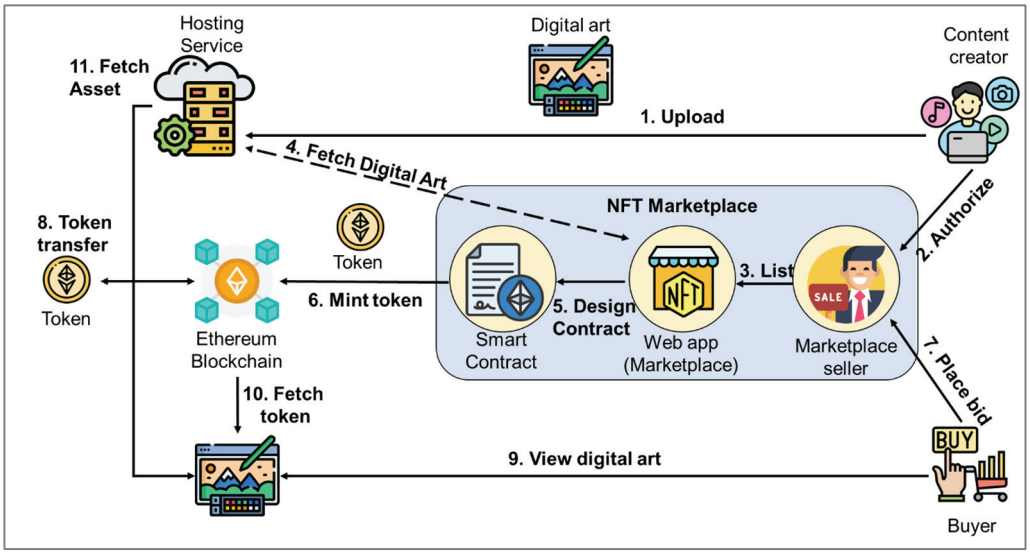


Fig. 1. Process flow of a quantum NFT marketplace.

The NFT marketplace interactions continues in the loop from Step 3–7 where with each sale, the seller is required to pay royalty fees as the copyright of the NFT, example an artwork belongs solely to the content creator. Each buyer has the right to sell it further to make profit but cannot make claims on the original art as part of a copyright infringement policy [23-25].

The University of Lleida, Spain published a study in February 2023 addressing the vulnerability of NFT plagiarism for copyright infringement for the Metaverse environment. The objective of the study is to merge classical copyright law with the emerging Metaverse environment supported by proof of content ownership and a copyright management system. The study proposes a decentralized web application for managing copyright and ownership management, termed CopyrightLY. The platform implements blockchain and semantic web technologies to aid in managing copyright claims in the Metaverse and is developed for the future European Internet ONTOCHAIN project. The study's architecture, as illustrated in Fig. 1, is developed on an on-chain blockchain environment based on the implementation of smart contracts used for managing all authorship claims to the content. The smart contract registers and links all content claims with the associated user account claiming authorship. All media and documents pertaining to the digital content are stored in the Interplanetary File System storage platform.

A secondary method to add further proof to the content creator's claim to authorship along with evidence stored in blockchain applications is via oracles. Oracles provide verifiable information about all content data stored in off-chain environments related to the original content creator's social media account, such as YouTube, Facebook, and X (formerly Twitter). The oracle via application programming interfaces (API) verifies the content creator's social media assets. For example, using YouTube's API, a predefined identifier is added to the video description unique to the content creator. During authorship claim complaints, CopyrightLY confirms the authorship claimant's on-chain account has direct control

over the off-chain social network account assets, such as videos on Facebook and YouTube. CopyrightLY implements the ChainLink mechanism present in the blockchain ecosystem to establish access between on-chain and off-chain accounts for reliably managing all authorship complaints. All malicious ownership complaints are easily and verifiably condemned by the proposed CopyrightLY platform, thus protecting the rights of content creators [26].

Three off-chain modules which interact with the on-chain CopyrightLY platform, which include the Web front-end, the back-end monitoring all events in the blockchain, and the Rights module. The first module, Web front-end allows interaction with the users by linking their Ethereum wallets to increase verifiability of the user during any authorship complaints. A third party such as a government issued verification process can be used to increase trust in the user identity verification process. This module enables the authentic content creator which staked original claim to establish complete proof by linking their government issued legal identities and their social media accounts. During a litigation process, this step strengthens the statement of the original content to have final claim over the original content.

The second off-chain module allows users to monitor all back-end events in the blockchain without requiring direct interaction. The module is built on the Graph indexing protocol, required for querying in the Ethereum blockchain network and presents the events generated by smart contracts, and is accessible using the GraphQL API. This step monitors all changes in ownerships of NFTs and their minting. The final module, the Rights module generates license NFTs allowing them to be traded in the Metaverse marketplaces. The module using the GraphSQL API, monitors changes in content ownership and retrieves semantic metadata from the Interplanetary File System. Buyers of NFT can query using the SPARQL API to verify if the NFT allows permission for secondary sales and reuse based on the context of the Metaverse virtual location [27].

In an ongoing study being conducted at the Zhejiang University, China [28], focuses on addressing the challenge of fraudulent NFTs used to steal a user's entire crypto wallet. Furthermore, fraudulent NFTs are sold through illegal digital stores on the Metaverse, resulting in buyers being flagged for copyright infringement by the original NFT owner. The study presents an anti-theft mechanism, termed as TokenPatronus using a decentralized solution for access control, risk management and arbitration process. ERC-721G smart contract standard is proposed to interact with the oracle to prevent NFT theft. Once an NFT is minted by the content creator, they can decide to lock the token via the front-end web application and prevent future transactions associated with the NFT. The decentralized access control module provides security measures requiring the owner of the NFT to verify their ownership using a wallet signature to prevent the NFT from being traded once it is locked by the content creator.

As a user intends to transfer the token to a buyer or to an NFT marketplace seller, the digital rights management system requires the creator to confirm that they accept the security risks and bear the responsibility of any NFT fraud.

When a user buys an NFT, the token is automatically locked. If a hacker manages to gain access to the owner's wallet, the digital rights management system is required to process all transactions and determine if the transfer of NFT is suspicious, hacked, or legitimate.

A decentralized risk management engine as part of the digital rights management system, evaluates the transfer of the NFT based on the collections the NFT is part of, the associated wallet address of the registered owner of the NFT, the contract status of the token (locked/unlocked), and signs of any abnormal records of transactions using the NFT. The value of the NFT is observed and if the transaction demonstrates a lower value than the market value, the transfer of the NFT is put on hold.

In the event, the token is hacked, the digital rights management system locks the transaction, and the original owner has the right to recover the NFT using a decentralized arbitration system.

The decentralized arbitration system requires the claimant to submit a deposit to prevent fraudulent reports by malicious users to stake copyright claims. The price of the deposit is determined based on the value of the NFT.

A Byzantine fault tolerance mechanism is deployed to prevent the arbitration system from cheating the original owner of the NFT. An incentive in the form of a monetary reward is offered to the jury members to encourage participation in the arbitration process.

The claimant of copyright challenge over the NFT is required to upload a conversation log between the content owner and the buyer to demonstrate the authenticity of transfer of ownership.

If the contract is deemed to be fraudulent, the arbitration system returns the token back to the original claimant's wallet address and the transaction fees born from staking the claim on the NFT are paid by the claimant.

Several other copyright infringement challenges of the NFTs are pertaining to its long-term preservation to maintain their authenticity. Traditionally NFTs are reliant on the content owner in possession of a private key associated with the private/public key pair for verifiable proof of ownership of the object. However, the strong dependence of the NFT authentication process using third party organizations such as NFT exchanges and centralized databases complicates proving the authenticity of ownership using the token. The implementation of blockchain technology for authentication is crucial for storing the public/private key pair and digital signatures for extended periods. However, data such as the true identity of the NFT creator or the association of the NFT with the copyrighted object is not stored in the NFT itself and thus the decentralized technology is not suitable for continual reliance for all future authentications. Furthermore, the lack of historical records of physical objects in the pre-blockchain era make establishing the true ownership of the NFT and its associated object. Without complete historical records stored in the blockchain, it is difficult to prove and justify copyright claims and prevent copyright infringement [29].

3.2 NFT-based Quantum Hypergraph States

Quantum hypergraph states are highly entangled multipartite quantum states derived from a mathematical hypergraph. In this context, the quantum states are associated with the vertices of the hypergraph, while the edges serve as connections to other qubits, collectively forming a non-separable many-body quantum state. Notably, this double hypergraph bears resemblance to the hypergraph state discussed in reference, with the distinction that each vertex has a parallel counterpart.

We introduce a novel approach for establishing a fundamentally quantum blockchain, leveraging the entanglement of such states as an alternative to traditional ledger and hash functions. To provide a foundational understanding of a hypergraph state, consider that a similar quantum state can be constructed from a mathematical hypergraph with k hyperedges (each connecting 2k qubits) and n vertices. Remarkably, the number of vertices in the hypergraph corresponds to n, which is twice the number of qubits within the quantum framework.

Initially, all qubits exist in pairs of Bell states, wherein one qubit belongs to class A, and the other is associated with class B. Subsequently, a controlled-phase operation with a phase angle of $\pi/2$ is executed on each k-hyperedge of both class A and B. To illustrate, consider a double hypergraph with four vertices labeled as 1, 2, 3, and 4, where each vertex contains two qubits, representing classes A and B. These

qubits of classes A and B are entangled in Bell states with their counterparts at the respective vertices. The weighted double hypergraph states can be generated by introducing a phase to each qubit through local operations.

4. Conclusion

In this paper, we investigate the security measures implemented by NFT marketplaces in different countries. For example, Tokenproof, a startup in the United States, focuses on securing NFTs through one-time verification, disconnected wallet interactions, QR code authentication, and phishing prevention. OpenSea, a major NFT marketplace both in the United States and globally, utilizes image recognition technology, human review, and malicious URL scanning to prevent NFT theft and copyminting. In Singapore, Crypto.com, a prominent NFT marketplace and cryptocurrency exchange, enhances security by offering withdrawal address whitelisting, 24-hour withdrawal locks, mandatory whitelist withdrawals, and proactive monitoring for scams and fraudulent activities. In Canada, Haloo provides instant trademark searches, simplified trademark application processes, proactive monitoring for trademark infringement, and legal enforcement against infringers. The report also explores the technological advancements in NFT security in Australia, where Immutable, a gas-free NFT marketplace, leverages ZK-rollups and smart contracts to ensure the uniqueness and non-fungibility of NFTs. They also offer a trustless bridge between layer-1 and layer-2 networks to enhance security and transparency. We propose a quantum NFT solution that can enhance the security of Metaverse and copyrights protection. In future studies, we will focus on the implementation side of the proposed idea to prove its feasibility and cost effectiveness in Metaverse market place.

Acknowledgement

This study was supported by the Research Program funded by Seoul National University of Science and Technology.

References

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & Information Systems Engineering*, vol. 59, pp. 183-187, 2017. https://doi.org/10.1007/s12599-017-0467-3

[2] W. Meng, J. Wang, X. Wang, J. Liu, Z. Yu, J. Li, Y. Zhao, and S. S. Chow, “Position paper on blockchain technology: smart contract and applications,” in *Network and System Security*. Cham, Switzerland: Springer, 2018, pp. 474-483. https://doi.org/10.1007/978-3-030-02744-5_35

[3] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352-375, 2018. https://doi.org/10.1504/IJWGS.2018.095647

[4] A. A. Monrat, O. Schelen, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” *IEEE Access*, vol. 7, pp. 117134-117151, 2019. https://doi.org/10.1109/access.2019.2936094

[5] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer,* vol. 50, no. 9, pp. 14-17, 2017. https://doi.org/10.1109/mc.2017.3571047

[6] Y. Fu and J. Zhu, "Big production enterprise supply chain endogenous risk management based on blockchain," *IEEE Access*, vol. 7, pp. 15310-15319, 2019. https://doi.org/10.1109/access.2019.2895327

[7] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62-75, 2019. https://doi.org/10.1016/j.jnca.2019.02.027

[8] O. Novo, "Blockchain meets ioT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184-1195, 2018. https://doi.org/10.1109/jiot.2018.2812239

[9] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 88-122, 2022. https://doi.org/10.1109/comst.2022.3141490

[10] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): overview, evaluation, opportunities and challenges," 2021 [Online]. Available: https://arxiv.org/abs/2105.07447.

[11] U. W. Chohan, "Non-fungible tokens: blockchains, scarcity, and value," Critical Blockchain Research Initiative (CBRI) Working Papers, 2021 [Online]. Available: https://dx.doi.org/10.2139/ssrn.3822743.

[12] L. J. Trautman, "Virtual art and non-fungible tokens," *Hofstra Law Review*, vol. 50, pp. 361-426, 2022. https://dx.doi.org/10.2139/ssrn.3814087

[13] L. Kugler, "Non-fungible tokens and the future of art," *Communications of the ACM*, vol. 64, no. 9, pp. 19-20, 2021. https://doi.org/10.1145/3474355

[14] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "Patents and intellectual property assets as non-fungible tokens; key technologies and challenges," *Scientific Reports*, vol. 12, no. 1, article no. 2178, 2022. https://doi.org/10.1038/s41598-022-05920-6

[15] C. Pinto-Gutierrez, S. Gaitan, D. Jaramillo, and S. Velasquez, "The NFT hype: what draws attention to non-fungible tokens?," *Mathematics*, vol. 10, no. 3, article no. 335, 2022. https://doi.org/10.3390/math10030335

[16] IBM quantum experience [Online]. Available: https://quantum-computing.ibm.com/.

[17] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: a provably secure proof-of-stake blockchain protocol," in *Advances in Cryptology – CRYPTO 2017*. Cham, Switzerland: Springer, 2017, pp. 357-388. https://doi.org/10.1007/978-3-319-63688-7_12

[18] K. Tamura and Y. Shikano, "Quantum random number generation with the superconducting quantum computer IBM 20Q Tokyo," 2020 [Online]. Available: https://ia.cr/2020/078.

[19] S. R. Moulick and P. K. Panigrahi, "Quantum cheques," *Quantum Information Processing*, vol. 15, pp. 2475-2486, 2016. https://doi.org/10.1007/s11128-016-1273-4

[20] M. Choi, A. E. Azzaoui, S. K. Singh, M. M. Salim, S. R. Jeremiah, and J. H. Park, "The future of Metaverse: security issues, requirements, and solutions," *Human-Centric Computing and Information Sciences*, vol. 12, article no. 60, 2022. https://doi.org/10.22967/HCIS.2022.12.060

[21] R. Almodfer, M. Mudhsh, S. Chelloug, M. Shehab, L. Abualigah, and M. Abd Elaziz, "Quantum mutation reptile search algorithm for global optimization and data clustering," *Human-centric Computing and Information Sciences*, vol. 12, article no. 30, 2022. https://doi.org/10.22967/HCIS.2022.12.030

[22] A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A quantum approximate optimization algorithm based on blockchain heuristic approach for scalable and secure smart logistics systems," *Human-centric Computing and Information Sciences*, vol. 11, article no. 46, 2021. https://doi.org/10.22967/HCIS.2021.11.046

[23] H. Hu and B. Lee, "Applying token tagging to augment dataset for automatic program repair," *Journal of Information Processing Systems*, vol. 18, no. 5, pp. 628-636, 2022. https://doi.org/10.3745/JIPS.04.0251

[24] A. E. Azzaoui and J. H. Park, "Post-quantum blockchain for a scalable smart city," *Journal of Internet Technology*, vol. 21, no. 4, pp. 1171-1178, 2020.

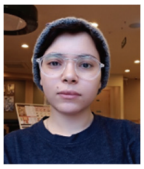
[25] S. K. Singh, A. E. Azzaoui, M. M. Salim, and J. H. Park, "Quantum communication technology for future ICT-review," *Journal of Information Processing Systems*, vol. 16, no. 6, pp. 1459-1478, 2020. https://doi.org/10.3745/JIPS.03.0154

[26] H. J. Kwon, A. El Azzaoui, and J. H. Park, "MetaQ: a quantum approach for secure and optimized Metaverse environment," *Human-centric Computing and Information Sciences*, vol. 12, article no. 42, 2022. https://doi.org/10.22967/HCIS.2022.12.042

[27] A. El Azzaoui, M. M. Salim, and J. H. Park, "Secure and reliable big-data-based decision making using quantum approach in IIoT systems," *Sensors*, vol. 23, no. 10, article no. 4852, 2023. https://doi.org/10.3390/s23104852

[28] A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A quantum approximate optimization algorithm based on blockchain heuristic approach for scalable and secure smart logistics systems," *Human-centric Computing and Information Sciences*, vol. 11, article no. 46, 2021. https://doi.org/10.22967/HCIS.2021.11.046

[29] A. E. Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated quantum cloud architecture for medical big data security," *Journal of Network and Computer Applications*, vol. 198, article no. 103304, 2022. https://doi.org/10.1016/j.jnca.2021.103304



Abri El Azzaoui **https://orcid.org/0000-0002-9406-8932**

She received a B.S. degree in computer science from the University of Picardie Jules-Verne, Amiens, France. And a master's degree from the Seoul University of Science and Technology, Seoul, South Korea. She is currently pursuing a PhD degree in computer science and engineering with the Ubiquitous Computing Security (UCS) Laboratory, Seoul National University of Science and Technology, Seoul, South Korea, under the supervision of Prof. Jong Hyuk Park. Her current research interests include quantum communication, blockchain, Internet-of-Things security, and cloud security. She is also a reviewer of the *IEEE Access*, and *IEEE Transactions on Industrial Informatics*.

JaeSoo Kim **https://orcid.org/0009-0008-6534-0811**

He received his Ph.D. in computer science from University of Otago in New Zealand. Until 2003 he was a full-time professor at Zayed University, UAE. Currently he is a full-time professor at Seoul National University of Science and Technology, Seoul, Korea. His current research interests include computational intelligence, artificial intelligence, and knowledge engineering.