Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 18

February 2024

Blockchain Applications in Higher Education Based on the NIST Cybersecurity Framework

Brady Lund Ph.D.
University of North Texas, brady.lund@unt.edu

Recommended Citation

Lund, Brady Ph.D. (2024) "Blockchain Applications in Higher Education Based on the NIST Cybersecurity Framework," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 18.
DOI: https://doi.org/10.62915/2472-2707.1178
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/18

Blockchain Applications in Higher Education Based on the NIST Cybersecurity Framework

Abstract

This paper investigates the integration of blockchain technology into core systems within institutions of higher education, utilizing the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as a guiding framework. It supplies definitions of key terminology including blockchain, consensus mechanisms, decentralized identity, and smart contracts, and examines the application of secure blockchain across various educational functions such as enrollment management, degree auditing, and award processing. Each facet of the NIST Framework is utilized to explore the integration of blockchain technology and address persistent security concerns. The paper contributes to the literature by defining blockchain technology applications and opportunities within the education sector.

Keywords

Blockchain, Higher Education, Cybersecurity, Security Threats, National Institute of Standards and Technology

Blockchain Applications in Higher Education Based on the NIST Cybersecurity Framework

Brady D. Lund
Department of Information Science
University of North Texas
Denton, TX, USA
Brady.Lund@unt.edu
0000-0002-4819-8162

Abstract— **Abstract— This paper investigates the integration of blockchain technology into core systems within institutions of higher education, utilizing the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as a guiding framework. It supplies definitions of key terminology including blockchain, consensus mechanisms, decentralized identity, and smart contracts, and examines the application of secure blockchain across various educational functions such as enrollment management, degree auditing, and award processing. Each facet of the NIST Framework is utilized to explore the integration of blockchain technology and address persistent security concerns. The paper contributes to the literature by defining blockchain technology applications and opportunities within the education sector.**

Keywords—Blockchain, Higher Education, Cybersecurity, Security Threats, National Institute of Standards and Technology

I. Introduction

In the constantly evolving landscape of academia, institutions of higher education (IHEs) face increasing challenges in ensuring the security and integrity of sensitive data that they manage. Blockchain technology has gained prominence in recent years for its potential to revolutionize data management and security and may be one approach to maintaining needed security and integrity. This paper explores the application of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework to harness the full potential of blockchain in higher education settings. By merging the principles of NIST's framework with blockchain technology, institutions can fortify their cybersecurity measures and develop greater organizational well-being. The primary objective of this paper is to describe how the NIST Cybersecurity Framework can be strategically employed to identify security threats within an organization and seamlessly integrate diverse blockchain technologies to help address these threats. This paper will discuss the nature of blockchain, with a particular focus on enhancing the efficiency and security of critical functions such as enrollment management, degree auditing, and award processing. By addressing these unique challenges faced by educational departments, this paper aims to suggest practical measures for bolstering cybersecurity measures in institutions of higher education.

II. Blockchain Applications

Before discussing how blockchain technologies and the NIST Framework can be integrated into higher education systems, it is important to note in general how these technologies are currently applied in the cybersecurity context, including the important concepts that underpin the technology.

A. Key Definitions for Blockchain Technology

Blockchain serves as a decentralized and secure foundation for data storage, authentication, and sharing [1]. Central to its operation are mutual agreements between nodes, a distributed ledger, and cryptographic signatures. The decentralized nature of blockchain ensures that no single entity existing on the blockchain has control over the entire network, enhancing security and resilience against malicious attacks to an extent that was not possible with past technologies and cybersecurity approaches [2].

With blockchain technology, a distributed ledger mechanism is used to create transparency and trust among participants. Each node, or participant in the network, maintains a copy of the ledger, creating a tamper-resistant record of transactions, also known as an immutable audit trail [3]. Blocks of data are chained together, creating the basic elements documented on this ledger. Cryptographic signatures ensure the authenticity of data, providing a robust mechanism for verification and validation. The following paragraphs describe key aspects of blockchain that make it a valuable technology for securing information systems.

A consensus mechanism is the process of reaching consensus on transactions that occur on the blockchain [4]. Traditionally, two methods have been used for consensus in blockchain: proof of work (PoW) and proof of stake (PoS). Proof of work was historically the more common method for blockchain applications such as cryptocurrency. It is the consensus mechanism used by Bitcoin, the most popular cryptocurrency available today. However, a proof of work mechanism has significant downsides, as it involves having participants on the blockchain compete to solve complex mathematical puzzles in order to determine who gets to add the next verified block to the blockchain, which takes considerable

computing power and energy and requires some reward system for those who participate on the blockchain. Conversely, in proof of stake mechanisms, validators are selected based on the amount of collateral they are willing to "stake" towards the transactions. PoS has become the more common consensus mechanism in recent years. However, this method has issues as well, in terms of limited authority of exchanges by a central unit, such as a university itself. In such cases, a proof of authority (PoA) mechanism could be ideal [5]. In this system, consensus is reached based on participants' pre-assigned authority, allowing for a level of control over the system without compromising the privacy and security of all other participants in the system.

Decentralized identity verification is the concept of digital identities being distributed across a network of nodes within a blockchain, rather than being held and managed by a centralized authority, such as an admissions office at a university [6]. Users of the system can determine what aspects of their digital identity to share. Credentials that have been verified on the blockchain can be shared in a tamper-evident manner, which allows for proof of identity to be shared without sharing unnecessary details about the individual. For instance, if a proof of social security number was needed in order to enroll at a university, a credential could be added to the blockchain that will trigger a smart contract allowing the student to continue the admissions process, without making the actual social security number available to any system in the university that could become compromised. Alternatively, if proof of identity was needed to be shared among two human users, then the exchange of cryptographic keys can occur between these users, in the same way that cryptocurrencies are exchanged on a blockchain [7]. This mitigates the likelihood that the system can be hacked and this personal information revealed.

Smart Contracts are rule-based criteria that allow for terms of an agreement to be enforced automatically without needing external verification from a third party [8]. For instance, if a university has criteria that warrants automatic acceptance into a particular program, such as a 3.5 GPA, then a smart contract could verify this GPA and process acceptance without the need for verification from an admissions coordinator. This automation of processes also limits the potential for interference from external parties, such as hacking into an admissions system to grant admission to someone who does not meet the acceptance criteria. Today, smart contracts can be built onto a blockchain to ensure heightened security [9].

Permissioned access in the context of blockchain is a system where not all individuals have equal access to the blockchain and its data [10]. Within an institution of higher education, students, staff, and faculty may have access to a blockchain containing various records, but general members of the public should not have equal access. New members would be authorized beforehand, perhaps by completing an admissions interest form for students or accepting a job offer in the case of staff and faculty. Access control mechanisms will regulate who can participate in what processes on the blockchain [11]. Access policies can control who can access certain resources based on their assigned roles, attributes, time, or other factors.

B. Some Issues and Limitations wth Blockchain Technology

One of the most significant issues with blockchain technology, as currently constructed, is the amount of energy required to facilitate such a system. Depending on the type of consensus mechanism used (proof of work, in particular, exhausts tremendous energy), the cost of energy is prohibitive. This also makes scalability an issue. As the number of transactions on the blockchain increases, the network's performance is likely to decline and require greater energy to sustain.

Additionally, while blockchain enhances security, it is not a perfect system. Proof of work systems are particularly vulnerable due to issues where a very powerful miner could theoretically gain outsized control of the whole system, which is why a proof of authority mechanism is encouraged for higher education applications [12]. Regular surveillance and maintenance of the blockchain is also necessary to ensure that the network is not compromised in some unforeseen way.

III. National Institute of Standards and Technology

To provide structure to learning about the why and how of blockchain for cybersecurity and how these technologies are effectively managed, it is valuable to refer to relevant policy frameworks. The most important of these frameworks in the United States is the cybersecurity framework published in 2014 by the National Institute of Standards and Technology (NIST). The section that follows provides background on the NIST and its role in these cybersecurity discussions.

The NIST is a federal agency in the United States that operates as part of the U.S. Department of Commerce. Its objective is to promote innovation and industrial competitiveness in the United States by advancing the measurement of science, scientific standards, and technological innovation. To this end, it has published many frameworks to guide our understanding of science and technology practices, including its 2014 cybersecurity framework.

A. 2014 NIST Cybersecurity Framework

The NIST Cybersecurity Framework was created in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which was issues under the Obama Presidential Administration in 2013. This framework provides guidelines, standards, and best practices to guide organizations in managing cybersecurity risks and implementing new cybersecurity technologies. The NIST "Framework for Improving Critical Infrastructure Cybersecurity" was originally published in 2014 and was updated in 2018. The framework consists of four core elements:

- Functions are the basic cybersecurity activities that help manage organizational risk. These functions include the

identification of risk, the protection of the organization against risk, the detection of threats, the response to threats, and the recovery from threats.
- Categories are the subdivisions of functions that align with specific needs and activities within an organization, such as the management of particular assets.
- Subcategories are the further divisions of a category into specific outcomes of activities, such as the investigation of notifications of detection systems related to those particular assets.
- Informative References are the specific references to standards and guidelines that direct actions within the subcategories.

An example of this framework in practice is the following:

- Function: Identification of Risk
- Category: Asset Management
- Subcategory: Student Information System
    - Activity: Regularly update and maintain inventory of student records to limit the potential for security breaches.
- Informative Reference: ISO/IEC 27001:2013 v- Information Security Management System (ISMS) standard.

In this example, we have noted that we have a student information system, which is a key asset within our university. We want to ensure that this system is resilient to cyberthreats by regularly updating the data and infrastructure and have identified a reference that can guide our analysis of the system. The different types of functions will be explored in greater detail in the following sections.

The NIST framework also specifies tiers related to the level of rigor applied in addressing a particular cybersecurity risk and response [13]. Four tiers are specified. The first of these tiers is "partial," in which risks are managed informally, with limited organizational awareness of the risk. The second tier is "risk informed," where management and cybersecurity professionals are made formally aware of a risk but may not have an officially established policy or approach to address this risk. The third tier is "repeatable," where a formal (static), organization-wide policy is implemented. Tier four is "adaptive," where policy and standard practices not only formally exist but also evolve dynamically as a result of prior experiences and new information or indicators. The above example of the student information system may fall into tier three, as it appears to follow a formal policy, but may not reach the level of awareness reserved for tier four.

B. 2018 NISTIR 8202

In 2018, "NISTIR 8202: Blockchain Technology Overview" was published. This document presents an introduction to blockchain technology, including in relation to their usage in cybersecurity. Blockchain is valuable for cybersecurity due to its tamper resistant design, where a transaction, once it has been integrated into the blockchain, cannot be altered. The existence of a transaction log, which allows an analyst to audit any incidences, and distributed ownership, where no one authority has full ownership over the blockchain itself, further enhance its usage as a security tool, as noted by the authors. It is important to note that this document stops short of offering any policy. Instead, it references the NIST Cybersecurity Framework, stating that "its standards are broad enough to cover blockchain technology and to help institutions develop policies and processes that identify and control risks affecting blockchain technology" [14].

IV. Integration of NIST Standards into Higher Education Blockchain System

This section explores three vital systems within higher education that have elevated risks of attacks due to their sensitive nature: admissions and enrollment processing, where admissions numbers and enrollment in courses are capped to ensure manageable program and class sizes, and spots in certain programs and classes can be highly valued; degree auditing and grade entry, where faculty enter grades for students and the ability to change these grades without being detected would be valued; and award processing, where determinations of whether a student has fulfilled all the requirements to receive their degree are critical. This section will discuss how the NIST framework, combined with blockchain technology, can be used to ensure that these systems remain secure and tamper resistant. With all these systems integrated on a single blockchain, it could make for a seamless process for the student from admission to degree completion.

A. Cybersecurity Risks for Admissions and Enrollment Processing, Grade Entry, and Award Processing

The first function within the NIST Cybersecurity Framework centers on risk identification, a critical task given the multitude of risks inherent in the three target systems. Asset management is the primary sphere of activity within each of these systems. The overarching objective of institutions of higher education is to guide students from admission to degree completion, necessitating the effective management of assets—in this context, the students and their continuing enrollment [15]. This management is crucial to mitigate the risk of loss or corruption of vital data, encompassing enrollment information, grades, and progress toward degrees.

Within this landscape, adversaries may direct their focus towards admissions and enrollment processes, enticed by the prospect of securing limited program spots. By manipulating such data, these adversaries can circumvent legitimate competition, skew class sizes, and tarnish the institution's credibility. More significantly, breaches in these systems expose sensitive student information, including addresses and social security numbers, creating avenues for identity theft and financial harm [16].

Academic records represent another vulnerable facet. Unauthorized alterations to grades can distort student progress and assessments, compromising the fairness of academic

evaluations and disadvantaging deserving students. Hackers can exploit system vulnerabilities, utilizing stolen grades and records akin to stolen diplomas, thereby casting doubt on the institution's academic integrity and potentially hindering students' future prospects.

The award processing stage, the culmination of years of dedicated effort, is not immune to cyber threats. Errors or manipulations during this phase could result in the issuance of undeserved degrees, eroding the institution's reputation and diminishing the hard-earned achievements of all graduates. Conversely, system malfunctions or cyberattacks may lead to delays or even denials of degrees for qualified students, introducing unnecessary stress and hardship at a critical juncture. As such, safeguarding these stages is paramount to upholding the institution's integrity, protecting sensitive data, and ensuring a fair and secure academic environment [17].

B. Blockchain Solutions for Addressing Risks

Utilizing blockchain technology would enable potential students to create a digital student identity within a blockchain-based system and be able to enroll, receive grades, and receive their degree without the university having direct ownership of all student data and requiring human representatives to verify credentials. This would dramatically reduce the number of vulnerabilities within organizational systems. A proof of authority consensus mechanism would ensure that the university maintains appropriate control of resources, while ensuring security for users. Permissioned access further ensures that only authorized users – potential, current, and former students, as well as staff and faculty – have access to the system and can access any of the information stored on the blockchain, which will prevent unauthorized access and threats of cyberattack. Cryptographic keys, which users can store on their private devices, would govern access, allowing for decentralized identity management.

Smart contracts can validate academic credentials based upon predefined criteria, directly triggering steps within a workflow. For instance, when a transcript is requested from another institution, a request could be sent to that institution, which could provide information that is automatically validated via the smart contract to ensure minimum qualifications are met, without needing human access to a report. With no need for manual verification, the whole admissions process becomes more efficient and precise, reducing bias in evaluation of applications and potential hacking of the system. This technology can be translated to grade entry, where the students academic transcript for the university is held on a blockchain and new “transactions,” or grades for courses, are added to this record, which can only be accessed by authorized users with appropriate keys. Smart contracts can also be used to determine whether degree requirements have been met and to award the degree, without the need for manual verification. This would allow for some reallocation of organizational resources to more human-centric needs and roles.

A key benefit of this system is the immutable audit trail created through the use of blockchain. Every action that occurs on the blockchain, from the submission of an application, to acceptance of an application, to an entry of a grade, to awarding of degree, will be timestamped and etched into the digital ledger for auditing. Administrators can see exactly when transactions occur, what kind of transaction, and the public id of who was involved, but not specific details that could compromise privacy of those individuals and transactions. A blockchain system enables the delicate balance between transparency and security.

An additional benefit of using this system is the capacity to utilize non-fungible tokens (NFTs) to validate the authenticity of intellectual property, awards, and certifications. Content in class papers and scholarly contributions added to an institutional repository could be validated for originality by creating an NFT for each item [18]. Similarly, awards presented by the university, and even academic degrees, could be maintained using this technology. Forgeries and plagiarism would be significantly reduced.

C. Identifying Threats to the System

Blockchain technology offers a considerable step forward in securing organizational data and streamlining organizational processes. The proof of authority consensus mechanism overcomes a few classic issues with blockchain, such as the extent to which one bad actor could compromise the system. However, this technology is not without vulnerabilities. As indicated in the NIST Cybersecurity Framework, it is critical to anticipate and quickly identify threats to the system in order to build resilience and trust in the system among its participants. Prevention of threats is important, as the process of recovery after an attack, as discussed in the following section, is often costly.

Smart contracts, while an ideal solution to validating credentials and transactions, are not free from all possible attacks. If the underlying code in the smart contracts were to be compromised, the criteria for the smart contracts could be altered and unauthorized to sensitive information stored in the blockchain could be exploited [19]. While the fact that the smart contracts are built onto the blockchain will help to combat some of the potential exploits of the code, it is not perfect. As such, continual review of the blockchain and smart contract code, penetration testing to determine the likelihood and extent of threats emerging, and communication about issues as they emerge.

Decentralized identity on the blockchain can be susceptible to an internal threat from another user like a fellow student. Users could try to cloak or forge their credentials in order to gain the trust of others. In order to combat this potential attach, strong countermeasures are needed, like non-interactive zero-knowledge proofs. Zero-knowledge proofs allows users to provide evidence of knowledge or access to certain information on the blockchain without exposing that information to the other user. In the context of cryptocurrency, these types of

proofs allow users to verify that a certain amount of currency is held by a user attempting to make a transaction, without disclosing the specific amount or type of cryptocurrency that is held. The same principle could extend to university systems, where a student, for instance, may need to prove that they are enrolled in the university in order to receive counseling or library services, without wanting to provide personal information directly to these entities.

Additionally, anomaly detection algorithms can be used to monitor the blockchain and identify unexpected behavior by certain users (high level of transactions, unexpected transactions) and mark it as potential fraud for further investigation. If we expect a certain user on the blockchain to only participate in certain transactions with a certain frequency and they are suddenly participating in different transactions at a much higher rate, then it may suggest questionable behavior – perhaps the user has found a way to access information they should not. The user's compromised credentials should be revoked, though this should be done carefully as it will result in additional work for the user to reestablish those credentials.

External threats to the system also exist. Social engineering and phishing persist. As secure as the underlying technology may be, the system is only as resilient as its least-secure user. If a user reveals their private key, used to access and perform transactions on the blockchain, or other personal data, then this can be used by another user to pose as them. As such, it is critical to maintain effective cyber security training for all system users. Additionally, resiliency must be built to prevent the impact of system outages, which could disrupt or corrupt transactions on the blockchain. If some nodes go offline, then those that remain online gain more power, which could increase susceptibility to attack. Monitoring performance of the system at all times, and especially in these unexpected circumstances, is vital.

D. Response and Recovery from Threats

Response and recovery from threats is costly in terms of time, energy, and money [20]. For this reason, it is important to always be comprehensive to avoid the recurrence of an issue. Fortunately, there are established processes to follow in identifying the cause of issues and preventing them from emerging again. These processes should be built into the planning when implementing the NIST Cybersecurity Framework.

If a smart contract has been exploited, the first step must be to isolate any affected contracts. This may include temporarily pausing all actions involving the contract and its workflows. For instance, if the smart contract was used to verify state of residency for in-state tuition rates, then this validation may need to be temporarily paused while a patch is developed. It is critical to ensure that all smart contracts and functions tied to the issue are addressed, or new vulnerabilities will be opened. During the pause, analysts should identify the vulnerability that enabled the smart contract to be manipulated. A patch should then be applied that eliminates this vulnerability and the patch should be tested in a controlled environment to ensure the solution eliminates the issue. Once the patch has been sufficiently proven, then it may be redeployed.

One of the more damaging attacks would be a system outage or consensus mechanism issue [21]. In these cases, serious loss of data is possible. Plans to recover data must be a priority, as are plans to communicate issues with affected individuals and entities. In the case of consensus mechanism-based attack, a patch needs to be made to the mechanism – generally, the proof of authority design should prevent this type of attack, but it could still fall victim to hacking of those nodes that have authority. In these cases, it will also be important to hard fork the blockchain to sever ties with the compromised network, which would be a drastic move that could disrupt major functions of the system. Again, communication will be critical in these situations.

In the case of a breach of the system due to social engineering and phishing attacks, an audit of the issues that enabled the breach should be taken [22]. Resulting from this audit should be a set of measures to improve security awareness training for system users. Frequently refreshers and testing of users cybersecurity resilience through fabricated phishing messages should occur, as should be the case with any information system. Users are the most critical resources for preventing attacks on the system.

V. Conclusion

Institutions of higher education must face the imperative of safeguarding their sensitive data or risk compromising their obligations to students and employees. Traditional cybersecurity measures can offer protections against many cyber threats that exist today, but blockchain technology offers a dramatic shift in the capacity to prevent attacks from compromising a system. The NIST Cybersecurity Framework provides a structure through which IHEs can comprehend threats to cybersecurity, understand how blockchain technology can be integrated to support existing system roles, and monitor and ensure security into the future. By harnessing the power of smart contracts, decentralized identity verification, and permissioned access, IHEs can revolutionize the admissions, grading, and degree awarding process to mitigate human interference and build resilience against cyberthreats. Success in these endeavors to promote cybersecurity will rely on effective communication and stakeholder buy-in.

REFERENCES

[1] A. A. Monrat, O. Schelén, 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

[2] M. Di Pierro, "What is the blockchain?," Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017. https://doi.org/10.1109/MCSE.2017.3421554

[3] D. Saxena and J. K. Verma, "Blockchain for public health: Technology, applications, and a case study," in Computational Intelligence and Its Applications in Healthcare, Academic Press, 2020, pp. 53-61.

[4] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," IEEE Access, vol. 9, pp. 43620-43652, 2021. https://doi.org/10.1109/ACCESS.2021.3065880

[5] M. A. Manolache, S. Manolache, and N. Tapus, "Decision making using the blockchain proof of authority consensus," Procedia Computer Science, vol. 199, pp. 580-588, 2022. https://doi.org/10.1016/j.procs.2022.01.071

[6] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," Blockchain: Research and Applications, vol. 2, no. 2, article 100014, 2021. https://doi.org/10.1016/j.bcra.2021.100014

[7] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, et al., "Decentralized identity: Where did it come from and where is it going?," IEEE Communications Standards Magazine, vol. 3, no. 4, pp. 10-13, 2019. https://doi.org/10.1109/MCOMSTD.2019.9031542

[8] M. Kolvart, M. Poola, and A. Rull, "Smart contracts," in The Future of Law and Technologies, Springer, 2016, pp. 133-147. https://doi.org/10.1007/978-3-319-26896-5_7

[9] Z. Zheng, S. Xie, H. N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems, vol. 105, pp. 475-491, 2020. https://doi.org/10.1016/j.future.2019.12.019

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), Aug. 2016, pp. 25-30. https://doi.org/10.1109/OBD.2016.11

[11] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Jan. 2018, pp. 1575-1578. https://doi.org/10.1109/EIConRus.2018.8317400

[12] I. Lin and T. Liao, "A survey of blockchain security issues and challenges," International Journal of Network Security, vol. 19, no. 5, pp. 653-659, 2017. https://doi.org/10.6633/IJNS.201709.19(5).01

[13] M. Scofield, "Benefiting from the NIST cybersecurity framework," Information Management, vol. 50, no. 2, pp. 25-28, 2016.

[14] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, 2018, pp. 37.

[15] M. Rymarzak and D. Trojanowski, "Asset management determinants of Polish universities," Journal of Corporate Real Estate, vol. 17, no. 3, pp. 178-197, 2015. https://doi.org/10.1108/JCRE-02-2015-0006

[16] L. Seda, "Identity theft and university students: do they know, do they care?," Journal of Financial Crime, vol. 21, no. 4, pp. 461-483, 2014. https://doi.org/10.1108/JFC-05-2013-0032

[17] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Future Internet, vol. 13, no. 2, article 39, 2021. https://doi.org/10.3390/fi13020039

[18] H. R. Saeidnia and B. D. Lund, "Non-fungible tokens (NFT): a safe and effective way to prevent plagiarism in scientific publishing," Library Hi Tech News, vol. 40, no. 2, pp. 18-19, 2023. https://doi.org/10.1108/LHTN-12-2022-0134

[19] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," IEEE Access, vol. 8, pp. 24416-24427, 2020. https://doi.org/10.1109/ACCESS.2020.2970495

[20] J. Chapman, A. Chinnaswamy, and A. Garcia-Perez, "The severity of cyber attacks on education and research institutions: a function of their security posture," in Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security, Jan. 2018, pp. 111-119.

[21] K. C. Moke, T. J. Low, and D. Khan, "IoT blockchain data veracity with data loss tolerance," Applied Sciences, vol. 11, no. 21, p. 9978, 2021. https://doi.org/10.3390/app11219978

[22] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4, article 89, 2019. https://doi.org/10.3390/fi11040089