Volume 2 Issue 2 (2025) 107-127
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v2i2.36
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Legal Analysis of The NFT (Non-Fungible Token) Based Digital Vaccine Certificate System in Digital Free Trade: Security, Privacy, and International Recognition Aspects

Vasio Sarmento Soares[1]*, Sundaru Guntur Wibowo[2], Syahrul Anwar[3]
[1]Institute of Business Timor Leste, Timor Leste
[2]Politeknik Negeri Madiun, Indonesia
[3]Politeknik Siber Cerdika Internasional, Indonesia
Corresponding Author: vasio.soares@iob.edu.tl

ABSTRACT

This study analyzes the legal framework of Non-Fungible Token (NFT)-based digital vaccine certificates in the context of digital free trade, focusing on security, privacy, and international recognition. Using normative and comparative legal research methods with a multidisciplinary approach, the study integrates perspectives from law, digital technology, and international policy. The study examines three main aspects: first, security, evaluating how NFTs ensure authenticity, data integrity, and protection against manipulation through encryption, blockchain, and smart contracts; second, privacy, analyzing how personal data and the privacy rights of certificate holders are protected under national and international regulations, emphasizing data minimization, user consent, and secure access; and third, international recognition, assessing the extent to which NFT-based certificates can be recognized globally, highlighting regulatory harmonization and legal barriers. The findings indicate that NFT-based vaccine certificates provide strong technical security and privacy protection, but legal recognition across jurisdictions remains inconsistent. The study concludes that while NFTs have significant potential to facilitate secure and verifiable digital health credentials in global trade, harmonization of national and international regulations and the implementation of legal standards are crucial to ensure their effectiveness and legal validity worldwide.

Keywords: NFT-based vaccine certificates, digital security, data privacy, international recognition, digital free trade

Article received on 04-07-2025 — Final revised on 06-11-2025 — Approved on 08-12-2025

Introduction

The development of digital technology has significantly impacted various aspects of human life, including the health sector, public administration, and international trade, by providing more efficient, transparent, and integrated information management mechanisms.

The COVID-19 pandemic has become a major driver for accelerating the adoption of digital innovations, one of which is the implementation of digital vaccine certificates, which play a strategic role in facilitating individual mobility while supporting efforts to control the spread of disease. These certificates serve as proof of immunization that can be verified quickly, accurately, and internationally recognized, thus facilitating the validation of vaccination status at borders and in the context of global trade. However, the implementation of digital vaccine certificates presents complex challenges, particularly related to data security, which requires protection against manipulation and illegal access; individual privacy, which requires the fulfillment of the right to personal data in accordance with national and international regulations; and cross-border document recognition, which requires harmonization of regulations and uniform legal standards for certificates to be legally accepted across jurisdictions. Therefore, the development and implementation of digital vaccine certificates requires a multidisciplinary approach that integrates legal, technological, and international policy aspects to ensure a secure, effective, and globally recognized system (Joy et al., 2022).

With the advancement of blockchain technology, the concept of NFT (non-fungible token)-based digital vaccine certificates has emerged as a promising innovation in digital health document management. NFTs are unique digital assets stored on a blockchain network, ensuring the authenticity, integrity, and transparency of every issued document. Unlike conventional digital certificates, which can be copied or altered, NFTs provide a unique identity for each certificate and a verification mechanism that is difficult to counterfeit, thereby increasing the level of trust for both users and relevant authorities. The implementation of NFT-based vaccine certificates has significant potential to increase efficiency in digital free trade, as cross-border digital document recognition is key to labor mobility, the smooth export and import of goods and services, and the security of international digital transactions. Therefore, the use of NFTs not only presents a technical innovation that strengthens the verification system but also raises various legal and policy implications that require comprehensive review, including those related to personal data protection, cybersecurity, and cross-jurisdictional regulatory harmonization, so that these certificates can be effectively implemented and recognized globally (Dowling, 2022).

Amid the accelerating digitization of global healthcare and mobility, the use of NFTs as the basis for digital vaccine certificates offers significant potential in supporting digital free trade and cross-border mobility. However, their implementation is not without serious challenges. Legally, doubts remain about whether NFT-based certificates can be recognized as official and legally valid documents, their level of compliance with personal data protection regulations, and the extent to which they are recognized in various jurisdictions with differing definitions of digital documents. From a technological perspective, although blockchain promises security, transparency, and resistance to counterfeiting, its implementation still faces risks of data manipulation, cyberattacks, and potential weaknesses in the integrity of smart contracts. Therefore, this study aims to analyze the legal and technical aspects of NFT-based digital vaccine certificates—including security, privacy, and international recognition—and evaluate the extent to which national regulations and international frameworks need to be synergized so that such systems can be implemented reliably, legally, and effectively in the context of digital free trade (Wilson et al., 2022).

Based on this background, this study focuses its analysis on three key interrelated issues in the use of Non-Fungible Token (NFT)-based digital vaccine certificates in digital free trade. First, the security aspect requires not only guarantees of the certificate's authenticity and integrity but also a critical assessment of how its technological

infrastructure—including encryption, blockchain mechanisms, and smart contracts—can provide consistent protection against technical threats without ignoring its potential vulnerabilities. Second, the privacy aspect highlights the need to comply with the principles of personal data protection, particularly regarding health information. Therefore, the use of NFTs as a certification medium does not simply rely on its technological superiority but also ensures that data processing is carried out proportionally, transparently, and respects individual control over their data. Third, the aspect of international recognition demands cross-border regulatory harmonization so that NFT-based digital vaccine certificates can be accepted and legally used in global mobility and digital trade transactions. Through these three analytical focuses, the study aims to provide a more structured mapping of the conditions, opportunities, and legal challenges that must be overcome to realize a secure, privacy-oriented, and internationally recognized NFT-based digital vaccine certificate system (Aharon & Demir, 2022).

A variety of previous literature and research provides a relevant foundation for this topic, although significant research gaps remain. Research on the use of NFTs in digital security, such as that presented by (Bamakan et al., 2022), highlights blockchain's ability to maintain data integrity and minimize the risk of counterfeiting. However, these studies focus primarily on digital assets and the financial sector, thus failing to examine the application of NFTs in a healthcare context, particularly as vaccine certificates. Furthermore, studies related to personal data protection and digital privacy, such as the GDPR (EU, 2018) and the Indonesian ITE Law (2022), emphasize important principles such as data minimization, data subject rights, and user consent, but most have not directly linked these principles to the use of NFTs as healthcare documents. Meanwhile, research on the recognition of digital documents across borders, such as the UN e-Cert initiative and the OECD Digital Trade report (2021), indicates that harmonization of international regulations is a major challenge to the global acceptance of digital documents. Thus, existing studies rarely comprehensively explore the recognition of NFT-based vaccine certificates in the context of digital free trade. This research aims to fill this gap through a multidisciplinary approach that integrates legal, technological, and international policy aspects.

Based on the available literature review, a significant research gap exists regarding the use of Non-Fungible Token (NFT)-based digital vaccine certificates, particularly in integrating legal, technological, and international recognition aspects. To date, existing research tends to be fragmented: much of it addresses only the theoretical potential of blockchain security, data protection issues, or the possibility of cross-border regulatory harmonization, without empirical evidence demonstrating actual implementation or official acceptance by specific jurisdictions. This lack of empirical evidence leaves many claims regarding the effectiveness or feasibility of using NFTs as vaccine certificates at the assumption level, thus lacking a solid basis for policy formulation. Given that the application of NFTs for vaccine certificates carries legal consequences related to document validity, privacy standards, and international recognition in free digital trade, this gap between theory and practice is a crucial issue that needs to be bridged. Therefore, this study aims to address this gap through a multidisciplinary approach that not only examines theoretical feasibility but also examines regulatory readiness, available empirical evidence, and practical limitations affecting the feasibility of implementation, resulting in a more comprehensive understanding of the prospects for implementing NFT-based digital vaccine certificates (Chalmers et al., 2022).

This research uses normative and comparative legal methods combined with a multidisciplinary approach to produce a comprehensive analysis of NFT-based digital

vaccine certificates. The normative approach examines national laws and regulations, including the Electronic Information and Transactions Law (ITE Law), the Intellectual Property Law, and personal data protection regulations, as well as international standards governing digital documents and privacy. The goal is to evaluate the extent to which the NFT system complies with existing legal frameworks and ensures legal certainty for certificate holders. The comparative approach compares practices and regulations across countries that have implemented digital certificates or NFT technology, enabling the identification of best practices, legal barriers, and opportunities for international regulatory harmonization. The multidisciplinary approach integrates legal, digital technology, and free trade policy perspectives, including blockchain, smart contract, and encryption mechanisms, to produce a comprehensive, applicable, and relevant analysis addressing the needs of global mobility and cross-jurisdictional document recognition. The synergy of these three approaches allows the research to simultaneously assess the legal, technical, and policy implications, while providing practical and implementable recommendations for the implementation of secure, legally valid, and internationally accepted NFT-based digital vaccine certificates (Valeonti et al., 2021).

This study adopts three main theoretical frameworks—Legal Tech and E-Governance, Digital Privacy and Data Protection, and Digital Trade and Cross-Border Recognition—to comprehensively analyze a Non-Fungible Token (NFT)-based digital vaccine certificate system. The Legal Tech and E-Governance framework helps assess how technological innovations such as blockchain and NFTs can be integrated into public administration systems without compromising the principle of legal certainty, while the Digital Privacy and Data Protection theory is used to evaluate the protection of data subjects' rights through the implementation of data minimization, explicit consent, and secure access control. The Digital Trade and Cross-Border Recognition theory maps the position of digital certificates within the international regulatory structure, including issues of cross-jurisdictional harmonization, potential legal disputes, and the recognition mechanisms for digital documents in the context of global mobility and free trade transactions (Ante, 2022).

Using this theoretical framework, this study examines three core issues: security, privacy, and international recognition. The security aspect is analyzed through an evaluation of the effectiveness of blockchain, smart contracts, and encryption mechanisms in maintaining the authenticity, integrity, and resistance of certificates to data manipulation. The privacy aspect is analyzed based on compliance with national provisions and international standards regarding personal data protection, including provisions regarding consent, access rights, and data control by certificate holders. Meanwhile, the international recognition aspect examines the challenges of regulatory harmonization, cross-border legal barriers, and mechanisms for accepting digital documents relevant to free digital trade. However, so far, comparative research in this area has tended to be descriptive in nature and has not provided sufficient doctrinal depth. Therefore, a more in-depth engagement with specific statutory provisions, jurisprudence, and binding international instruments is essential to strengthen the legal argument (Ali et al., 2023).

The results of this study are expected to make significant contributions from a practical, academic, and strategic perspective. Practically, the findings of this study can serve as a reference for governments, regulators, and industry players in formulating policies for implementing NFT-based digital vaccine certificates that are secure, legally valid, and internationally accepted. Academically, this research enriches the discourse on the interaction between digital technology innovation and global legal certainty, as well as increasing understanding of personal data protection and cross-jurisdictional document

recognition. Strategically, the results of this study support the development of public policies and digital free trade strategies that address data security, individual privacy, and the need for global interoperability. Thus, this research not only provides theoretical implications but also presents relevant practical recommendations for the development of digital technology regulations and policies at the national and international levels (Umar, Gubareva, et al., 2022).

Research Method

This research uses normative and comparative legal methods with a multidisciplinary approach to examine the NFT-based digital vaccine certificate system in the context of digital free trade. Normative legal methods are applied to analyze legislation, legal doctrine, and scientific literature discussing digital documents, personal data protection, and the use of blockchain in authentication systems. This approach provides a conceptual and normative basis for assessing the position of NFT-based vaccine certificates within national and international legal systems. Furthermore, a multidisciplinary approach is used to comprehensively integrate legal aspects, digital technology, and international policy (Wang, 2022).

A comparative method was applied to compare the regulatory frameworks and practices for the use of digital vaccine certificates or blockchain/NFT technology across several jurisdictions. The selection of comparison jurisdictions was based on technical and normative relevance criteria, namely: (a) countries with strong and globally recognized data protection regulations, (b) countries that have implemented standardized digital health certificate systems, and (c) countries that have explored or utilized blockchain technology in public services. Based on this, the European Union, the United States, Singapore, and South Korea were selected as the focus of the comparison because they represent different yet significant regulatory models and technological approaches to analysis (Pinto-Gutiérrez et al., 2022).

This research is a library research, so all data was obtained through legal documents, international policies, scientific literature, and technical reports. It did not involve interviews or other empirical data collection techniques. The data analyzed included official government documents, digital regulations, data protection policies, guidelines from international institutions, and academic and technical publications related to NFTs, blockchain, and digital certificates. The primary focus of data collection was to obtain a legal basis and technical framework that could explain the security, privacy, and international recognition aspects of NFT-based digital vaccine certificates (Kugler, 2021).

The primary data in this study includes national laws and regulations such as the ITE Law, the Personal Data Protection Law, and provisions related to electronic signatures and digital documents. At the international level, primary data includes the European Union's GDPR, WHO guidelines on digital health, the UN e-Cert standard, and regulations on cross-border digital trade. Meanwhile, secondary data was obtained from scientific articles, books, research reports, technology white papers, and case studies of digital certificate implementation in the countries being compared (Rehman et al., 2021).

Data collection techniques were conducted through literature review and document analysis. The literature review focused on searching academic literature and scientific publications related to digital law, NFTs, blockchain, and digital health certificates. Meanwhile, document analysis was conducted to examine relevant national and international legal provisions. This analysis included analyzing regulatory structures, identifying norms governing personal data, evaluating security standards, and reviewing

provisions regarding interoperability and cross-border recognition of digital certificates (Chandra, 2022).

Using a comparative approach, the study constructs an analytical matrix comparing key characteristics of each jurisdiction, such as data protection standards, blockchain adoption in public services, the implementation of digital health certificates, and the legal frameworks related to digital identity and cross-border transactions. This approach allows for identification of fundamental similarities and differences between countries and assesses their implications for the adoption of NFT-based vaccine certificates in the context of digital free trade (Abid et al., 2022).

Data analysis was conducted qualitatively using two techniques: content analysis and legal analysis. Content analysis was used to identify patterns, themes, and key principles related to security, privacy, and international recognition. Meanwhile, legal analysis was used to assess the compliance of NFT-based vaccine certificates with the applicable regulatory framework, potential legal conflicts, regulatory gaps, and the legal consequences of using NFTs in public services. This combined analysis yielded a comprehensive understanding of the legal standing and challenges of implementing NFT-based digital vaccine certificates (Mithani et al., 2022).

To ensure data validity and reliability, the study employed a source triangulation strategy by comparing various types of legal documents, scientific literature, and technical reports from international organizations. Furthermore, validity was strengthened through cross-checking of regulations and global standards, particularly those related to data security, interoperability, and cross-jurisdictional recognition. A peer-reviewed literature review was also used to strengthen the reliability of the analysis and ensure that the findings were soundly grounded in academic and technical terms (Razzaq et al., 2022).

Result and Discussion

Table 1. Findings on the Security Aspects of NFT-Based Digital Vaccine Certificates

Security Aspect	Research Findings	Critical Interpretation (Integration with Main Argument)	Legal and Technical Implications
Data Authenticity	NFTs record each certificate with a unique identity on blockchain, reducing the risk of counterfeiting.	Despite improving authenticity, NFT-based documents still lack explicit legal recognition. This reinforces the study's argument that legal frameworks must formally acknowledge NFT certificates for use in digital free trade.	Regulations must define NFT certificates as legally valid documents and establish standardized verification mechanisms recognized across jurisdictions.
Data Integrity	Smart contracts automatically and transparently log any changes made to the data.	Technical transparency does not automatically align with legal or administrative processes, particularly regarding error correction and liability. This supports the main argument that digital integrity must be harmonized with formal legal procedures.	Clear rules are needed on audit trails, data correction mechanisms, and shared legal/technical responsibility to ensure integrity in cross-border digital transactions.
Protection Against Cyber Attacks	Encryption and decentralized blockchain	Network-level security does not eliminate vulnerabilities at access points such as servers or digital	Governments must set minimum security requirements and adopt

Security Aspect	Research Findings	Critical Interpretation (Integration with Main Argument)	Legal and Technical Implications
	architecture reduce the likelihood of cyber attacks.	wallets. This highlights the study's core argument that cross-border standardization of cybersecurity is essential for global acceptance.	international cybersecurity standards to ensure cross-border validity of digital vaccine certificates.

The research indicates that the NFT-based digital vaccine certificate system demonstrates significant security strengths, particularly through the integrated implementation of blockchain technology, smart contracts, and data encryption. Technically, the use of blockchain enables the unique and immutable recording of each certificate, while smart contracts provide automated management of data validation and verification, thereby ensuring the integrity and authenticity of the stored information. Encryption further strengthens protection against unauthorized access or data manipulation, making NFT certificates reliable as digital proof of vaccination. However, from a legal perspective, while this technology offers high security, there is an urgent need for regulations that explicitly recognize NFTs as valid legal documents. This legal recognition is crucial for digital vaccine certificates to be accepted within the context of free digital trade, support global mobility, and ensure legal certainty for certificate holders and related parties in cross-jurisdictional transactions. Therefore, the integration of robust technical mechanisms and a clear legal framework is key to the effectiveness and legitimacy of NFT use in digital vaccine certificates.

Table 2. Findings on the Privacy Aspects of NFT-Based Digital Vaccine Certificates

Privacy Aspect	Research Findings	Critical Interpretation (Integration with Main Argument)	Legal and Technical Implications
Data Protection Compliance	The NFT system allows certificate holders to fully control access to their personal data.	Although enhancing user control, these mechanisms have not been fully tested within administrative legal frameworks. This reinforces the study's main argument that alignment with the PDPA, GDPR, and international regulations is essential for global legitimacy.	Harmonization between NFT-based data governance and international regulations (PDPA, GDPR) is required for recognition in digital free trade settings.
Data Minimization	Only data relevant to vaccination is stored in the NFT certificate, reducing the risk of personal data exposure.	While consistent with global privacy principles, potential metadata leakage through blockchain hashing requires critical evaluation. This supports the argument that privacy analysis must integrate legal and technical dimensions.	Regulations must define which minimal data elements may be stored on-chain and ensure cross-jurisdictional compliance with data minimization norms.
Access Security	Blockchain-based systems provide multi-layer authentication for accessing digital certificates.	Technological security must be supported by institutional safeguards, such as platform accountability and health authority oversight. This affirms the argument that standardized international security norms are	Governments must adopt unified global standards for access security—such as multi-factor authentication—to ensure privacy protection in cross-border digital transactions.

Privacy Aspect	Research Findings	Critical Interpretation (Integration with Main Argument)	Legal and Technical Implications
		necessary.	

The study's findings demonstrate that the NFT-based digital vaccine certificate system effectively protects personal data through the implementation of strict access controls, data minimization principles, and a clear and transparent user consent mechanism. Technically, this mechanism provides certificate holders with greater control over their personal information while reducing the risk of data misuse, thus complying with internationally recognized digital privacy principles. However, the successful implementation of this system on a global scale depends heavily on the alignment of national regulations with international standards, including cross-jurisdictional data protection provisions. This alignment is crucial for the legal recognition of NFT-based vaccine certificates across countries, supporting international mobility and free digital trade, and minimizing potential legal risks or privacy violations resulting from regulatory differences between countries. Therefore, the integration of technical aspects that safeguard privacy and legal harmonization at the national and international levels are key factors in the implementation of secure, legitimate, and trustworthy digital vaccine certificates globally.

Table 3. Findings on the International Recognition of NFT-Based Digital Vaccine Certificates

Aspects of International Recognition	Findings (with Critical Interpretation)	Legal and Technical Implications (Integrated with Main Argument)
Regulatory Harmonization	Although jurisdictions such as the EU, Singapore, and South Korea have begun testing digital health certificates, the regulatory disparities highlight the absence of a global consensus on whether NFTs qualify as legally recognized health documents. This reflects a significant gap between technological innovation and regulatory preparedness.	This gap underscores the need for an international legal framework capable of aligning NFT-based certificates across borders, particularly to ensure their legitimacy within the demands of digital free trade, which relies heavily on cross-country interoperability.
Global Mobility	While blockchain-based NFTs technically support rapid and accurate cross-border verification, the absence of harmonized legal recognition prevents the full realization of these technical advantages in global mobility arrangements.	To enable NFTs to function effectively as cross-border digital health credentials, binding international agreements or national regulatory adjustments are required to standardize digital health certificate systems in the global digital trade ecosystem.
Legal Obstacles	Differences in the definition of valid digital documents, validation mechanisms, and personal data protection frameworks among countries reveal that NFT adoption faces substantial normative, not merely technical, barriers.	Harmonizing data protection standards and aligning the legal definition of digital health documents is essential for global acceptance of NFT-based certificates and for integrating such systems into international digital free-trade frameworks.

The study's findings indicate that NFT-based digital vaccine certificates have a significant potential for international recognition, thanks to their fast, secure, and transparent blockchain-based verification mechanisms, which facilitate document validation across jurisdictions. However, their implementation faces several legal challenges, such as differing definitions of official documents, variations in personal data protection regulations, and inconsistencies in digital document recognition standards across countries. These conditions pose a major obstacle to the acceptance of NFTs as valid vaccine certificates in the context of free digital trade and global mobility. Therefore, the study emphasizes the need for cross-border regulatory harmonization and consistent application of international standards, so that NFT-based certificates not only meet technical and security requirements but also gain global legal recognition. Synergy between law, technology, and international policy is crucial to ensuring the effective, valid, and internationally acceptable implementation of digital vaccine certificates.

Security Aspects of NFT-Based Digital Vaccine Certificates

Research findings indicate that the use of NFTs in digital vaccine certificates leverages blockchain technology to uniquely record each document, giving the certificate a digital identity that cannot be duplicated or altered. This mechanism ensures document authenticity, maintains information integrity, and minimizes the potential for forgery, in line with the findings of (Nabil et al., 2022) regarding the role of blockchain in ensuring the security and transparency of digital transactions. Furthermore, the implementation of smart contracts in NFTs enables automatic, fast, and transparent verification, allowing all relevant parties, including health authorities, regulatory agencies, and certificate holders, to validate vaccination status with a high level of confidence. These technical advantages position NFTs as an effective solution for managing digital vaccine certificates, particularly in the context of digital free trade and international mobility, where document validity and security are essential factors.

The research findings show that smart contracts are a key element in the NFT system, as they automatically record every change or transaction in the digital vaccine certificate data while maintaining the integrity and consistency of the information stored on the blockchain. This mechanism allows for rapid identification of any unauthorized data manipulation or modification attempts, thereby increasing the security and reliability of the certificate. These findings align with research by (Hernández-Ramos et al., 2021), which emphasizes the importance of smart contracts in maintaining data resilience and transparency of digital transactions on the blockchain. By implementing smart contracts, the certificate verification process becomes more efficient, automated, and reliable for all relevant parties, including health authorities, regulatory agencies, and certificate holders. Therefore, the NFT system not only strengthens the technical aspects of security but also provides legal certainty and protection against potential data misuse, particularly in the context of free digital trade and international mobility.

Research findings indicate that the implementation of strong data encryption, combined with a decentralized blockchain structure, significantly improves the security of NFT-based digital vaccine certificates against cyber threats. This decentralization ensures the absence of a single point of failure, a common target for hacker attacks, effectively mitigating the risk of data manipulation and loss. Furthermore, the encryption mechanism secures sensitive information by encoding data so that only authorized parties can access and verify it, thus maintaining data integrity and confidentiality. These findings align with those of

(WILFORD et al., 2021), who emphasized that a decentralized structure is crucial for maintaining the resilience and security of digital data systems, while also enhancing the reliability of cross-jurisdictional digital document management. Therefore, the combination of encryption and decentralization not only strengthens the technical aspects of security but also builds trust between users and relevant authorities in the authenticity and validity of digital vaccine certificates, particularly in the context of free digital trade and international mobility.

From a legal perspective, although the NFT system provides a high level of technical security through the implementation of blockchain, smart contracts, and encryption, the existence of regulations that expressly recognize NFTs as legitimate digital documents remains an urgent need. Without formal legal recognition, NFT-based digital vaccine certificates risk not being accepted as legal documents in the context of cross-border transactions, international mobility, and digital free trade, thus creating legal uncertainty for certificate holders and related parties. This aligns with the findings of De Filippi & Wright (2018), who emphasized the various legal challenges arising from the use of blockchain, including the legal status of digital assets, the certainty of document recognition, and the protection of data subjects' rights. Therefore, aligning technological innovation with a clear legal framework is a crucial prerequisite for NFTs to function not only as a secure technical mechanism but also as a legal instrument recognized nationally and internationally (Zang et al., 2023).

Research indicates that implementing an automated verification mechanism through NFT significantly accelerates and simplifies the validation process for digital vaccine certificates at various checkpoints, both at international borders and in healthcare facilities. This system allows authorities to directly verify the authenticity and integrity of documents without undergoing time-consuming manual procedures, thereby increasing operational efficiency and reducing administrative costs. A similar implementation is seen in the European Union for COVID-19 digital certificates, where the digitization of health documents has been shown to facilitate cross-border mobility in a faster and more secure manner (European Commission, 2021). Therefore, the integration of NFT technology not only strengthens the technical aspects of verification but also supports global mobility and the reliability of digital health systems, making it an effective solution for cross-jurisdictional health document management and free digital trade (Montanari Vergallo et al., 2021).

The research findings show that NFT's ability to maintain document integrity plays a significant role in the context of digital free trade, where digital vaccine certificates are often a crucial requirement for labor movement, goods shipments, and cross-border transactions. The blockchain and smart contract technology integrated into NFTs guarantee that each document cannot be manipulated, can be quickly verified, and is transparent to authorities, thereby minimizing the risk of fraud or forgery that could disrupt the smooth flow of international trade and mobility. These findings align with the OECD (2021) report, which emphasizes the importance of the security and reliability of digital documents in supporting cross-border trade, harmonizing international regulations, and increasing administrative efficiency. Therefore, the implementation of NFTs not only offers technical innovation in document verification but also makes a strategic contribution to the smooth flow of digital trade and secure and legally valid global mobility (Georgoulias et al., 2023).

The research findings indicate that while NFTs provide a high level of security through the implementation of smart contracts and data encryption, there are a number of technical risks that require attention. These risks include the possibility of bugs or programming errors in smart contracts, as well as potential vulnerabilities in encryption

algorithms that have not been thoroughly tested on a global scale, potentially threatening the integrity of the certificates. These findings align with a study by (Arif et al., 2022), which emphasized the need for continuous technical oversight in blockchain implementations, including through code audits, penetration testing, and periodic security evaluations. Therefore, to ensure the reliable functioning of NFTs in the implementation of international digital vaccine certificates, additional security measures, regular technology updates, and a comprehensive risk mitigation strategy are needed to ensure the authenticity, integrity, and user trust in digital documents.

Within the national legal framework, the implementation of NFTs as digital vaccine certificates requires firm legal recognition and protection through applicable regulations, such as the Electronic Information and Transactions Law (ITE) and the Personal Data Protection Law. These regulations need to affirm the legal status of NFTs so that these documents are not merely technical but are recognized as valid evidence in the context of digital administration and transactions at the national level. Compliance with existing regulations is essential to guarantee legal certainty for certificate owners and authorities, while also ensuring the protection of personal data rights through the principles of data minimization, user consent, and secure access management. Furthermore, formal recognition of NFTs within the national legal system allows for the legal use of digital vaccine certificates in a variety of activities, from domestic mobility to engagement in digital free trade, thus harmonizing technological innovation and the national legal framework, supporting the implementation of secure, legitimate, and trustworthy digital certificates (Zhu et al., 2023).

The analysis shows that the implementation of NFT security technology in digital vaccine certificates must be supported by clear technical and legal standards to ensure the reliability and legal certainty of the documents. These technical standards include system security certification, regular audits of smart contracts, and penetration testing to detect and repair potential vulnerabilities, so that data integrity, authenticity, and security can be consistently maintained. From a legal perspective, regulations governing the validity of digital documents must be enforced so that NFTs are recognized as legal documents and accepted both nationally and internationally. This integrated approach aligns with Kshetri's (2017) recommendations, which emphasize the importance of synergy between technical mechanisms and legal certainty in managing blockchain-based digital assets. Therefore, the integration of technical and legal standards is a crucial prerequisite for NFT-based digital vaccine certificates to be not only technically secure but also to have clear and reliable legal legitimacy in the context of free digital trade and global mobility (Halpin, 2022).

The study's conclusions confirm that NFT-based digital vaccine certificates can guarantee the authenticity and integrity of documents through blockchain, smart contracts, and encryption, creating unique and difficult-to-manipulate digital identities. However, NFT implementation cannot simply rely on technical aspects; it requires clear legal recognition at the national and international levels for the certificates to be accepted in various administrative and global mobility contexts. Ongoing technical oversight, such as smart contract audits, security certifications, and cyber risk assessments, is also crucial to maintaining system reliability. Therefore, the success of NFT implementation depends on a combination of robust technology, legal certainty, and consistent risk management (Agbedanu et al., 2022).

Privacy Aspects of NFT-Based Digital Vaccine Certificates

The research findings show that the NFT system for digital vaccine certificates gives owners full control over their personal data through encryption, authentication, and access rights settings, enabling direct monitoring and management of data usage. This approach aligns with the principles of the GDPR (2018), which emphasizes the individual's right to determine access and consent to sensitive data, including health information. Thus, NFTs serve not only as administrative documents but also as a mechanism that strengthens privacy protection, increases transparency, and provides security for data owners. This full control is crucial in international mobility and digital commerce, where health data is often a cross-border requirement and must be managed securely and in accordance with global privacy standards (Marelli, 2023).

Research findings indicate that the application of data minimization principles in the NFT system for digital vaccine certificates significantly strengthens the privacy protection of certificate holders. This system stores only strictly necessary vaccination information, thereby reducing the exposure of personal data and minimizing the risk of misuse or leakage of sensitive information. This approach aligns with (Hadasik & Mach-Król, 2024) view that data restriction is a key strategy in maintaining privacy. Through selective encryption, decentralized storage, and access granted only to authorized parties with the certificate holder's consent, NFTs ensure security and compliance with regulations such as the PDP Law in Indonesia and the GDPR in the European Union. Therefore, the application of data minimization principles is a crucial element in ensuring that NFT-based digital vaccine certificates are secure, legally valid, and globally accepted while maintaining user trust (Banerjee et al., 2022).

Research findings indicate that access security mechanisms play a critical role in protecting the privacy of NFT-based digital vaccine certificate holders. Through a combination of dual authentication and blockchain-based access control, the system can prevent unauthorized access, transparently record all access activity, and enable holders to monitor their data usage. This aligns with the findings of (Marques, 2021) that blockchain provides decentralized access control that strengthens security and minimizes the risk of data misuse. When combined with encryption and data minimization principles, this mechanism creates a secure environment for certificate holders to manage their personal information. In the context of international mobility and digital commerce, robust access security is crucial for maintaining the validity and confidentiality of health data, while ensuring compliance with national and global data protection standards.

Research findings indicate that, from a national legal perspective, the implementation of NFTs as digital vaccine certificates must comply with the provisions of the Indonesian Personal Data Protection Law, which requires explicit consent from data subjects before any personal information can be processed or shared. This principle affirms an individual's right to control the use of their personal data, including sensitive health information, so that any data access or transaction can only be carried out with the direct permission of the certificate owner. Therefore, the implementation of NFTs needs to be designed so that this consent mechanism is technically integrated, for example through a smart contract that ensures any use or verification of data occurs only after the certificate owner's consent has been granted. The implementation of this explicit consent principle not only provides legal certainty for data owners but also strengthens the status of digital certificates as official documents valid under national law. Furthermore, the integration of this principle supports accountability and transparency in data management, reduces the risk of privacy violations, and forms the basis for the implementation of secure, valid, and legally acceptable NFT-based digital vaccine certificates, both nationally and in cross-border trade and mobility.

The research analysis shows that harmonizing privacy regulations is a crucial challenge in the cross-border implementation of NFT-based digital vaccine certificates. Differences in definitions, principles, and standards for personal data protection across jurisdictions, including regulations regarding the collection, storage, use, and transfer of sensitive information such as health data, create potential legal inconsistencies when certificates are used internationally. A document that is valid under the regulations of one country may not meet the legal or technical requirements of another. Therefore, global recognition of NFT-based digital certificates requires an approach that takes these regulatory variations into account, including the adoption of international best practices, the development of interoperability mechanisms, and cross-border agreements on data protection. This approach not only ensures the protection of individual privacy rights but also strengthens the legal legitimacy of certificates, builds trust between countries, and supports secure and legitimate international mobility and free digital trade. Therefore, harmonizing privacy regulations is a crucial prerequisite for the implementation of globally recognized NFT-based digital vaccine certificates, while maintaining a balance between technological innovation and compliance with international law (Bampalas & Rantos, 2022).

Based on previous literature findings (Kshetri, 2017; De Filippi & Wright, 2018), the implementation of innovative technologies such as NFTs must be accompanied by a clear and robust privacy regulatory framework, as the absence of such regulations can pose legal and social risks to data owners. This becomes even more crucial in the context of digital vaccine certificates, given the highly sensitive nature of the data processed, particularly individual health information, which, if misused, could seriously impact the privacy and security of data subjects. This literature emphasizes the need to integrate technical mechanisms, such as encryption, access control, and smart contracts, with adequate legal certainty to optimally protect individual rights. Without clear regulations, NFTs face the risk of legal challenges related to document validity, cross-jurisdictional recognition, and compliance with national and international data protection standards, as well as the potential for social conflict due to public concerns about the misuse of personal information. Therefore, the implementation of NFTs in digital certificate management requires a comprehensive approach, combining technological innovation with legal certainty and privacy protection principles, so that the system developed is not only technically secure and efficient, but also legally valid and socially acceptable globally (Mekacher et al., 2022).

The research indicates that NFTs provide a high level of transparency in the recording and verification of digital vaccine certificates, as every transaction and data change is permanently recorded on a decentralized blockchain. This advantage allows authorized parties to validate documents quickly, accurately, and transparently, thereby strengthening trust in the certificate's authenticity. However, this high level of transparency also poses challenges related to personal data protection, as sensitive information such as vaccination status can be exposed if not managed through adequate access control mechanisms. Therefore, the implementation of NFTs must be accompanied by a strict access control system, including user authentication, data encryption, and selective access rights settings, so that only authorized parties can access personal information. This approach aligns with the findings of (Chiacchio et al., 2022), who emphasized that while blockchain enhances the transparency and security of digital transactions, privacy protection remains a crucial aspect that must be supported by additional technical mechanisms. By integrating a balance between transparency and access control, NFTs not only guarantee the reliability and authenticity of digital vaccine certificates but also protect individual privacy rights,

ensure compliance with national and international data protection regulations, and support the use of secure digital documents in the context of global mobility and free digital trade.

The research indicates that the implementation of smart contracts in the NFT system for digital vaccine certificates enables an automated access approval mechanism, where data owners have full control over who is authorized to verify the certificate and in what context the information can be accessed. This mechanism not only increases the effectiveness and speed of the verification process but also ensures that the certificate owner's privacy rights are consistently and transparently respected. Through smart contracts, each access request is automatically executed according to the rules set by the data owner, thereby reducing the risk of misuse or unauthorized access. This approach aligns with the privacy-by-design principle advocated by the GDPR, which emphasizes that data protection should be integrated from the system design stage, not simply as an additional step. With smart contracts supporting automated access approval, digital certificates can maintain a balance between transparency, operational efficiency, and privacy protection, ensuring that certificate owners are confident that their sensitive health information is only used with permission and for approved purposes. This is particularly relevant in the context of international mobility and free digital trade, where document verification processes must be fast, legally valid, and maintain the security and confidentiality of personal data across jurisdictions (Arcenegui et al., 2021).

The research findings confirm that international recognition of NFT-based digital vaccine certificates requires compliance with global data protection standards, ensuring that the processing and transfer of certificate holders' personal information does not violate regulations or laws in the destination country. Given that each country has different rules regarding the collection, storage, use, and distribution of sensitive data, including health data, a certificate that is legally valid in one jurisdiction may not be recognized in another. Therefore, the implementation of NFTs must integrate cross-border interoperability mechanisms, the adoption of international best practices, strong data encryption, and the regulation of access rights in accordance with privacy protection principles. This aligns with the findings of the OECD Digital Trade Report (2021), which highlights the importance of digital document security and compliance with global data protection regulations to support cross-border digital trade and international mobility. Therefore, integrating international legal compliance is crucial for the legal recognition of NFT certificates, ensuring secure data exchange, and building stakeholder trust in the context of free digital trade and global mobility (L. Wu et al., 2023).

The study's conclusions indicate that NFT-based digital vaccine certificates offer technical advantages in protecting privacy through encryption, access control, smart contracts, and data minimization principles, allowing certificate holders to control who can access their information. However, privacy protection cannot rely solely on technology, as differences in data protection standards, official document definitions, and legal requirements across countries can hinder the global recognition and use of certificates. Therefore, a clear legal basis, harmonization of international regulations, and a cross-jurisdictional interoperability system are needed to consistently protect individual privacy rights. By integrating technical aspects and an international regulatory framework, NFT-based vaccine certificates can be used securely, legally, and effectively in global mobility and digital commerce (Umar, Polat, et al., 2022).

International Recognition Aspects of NFT-Based Digital Vaccine Certificates

Research findings indicate that regulatory harmonization between countries remains a major challenge in the international implementation of NFT-based digital vaccine certificates, primarily due to differing definitions and requirements for valid digital documents across jurisdictions. This discrepancy can create legal risks when NFT certificates valid in one country are not recognized in another, thus hindering global digital mobility and trade. To ensure international recognition, a comprehensive strategy is needed, including the adoption of global best practices, interoperability mechanisms, and cross-border agreements on data protection standards and the validity of digital documents. These harmonization efforts will not only increase trust between countries but also ensure that the use of NFTs remains secure, legal, and compliant with regulations, supporting global mobility and free digital trade (Chowdhury et al., 2023).

The findings of a case study in the European Union demonstrate that COVID-19 digital certificates can be verified across borders thanks to the use of blockchain and uniform interoperability standards. Blockchain ensures data security, transparency, and impermeability, while interoperability harmonizes data formats, verification protocols, and authentication procedures across member states, enabling efficient validation processes without technical or legal barriers. These findings align with a 2021 OECD report, which emphasized the importance of international standards to ensure the validity and trustworthiness of digital documents across borders. Similar principles can be applied to NFT-based vaccine certificates to facilitate global mobility, support digital trade, and ensure secure and regulatory data management. Therefore, the integration of blockchain and interoperability standards is key to the recognition and use of digital certificates globally (Yousaf & Yarovaya, 2022).

The study indicates that the use of NFTs in digital vaccine certificates enables fast, automated, and accurate document verification through blockchain technology, which permanently and transparently records every transaction. This mechanism eliminates the need for manual verification processes, minimizes the risk of human error, and ensures that vaccination status can be instantly confirmed by authorities in various locations. This advantage is highly relevant in the context of global labor mobility, where proof of vaccination is required when moving between countries, and in digital free trade, where health documents or related certifications can be prerequisites for cross-border shipments. With blockchain-based verification, each NFT certificate guarantees the integrity and authenticity of documents, speeding up administrative processes and increasing the level of trust between parties involved in international mobility and cross-jurisdictional transactions. Therefore, the implementation of NFTs not only brings technical innovations to digital document management but also supports operational efficiency, legal compliance, and data protection, while opening up opportunities for broader integration into digital trade and global mobility systems (Far et al., 2022).

Research findings indicate that one of the main obstacles to the implementation of NFT-based digital vaccine certificates is legal barriers, particularly when national regulations have not yet officially recognized NFTs as legally valid documents. This unclear legal status creates uncertainty for companies, institutions, and individuals utilizing NFTs for international trade, labor mobility, or cross-jurisdictional transactions, as technically valid documents may not be legally accepted in some countries. This situation increases administrative risks, including the possibility of document rejection, difficulty meeting local regulatory requirements, and potential legal disputes due to differing interpretations of the validity of digital certificates. Therefore, formal legal recognition of NFTs at the national level is crucial for digital certificates to not only function technically but also have clear legal

legitimacy and be officially accepted. This situation emphasizes the need for regulatory harmonization, national policy updates, and the development of a legal framework responsive to blockchain innovation, so that NFTs can be used safely, legally, and globally recognized in the context of international trade and cross-border mobility without creating legal uncertainty for users or authorities (Chirtoaca et al., 2020).

Findings from previous literature (Xia et al., 2022) confirm that for blockchain-based digital documents, including NFT-based digital vaccine certificates, to be recognized across jurisdictions, a clear and structured legal framework is required. Without an international agreement establishing document validity or national regulatory adjustments aligned with blockchain technology principles, certificates that are technically valid in one country are not automatically legally recognized in another. This discrepancy has the potential to create significant barriers to international labor mobility, cross-border digital trade, and the exchange of information between countries, as documents lacking legal recognition can be rejected by authorities or relevant parties. Therefore, regulatory harmonization through multilateral agreements or domestic legal reform is a strategic step to ensure the validity and reliability of NFT certificates globally. This approach not only provides legal certainty for certificate holders and users of digital services but also supports the interoperability of blockchain systems across borders, maintains data integrity, and strengthens trust between countries in the management of sensitive digital documents, particularly those related to health information and international mobility.

For NFT-based digital vaccine certificates to achieve widespread acceptance in free digital trade, an international agreement is needed that establishes uniform technical and legal standards. These technical standards include security protocols, encryption, and smart contracts to automatically regulate data access rights, allowing certificates to be verified quickly and securely across jurisdictions. From a legal perspective, cross-border recognition is necessary so that technically valid certificates also have legal legitimacy recognized for international mobility and transactions. Integrating these technical standards and legal certainty will strengthen security, global blockchain interoperability, and trust between countries, enabling NFT certificates to function as legitimate, secure, and effective official instruments in the international digital trade ecosystem (Cornelius, 2021).

The application of NFTs to digital vaccine certificates can accelerate document verification at international borders thanks to a blockchain system that provides permanent, transparent, and tamper-proof records, allowing authorities to ensure document authenticity without lengthy administrative procedures. This efficiency is relevant in the context of digital free trade, which requires speed, accuracy, and security in the mobility of labor and the flow of goods. By minimizing inspection time, human error, and the risk of counterfeiting, NFT technology supports the smooth flow of international trade while strengthening legal certainty and the protection of sensitive data. This integration also increases trust between countries, making NFTs an effective strategy for strengthening operational efficiency and information security in modern border systems (C.-H. Wu & Liu, 2022).

The research findings indicate that differences in regulations between countries, particularly regarding personal data protection and the recognition of official documents, are a major obstacle to the implementation of NFT-based digital vaccine certificates. Each jurisdiction has different rules and definitions of digital documents, so a certificate that is technically valid in one country may not be legally accepted in another. This discrepancy has the potential to lead to document rejection, administrative disputes, and legal uncertainty. To address this, international regulatory harmonization, the implementation of global best

practices, and interoperability mechanisms are needed to ensure NFT certificates are legally recognized across jurisdictions. These efforts are crucial to maintain consistent privacy protection, support workforce mobility, and facilitate secure and legal cross-border data exchange and trade (Alkhudary et al., 2023).

Research findings indicate that several countries have tested NFT-based digital vaccine certificates to assess blockchain's ability to quickly and securely verify health documents. While initial results demonstrate significant potential, global recognition cannot be achieved through national implementation alone. Regulatory harmonization and the implementation of international standards are needed to ensure NFT certificates are recognized across jurisdictions while still protecting personal data. This effort aligns with OECD (2021) recommendations and the UN e-Cert initiative, which emphasize the importance of security, interoperability, and global recognition of digital documents. Therefore, the adoption of NFTs as an official instrument at the international level requires a synergy between technical innovation, legal certainty, and the protection of individual rights so that digital certificates can be used legally, securely, and effectively across countries (Hartwich et al., 2024).

The study's conclusions confirm that NFT-based digital vaccine certificates have the potential for international recognition due to their support for blockchain technology, smart contracts, and encryption, which enable fast, secure, and transparent verification. However, global recognition cannot be achieved through technical excellence alone, as legal barriers remain, such as differences in the definition of official documents, data protection standards, and legal requirements between countries. Therefore, harmonization of international regulations, international agreements on document validity and interoperability, and the consistent implementation of global technical standards are needed to ensure the security and integrity of certificates. If technical, legal, and international standards can be aligned, NFT-based vaccine certificates can be effectively used in international mobility and digital commerce, while protecting individual privacy rights and strengthening global trust in digital documents (Flick, 2022).

Conclusions

The use of NFTs offers significant potential in terms of security, privacy, and international recognition. Technically, blockchain technology, data encryption, and smart contracts can maintain the authenticity, integrity, and confidentiality of certificates, thereby increasing trust in cross-border verification. From a privacy perspective, the data control mechanism by the owner, the principle of information minimization, and user consent demonstrate compliance with national and international data protection standards. However, the implementation of NFTs as vaccine certificates still faces substantial normative barriers, particularly related to the diversity of legal standards across countries, the formal recognition of NFTs as legitimate health documents, and the asymmetry of global data protection regimes. To address the issue of feasibility of implementation across various legal systems, this study recommends several normative steps: harmonization of regulations across jurisdictions through a mutual recognition agreement model; adjustment of national regulations to include the category of blockchain-based digital health documents; development of international technical and legal standards regarding interoperability, security, and data protection; and the establishment of a collaborative forum between regulators, international organizations, and technology developers to ensure consistent and legitimate implementation globally. Thus, while NFTs demonstrate high technical feasibility, their successful implementation depends heavily on the readiness of legal systems and

coordination between countries, while also opening up space for further research on blockchain integration with public health policy and international trade governance.

Acknowledgement

The author would like to express sincere appreciation to all parties who supported the completion of this study. Special thanks are extended to legal scholars and digital technology experts who provided valuable insights regarding NFT-based digital vaccine certificate systems. The author also acknowledges the guidance and constructive feedback from academic mentors and colleagues. It is hoped that this research contributes to the development of secure, privacy-oriented, and internationally recognized digital certification systems within the context of digital free trade.

References

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2022). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Software: Practice and Experience, 52(4), 841–867. https://doi.org/10.1002/spe.2983

Agbedanu, P. R., Bawah, F. U., Akoto-Adjepong, V., Awarayi, N. S., Nti, I. K., Boateng, S., Nimbe, P., & Nyarko-Boateng, O. (2022). BLOCOVID: A blockchain-based COVID-19 digital vaccination certificate verification system. 2022 International Conference on Engineering and Emerging Technologies (ICEET), 1–6. https://doi.org/10.1109/ICEET56468.2022.10007366

Aharon, D. Y., & Demir, E. (2022). NFTs and asset class spillovers: Lessons from the period around the COVID-19 pandemic. Finance Research Letters, 47, 102515. https://doi.org/10.1016/j.frl.2021.102515

Ali, O., Momin, M., Shrestha, A., Das, R., Alhajj, F., & Dwivedi, Y. K. (2023). A review of the key challenges of non-fungible tokens. Technological Forecasting and Social Change, 187, 122248. https://doi.org/10.1016/j.techfore.2022.122248

Alkhudary, R., Belvaux, B., & Guibert, N. (2023). Understanding non-fungible tokens (NFTs): insights on consumption practices and a research agenda. Marketing Letters, 34(2), 321–336. https://doi.org/10.1007/s11002-022-09655-2

Ante, L. (2022). The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. FinTech, 1(3), 216–224. https://doi.org/10.3390/fintech1030017

Arcenegui, J., Arjona, R., Román, R., & Baturone, I. (2021). Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs. Sensors, 21(9), 3119. https://doi.org/10.3390/s21093119

Arif, M., Shamsudheen, S., Ajesh, F., Wang, G., & Chen, J. (2022). AI bot to detect fake COVID-19 vaccine certificate. IET Information Security, 16(5), 362–372. https://doi.org/10.1049/ise2.12063

Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Scientific Reports, 12(1), 2178. https://doi.org/10.1038/s41598-022-05920-6

Bampalas, C., & Rantos, K. (2022). Blockchain-based vaccination certificates management. Proceedings of the 26th Pan-Hellenic Conference on Informatics, 309–316. https://doi.org/10.1145/3575879.3576010

Banerjee, P., Bilgaiyan, S., & Tikmani, A. (2022). COVID-19 Test Report and Vaccine Certificate Verification Through Blockchain and E-Commerce (pp. 181–195). https://doi.org/10.4018/978-1-6684-4969-1.ch009

Chalmers, D., Fisch, C., Matthews, R., Quinn, W., & Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? Journal of Business Venturing Insights, 17, e00309. https://doi.org/10.1016/j.jbvi.2022.e00309

Chandra, Y. (2022). Non-fungible token-enabled entrepreneurship: A conceptual framework. Journal of Business Venturing Insights, 18, e00323. https://doi.org/10.1016/j.jbvi.2022.e00323

Chiacchio, F., D'Urso, D., Oliveri, L. M., Spitaleri, A., Spampinato, C., & Giordano, D. (2022). A Non-Fungible Token Solution for the Track and Trace of Pharmaceutical Supply Chain. Applied Sciences, 12(8), 4019. https://doi.org/10.3390/app12084019

Chirtoaca, D., Ellul, J., & Azzopardi, G. (2020). A Framework for Creating Deployable Smart Contracts for Non-fungible Tokens on the Ethereum Blockchain. 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 100–105. https://doi.org/10.1109/DAPPS49028.2020.00012

Chowdhury, M. A. F., Abdullah, M., Alam, M., Abedin, M. Z., & Shi, B. (2023). NFTs, DeFi, and other assets efficiency and volatility dynamics: An asymmetric multifractality analysis. International Review of Financial Analysis, 87, 102642. https://doi.org/10.1016/j.irfa.2023.102642

Cornelius, K. (2021). Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs). Information, 12(9), 358. https://doi.org/10.3390/info12090358

Dowling, M. (2022). Fertile LAND: Pricing non-fungible tokens. Finance Research Letters, 44, 102096. https://doi.org/10.1016/j.frl.2021.102096

Far, S. B., Bamakan, S. M. H., Qu, Q., & Jiang, Q. (2022). A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. Procedia Computer Science, 214, 755–762. https://doi.org/10.1016/j.procs.2022.11.238

Flick, C. (2022). A critical professional ethical analysis of Non-Fungible Tokens (NFTs). Journal of Responsible Technology, 12, 100054. https://doi.org/10.1016/j.jrt.2022.100054

Georgoulias, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E. (2023). COVID-19 Vaccination Certificates in the Darkweb. Digital Threats: Research and Practice, 4(1), 1–17. https://doi.org/10.1145/3530877

Hadasik, B., & Mach-Król, M. (2024). On Enhancing the COVID-19 Certification System for the Digitally-Illiterate People Inclusion in the European Union. Digital, 4(1), 182–194. https://doi.org/10.3390/digital4010009

Halpin, H. (2022). A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy? Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–8. https://doi.org/10.1145/3538969.3544459

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2024). Probably something: a multi-layer taxonomy of non-fungible tokens. Internet Research, 34(1), 216–238. https://doi.org/10.1108/INTR-08-2022-0666

Hernández-Ramos, J. L., Karopoulos, G., Geneiatakis, D., Martin, T., Kambourakis, G., & Fovino, I. N. (2021). Sharing Pandemic Vaccination Certificates through Blockchain: Case Study and Performance Evaluation. Wireless Communications and Mobile Computing, 2021(1). https://doi.org/10.1155/2021/2427896

Joy, A., Zhu, Y., Peña, C., & Brouard, M. (2022). Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens. Strategic Change, 31(3), 337–343. https://doi.org/10.1002/jsc.2502

Kugler, L. (2021). Non-fungible tokens and the future of art. Communications of the ACM, 64(9), 19–20. https://doi.org/10.1145/3474355

Marelli, L. (2023). The Italian debate on the digital COVID certificate: co-producing epistemic and normative rationalities. Science as Culture, 32(4), 505–534. https://doi.org/10.1080/09505431.2023.2211761

Marques, J. G. (2021). The EU Digital COVID Certificate: Should We Differentiate Between Previously Infected and Fully Vaccinated People? Acta Médica Portuguesa, 34(11), 803–804. https://doi.org/10.20344/amp.16830

Mekacher, A., Bracci, A., Nadini, M., Martino, M., Alessandretti, L., Aiello, L. M., & Baronchelli, A. (2022). Heterogeneous rarity patterns drive price dynamics in NFT collections. Scientific Reports, 12(1), 13890. https://doi.org/10.1038/s41598-022-17922-5

Mithani, S. S., Bota, A. B., Zhu, D. T., & Wilson, K. (2022). A scoping review of global vaccine certificate solutions for COVID-19. Human Vaccines & Immunotherapeutics, 18(1), 1–12. https://doi.org/10.1080/21645515.2021.1969849

Montanari Vergallo, G., Zaami, S., Negro, F., Brunetti, P., Del Rio, A., & Marinelli, E. (2021). Does the EU COVID Digital Certificate Strike a Reasonable Balance between Mobility Needs and Public Health? Medicina, 57(10), 1077. https://doi.org/10.3390/medicina57101077

Nabil, S. S., Alam Pran, M. S., Al Haque, A. A., Chakraborty, N. R., Chowdhury, M. J. M., & Ferdous, M. S. (2022). Blockchain-based COVID vaccination registration and monitoring. Blockchain: Research and Applications, 3(4), 100092. https://doi.org/10.1016/j.bcra.2022.100092

Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D., & Velasquez, S. (2022). The NFT Hype: What Draws Attention to Non-Fungible Tokens? Mathematics, 10(3), 335. https://doi.org/10.3390/math10030335

Razzaq, A., Mohsan, S. A. H., Ghayyur, S. A. K., Al-Kahtani, N., Alkahtani, H. K., & Mostafa, S. M. (2022). Blockchain in Healthcare: A Decentralized Platform for Digital Health Passport of COVID-19 Based on Vaccination and Immunity Certificates. Healthcare, 10(12), 2453. https://doi.org/10.3390/healthcare10122453

Rehman, W., Zainab, H. e, Imran, J., & Bawany, N. Z. (2021). NFTs: Applications and Challenges. 2021 22nd International Arab Conference on Information Technology (ACIT), 1–7. https://doi.org/10.1109/ACIT53391.2021.9677260

Umar, Z., Gubareva, M., Teplova, T., & Tran, D. K. (2022). Covid-19 impact on NFTs and major asset classes interrelations: Insights from the wavelet coherence analysis. Finance Research Letters, 47, 102725. https://doi.org/10.1016/j.frl.2022.102725

Umar, Z., Polat, O., Choi, S.-Y., & Teplova, T. (2022). Dynamic connectedness between non-fungible tokens, decentralized finance, and conventional financial assets in a time-frequency framework. Pacific-Basin Finance Journal, 76, 101876. https://doi.org/10.1016/j.pacfin.2022.101876

Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., & Chalkias, K. (2021). Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs). Applied Sciences, 11(21), 9931. https://doi.org/10.3390/app11219931

Wang, Y. (2022). Volatility spillovers across NFTs news attention and financial markets. International Review of Financial Analysis, 83, 102313. https://doi.org/10.1016/j.irfa.2022.102313

WILFORD, S. H., MCBRIDE, N., BROOKS, L., EKE, D. O., AKINTOYE, S., OWOSENI, A., LEACH, T., FLICK, C., FISK, M., & STACEY, M. (2021). The Digital Network of Networks: Regulatory Risk and Policy Challenges of Vaccine Passports. European Journal of Risk Regulation, 12(2), 393–403. https://doi.org/10.1017/err.2021.35

Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. Business Horizons, 65(5), 657–670. https://doi.org/10.1016/j.bushor.2021.10.007

Wu, C.-H., & Liu, C.-Y. (2022). Educational Applications of Non-Fungible Token (NFT). Sustainability, 15(1), 7. https://doi.org/10.3390/su15010007

Wu, L., Lu, W., Peng, Z., & Webster, C. (2023). A blockchain non-fungible token-enabled 'passport' for construction waste material cross-jurisdictional trading. Automation in Construction, 149, 104783. https://doi.org/10.1016/j.autcon.2023.104783

Xia, Y., Li, J., & Fu, Y. (2022). Are non-fungible tokens (NFTs) different asset classes? Evidence from quantile connectedness approach. Finance Research Letters, 49, 103156. https://doi.org/10.1016/j.frl.2022.103156

Yousaf, I., & Yarovaya, L. (2022). The relationship between trading volume, volatility and returns of Non-Fungible Tokens: evidence from a quantile approach. Finance Research Letters, 50, 103175. https://doi.org/10.1016/j.frl.2022.103175

Zang, S., Zhang, X., Xing, Y., Chen, J., Lin, L., & Hou, Z. (2023). Applications of Social Media and Digital Technologies in COVID-19 Vaccination: Scoping Review. Journal of Medical Internet Research, 25, e40057. https://doi.org/10.2196/40057

Zhu, D. T., Serhan, M., Mithani, S. S., Smith, D., Ang, J., Thomas, M., & Wilson, K. (2023). The barriers, facilitators and association of vaccine certificates on COVID-19 vaccine uptake: a scoping review. Globalization and Health, 19(1), 73. https://doi.org/10.1186/s12992-023-00969-y