Integrating Blockchain dApp Development in Cybersecurity Education via Real-World Applications

Javonte L. Carter
Florida A&M University
Tallahassee, FL, USA
javonte1.carter@famu.edu

Inioluwa Kola-Adelakin
Florida A&M University
Tallahassee, FL, USA
inioluwa1.kolaadelak@famu.edu

Jerry Miller
Florida A&M University
Tallahassee, FL, USA
Jerry.Miller@famu.edu

Hongmei Chi
Florida A&M University
Tallahassee, FL, USA
hongmei.chi@famu.edu

ABSTRACT

This paper presents a structured pedagogical framework for integrating blockchain decentralized application (dApp) development into cybersecurity education through experiential, project-based learning. The framework is implemented via a series of laboratory modules that immerse students in authentic, project-based activities grounded in real-world use cases, including blockchain-based diploma and transcript verification, cryptocurrency (Bitcoin) forensic analysis, and secure supply chain management. Through these activities, students gain practical exposure to distributed systems, smart contracts, and security mechanisms within blockchain environments. Preliminary classroom outcomes demonstrate increased student interesting in learning dApp development, enhanced conceptual understanding of blockchain and cybersecurity principles, and improved preparedness for industry and research-oriented roles. Overall, the proposed framework aims to (1) strengthen students' skills and awareness of blockchain source code vulnerabilities, along with associated detection and mitigation techniques; (2) systematically integrate blockchain vulnerability concepts into information technology and cybersecurity curricula; and (3) prepare future IT professionals with a solid understanding of blockchain attack surfaces and defensive strategies in real-world contexts.

CCS CONCEPTS

• **Security and privacy → Cryptography**; **Blockchain Forensic**; • **Computer science education**; • **Vulnerability Management**;

KEYWORDS

Digital Credentials, Cryptocurrency Forensics, and Supply Chain Applications, dApp.

ADMI 2026, March 26–29, 2026, 0rangeburg, SC, USA

ACM ISBN 979-8-4007-1277-7/2026/04…$15.00
https://doi.org/10.1145/3696673.3723086

ACM Reference Format:
Javonte L. Carter, Inioluwa Kola-Adelakin, Jerry Miller, and Hongmei Chi. 2026. Integrating Blockchain dApp Development in Cybersecurity Education via Real-World Applications. In *2026 ACM Conference (ADMI 2026), March 26–29, 2026, 0rangeburg, SC, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3696673.3723086

1 INTRODUCTION

As the role of blockchain technologies gradually increases in our lives, source code security becomes a significant issue to protect against malicious attempts. Therefore, there must be no errors made by the software architecture engineers to create secure and reliable blockchain-based software. Training our future blockchain developers in writing secure dApps is critical in applying blockchain technology in real-world applications [11]. However, there are significant needs in the education and training of a blockchain-ready developer workforce [1, 10].

In recent years, Blockchain in the form of dApps have seen widespread adoption. From cryptocurrency to supply chain management, these techniques have offered a means for automation and process optimization. With the advent of ML, the adoption of blockchain-based security research has increased as well, as have practical applications, including intrusion detection and malware analysis. The synergy between blockchain technology and Cybersecurity promises exciting possibilities. Unfortunately, advancements in Blockchain and Cybersecurity have not produced concurrent consumer education. For example, consumers often do not fully appreciate the security implications of choosing proper passwords or how machines can learn from data to detect cyberattacks. In academia, the terrain for providing blockchain-centered education on Cybersecurity is in its infancy, with many institutions offering limited or very technical cybersecurity and Blockchain technology learning opportunities. Acknowledging the benefits Blockchain provides, there is a strong need to merge these concepts into computing education at all levels [12, 13].

Creating a cybersecurity-ready workforce that can defend evolving, 21st century cyber threats is necessary. However, there are significant needs in the education and training of a blockchain-ready workforce. One major impediment to blockchain education is content delivery style. Security classes consist of highly Blockchain technical lectures, dense handouts, and complex content that does

not fully engage students, in some way we ignore the venerability of blockchain codes. Innovative techniques are needed that incorporate cybersecurity content in accessible and creative ways. Hands-on labs with Blockchain vulnerability detection are rarely shown in cybersecurity education. Hands-on labs have been shown to improve learning comprehension via learning by doing. In this paper, we designed a set of hands-on labs to help blockchain developers and cybersecurity workforce to be aware of Blockchain vulnerability[15].

This paper highlights the gaps in the nation's cybersecurity education-related blockchain technology and training landscape and provides a successful framework that holds promise as a model for addressing the skills gap in blockchain vulnerability detection. Targeting key concepts is ideal for reinforcing the current blockchain tech curriculum, improving students' blockchain developer programming skills, and equipping students with analysis tools to form a secure blockchain programming habit [17, 21]. There is high demand in demonstrating the gaps between curriculum and industry addressed in this paper.

The rest of this paper is organized as follows. Section II presents a literature review on cybersecurity workforce statistics, talents that have been reported to be missing in new graduates, needs and tactics used to fill the gap between education and the industry's market, and academic efforts to raise awareness on source code vulnerabilities. Section III covers a detailed description of the techniques used in designing these hands-on labs and a general overview of this framework. Details on the concepts covered and tools used for each hands-on lab category are provided in Section IV. Students' Feedback, Statistics on survey responses are provided in section V. Finally. Section VI provides the conclusion and future works.

2 RELATED WORK

In this section, we first describe previous studies on blockchain vulnerability detection. Then, we review the prior work on blockchain-centered education on Cybersecurity and dApp Development.

2.1 Blockchain Vulnerability Detection

Blockchain with smart contract has been increasingly used in finance, management, medical treatment, Internet of things, supply chain and other fields, and smart contract is believed to be the next generation of automation in inter-party agreements in the blockchain-based systems [25]. Many methods have proposed for smart contract detection. Parizi et al. [20] carried out a far-reaching experimental assessment of current static smart contracts security testing tools, for the most widely used Blockchain, the Ethereum and its domain-specific programming language, Solidity, to provide the first body of knowledge for creating more secure blockchain-based software. Ressi et al.[23] proposed a degree-free graph convolutional neural network (DR-GCN) and a novel temporal message propagation network (TMP) to learn from the normalized graphs for smart contract vulnerability detection. Specifically, they constructed a contract graph to represent both syntactic and semantic structures of a smart contract function, and they designed an elimination phase to normalize the graph in order to highlight the major nodes. Liu et al. [16] systematically analyzed four four perspectives on how smart contracts empower Industry 4.0 and explored the potential transition from digital industry to trusted industry through case studies. Vidal et al. [28] proposed Dynamit, a monitoring framework to detect reentrancy vulnerabilities in Ethereum smart contracts. Dynamit extracts features from transaction data and uses a machine learning model to classify transactions as benign or harmful. Dynamit can find the contracts that are vulnerable to reentrancy attacks, and it also can get an execution trace that reproduces the attack. Li et al. [15] studied the vulnerability detection of Golang chaincodes. First, they summarized 17 kinds of Golang chaincode vulnerabilities by investigating existing research. Second, they proposed a chaincode vulnerability detection framework by combining the dynamic symbolic execution and the static abstract syntax tree analysis technology. They also implement a supporting-tool that can detect the above 15 types of vulnerabilities.

2.2 Cybersecurity Education

The shortage of skilled professionals in Cybersecurity is one of the strongest in computer science [27]. The 2025 (ISC)2 Cybersecurity Workforce Report revealed a current gap of 3.1 million jobs in Cybersecurity[2]. Moreover, the qualifications of the existing workforce are largely believed to be insufficient jobs. The recent State of Cybersecurity Report of the Information Systems Audit and Control Association (ISACA) indicated that over 60 percentage of cybersecurity teams in the U.S. are understaffed and 50% of cybersecurity job applicants are not well qualified[9]. The source code vulnerabilities threaten the security of software systems, which has attracted more attention in both academia and industry[8, 19]. To enhance cybersecurity education, several studies leverage blockchain technology for cybersecurity education enhancement. Mittal et al. [23]. proposed a pedagogical tool for training in Blockchain using an adversarial sandbox adaptive serious game approach for students and technology professionals. They further proposed use of A.I. to enhance Non-Playable Character (NPC) interactivity based on player's responses. They planned to evaluate this serious game on a subjective metrics that is based on a game experience questionnaire. Tu [26] expounded a blockchain-based architecture for transform centralised model of awarding and validation in to decentralized ledger of secured database. The database is shared, replicated, and synchronized for validation among the universities, partner institutions, professionals, statutory or regulatory bodies and industry bodies across the internet. The architecture offers secured collaborative validating system by qualification exchange with Blockchain using trust methods within the decentralized topology. Maulani et al.[18] described the security of blockchain technology in digital certificates, and it aims to investigate the viability, efficacy and challenges of blockchain technology in qualification validation, with an emphasis on implementing Blockchain for academic and non-academic authorizations. The work in [18] is an exploratory research devoted to architecture to transform the awarding of centralized degree apprenticeship certification and validation to a decentralized ledger from a convenient database.

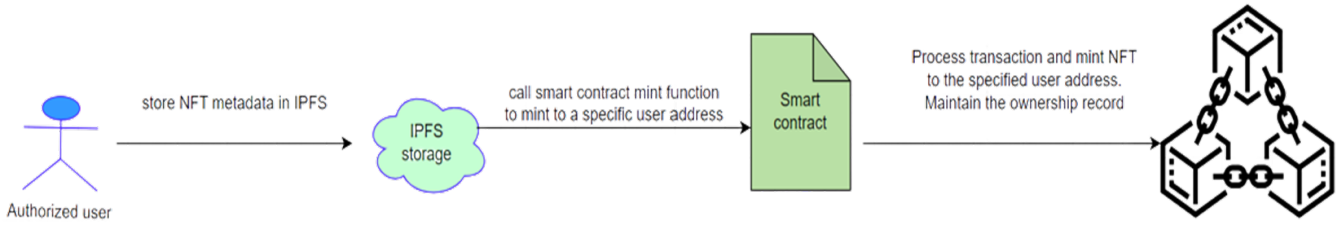

Figure 1: NFT mint process without off-chain implementation

2.3 dApp Development

There is a critical need for research focused on designing and evaluating hands-on lab modules that integrate blockchain dApp development into cybersecurity curricula through real-world applications in higher education [14]. Such labs can enable students to move beyond conceptual understanding by engaging in experiential learning that combines secure smart contract design, threat modeling, and deployment on blockchain platforms. By situating learning within the context of enhancing transparency and trust in higher education institutions, this research can contribute to more effective pedagogical approaches that prepare students to build, assess, and secure blockchain systems in practice, ultimately strengthening both cybersecurity education and institutional trust infrastructures [11]. Blockchain technology, combined with Self-Sovereign Identity (SSI), offers a promising foundation for addressing these challenges by enabling decentralized, tamper-resistant, and verifiable academic credentials [22]. SSI empowers learners with ownership and control over their identities and credentials, while blockchain ensures immutability, transparency, and verifiability without reliance on centralized authorities [5].

3 HANDS-ON LAB DESIGN

In this study, we administered a Pre- and Post-survey to assess students' knowledge and comprehension of the topic prior to and following lab completion. Students were required to complete a pre-survey questionnaire designed to assess their level of knowledge and experience with the topic. While working in the lab, students were provided with supplementary learning materials to aid in their comprehension of the concepts being discussed. In addition, students have constant access to instructors and graduate assistants for questioning. After completing the hands-on lab, students are given a post-survey to assess their understanding of the concepts covered in the lab. On the basis of the results of the post-survey, they are provided with additional complementary learning materials, and the subsequent lab is designed to complement and enhance their comprehension of the previous lab [24].

Blockchain has become necessary for many different societal industries and ordinary lives, including cryptocurrency technology, supply chain, health care, public safety, education, etc. Therefore, training our future blockchain developers to know blockchain programming vulnerability and IT students' cybersecurity is in high demand [7]. In this work, we propose a framework including learning modules and hands-on labs to guide future I.T. professionals towards developing secure blockchain programming habits and mitigating source code vulnerabilities at the early stages of the software development lifecycle following the concept of Secure Software Development Life Cycle (SSDLC)

3.1 How to Create Non-Fungible Tokens (NFT)

In the first category of the lab, students are introduced to general knowledge of blockchain technology, how to program using the Ethereum Solidity programming language, and the IPFS technology. In the first part of the lab, we introduce students to how smart contracts work and the layout structure of the popular Ethereum programming language. We further introduced them to the Openzeppelin smart contract library and how to implement them in smart contract design. In this lab, we introduce the students to different ERC (Ethereum Request for Comments) tokens based on fungibility design and their respective applicable use cases. We expanded on the ERC1155 and ERC721 token standards and structured the lab to give the students hands-on experience developing their own NFTs (Non-Fungible Tokens). At the end of the lab, the students had created an ERC721 NFT standard and ERC1155 standard and understood the differences between the two NFT standards and the effective use case for each. To expand the knowledge of students on smart contract security, we show them the importance of protective modifiers and how to use them, and the implications if not used where it is needed.

3.2 Off-Chain Transaction and NFT Royalty

In this lab, we further educate the students about blockchain technology, how to create off-chain transactions, and the security vulnerabilities associated with the design of the off-chain transaction. We also exposed them to the different EIP (Ethereum Improvement Proposals) designs for off-chain signature design and how to verify the signature on-chain in the smart contract. To expand the knowledge of off-chain signature design and on-chain verification, we developed a smart contract that is compatible with both EIP 191, EIP712, and EIP 1271 (the signature standard for smart contract wallets). In addition to general knowledge of blockchain technology, we introduced the students to how to write functionality test using JavaScript test library, Chai and exposed them to hardhat frameworks and its libraries. We test the smart contract for the different signature support we designed in the smart contract. Additionally, we educate them about NFT royalty, the benefits of royalty, how to implement royalty standards in NFT smart contracts, and the application of NFT royalty in everyday business activities. And

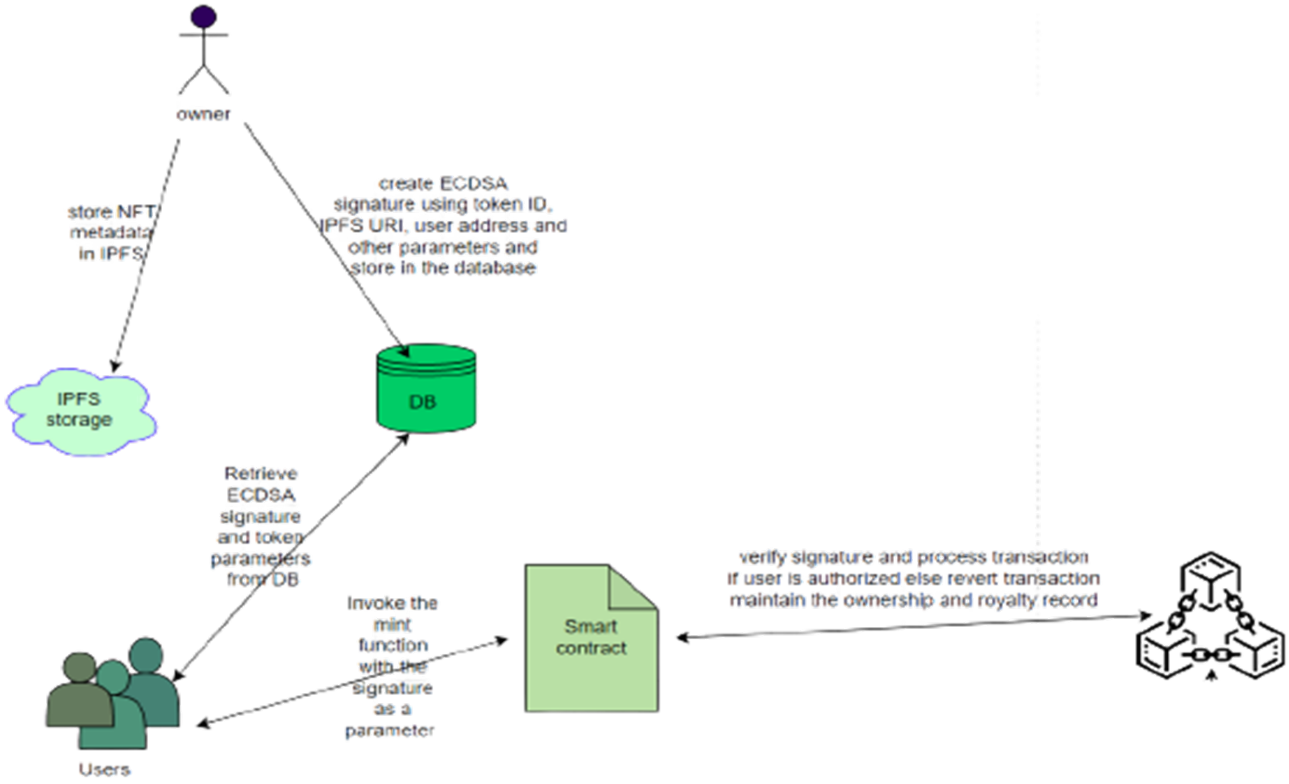

Figure 2: EIP 712 ECDSA off-chain signature implementation

finally, to further expand the knowledge of students, we introduce the students to the Ethereum ECDSA (Elliptic Curve Digital Signature Algorithms) signature design for off-chain transactions. The students were introduced to different EIP (Ethereum Improvement Proposal) standards, and the security vulnerabilities associated with the EIP 191 and iterated on the advantages of EIP712 over the EIP 191 standard. Figure 1 and Figure 2 show an overview of NFT minting process without off-chain implementation and off-chain implementation using EIP 712 ECDSA, respectively.

3.3 dApp for Students' Credentials

To bridge the gap between theoretical instruction and practical implementation of blockchain-based credentialing systems, this hands-on designs a hands-on laboratory module centered on issuing academic diplomas and transcripts as blockchain transactions. As shown in Fig. 3, the lab is structured to guide students through the complete lifecycle of digital credential management, from secure issuance to decentralized verification, using blockchain as the underlying trust infrastructure. Students generate cryptographic hashes of diploma or transcript documents, which are then anchored to the blockchain through smart contract transactions. This approach allows any verifier to confirm the authenticity and integrity of a credential by recomputing and comparing hashes,

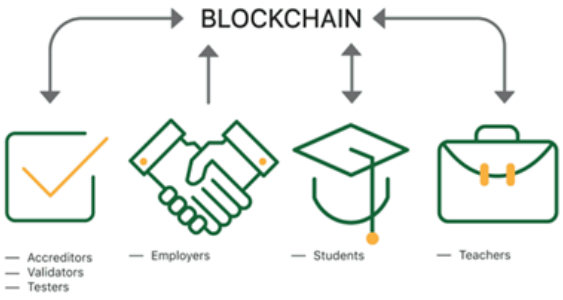

Fig. 3: Integrating blockchain into higher Education Credential verification system

thereby ensuring immutability while maintaining off-chain data confidentiality.

Verification workflows are also implemented as part of the lab, enabling students to design decentralized applications (dApps) that allow employers or academic institutions to validate credentials without intermediary involvement. In Table 1, the possible attacks and mitigation are listed and students are given chance to implement and mitigate the risk in their hands-on lab.

Table 1: Attacks & Mitigation

Attack	Description	Impact	Mitigation
Data Manipulation Attack	Insider or hacker modifies stored data before hashing	Fake grades or altered diplomas	Store hashes on blockchain
Smart Contract Bugs	Logic flaws allow unauthorized minting	Fraudulent diplomas	Smart contract audits, testnets
Privacy Leakage	Personal data on public chain	Legal & ethical risks	Encrypt or hash before storing

3.4 Common Smart Contract Vulnerabilities and Exposures

The third category of this hands-on lab is divided into two. The first part includes secure coding practices and how to manually investigate smart contracts for potential vulnerabilities. The second part educates the students on how to use smart contract security tools to investigate vulnerabilities. In the first part, we provided the students with smart contracts with eight different vulnerabilities. Having provided the students with basic knowledge of how to write a secure smart contract and educative materials to learn about smart contracts vulnerabilities, the students are required to identify the vulnerabilities in these smart contracts, explain the implications of the vulnerability, and fix them manually. This task was designed to expand the students' knowledge, help them gain hands-on experience, and teach them how to write a secure smart contract. We expose the students to smart contract security tools in the second half. Although there are many automated smart contract security tools, we use Slither because it is free, beginner friendly, explains the vulnerability in detail and example code, and suggests how the vulnerability can be fixed. Slither is a static analysis framework for smart contracts; it helps to identify vulnerabilities in solidity smart contracts code in a few seconds. It can also be used for code optimization and smart contract code review. We set up Slither in the Ubuntu environment to analyze smart contracts with different vulnerabilities. We also provide the unit test file for the smart contract to ensure that the smart contract complies with the design specifications after the vulnerabilities are fixed. Using this tool to be mindful of the vulnerabilities and audit their smart contract's possible vulnerabilities even in the development phase.

4 STUDENT'S FEEDBACK

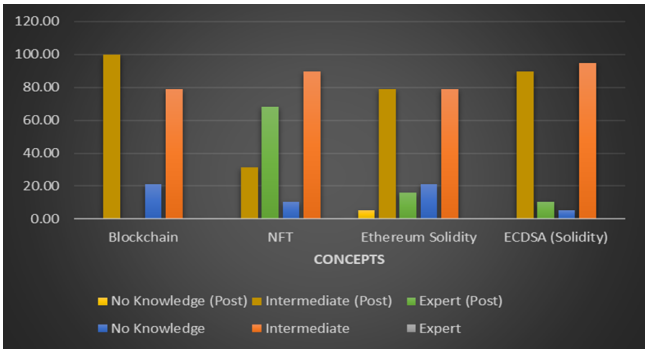

Fig. 4: Summary of Students' Feedback from Hands-on labs

Table 2: Students' level of familiarity with concepts after taking hands-on labs

Concept Names	No knowledge	Intermediate
Blockchain	21%	79%
NFT	11%	89%
Ethereum Solidity	21%	79%
ECDSA	5%	95%
dApp	20%	80%

This research was carried out at Florida Agricultural and Mechanical University during the summer and fall semesters of 2024 and 2025. Students in the following classes were given blockchain hands-on labs: Introduction to Computer Security, Network Security and Cryptography, and Cyber-security. During the presurvey, students were asked about their level of familiarity with the concepts we were going to present, and after the hands-on lab, they were given a few quiz questions to test their knowledge and understanding. Preliminary results are shown in Figure 4. The test subjects included 38 undergraduate computer science majors and 7 graduate computer science students. The results of the questionnaire are presented below.

4.1 Blockchain applications

Survey results show that many (78.9%) students had beginner knowledge of blockchain technology, and only 21.1% of them had no familiarity with the concept. Similarly, 89.5% of the students have general knowledge of NFTs, and 10.5% of the students had no familiarity with the concept of NFTs. Also, most students are unfamiliar with the smart contract programming language Solidity and have never developed any blockchain applications before this hands-on lab.Table 1 shows the students familiarity with the concepts discussed after taking the labs.

The result of the survey shows there is an opportunity to increase awareness of blockchain technology and its application among computer science students. And to further expand their knowledge on how to design scalable blockchain applications and write a secure smart contract. At the end of the introductory hands-on labs, we conducted another survey to measure the improvement in the students' understanding and knowledge of the concepts discussed in the lab. The Figure 3 shows how the students' knowledge has improved after completing the introductory hands-on labs.

4.2 Secure Smart contract

Although many of the students have learn about blockchain technology and NFTs the survey shows that an overwhelming majority, 90% of the students have no familiarity with smart contract vulnerabilities and only 10% of the students have general knowledge about the concept of smart vulnerability. We also carried out a pre- and post-survey to evaluate the effectiveness of the hands-on labs for this category. The Figure 3 shows the statistical plot of the effectiveness of the survey.

We also asked the students some questions about their interest in blockchain technology and their interest in learning about smart contract development and smart contract vulnerabilities.

- 62.5% of the students are inspired to learn more about NFTs by the hands-on lab
- The lab increases the interest of 64% of the students in blockchain technology
- More than 60% of the students would like to learn more about smart contract vulnerabilities

5 CONCLUSION

This study presents a comprehensive method for teaching students about blockchain technology and identifying flaws in smart contract development and blockchain applications. This study aims to teach students how to develop a secure blockchain application and identify and protect against potential threats in blockchain applications using a variety of methods and techniques. Software engineers must be aware of these vulnerabilities and take the necessary precautions to thwart attacks. By adhering to the design guidelines discussed in the studies, students can design a secure blockchain application that is resistant to vulnerabilities. In future, we will consider various blockchain vulnerability and develop more teaching materials for cybersecurity educations, especially for dealing with future quantum attacks [3, 4].

Future work will focus on expanding, refining, and systematically evaluating the proposed framework for integrating blockchain dApp development into cybersecurity education. A key direction involves incorporating post-quantum cryptography (PQC) [6] into the curriculum to address emerging quantum-era threats to blockchain systems. Given the reliance of blockchain platforms on classical public-key cryptographic primitives (e.g., ECDSA and RSA), future laboratory modules will introduce quantum-resistant signature schemes, hash-based cryptography, and lattice-based constructions [**?**]. Students will examine the implications of quantum computing on blockchain security, explore migration strategies toward PQC-enabled architectures, and evaluate trade-offs in performance, scalability, and interoperability [29].

ACKNOWLEDGMENTS

This research is based upon work supported in part by the National Science Foundation under NSF Grant CNS-xxxxxxx Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] 2017. *NATIONAL VULNERABILITY DATABASE, CVE-2017-13868 Detail. NVD.* Retrieved Januray 2, 2023 from https://nvd.nist.gov/vuln/detail/CVE-2017-13868

[2] 2020. *(ISC)2 Cybersecurity Workforce Study.* Retrieved Januray 12, 2023 from https://www.isc2.org/Research/Workforce-Study

[3] Sara Barj. 2024. CP-ABE-LWE-Based Smart Contract: A Novel Post-Quantum Smart Contract-Based Decentralized Application (DApp) for E-Health Records Management. In *2024 International Conference on Ubiquitous Networking (UNet)*, Vol. 10. IEEE, 1–10.

[4] Yaser Baseri, Abdelhakim Hafid, Yahya Shahsavari, Dimitrios Makrakis, and Hassan Khodaiemehr. 2025. Blockchain security risk assessment in quantum era, migration strategies and proactive defense. *IEEE Communications Surveys & Tutorials* (2025).

[5] K Sree Divya, G Swetha, Gomatam Mohana Charyulu, P Shyamala Madhuri, M Srividya, Modhi Lafta Mutar, and K Saikumar. 2024. Implementing Blockchain Based DApp for Secure Sharing of Students' Credentials. In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*. IEEE, 1–6.

[6] Mustafa El Bizri, Ahmad M El-Hajj, Layth Sliman, and Ali Massoud Haidar. 2026. Institutional Approaches to Post-Quantum Cryptography: A Comparative Analysis of Migration Frameworks. *IEEE Access* 14 (2026), 3259–3283.

[7] Gabriel Fernández-Blanco, Pedro García-Cereijo, Tiago M Fernández-Caramés, and Paula Fraga-Lamas. 2025. Hands-On Blockchain Teaching and Learning: Integrating IPFS and Oracles Through Open-Source Practical Use Cases. *Education Sciences* 15, 9 (2025), 1229.

[8] Itzhak Gershfeld and Arnon Sturm. 2024. Evaluating the effectiveness of a security flaws prevention tool. *Information and Software Technology* 170 (2024), 107427.

[9] Francois Goupil, Pavel Laskov, Irdin Pekaric, Michael Felderer, Alexander Dürr, and Frederic Thiesse. 2022. Towards Understanding the Skill Gap in Cybersecurity. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*. 477–483.

[10] Ping Han. 2025. AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. *Scientific Reports* 15, 1 (2025), 37327.

[11] Thushari Hapuarachchi, Mariyam Mapkar, Mohamed Rahouti, and Kaiqi Xiong. 2024. Advancing Blockchain Learning in STEM Education Through A Comprehensive Hands-On Educational Approach. In *2024 IEEE Integrated STEM Education Conference (ISEC)*. IEEE, 1–6.

[12] Peter Howson and Alex de Vries. 2022. Preying on the poor? Opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities. *Energy research & social science* 84 (2022), 102394.

[13] Md Rafiqul Islam, Muhammad Mahbubur Rahman, Md Mahmud, Mohammed Ataur Rahman, Muslim Har Sani Mohamad, et al. 2021. A review on blockchain security issues and challenges. In *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 227–232.

[14] Yerlan Kistaubayev, Francisco Liébana-Cabanillas, Aijaz A Shaikh, Galimkair Mutanov, Olga Ussatova, and Ainura Shinbayeva. 2025. Enhancing Transparency and Trust in Higher Education Institutions via Blockchain: A Conceptual Model Utilizing the Ethereum Consortium Approach. *Sustainability* 17, 20 (2025), 9350.

[15] Peiru Li, Shanshan Li, Mengjie Ding, Jiapeng Yu, He Zhang, Xin Zhou, and Jingyue Li. 2022. A Vulnerability Detection Framework for Hyperledger Fabric Smart Contracts Based on Dynamic and Static Analysis. In *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022*. 366–374.

[16] Yang Liu, Jinlong He, Xiangyang Li, Jingwen Chen, Xinlei Liu, Song Peng, Haohao Cao, and Yaoqi Wang. 2024. An overview of blockchain smart contract execution mechanism. *Journal of Industrial Information Integration* 41 (2024), 100674.

[17] Samreen Mahmood, Mehmood Chadhar, and Selena Firmin. 2022. Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies* 2022 (2022).

[18] Giandari Maulani, Gunawan Gunawan, Leli Leli, E Ayu Nabila, and W Yestina Sari. 2021. Digital Certificate Authority with Blockchain Cybersecurity in Education. *Int. J. Cyber IT Serv. Manag* 1, 1 (2021), 136–150.

[19] Omid Pahlavanpour and Shang Gao. 2024. A systematic mapping study on gamification within information security awareness programs. *Heliyon* 10, 19 (2024).

[20] Reza M Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Amritraj Singh. 2018. Empirical vulnerability analysis of automated smart contracts security testing on blockchains. *arXiv preprint arXiv:1809.02702* (2018).

[21] Zornitza Prodanoff, Cynthia White-Williams, and Hongmei Chi. 2021. Regulations and standards aware framework for recording of mhealth app vulnerabilities. *International Journal of E-Health and Medical Communications (IJEHMC)* 12, 3 (2021), 1–16.

[22] Sorravich Rattagool, Pawat Jiangthiranan, Peerawichaya Pholwiset, Theeraphat Wongnijasil, and Somchart Fugkeaw. 2025. A Verifiable and Secure E-Transcript System Using Self-Sovereign Id and Blockchain. In *2025 17th International Conference on Knowledge and Smart Technology (KST)*. IEEE, 52–57.

[23] Dalila Ressi, Riccardo Romanello, Carla Piazza, and Sabina Rossi. 2024. AI-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network and Computer Applications* 225 (2024), 103858.

[24] Maryam Taeb and Hongmei Chi. 2021. A personalized learning framework for software vulnerability detection and education. In *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*. IEEE, 119–126.

[25] Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks* 6, 2 (2020), 147–156.

[26] Xiaoqin Tu. 2024. Design of Modern Apprenticeship Management Wisdom Platform Based on Blockchain Technology. In *2024 4th International Conference on Computer Science and Blockchain (CCSB)*. IEEE, 212–218.

[27] Faheem Ullah, Xiaohan Ye, Uswa Fatima, Zahid Akhtar, Yuxi Wu, and Hussain Ahmad. 2025. What Skills Do Cyber Security Professionals Need? *arXiv preprint arXiv:2502.13658* (2025).

[28] Fernando Richter Vidal, Naghmeh Ivaki, and Nuno Laranjeiro. 2024. Vulnerability detection techniques for smart contracts: A systematic literature review. *Journal of Systems and Software* 217 (2024), 112160.

[29] Yong Wang and Eddie Shahril Ismail. 2025. A Review on the advances, applications, and future prospects of post-quantum cryptography in blockchain, IoT. *IEEE Access* (2025).