Advancing Blockchain Learning in STEM Education Through A Comprehensive Hands-on Educational Approach

Thushari Hapuarachchi
ICNS Lab and Cyber Florida
University of South Florida
Tampa, FL USA
saumya2@usf.edu

Mariyam Mapkar
CIS Dept.
Fordham University)
NY, NY USA
mmapkar@fordham.edu

Mohamed Rahouti
CIS Dept.
Fordham University)
NY, NY USA
mrahouti@fordham.edu

Kaiqi Xiong
ICNS Lab and Cyber Florida
University of South Florida
Tampa, FL USA
xiongk@usf.edu

***Abstract*—The escalating frequency of cybersecurity incidents and the critical importance of blockchain technology in modern society underscore the imperative for enriched, hands-on educational programs in undergraduate Computer Science and Engineering disciplines. This urgency is driven by the need to cultivate a workforce proficient in navigating and mitigating the complexities associated with digital security threats, alongside leveraging blockchain innovations for secure, decentralized solutions. Incorporating comprehensive, experiential learning opportunities into academic curricula will ensure that students are not only well-versed in theoretical knowledge but also proficient in applying practical solutions to real-world challenges, thereby significantly enhancing their preparedness for the demands of the tech industry. This work explores integrating blockchain technology into STEM education, focusing on cybersecurity through a hands-on learning approach. It aims to equip undergraduate students with practical experience in blockchain and cybersecurity, addressing the sector's complexities and its growing significance. Our work is to develop new modules and lab experiments, fostering real-world skills in these rapidly evolving fields. This initiative highlights the critical role of hands-on learning in understanding blockchain's foundational concepts and applications, preparing students for future challenges in technology and cybersecurity sectors.**

***Index Terms*—Blockchain, Cybersecurity, Cyber Infrastructure, Fabric, Hands-on Learning, Science, Technology, Engineering, and Mathematics (STEM)**

I. Introduction

In the rapidly evolving landscape of the digital age, the increasing sophistication of cybersecurity threats has rendered the traditional educational models inadequate [1]. It has become increasingly evident that undergraduate education must evolve, adopting adaptive, hands-on learning paradigms to address these challenges effectively [**?**], [2]. This need is further amplified by the meteoric rise of blockchain technology, which has emerged as a transformative force across numerous industries, particularly in strengthening cybersecurity measures.

Blockchain technology, with its unique capabilities, is set to overhaul the foundational structures of various sectors, especially those reliant on robust supply chains [3]–[5]. It promises to introduce unprecedented levels of transparency, traceability, and security, ensuring the integrity and verifiability of data [6]–[8]. This technological surge is reshaping job markets, creating a burgeoning demand for professionals proficient in these new paradigms.

In response to this shift, higher education institutions, particularly those specializing in Science, Technology, Engineering, and Mathematics (STEM) fields, are compelled to revisit and revitalize their curriculum. There is a pressing need to weave in-depth, hands-on learning experiences throughout the educational journey of undergraduate students [9]. Such experiences are crucial in cultivating a deep understanding of cybersecurity practices and blockchain technology applications.

To this end, colleges and universities must proactively develop and integrate cutting-edge laboratory modules, simulation environments, and real-world problem-solving opportunities into their programs. These practical components should be designed to build upon theoretical knowledge, fostering critical thinking, innovation, and the practical application of skills in live scenarios. Moreover, interdisciplinary approaches that combine elements of computer science, engineering, and business will be essential to provide students with a holistic understanding of how blockchain can be leveraged to fortify cybersecurity in various contexts.

By expanding the scope of their curricula to include these dynamic, practical learning opportunities in blockchain technologies, higher education institutions will not only prepare students to meet the current demands of the cybersecurity field but also to anticipate and adapt to its future evolutions. The aim is to equip the next generation of professionals with a versatile skill set that empowers them to navigate and lead in the ever-changing digital landscape, where cybersecurity and blockchain become increasingly intertwined.

Improving blockchain technology education for computer science students in particular requires a multifaceted approach that emphasizes both theoretical knowledge and practical skills. One effective strategy is the integration of hands-on, real-world experiences into the curriculum. This approach involves creating laboratory settings that simulate real-world scenarios, allowing students to engage in open-ended problem-solving and evidence-based learning. Further, to foster critical

thinking and adaptability, educational methods should encourage exploration, creativity, and innovative solution development. Collaborative teamwork in flexible lab environments and the creation of both digital and in-person learning communities are also crucial. These communities enhance student involvement and help overcome the limitations of conventional experimental learning methods.

The primary goals of our educational initiative are outlined as follows:

- Address the financial and computational resource challenges faced by many academic institutions, which stem from rapid advancements in hardware and software technologies.
- Ensure that students have easy and flexible access to experimental modules and resources, accommodating both remote and in-person experimental work.
- Assist students in understanding and applying fundamental concepts of blockchain technology to real-world cybersecurity scenarios.
- Equip students with the necessary technological proficiencies—both software and hardware—to critically analyze and assess security threats and countermeasures within blockchain infrastructures.

Our approach is designed to provide effective and efficient learning modules that account for the limited availability of computational resources and cater to the growing demands of the blockchain technology and cybersecurity sectors.

The structure of this document is organized as follows: Section II summarizes the state-of-the-art related to our work. Section III expands on our research objectives, detailing our methodology for integrating the hands-on-focused learning of Blockchain technology into STEM education for cybersecurity, and describes the laboratory modules created for effective student training. Section IV provides an overview of the key findings from our evaluation of the educational modules. The document concludes with Section V, which reflects on our findings and suggests directions for further research.

II. Related Work

The undergraduate cybersecurity curriculum, encompassing courses such as ethical hacking and software security, greatly benefits from the inclusion of real-world lab experiments for effective learning, as emphasized by [10], [11]. Traditional laboratory setups often leverage virtual machines (VMs) to ensure isolation, a method showcased in initiatives like SeedLAB [12], [13]. However, these arrangements, typically reliant on a singular VM, fail to accurately mimic the complex dynamics of real cyberattacks, which involve multiple computers with roles of attackers and defenders [14]. While advancements like those introduced by Willems and Meinel [15] have made strides in offering online lab assessments through VM platforms, enabling flexible and instantaneous configuration of virtual lab environments, a significant gap persists between these traditional lab settings and the intricate realities of contemporary cybersecurity. This gap underscores the critical need for more realistic and comprehensive training approaches to better equip future cybersecurity professionals.

Cybersecurity education, particularly when it involves hands-on lab experiments, is traditionally delivered in a face-to-face format, which simplifies the management of student laboratories [16]. However, the shift of these courses to an online framework introduces considerable challenges. Research across various studies [17]–[20] highlights a major hurdle in cybersecurity training: the scarcity of resources available to educational institutions and the constraints on students' time. This problem is especially pronounced at colleges lacking engineering departments and universities with finite computing assets, which serve a broad and varied student population.

In this study, our objective is to address the challenges recognized in the domain of blockchain technology education, thereby distinguishing our investigation from prior studies focused on blockchain education. Additionally, our research aims to confront two significant issues within the field as identified in the literature [17]–[20]: first, the deficiency of graduates who possess both the technical proficiency and critical thinking capabilities essential for addressing novel challenges in blockchain and cybersecurity; and second, the discrepancy between the content and learning resources currently available for blockchain courses and the practical, hands-on skills demanded by the blockchain technology sector.

The methodology proposed in this paper distinguishes itself from prior studies in various key aspects. It underscores the incorporation of portable, self-contained hands-on labs into the educational framework, thereby providing a learning experience (in blockchain technologies) that is both more authentic and comprehensive. This approach effectively navigates beyond the constraints of conventional laboratory settings, which typically do not reflect the complex nature of actual cybersecurity challenges. Additionally, it embraces an open-ended, evidence-based learning strategy, fostering exploration, creativity, and the generation of innovative solutions within the realms of cybersecurity and blockchain. This methodology is designed to bolster students' practical skills and their ability to adapt, attributes that are indispensable for their future professional engagements in these fast-paced sectors. By integrating blockchain technology into cybersecurity education through practical experiments and reflective learning, this approach introduces a pioneering direction in STEM education.

III. Methodology

Our approach is rooted in innovative methodologies designed to enhance learning outcomes. We emphasize open-ended design in lab experiments to encourage exploration and innovation among students. These experiments are underpinned by evidence-based learning practices that ensure active participation and deeper understanding of the subject matter. Additionally, we prioritize teamwork and collaboration in flexible lab environments, fostering a community of learning that extends beyond the traditional classroom setting. The development of digital and in-person learning communities is a key aspect of our methodology, aimed at enhancing

student involvement and providing a supportive educational ecosystem.

A. Innovative Hands-On Experiments

To address the evolving demands of the cybersecurity industry and enhance academic curricula, our initiative has been to develop laboratory modules with a specific focus on Blockchain technology, alongside a broader emphasis on cybersecurity principles. We recognize that cybersecurity programs often enroll students from varied backgrounds, many of whom may not possess the foundational knowledge in computer science and security. This diversity, while enriching, presents a significant challenge in designing laboratory assignments that cater to the entire student body effectively. The literature underscores this issue, noting the difficulty in creating labs that align with the capabilities of all students in a class [21], [22].

In response to this challenge, our approach in developing these lab modules has been to stratify them by complexity. This progressive structure ensures that students, regardless of their initial skill level, can find an entry point into the learning material. To further support students with limited backgrounds in the field, we have developed comprehensive step-by-step tutorials and demonstrations for each lab. These resources are designed to guide students through the learning process, ensuring they gain the necessary skills and understanding to progress.

Furthermore, recognizing the importance of effective instruction in the dissemination and application of these labs, we have prepared detailed instructor manuals for each module. These manuals are intended to assist educators in integrating the labs into their teaching portfolios, whether in academic courses or professional development workshops. By doing so, we aim to not only bridge the gap in students' foundational knowledge but also to empower educators to deliver high-quality, impactful learning experiences.

Overall, our initiative seeks to make a significant contribution to cybersecurity education by providing accessible, scalable, and pedagogically sound laboratory modules. By doing so, we hope to prepare a more diverse and well-equipped generation of students to meet the challenges of the cybersecurity field head-on. The cornerstone of this project is a series of practical lab experiments, utilizing the Fabric CI platform to provide hands-on experience in the fields of cybersecurity and blockchain. These include:

- *Cryptography labs*: Focused on secret-key encryption, these labs offer practical insights into encryption applications in cybersecurity.
- *Blockchain network and consensus labs*: Providing a deep dive into blockchain technology operations, these labs allow students to understand and engage with blockchain network functions and consensus mechanisms.
- *Smart contract labs*: Centered on the crafting and testing of smart contracts, with a particular focus on security aspects. These labs provide students with the opportunity to develop, deploy, and evaluate smart contracts, offering invaluable hands-on experience in a crucial area of blockchain technology.

1) Cryptography labs: In the realm of blockchain technology, cryptography serves as a crucial tool to safeguard user privacy and transaction details and uphold data integrity [23]–[25]. Digital currencies, like Bitcoin, leverage encryption techniques to secure transactions and counteract fraudulent activities. The use of intricate algorithms and cryptographic keys ensures the protection of these transactions, rendering them highly resistant to tampering or counterfeiting.

To enhance comprehension of cryptography within blockchain technology, we created a lab focused on secret-key cryptography and its application in ensuring the secure exchange of information distributed networks. As the first step in the lab, we guide students in creating files and transferring them between two nodes via the File Transfer Protocol (FTP). Then, a similar task is repeated using the Secure File Transfer Protocol (SFTP). Afterward, students will identify the differences between the two approaches using network traffic capture.

The next task focuses on the Data Encryption Standard (DES), a widely used secret-key algorithm for encrypting digital information. First, students are guided to generate and transfer a key to another node via SFTP. Then, they will encrypt a file using DES, transfer it to the other node via FTP, and decrypt it using the previously shared key. Additionally, to understand the idea behind different encryption modes, we direct students to encrypt an image using Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes. Then, students will identify the difference between the two modes by observing the resulting images. By the end of this lab, students are expected to gain a practical understanding of how secret-key cryptography is instrumental in enabling secure and immutable transactions on a blockchain.

2) Blockchain network and consensus labs: We initiate a lab to establish a fundamental grasp of blockchain technology through practical exercises. We use 'Bitcoind,' the original Bitcoin software implementation, to simulate the Bitcoin network. The network created in this lab has three nodes. After connecting all nodes as peers, students will generate blocks in one node and observe how all the nodes know it. Then, they create blocks in other nodes and explore the mechanism of earning rewards through multiple confirmations. Additional experimental tasks involve manipulating the Bitcoin network to allow unconnected segments to generate blocks and observing the outcomes when these segments reconnect. Upon completing this lab, students will have thoroughly understood the blockchain technology.

Consensus mechanisms play a crucial role in blockchain technology, with Proof of Work (PoW) and Proof of Stake (PoS) being the primary mechanisms [26], [27]. We have developed a lab to facilitate students' understanding of these mechanisms. The initial task involves understanding the PoW mechanism, for which we provide a simple Python script demonstrating its functionality. Students are expected to ex-

TABLE I
OUR PROPOSED BLOCKCHAIN HANDS-ON LABS.

Labs	Objectives	Time (Hrs)
Secret- and public-key cryptography	Learn secret-key cryptography concepts including hash algorithms and digital signatures	4
Bitcoin: reaching consensus in distributed systems	Gaining a fundamental understanding of blockchain technology via simulated Bitcoin network	2
Consensus mechanisms and mining	Understanding primary consensus mechanisms through practical tasks	3
Smart contract security attacks	Provide practical, hands-on experience in reentrancy attacks in smart contracts	2.5
Smart contract offline vs. online mode	Practice on development of Ethereum smart contract and decentralized applications (DApps)	5

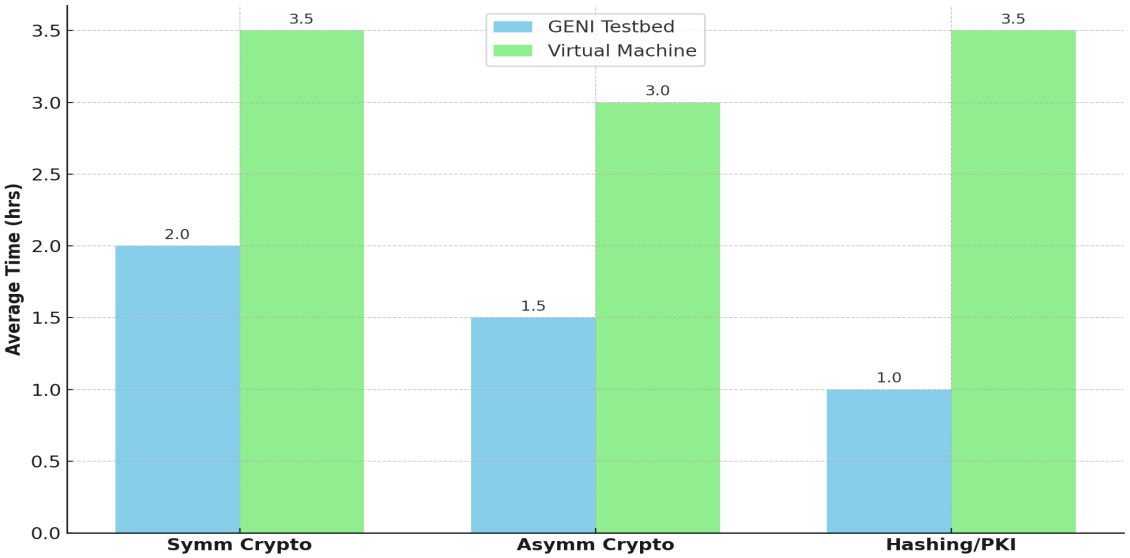

Fig. 1. Comparative average durations spent by students on labs exercises developed by us, utilizing either a virtual machine (VM) or a testbed.

ecute the given script in a VM and obtain outputs such as 'nonce' and the time to find the nonce. We then follow a similar procedure for PoS, allowing students to comprehend the process of selecting a validator by varying the amount of stake they hold. Moreover, practical exercises on Delegated Proof of Stake (DPoS) are also provided similarly. Towards the end of the lab, we also offer a demonstration of Bitcoin mining utilizing the PoW mechanism.

3) Smart contract labs: The initial lab in this series aims to equip students with hands-on experience regarding reentrancy attacks on smart contracts. It presents a valuable educational experience for computer science students by introducing two smart contracts: one susceptible to attacks serving as the victim and the other, an attacker contract. Participants conduct the attack using the SEED emulator, interacting with an internally deployed Ethereum blockchain. This practical approach not only deepens students' comprehension of the reentrancy vulnerability but also enhances their understanding and skills in blockchain technology, smart contract development, and blockchain interaction.

The second lab in our curriculum is designed to provide students with hands-on experience in developing Ethereum smart contracts. This lab introduces two different development approaches: online Integrated Development Environments (IDEs) like Remix for ease of use and offline tools such as Truffle to afford more control in local setups. Through this lab, students will take active roles in configuring their development environments and in creating, deploying, and testing Ethereum smart contracts. This practical engagement allows students to bridge the gap between theoretical concepts and real-world applications, bolstering their skills in both cybersecurity and blockchain technology. Upon completion of this lab, participants will have acquired significant practical knowledge in Ethereum smart contract development, preparing them for challenges in the blockchain industry.

The proposed hands-on labs outlined in Table I are designed to comprehensively cover essential aspects of blockchain technology, from the basics of cryptography to the intricacies of smart contracts and consensus mechanisms. These labs start with foundational knowledge in secret- and public-key cryptography, emphasizing hash algorithms and digital signatures, and extend to practical experiences with Bitcoin simulations, consensus mechanisms, and the security vulnerabilities of smart contracts. Each lab is tailored to provide a deep dive into its respective topic, ensuring that learners acquire the theoretical framework and practical skills necessary to understand and work with blockchain technology.

These practical labs are pivotal for enhancing blockchain

education, as they bridge the gap between theoretical concepts and real-world applications. By engaging students in simulations of Bitcoin networks, hands-on tasks in consensus mechanisms, and the development and security testing of smart contracts, these labs offer a well-rounded educational experience. This approach not only reinforces the learners' understanding of blockchain fundamentals but also equips them with the critical thinking and technical skills required to navigate and innovate within the blockchain space. Such experiential learning is crucial for preparing students for the complexities and challenges they will face in blockchain-related endeavors.

IV. Assessment and Evaluation

Previously, we conducted an analysis to evaluate student performance in practical cryptographic laboratories, comparing the use of a pre-established traditional virtual machine with a cyber infrastructure, specifically the GENI testbed [13]. In this assessment, students with comparable backgrounds in computer science and engineering were engaged in a series of cryptographic laboratories. These included tasks on symmetric encryption, asymmetric encryption, and hash functions along with Public-Key Infrastructure (PKI). We meticulously recorded the duration each student devoted to each laboratory task.

Subsequently, we computed the average time spent by the students on these three laboratory exercises across both the GENI testbed and the virtual machine platforms. The primary objective of this analysis was to methodically evaluate and refine the alignment between the course content and the advanced laboratories we developed, employing a cyber infrastructure/testbed. Additionally, we aimed to investigate how efficiently learners could accomplish the same tasks using traditional methods (virtual machine-based laboratory experiments).

As illustrated in Figure 1, the data reveals that the average time students spent on these laboratories using the GENI testbed was significantly less compared to the virtual machine. This suggests a notable improvement in efficiency, potentially attributable to the more sophisticated resources and tools available within the GENI testbed environment.

Our assessment and evaluation framework is multifaceted, designed to measure the effectiveness and impact of our educational content and methodologies comprehensively. This includes analyzing student performance metrics such as exam scores and lab success rates, as well as engagement and participation measures like class participation and lab attendance. We also conduct skill development assessments through pre- and post-course evaluations to gauge the growth in students' abilities and understanding. Additionally, feedback and surveys from students and instructors are integral to our evaluation process, providing insights into the effectiveness of our teaching methods and identifying areas for improvement. Practical application assessments, where students apply their learned skills in real-world contexts, are also a key component of our evaluation strategy.

In future efforts to evaluate the efficacy of the educational materials proposed in this paper, we will implement a comprehensive and multi-dimensional strategy. This strategy will integrate a variety of metrics and feedback systems to thoroughly determine the impact of the pedagogical content and methods introduced. We will begin by closely monitoring student performance metrics. This will include the analysis of examination and quiz outcomes to identify knowledge enhancement following the integration of the new materials. The completion and success rates of laboratory experiments will also serve as an indicator of the practical skills students have developed, especially regarding the application of blockchain technology within cybersecurity.

We will then assess student engagement and participation. Metrics for this will include variations in class participation rates and laboratory attendance figures, with any increases potentially signifying a greater interest in the subject matter attributed to the new material. The progression of student skills will be evaluated through pre- and post-course evaluations, aimed at measuring the acquisition of specific competencies such as cryptography and the application of blockchain in cybersecurity. The caliber and originality of student projects will provide a metric for understanding the extent of concept application.

Student feedback and surveys will be essential in appraising the subjective reception and comprehensibility of the new material. Observations from instructors will also play a critical role in determining the influence of the material on student performance and involvement. This feedback will help identify successful elements and areas needing refinement. The real-world application of the skills imparted and the level of innovation in student projects will offer significant insights into the material's practical impact. The students' capacity for innovation and creativity in their projects will be indicative of their comprehensive understanding and engagement.

Additionally, the development of collaboration and teamwork abilities, crucial in cybersecurity, will be evaluated through group projects and peer assessments. This will not only reflect the students' grasp of the material but also their competency in a collaborative professional context. The long-term influence of the educational material is also of paramount importance. Post-graduate surveys and the monitoring of alumni career paths will provide data on the enduring value of the educational program in equipping students for professional roles in cybersecurity and blockchain.

Overall, the assessment of the proposed educational materials will be all-encompassing, employing both quantitative data and qualitative insights to ensure a robust evaluation of the material's role in advancing students' expertise and readiness for the challenges in cybersecurity and blockchain domains.

V. Conclusion

This word emphasized the transformative power of hands-on, practical learning experiences in the realms of cybersecurity and blockchain technology. By incorporating innovative educational strategies, the initiative aimed to equip students

with both the theoretical knowledge and practical skills necessary to navigate and excel in these rapidly evolving technological fields. The commitment to providing a comprehensive, experiential learning environment is aimed at preparing students for the professional challenges ahead, ensuring they emerge as competent, innovative, and adaptable professionals ready to contribute to the advancement of cybersecurity and blockchain industries. This approach not only fosters a deeper understanding and engagement with the material but also positions students to make significant contributions to their fields, armed with a blend of critical thinking, technical prowess, and practical experience related to the cybersecurity discipline.

ACKNOWLEDGMENT

The authors would like to thank the National Science Foundation (NSF) for partially sponsoring the work under grants #2236280, #1633978, #1620871, #1620862, and #1636622, and BBN/GPO project #1936 through an NSF/CNS grant. We also thank the Florida Center for Cybersecurity (Cyber Florida) for a seed grant. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied by NSF.

REFERENCES

[1] W. J. Triplett, "Addressing cybersecurity challenges in education," *International Journal of STEM Education for Sustainability*, vol. 3, no. 1, pp. 47–67, 2023.

[2] M. Rahouti, "Board 129: facilitation of cybersecurity learning through real-world hands-on labs," in *2019 ASEE Annual Conference & Exposition*, 2019.

[3] A. Ali, M. Rahouti, S. Latif, S. Kanhere, J. Singh, U. Janjua, A. N. Mian, J. Qadir, J. Crowcroft *et al.*, "Blockchain and the future of the internet: A comprehensive review," *arXiv preprint arXiv:1904.00733*, 2019.

[4] S. K. Jagatheesaperumal, M. Rahouti, K. Xiong, A. Chehri, N. Ghani, and J. Bieniek, "Blockchain-based security architecture for unmanned aerial vehicles in b5g/6g services and beyond: A comprehensive approach," *arXiv preprint arXiv:2312.06928*, 2023.

[5] A. Miah, M. Rahouti, S. K. Jagatheesaperumal, M. Ayyash, K. Xiong, F. Fernandez, and M. Lekena, "Blockchain in financial services: Current status, adoption challenges, and future vision," *International Journal of Innovation and Technology Management*, vol. 20, no. 08, p. 2330004, 2023.

[6] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67 189–67 205, 2018.

[7] M. Smith, A. Castro, M. Rahouti, M. Ayyash, and L. Santana, "Screencoin: A blockchain-enabled decentralized ad network," in *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*. IEEE, 2022, pp. 1–6.

[8] X. Cao, M. Rahouti, S. K. Jagatheesaperumal, and K. Xiong, "Psychological information sharing using ethereum blockchain and smart contracts," in *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2023, pp. 561–568.

[9] J. P. Barber, *Facilitating the integration of learning: Five research-based practices to help college students connect learning across disciplines and lived experience*. Taylor & Francis, 2023.

[10] K. Xiong and Y. Pan, "Understanding protogeni in networking courses for research and education," in *Proceedings of the GENI Research and Educational Experiment Workshop (GREE)*. IEEE, 2013, pp. 119–123.

[11] L. Topham, K. Kifayat, Y. A. Younis, Q. Shi, and B. Askwith, "Cyber security teaching and learning laboratories: A survey," *Information & Security*, vol. 35, no. 1, p. 51, 2016.

[12] W. Du, "Seed: hands-on lab exercises for computer security education," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 70–73, 2011.

[13] M. Rahouti, K. Xiong, and J. Lin, "Leveraging a cloud-based testbed and software-defined networking for cybersecurity and networking education," *Engineering Reports*, vol. 3, no. 10, p. e12395, 2021.

[14] M. Rahouti and K. Xiong, "A customized educational booster for online students in cybersecurity education." in *CSEDU (2)*, 2019, pp. 535–541.

[15] C. Willems and C. Meinel, "Online assessment for hands-on cyber security training in a virtual lab," in *Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2012, pp. 1–10.

[16] M. Rahouti, K. Xiong, and J. Lin, "Developing blockchain learning lab experiments for enhancing cybersecurity knowledge and hands-on skills in the cloud," in *International Conference on Computer Science and Education*. Springer, 2022, pp. 438–448.

[17] D. E. Tromblay, "National protection and programs directorate," in *The Handbook of Homeland Security*. CRC Press, 2023, pp. 99–105.

[18] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Education and Information Technologies*, vol. 28, no. 9, pp. 11 759–11 791, 2023.

[19] M. Matheny, "Cloudpassage study finds us universities failing in cybersecurity education," *CloudPassage,[online] Available at: https://www. cloudpassage. com/company/press-releases/cloudpassagestudy-finds-us-universities-failing-cybersecurity-education/(accessed 03.12. 2018)*, 2016.

[20] M. Nizich, "Preparing the cybersecurity workforce of tomorrow," in *The Cybersecurity Workforce of Tomorrow*. Emerald Group Publishing Limited, pp. 117–146, 2023.

[21] R. S. Cheung and J. P. Cohen, "Challenge based learning in cybersecurity education," 2011.

[22] W. B. Gaskins, J. Johnson, C. Maltbie, and A. Kukreti, "Changing the learning environment in the college of engineering and applied science using challenge based learning." *International Journal of Engineering Pedagogy*, vol. 5, no. 1, 2015.

[23] N. Paykari, D. Lyons, and M. Rahouti, "Assessing blockchain consensus in robotics: A visual homing approach," in *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2023, pp. 0577–0583.

[24] M. Rahouti, D. Lyons, S. K. Jagatheesaperumal, and K. Xiong, "A decentralized cooperative navigation approach for visual homing networks," *IT Professional*, vol. 25, no. 6, pp. 71–81, 2023.

[25] M. Rahouti, D. M. Lyons, and L. Santana, "A lightweight blockchain framework for visual homing and navigation robots," in *International Conference on Robotics and Networks*. Springer, 2022, pp. 91–104.

[26] M. Rahouti, D. Lyons, and L. Santana, "Vrchain: A blockchain-enabled framework for visual homing and navigation robots," *arXiv preprint arXiv:2206.11223*, 2022.

[27] K. Martin, M. Rahouti, M. Ayyash, and I. Alsmadi, "Anomaly detection in blockchain using network representation and machine learning," *Security and Privacy*, vol. 5, no. 2, p. e192, 2022.