LEVERAGING ARTIFICIAL INTELLIGENCE TO IMPROVE BLOCKCHAIN EDUCATION: A COMPREHENSIVE APPROACH TO ADDRESSING CRYPTOCURRENCY SECURITY RISKS AND TRANSACTION MONITORING

Research Paper

George Antoine Helou, Swiss School of Business and Management, Geneva, Switzerland, georgehelou@mail.com

"Abstract"

This research paper explores the potential use of artificial intelligence (AI) to improve blockchain education, and to address security risks and transaction monitoring associated with cryptocurrency integration. It highlights the need for practical skills and situational competencies, in addition to theoretical familiarity, in educational programmes. Furthermore, the paper discusses the opportunities and challenges of using AI to enhance blockchain education and strengthen security. It also proposes pragmatic recommendations for educators and academic institutions to bridge the gap between theory and practice. The literature review highlights the gaps in current approaches to blockchain education, and the potential of AI-based transaction monitoring techniques to prevent fraud in decentralised environments.

Keywords: Artificial Intelligence, Education, Blockchain, Cryptocurrency, Security Risks, Transaction Monitoring, Fraud, Money Laundering

1 Introduction

This paper explores potential applications of artificial intelligence (AI) to improve blockchain education, with a focus on addressing security risks and transaction monitoring needs arising from cryptocurrency integration. The decentralised and pseudo-anonymous nature of most blockchain architectures, combined with the rise of cryptocurrencies, presents new challenges, including risks related to money laundering, fraud, hacking and other financial crimes that exploit the limited transparency and oversight inherent in these structures (Liu et al., 2020).

As the adoption of blockchain technology accelerates in finance, government, healthcare, and other sectors, educational programmes are responding by incorporating more conceptual foundations on topics such as distributed ledgers, consensus protocols, smart contracts, decentralised applications, wallets, and cryptography (Nugent et al., 2016). However, there remain persistent gaps between the dynamic pace of innovation and the responsiveness of pedagogical approaches (Oke and Fernandes, 2020). Current curricula tend to focus on lectures, readings, videos and tests that emphasise building students' theoretical familiarity at the expense of developing the practical skills and situational competencies required by industry (Alexander et al., 2017). Graduates often lack the practical skills to develop, manage, integrate, and troubleshoot blockchain systems to the standards required in real-world work environments.

It is clear from the literature that AI offers significant potential opportunities to enhance blockchain education if implemented thoughtfully and to strengthen security, particularly in the areas of transaction monitoring, verification and protection (Cronin and MacLaren, 2018). Advanced algorithms and automation can enable more sophisticated detection of suspicious patterns of encrypted flows across decentralised networks, and help enforce compliance through smart contract rules encoded directly into blockchain architectures (Hassan et al., 2022). However, given the risks posed by opaque AI systems, maintaining human oversight and ethics is critical.

The paper is structured around several core sections. First, the introductory background provides a framework for the research focus, domains and objectives. Next, a literature review provides a contextual basis for prevailing approaches to blockchain education and the security risks posed by cryptocurrency integration. This grounds the study within current academic discourse and perspectives. Details of the pragmatic qualitative methodology follow, including the rationale for the thematic analysis of secondary sources. The results of the literature analysis highlight key themes related to pedagogical gaps, technological risks and potential AI applications. In response, pragmatic recommendations are proposed for educators, academic institutions, and industry partners in the areas of curricula, teaching practices, funding, regulatory policy, and collaborative initiatives. Finally, the conclusion summarises the findings, discusses limitations, and identifies spaces for additional research to further advance understanding of optimal practices and policies at the intersection of blockchain, AI, security, and professional education.

By exploring these spaces, this study aims to highlight current limitations in blockchain education while proposing initial scaffolding to bridge theory and practice. As rapid digital transformation impacts finance and other industries, developing dynamic learning systems and fostering collaborative leadership between academia and industry partners is essential to equip graduates with the interdisciplinary knowledge, critical thinking skills, and ethical orientation needed to harness the risks and opportunities of blockchain.

2 Literature Review

This literature review examines the dominant approaches to blockchain education, while summarising the key security risks posed by cryptocurrency integration. It highlights the emerging potential of AI-assisted transaction monitoring techniques to enhance financial oversight and fraud prevention in decentralised environments. This provides an academic foundation to contextualise the study's examination of strategies to enhance blockchain capability development through the use of AI.

2.1 Current approaches to blockchain education

As the adoption of blockchain technology accelerates across industries, the integration of related topics into university curricula is expanding in parallel in many business, technology, engineering and computer science programmes worldwide (How and Cheah, 2023). However, gaps remain between the rapid pace of innovation and the ability of educational institutions to equip students with dynamic skills tailored to industry needs (Sahin and Celikkan, 2020). Pedagogical approaches prioritise lectures, readings, videos and tests that focus on building theoretical familiarity with basic blockchain concepts. Common topics include distributed ledgers, hashes, blocks, mining, wallets, consensus protocols, smart contracts, and decentralised applications (Antal et al., 2021; Sharma et al., 2022). Students will gain a basic understanding of the technical components that underpin blockchain-based systems. However, opportunities to apply this knowledge through practical exercises, collaborative projects, case studies and simulations remain limited in most traditional curricula.

According to recent research, this theoretical focus does not provide learners with sufficient contextualisation or experiential competence development based on real-world practices, tools, and problem solving (Darling-Hammond et al., 2020). As graduates transition into workplace roles, many lack the practical skills to design, implement, integrate, manage, or debug complex blockchain solutions to rigorous industry standards (Sahin and Celikkan, 2020; Fu et al., 2018). Employers report that new hires, even from top programmes, struggle to translate conceptual knowledge into situated applications tailored to dynamic project needs.

In response, scholars call for a better balance between the teaching of basic skills and the application of contextual knowledge, especially in the current era of curriculum design and pedagogy (Shahjahan et al., 2022). In this context, more project-based learning, hackathons, simulations, and design exercises will expose learners to the most common workplace challenges and provide practical solutions from a complex problem-solving perspective. Case studies and industry projects are designed to provide this kind of context and cognitive bridge, among other means. Another promising partnership paradigm is the alignment of content delivery with concrete expectations and workflows, whether through adjunct faculty, internships, mentors, or capstone projects.

Some universities have begun to see the labour market as a unique need to initiate entirely new degree programmes, which is central to blockchain. This is another argument for such programmes to remain a much specialised offering at a few universities, rather than a general part of the course offering. Today, they are further complemented by the emergence of other types of flexible massive open online courses (MOOCs), which provide modular access to knowledge on blockchain. Such a best practice of their sequencing and scaffolding into coherent curricula - from resource development to career-relevant competencies - is maturing and will strengthen over time (Hassan et al., 2022). Despite the fact that MOOCs democratise knowledge, such training places additional demands on most learners, who require intensive technical training to practice these skills.

2.2 Security risks in integrating cryptocurrencies

The mainstreaming of financial systems towards cryptocurrencies based on public blockchain architectures is likely to bring great benefits, but also large security vulnerabilities and regulatory risks that pose challenging technical and governance issues (Bhushan et al., 2020; De Filippi et al., 2020). In other words, the presence of transparency constraints and the decentralised nature of the distributed ledger create risks and instabilities different from those of traditional central intermediaries in finance (Liu et al., 2020). Ongoing regulatory gaps, which leave most cryptocurrencies well beyond the scope of know-your-customer (KYC) and other established prudential controls in traditional finance, only exacerbate the situation.

Several recurring risks permeate the current discourse on cryptocurrency integration and adoption. First, the pseudo-anonymity and privacy afforded by most blockchain systems facilitates money laundering on a significant scale by obscuring the origins and pathways of transactions (McCord et al., 2022). Related risks highlighted in the literature include terrorist financing and weapons proliferation through clandestine cross-border exchanges that circumvent jurisdictional controls and reporting requirements (Schmidt, 2021). Tax evasion also persists through the avoidance of reporting that is otherwise required for traditional assets.

Furthermore, the cryptocurrency environment remains highly vulnerable to large-scale hacking, fraud and theft. Liu et al. (2020) tracked numerous exchange hacks that resulted in billions in losses between 2013 and 2019 due to a combination of technical vulnerabilities, inadequate security protocols, and limited investor protections. Without centralised authorities, it is extremely difficult to pursue investigations and recover from incidents. Market manipulation through pump-and-dump schemes coordinated through social media channels also thrives amid minimal governance, oversight, and financial controls compared to traditional equity and commodity markets overseen by regulators (Gazi, 2021). Inadequate safeguards expose new retail investors to unnecessary risks.

In addition, Bansod and Ragha (2022) highlight the disproportionate use of cryptocurrencies by criminal enterprises and illicit underground markets, which exploit pseudo-anonymity mechanisms such as coin-mixing and privacy-enhanced coins, such as Monero, designed to hide transaction details. While most activity may be legitimate, the inherent limitations of transparency make monitoring and investigation more difficult, facilitating illicit exploitation. While innovating beyond traditional models, cryptocurrencies introduce security and regulatory complexities unlike any previous financial system. The main challenge stems from decentralised, cross-border transaction flows that do not rely on centralised intermediaries for governance, oversight and control (Liu et al., 2020). Mature regulations and compliance mechanisms common to mainstream banking and finance are not directly transferable to this paradigm (Anagnostopoulos, 2018). Preventing exploitation will require sophisticated solutions that are explicitly tailored to decentralised environments. Education, once again, emerges as having a critical role to play in developing professionals with the interdisciplinary fluency to responsibly navigate this high-risk landscape.

2.3 Role of transaction monitoring in fraud detection and prevention

Transaction monitoring is one of the main techniques used by financial institutions to analyse internal networks for indicators of potential misconduct requiring intervention, including money laundering, terrorist financing, fraud, tax evasion and other illicit activities (Roszkowska, 2021). By closely tracking and analysing data flows between accounts, wallets, applications and partners over time, suspicious behaviour and activity can be identified and flagged for further investigation (Sun et al., 2022). From a different perspective, Sarker et al. (2024) argue that consistent a priori definition of comprehensive indicators is proving challenging, and traditional rules-based monitoring systems are limited in their ability to adapt to unknown emergent exploitation techniques.

In response, artificial intelligence and machine learning are being rapidly adopted to enable more sophisticated transaction monitoring capable of learning to detect previously unseen patterns of abuse (King, 2020). Advanced neural networks can model basic user and system behaviour to identify statistical anomalies and outliers that indicate misconduct. Dimolianis (2022) argues that, unlike static rules-based protocols, intelligent solutions update detection protocols in real time by incorporating new data and behaviours. With continuous tuning, machine learning algorithms adaptively improve monitoring accuracy over time and minimise false positives. This provides fraud monitoring professionals, compliance officers and investigators with targeted alerts that warrant additional scrutiny, rather than overwhelming volumes of unactionable noise.

Automation in smart contract analytics, coupled with AI-based monitoring, integrates them to enhance oversight capabilities in a blockchain environment (King, 2020). The article by Garriga et al. (2021) summarises that the code automatically requires registrations, permissions and other types of constraints that are mapped to real-world identities and entities in cryptocurrency and blockchain networks. This, in turn, facilitates automated interventions that are enforced in real time and integrated directly into transactions, thus eliminating an over-reliance on deductive human analysis performed after the fact (Witt et al., 2019). Consequently, the combination of these tools provides state-of-the-art high-risk monitoring, with advanced alerts and pre-configured controls specifically tailored to the characteristically high risks of pseudonymous cryptocurrency networks.

Ensuring that there is still a reasonable form of transparency around AI systems and human oversight is necessary due to some of the inherent limitations of the technology, to avoid it becoming a Frankenstein creator that overreaches or shows bias (Bagaric et al., 2021). Further research is needed to develop best practices that balance automation, security and ethics across applications. But thoughtfully implemented, AI and smart contracts could provide a mechanism to import elements of governance and oversight necessary for the legitimate integration of cryptocurrencies into mainstream finance. Again, education emerges as a top priority to ensure professionals with the skills and moral character to responsibly operationalise such emerging tools.

Even in the contemporary literature, the gaps in blockchain pedagogy in the development of basic understanding and practical skills remain. These new critical security vulnerabilities come with the addition of cryptos, AI and smart contracts, which offer potential improvements in terms of oversight and security assurance if used transparently. These new perspectives provide an academic basis for exploring how blockchain education could be improved through AI, applied where appropriate.

3 Research Methodology

This research uses a qualitative method with a pragmatic research philosophy and thematic analysis of academic literature on blockchain education strategies and cryptocurrency risks. These particular methods do not pretend to be generalisable inferential statistics or causal hypotheses derived from quantitative techniques (Tracy, 2019). As blockchain is a complex, emergent phenomenon, flexible approaches to exploratory research best characterise this rapidly evolving field, where insights are tentative and drawn from best practices that are still coalescing from different scientific disciplines and their reflective communities (Yeung, 2021).

The thematic analysis involves an organised way of recognising reference points and structures placed throughout data collection to carry out qualitative source synthesis (Braun and Clarke, 2012). It consists of multi-step passes of coding and annotating text excerpts to classify segments based on shared meaning. These codes are further consolidated iteratively into salient themes abstracting higher-level patterns and relationships. Resulting themes then consolidate findings focused on gaps in prevailing blockchain pedagogy approaches, risks introduced by cryptocurrencies, and potential AI applications warranting consideration.

However, this study is oriented through the lens of pragmatist interpretivism, leading to drawing practical insights into the proposed research applicable by educational institutions, faculty, industry, and, thus, the researchers alike. They draw from research on blockchain in education and cryptocurrency risks based solely on secondary sources, particularly academic journals and industrial reports of existing peer-reviewed studies. The researcher could have gathered primary data from interviews, focus groups, surveys, or observations with students, instructors, and practitioners that might have augmented the proposed analysis by Wiggins et al. (2017) with more experiential perspectives. However, time and feasibility constraints held him back from moving to the next level. Hence, the current work remains secondary research. To initiate academic rigour, purposive sampling was used in conjunction with initially searching highly reputable peer-reviewed journals, forming the base for the literature on blockchain education.

Firstly, the pragmatic exploratory approach allows for the kind of flexibility that should be brought to bear on how this rapidly changing area is explored, as best practice continues to coalesce among many different stakeholders. Any prescriptive or definitive findings are therefore kept in check, and this view should be seen more as a basic framework that will move the discourse forward and act as a real catalyst for generating change. As Omér and Lien (2022) suggest, further mixed-methods research should be conducted in the future, based on omnibus primary data collection at this early stage, as blockchain technology, associated risks, educational practices and labour needs mature over the next decade or so.

However, there is a need to work in a reasoned way on provisional foundations in the interim period of the literature that is still dominated by secondary literature. The methodology ensures sufficient balance in terms of what is feasible by academic standards within the limitations of the exploratory research investigation. This is useful in synthesising key themes and insights to guide applied recommendations on how to enhance thoughtful pedagogy in blockchain using tools such as AI, which was previously identified as a critical foundational practice (Erickson et al., 2013). However, technologies that study different systems, risks, educational systems and associated risks, among others, will be essential for this ongoing mixed methods research to evolve.

4 Results and Findings

A thematic analysis of the literature revealed several key findings regarding the current limitations of blockchain education approaches, the risks posed by cryptocurrencies, and the potential applications of AI and smart contracts. Most programmes emphasise theoretical knowledge through lectures, readings, videos and tests, without sufficient practical projects, simulations or collaborative exercises to develop contextual competencies. Students gain a basic understanding, but lack opportunities to apply concepts through situated learning. These risks can have different security dimensions, such as money laundering, tax evasion, hacking, fraud, exploitation by criminals and, not least, manipulation. It is this total composition of transparency, together with anonymity, lack of supervision and decentralisation that distinguishes it from the conventional finance class. Transparency has its limits in terms of vulnerability to systemic vision, when the very fact of limited transparency leads to incredibly loose security and lack of accountability mechanisms. All of this takes place in a decentralised architecture with the need for sophisticated precautions.

AI, with its advanced behavioural modelling, can dynamically determine suspicion, which is an indispensable indicator of any misconduct. Machine learning can find patterns of exploitation that were previously unknown to humans or closed to detection by rule-based systems. Smart contracts can be implemented by directly scripting KYC and AML controls into self-executing decentralised applications through automated verifications and permissions mapped to real-world identities.

AI combined with smart contracts can enable such real-time monitoring, risk assessment, alerts and automated intervention at the level of a pseudonymous cross-border cryptocurrency transaction. However, fair conduct and appropriate transparency will become an indispensable issue, requiring assurance for one reason only - that automation does not take over the process designed and developed, making it too invasive or introducing bias or other unintended forms of harm to the attractiveness of the solution. There is still a need for more in-depth research to find the best practices.

In summary, while conceptual knowledge is still very important, current pedagogy calls for a significant increase in simulations, labs, workshops and collaborative projects to develop situational competencies through applied learning. Cryptocurrencies pose significant systemic security vulnerabilities alongside traditional centralised financial paradigms. However, AI, thoughtfully applied and working on smart contracts, shows the ability to reduce risks at an advanced level of behavioural monitoring and automatically tailored protection. This remains the most important criterion for keeping AI systems ethically correct and under control.

5 Recommendations

This section proposes an integrative, AI-driven framework with pragmatic recommendations to improve blockchain education and security through expanded applied learning and ethical automation:

5.1 Curricula

- Increase intensive hands-on labs, workshops, hackathons and collaborative projects to complement conceptual foundations with experiential skills development based on real-world practices.
- Develop dedicated smart contract courses that implement compliance rules such as KYC into executable decentralised applications to strengthen safeguards.
- Require ethics and philosophy modules focused on cultivating accountability in the use of powerful emerging technologies like AI and blockchain.

5.2 Pedagogy

- Provide extensive faculty training in the facilitation of immersive simulations, design sprints, and adaptive case-based learning to continuously engage students in applied problem solving.
- Encourage the development of original contextual learning activities and assessments through grants, release time and support teams for interdisciplinary collaboration.
- Maintain small seminar courses based on discussion, debate, reflection and peer learning alongside project delivery.

5.3 Technology & resources

- Develop blockchain sandbox environments tailored for educational use, enabling iterative experimentation by students with modelled risks, tools and data for applied learning.
- Provide access to datasets and platforms that enable hands-on development of AI behavioural models for financial crime detection in sample transaction datasets.
- Pursue public-private partnerships with technology companies to provide flexible, enterprise-grade platforms and software to support experiential learning.

5.4 Policy & governance

- Implement consistent standards, templates and processes for forming industry partnerships, balancing agile collaboration with necessary oversight.
- Encourage the development of non-credit professional development programmes through continuing education units and certifications to increase accessibility.
- Encourage consortia and communities of practice among institutions and partners to rapidly disseminate effective pedagogical innovations.

5.5 Culture & incentives

- Recognising teaching excellence in experiential and applied learning alongside research and publication in recruitment, tenure and promotion policies.
- Embed education departments in cross-disciplinary research centres focused on core technologies such as blockchain, AI and cybersecurity to strengthen the links between research and teaching.
- Provide release time and summer salary support for faculty to develop novel contextual learning activities and partnerships.

6 Conclusion and Future Research

The paper has synthesised the relevant academic literature using thematic analysis, and has been able to identify clear gaps that are lacking in the practical development of blockchain competencies within the prevailing paradigms of business education. However, an extensive focus on theoretical applications, consolidated through lectures, readings and exams, does not allow graduates to best serve the emerging needs of the industry due to insufficient situational learning and application. For example, the thematic analysis showed that cryptocurrencies, in a real sense, pose far greater systemic risks due to transactional anonymity and decentralisation than most traditional, centralised financial systems. However, the emerging technologies of AI and smart contracts, if introduced with due diligence and ethical considerations, point to promising tools to potentially enhance behavioural monitoring capabilities, together with protective automation tailored to decentralised architectures.

A number of targeted, pragmatic recommendations have been proposed to enhance experiential learning and facilitate the ethical integration of automation into curricula, pedagogy, learning resources, institutional policies and cultural incentives. Nevertheless, there are limitations to the findings, most notably the reliance on secondary source literature alone, given the conceptual nature of this initial study. Incorporating diverse primary data directly from students, educators, industry practitioners and policy makers through mixed methods, including interviews, focus groups, surveys and ethnographic observations, could significantly enrich the analysis by capturing the lived experiences and perspectives of stakeholders. Furthermore, longitudinal research is warranted as blockchain technologies rapidly mature, associated risks evolve, training practices adapt, and workplace needs change over the coming pivotal years.

This study aimed to constructively bridge theory and practice, fostering cross-disciplinary collaboration and innovation to meet the dynamic educational and industry demands arising from blockchain's increasing penetration in finance, government, healthcare, and other sectors. The development of agile, responsive learning systems that leverage new tools such as AI appears critical to adequately equipping graduates with the integrated knowledge, critical thinking skills, and ethical orientation needed to understand, harness, and regulate the risks and opportunities of blockchain. While not an exhaustive analysis, this research provides initial scaffolding and preliminary strategies for adapting prevailing academic paradigms through experiential learning and thoughtful integration of emerging technologies like AI, guided by humanistic values. However, further progress will require a sustained commitment to applied research and visionary leadership from educators, institutions and industry partners alike to elevate blockchain education to the highest standards demanded by these exponentially disruptive times.

In conclusion, there are immense challenges to navigate, but there are also tremendous opportunities for those institutions and graduates with the technical skills, wisdom, and social conscience to develop and lead blockchain's immense potential to benefit society, if properly cultivated through educational programmes that integrate technological innovation with ethics.

References

Alexander, B., Becker, S.A., Cummins, M. and Giesinger, C.H., (2017). Digital literacy in higher education, Part II: An NMC Horizon project strategic brief. Austin, TX: *The New Media Consortium*, pp. 1-37.

Anagnostopoulos, I., (2018). Fintech and RegTech: Impact on regulators and banks. *Journal of Economics and Business*, 100, pp.7-25.

Antal, C., Cioara, T., Anghel, I., Antal, M. and Salomie, I., (2021). Distributed ledger technology review and decentralised applications development guidelines. *Future Internet*, 13(3), p.62.

Bagaric, M., Svilar, J., Bull, M., Hunter, D. and Stobbs, N., (2021). The solution to the pervasive bias and discrimination in the criminal justice: Transparent artificial intelligence. *American Criminal Law Review*, 59(1).

Bansod, S. and Ragha, L., (2022). Challenges in making blockchain privacy compliant for the digital world: Some measures. *Sādhanā*, 47(3), p.168.

Bhushan, B., Khamparia, A., Sagayam, K.M., Sharma, S.K., Ahad, M.A., and Debnath, N.C., (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, 61, p.102360.

Braun, V. and Clarke, V., (2012). Thematic analysis. In APA Handbook of Research Methods in Psychology, Vol 2: Research designs, Washington, DC: *American Psychological Association*, pp.57-71.

Cronin, C. and MacLaren, I., (2018). Conceptualising OEP: A review of theoretical and empirical literature in Open Educational Practices. *Open Praxis*, 10(2), pp.127-143.

Darling-Hammond, L., Flook, L., Cook-Harvey, C., Barron, B. and Osher, D., (2020). Implications for educational practice of the science of learning and development. *Applied Developmental Science*, 24(2), pp.97-140.

De Filippi, P., Mannan, M. and Reijers, W., (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62, p.101284.

Dimolianis, M., (2022). Intelligent services for detection and mitigation of distributed denial-of-service attacks in programmable network environments. *London: Routledge*.

Fu, W., Liu, S. and Dai, J., (2018). E-learning, e-education, and online training.

Garriga, M., Dalla Palma, S., Arias, M., De Renzis, A., Pareschi, R. and Andrew Tamburri, D., (2021). Blockchain and cryptocurrencies: A classification and comparison of architecture drivers. *Concurrency and Computation: Practice and Experience*, 33(8), p.e5992.

Gazi, S., (2021). Reimagining a centralised cryptocurrency regulation in the US: Looking through the lens of crypto-derivatives. *Cambridge Law Review*, 6, p.97.

Hassan, M.U., Rehmani, M.H. and Chen, J., (2022). Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

How, M.L. and Cheah, S.M., (2023). Business Renaissance: Opportunities and challenges at the dawn of the quantum computing era. *Businesses*, 3(4), pp.585-605.

King, T.C., Aggarwal, N., Taddeo, M. and Floridi, L., (2020). Artificial Intelligence Crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26, pp.89-120.

Liu, Y., Yu, F.R., Li, X., Ji, H. and Leung, V.C., (2020). Blockchain and machine learning for communications and networking systems. *IEEE Communications Surveys & Tutorials*, 22(2), pp.1392-1431.

McCord, A., Birch, P. and Davison, A., (2022). Technology enabled crime: Examining the role of cryptocurrency. *Kriminologie-Das Online-Journal | Criminology-The Online Journal*, (4), pp.428-451.

Nugent, T., Upton, D. and Cimpoesu, M., (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, 5.

Oke, A. and Fernandes, F.A.P., (2020). Innovations in teaching and learning: Exploring the perceptions of the education sector on the 4th industrial revolution (4IR). *Journal of Open Innovation: Technology, Market, and Complexity*, 6(2), p.31.

Omér, D. and Lien, H.O.H., (2022). Exploring blockchain technology potential in Norwegian timber industry (Master's thesis). *Høgskolen i Molde-Vitenskapelig Høgskole I Logistikk*.

Roszkowska, P., (2021). FinTech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, 17(2), pp.164-196.

Sahin, Y.G. and Celikkan, U., (2020). Information Technology asymmetry and gaps between higher education institutions and industry. *Journal of Information Technology Education*: Research, 19, p.339.

Sarker, I.H., Janicke, H., Ferrag, M.A. and Abuadbba, A., (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, p.101110.

Schmidt, A., (2021). Virtual assets: Compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, 29(4), pp.332-363.

Shahjahan, R.A., Estera, A.L., Surla, K.L. and Edwards, K.T., (2022). "Decolonising" curriculum and pedagogy: A comparative review across disciplines and global higher education contexts. *Review of Educational Research*, 92(1), pp.73-113.

Sharma, T., Zhou, Z., Miller, A. and Wang, Y., (2022). Exploring security practices of smart contract developers. *arXiv preprint* arXiv:2204.11193.

Sun, Y., Xiong, H., Yiu, S.M. and Lam, K.Y., (2022). BitAnalysis: A visualisation system for Bitcoin wallet investigation. *IEEE Transactions on Big Data*, 9(2), pp.621-636.

Tracy, S.J., (2019). Qualitative research methods: Collecting evidence, crafting analysis, communicating impact. *Hoboken, NJ: John Wiley & Sons*.

Wiggins, B.L., Eddy, S.L., Wener-Fligner, L., Freisem, K., Grunspan, D.Z., Theobald, E.J., Timbrook, J. and Crowe, A.J., (2017). ASPECT: A survey to assess student perspective of engagement in an active-learning classroom. *CBE—Life Sciences Education*, 16(2), p.ar32.

Witt, C.M., Sandoe, K., Dunlap, J.C. and Leon, K., (2019). Exploring MBA student perceptions of their preparation and readiness for the profession after completing real-world industry projects. *The International Journal of Management Education*, 17(2), pp.214-225.

Yeung, K., (2021). The health care sector's experience of blockchain: A cross-disciplinary investigation of its real transformative potential. *Journal of Medical Internet Research*, 23(12), p.e24109.