Arbeidsnotat
Working Paper

2024:7

Luìs Manuel Nobre de Brito Elvas
Emmanuel Kafti Mawrides

Empowering patient-centric health data exchange : a blockchain-based framework for secure and efficient data sharing

Høgskolen i Molde
Vitenskapelig høgskole i logistikk

Luìs Manuel Nobre de Brito Elvas
Emmanuel Kafti Mawrides

Empowering patient-centric health data exchange : a blockchain-based framework for secure and efficient data sharing

Arbeidsnotat / Working Paper 2024:7

Høgskolen i Molde
Vitenskapelig høgskole i logistikk

Molde University College
Specialized University in Logistics

Molde, Norway 2024

ISSN 1894-4078

ISBN 978-82-7962-370-0 (trykt) ISBN 978-82-7962-371-7 (elektronisk)

Empowering Patient-Centric Health Data Exchange: A Blockchain-based Framework for Secure and Efficient Data Sharing

Authors:

Luìs Manuel Nobre de Brito Elvas* luis.m.elvas@himolde.no

Emmanuel Kafti Mawrides* emmanuel1.k.mawrides@himolde.no

*PhD. Candidate, Molde University College, Faculty of Logistics, Norway

Group advisor: Professor Alok Mishra, NTNU, Norway

Abstract: In the healthcare sector, the sharing of sensitive health data poses substantial privacy and security challenges that must be navigated with utmost care. With health data recognized by the European Commission as a unique and valuable resource for both retrospective and prospective research, and the Organisation for Economic Co-operation and Development (OECD) advocating for robust health data governance, there is a clear directive to harmonize individual privacy with the need for data accessibility. This paper proposes a conceptual blockchain framework designed to empower patients in the management and sharing of their medical information. Through this framework, patients would assume the role of data custodians, with the authority to grant access to their health records as they see fit. By leveraging blockchain technology's inherent qualities of decentralization, immutability, and transparency, our framework ensures that data sharing is secure, patient-centered, and conducted under the patient's consent. This approach not only upholds the privacy and autonomy of individuals but also streamlines the data sharing process. It is particularly advantageous for research centers, which can access necessary data without the procedural delays associated with traditional ethical approval processes. Our conceptual framework aims to redefine health data exchange, prioritizing patient control and trust, while fostering a more efficient and collaborative research environment.

Keywords: Blockchain; Healthcare; Data Privacy; Data Security; Data Autonomy; Information Systems; Patient Empowerment.

Introduction

Currently, the use of mobile smart devices for storing and managing users' most sensitive data is on the rise [1]. These advanced gadgets now collect, analyze, and store personal, financial, and even health-related information. The range of sensors on smartphones, smartwatches, and smart bands has also increased significantly, enabling unprecedented levels of user-health data collection. This data is typically aggregated in the user's smartphone, which serves as a gateway that integrates data from various end-user devices and backend systems.

The digitization of health records has been transformative for the healthcare industry, improving the efficiency and quality of care. However, the sensitive nature of personal health information (PHI) demands rigorous safeguards to protect patient privacy and ensure data security. The motivation for this conceptual framework arises from three key considerations:

1. **Patient Empowerment:** There is a growing recognition of the patient's right to control their own health data. By placing patients at the center of the data exchange process, we can enhance their autonomy and involvement in their healthcare journey.
2. **Data Accessibility for Research:** The potential of health data to revolutionize medical research is immense. Facilitating easier access to health data can accelerate discoveries and the development of new treatments, while still respecting the privacy and rights of individuals.
3. **Regulatory Compliance and Ethical Considerations:** With evolving regulations such as the General Data Protection Regulation (GDPR) in Europe, there is a pressing need for systems that comply with legal standards and ethical guidelines for data protection. Traditional mechanisms for data sharing are often slow and bureaucratic, impeding timely research and analysis.

By proposing a blockchain-based framework for health data exchange, we aim to address these challenges by creating a secure, transparent, and patient-driven model. Such a system has the potential to transform the landscape of health data governance, enhancing both privacy and utility. By conceptualizing a solution that is inherently secure, decentralized, and designed to facilitate consent-based sharing, we are motivated to bridge the gap between the protection of individual privacy and the collective benefits of shared health data.

Research Questions:

1. How can a blockchain-based framework enhance patient empowerment by providing patients with the tools and knowledge to manage and control access to their personal health data?
2. What are the potential benefits and challenges of facilitating easier access to health data for medical research through a blockchain-based system while ensuring privacy and compliance with regulatory standards?
3. How can blockchain technology ensure the secure and efficient sharing of Electronic Health Records (EHRs) among various healthcare stakeholders, including patients, doctors, hospitals, and researchers?

Blockchain technology can significantly impact remote health by certifying trust in devices and securely storing personal patient data [2]. This technology can be applied to an individual's EHR, which includes personal details (e.g., name, age, gender, weight, billing information), medical history, medications, and health problems. A critical issue in healthcare systems is maintaining the confidentiality and privacy of medical data, both at rest and in motion [3]. Secure sharing of medical data is essential, given its sensitivity and attractiveness to cybercriminals. A common yet simplistic approach is to index and encrypt EHRs before uploading them to a public or community cloud. However, this method is flawed as different data providers create incompatible indexes, hindering data sharing across medical organizations. Additionally, cloud providers may not be entirely

secure and could be vulnerable to attacks. A robust solution involving Blockchain and Distributed Ledger Technologies (B&DLT) could enable the creation of structured contracts for data access, standardized audits, and cryptographic algorithms to ensure data security and integrity.

Patient privacy can be compromised if EHR data leaks (e.g., medical conditions). B&DLT offers a promising solution for the secure and reliable sharing of such data, as most EHR data remains unchanged once recorded. Consequently, well-protected EHRs stored on B&DLT can be accessed more reliably by various medical institutions and individuals (such as doctors, hospitals, labs, and insurance companies).

The increase in healthcare sub-specialization has led to the diversification of patient care across different institutions and regions. While Primary and Palliative Care are mainly provided within residential settings, Secondary and Tertiary Care are delivered by specialized institutions without geographical or institutional links. Moreover, varying legal and administrative frameworks, such as state-owned, charity, and private providers, further complicate communication, and access among stakeholders.

Secondary and Tertiary Care often depend on advanced technologies available only in a limited number of institutions. The growing sub-specialization in medical care has made it challenging to house necessary specialists and technologies within a single institution. Due to the high financial costs of cutting-edge technology, patients, doctors, and health professionals frequently need to move between institutions to align patient needs with available resources and expertise.

Smartphones, within this user-centric privacy framework, serve as general health data gathering, aggregation, and storage devices and can be paired with additional devices [4]. In our proposed conceptual system, smartphones will securely collect and store all user-sensitive health data in an encrypted secure data vault (utilizing multi-factor unlocking mechanisms). Acting as a personal data gateway, the smartphone will facilitate data exchange between processors (notably large public hospitals of the National Health System) and anonymized user data. Users will have the power to approve or deny data access requests, ensuring that they remain in control of their health information. This functionality is a significant contribution to our work.

This conceptual proposal aims to facilitate a system where patients have enhanced control over their health data, ensuring secure, private, and efficient data sharing among healthcare stakeholders. This approach differs from others, such as those reviewed in [5], by incorporating identity management, coarse-grained data authentication and encryption, consortium blockchain, and smart contracts, while storing data on-chain with interdomain interoperability. Our system aims for secure and private interoperability among health data stakeholders, demonstrated through a proof of concept involving different health entities for health information sharing, unlike the supply chain focus in [6]. All solutions were developed on Ethereum blockchain technology, noted for its documentation, support, development scalability [7], and extensive use in healthcare applications [8]. Ethereum's flexibility in data storage allows different data types to be stored via smart contracts [9].

Literature Review

To be done .....

Methods

Figure 1 below shows a roadmap that our proposed study has followed, since the inception, that is the motivation of the study and research questions. The proposed strategy to be used in this study is action research. The research questions formulated are based on real life problems observed[10, 11]. Since this research tries to solve real life issues on patients' rights to control their own data while giving data accessibility for researchers while adhering to GDRP data protection by proposing a blockchain-based framework, action research as a strategy is justified [11]. Furthermore, action research is a collaborative approach that brings the stakeholders, in this case patients, doctors and medical institutions during the research process [10]. Action research is an iterative process which means that the researcher can adapt and refine the study as new information and insights emerge. It follows a cyclical process of planning, acting, observing and reflecting [12], thus it is suited for our study. Action research therefore lies between experimental strategies and field strategies, a perfect recipe for solving real-world problems in the field while having a framework where we can test for solutions that hence answering our research questions.

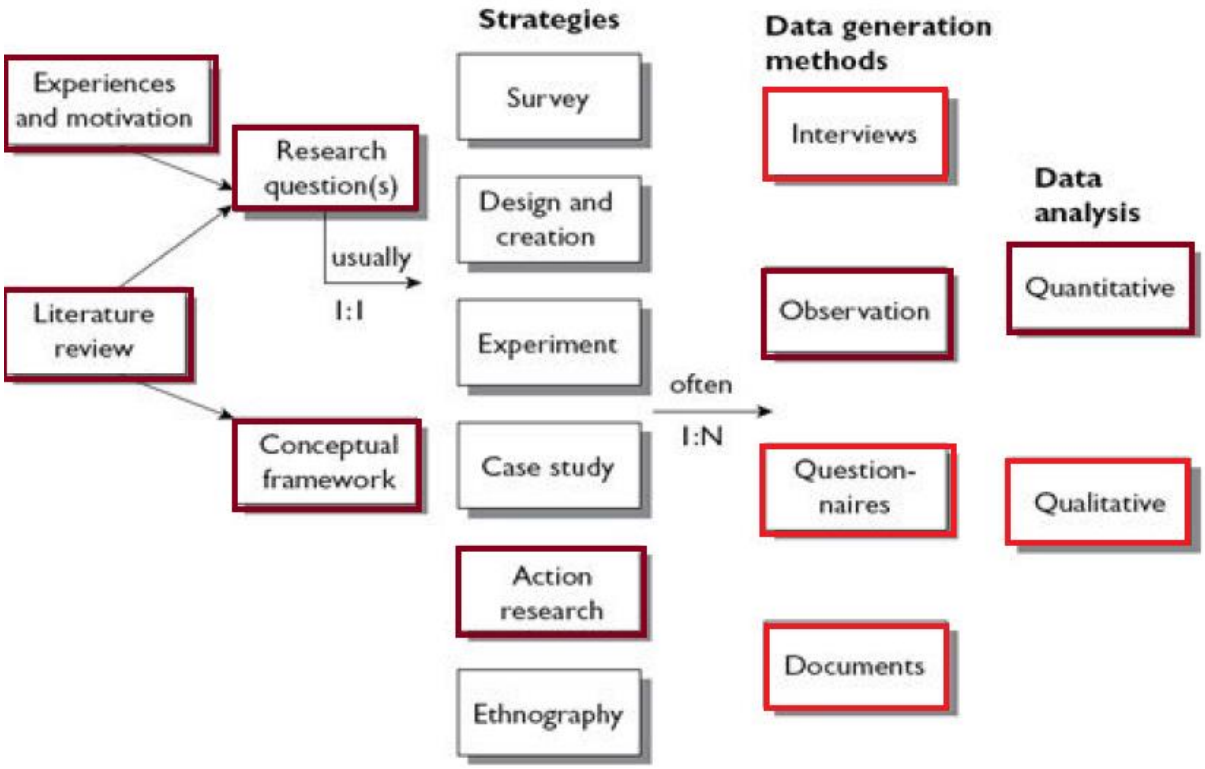

Figure 1. Research Roadmap [10]

We aim to gather both primary and secondary data for answering our research questions, thus we will employ a variety of data generation methods. Our main strategy is participant observation. We will also employ the use of interviews, documents, and questionnaires since having multiple data generation methods increases the validity and reliability of the data collected thus having an impact on our findings. We aim to do a quantitative data

analysis, although having multiple data generation methods makes our research susceptible to qualitative analysis as well.

Discussion

This conceptual framework leverages blockchain technology to address several critical challenges in health data management and exchange. The primary focus is on enhancing patient empowerment, ensuring data security, and facilitating data accessibility for research while complying with regulatory standards. How can a blockchain-based framework enhance patient empowerment by providing patients with the tools and knowledge to manage and control access to their personal health data?

1. How can a blockchain-based framework enhance patient empowerment by providing patients with the tools and knowledge to manage and control access to their personal health data?
2. What are the potential benefits and challenges of facilitating easier access to health data for medical research through a blockchain-based system while ensuring privacy and compliance with regulatory standards?
3. How can blockchain technology ensure the secure and efficient sharing of Electronic Health Records (EHRs) among various healthcare stakeholders, including patients, doctors, hospitals, and researchers?

Answering **question 1**, our conceptual study suggests that a blockchain-based framework can significantly enhance patient empowerment by offering robust tools and user-friendly interfaces for managing and controlling access to personal health data. By utilizing a decentralized ledger, patients are provided with a secure and transparent platform where they can easily grant, modify, or revoke access permissions to their health information without the need for intermediaries. This autonomy empowers patients, giving them control over who accesses their data and under what conditions. Furthermore, blockchain's token economics infrastructure simplifies the process of monetizing their data for those interested in sharing it [13, 14]. The integration of smart contracts automates data exchange processes based on predefined patient terms, ensuring that patients remain in control without requiring extensive technical knowledge. This approach places information-sharing power directly into the hands of patients.

Addressing **question 2**, our framework proposes several mechanisms to facilitate secure and accessible data sharing. Key among these is the use of smart contracts, which automate authorization and access processes[13]. When a patient grants access to a third party, the smart contract ensures that only the necessary data is shared and only for the specified duration[15]. The framework also employs cryptographic techniques to secure data during transmission and utilizes decentralized identifiers (DIDs) to ensure that data access is both secure and verifiable. For large data files, off-chain storage solutions are used, with only metadata and access logs stored on-chain, maintaining efficiency and security. This method ensures that health data can be accessed quickly

and securely, promoting timely medical research while protecting patient privacy and meeting regulatory standards.

The study addresses **question 3** by leveraging the transparency and auditability properties of blockchain technology. The immutable blockchain ledger provides a comprehensive record of all transactions, including data access requests and transfers. This transparency allows patients to track who accessed their data, what data was accessed, and for what purpose[16]. Decentralized applications (dApps) installed on smartphones can notify patients in real-time about data access, enhancing vigilance and control [17]. Smart contracts can further restrict access [13, 18], ensuring that only authorized individuals or entities can view the data, such as those who have fulfilled payment requirements or possess the necessary permissions. This continuous oversight and granular control help maintain the security and integrity of patient data across various healthcare stakeholders.
In summary, our conceptual proposal outlines a blockchain-based system designed to empower patients, facilitate secure and efficient data sharing, and enhance the transparency and auditability of health data exchanges. By placing control in the hands of patients and leveraging advanced blockchain technologies, this framework aims to address the critical challenges of data security, privacy, and regulatory compliance in the healthcare industry.

Contributions
The contributions of this proposal are multifaceted. Firstly, the framework emphasizes patient autonomy by providing robust tools for managing and controlling access to personal health data. Patients can grant, modify, or revoke access permissions through a secure and user-friendly interface, thus placing them at the center of the data exchange process. Secondly, by utilizing blockchain technology, the proposed system ensures that all data transactions are secure, transparent, and immutable. This enhances the trustworthiness of the data exchange process and protects patient information from unauthorized access and tampering. Thirdly, the framework promotes easier and secure access to health data for research purposes while respecting patient privacy and regulatory standards. Smart contracts automate the authorization process, allowing researchers to access only the necessary data for a specified duration, thereby accelerating medical discoveries and the development of new treatments.

Additionally, the proposed system is designed to comply with evolving regulations such as the General Data Protection Regulation (GDPR) in Europe. By ensuring data protection through advanced cryptographic techniques and decentralized identifiers (DIDs), the framework meets legal and ethical guidelines for data sharing and privacy. The use of off-chain storage for large data files, with only metadata and access logs stored on-chain, maintains system efficiency while ensuring data security. This approach balances the need for comprehensive data storage with the performance capabilities of blockchain technology. The framework supports interoperability among various healthcare stakeholders, including patients, doctors, hospitals, and researchers. Standardized data

formats and protocols facilitate seamless data exchange across different healthcare systems, improving coordination and collaboration in patient care.

Furthermore, patients receive real-time notifications via decentralized applications (dApps) whenever their data is accessed, promoting ongoing vigilance and control. The immutable blockchain ledger provides a transparent and auditable record of all data transactions, allowing patients to track access history and ensuring accountability. The conceptual system is designed to integrate with existing healthcare infrastructure, enabling the National Health System and other healthcare providers to participate in secure and efficient data exchanges. This integration supports the continuity of care and enhances the overall quality of healthcare services. Lastly, blockchain's immutable nature ensures that health data remains accurate and untampered, thereby enhancing the reliability and quality of patient records. Patients are motivated to keep their information up to date, further improving the accuracy of health data.
By addressing these key areas, this conceptual proposal aims to enhance health data governance, striking a balance between protecting individual privacy and unlocking the collective benefits of shared health data.

Limitations
Our conceptual framework, while offering promising solutions to various challenges in health data management and exchange, is not without limitations. Firstly, the study remains primarily theoretical, lacking empirical validation through real-world implementation or testing. Thus, the practical feasibility and effectiveness of the proposed framework remain unverified.

Secondly, blockchain technology poses various technical challenges, including scalability, interoperability, and energy consumption [19-21]. Addressing these challenges requires further research and innovation to ensure the successful implementation of the proposed framework.

Thirdly, implementing a blockchain-based system in healthcare requires significant technical expertise and resources. However, the study does not address potential barriers to adoption, such as the cost of implementation, resistance to change from healthcare stakeholders, and interoperability issues with existing systems.

Furthermore, while the study emphasizes compliance with regulatory standards, such as the General Data Protection Regulation (GDPR), it does not thoroughly explore the complexities of ensuring compliance across different jurisdictions or address potential legal challenges associated with data sharing and privacy.

Moreover, blockchain technology is not immune to security breaches or privacy vulnerabilities. The study does not thoroughly explore potential risks and vulnerabilities associated with storing sensitive health data on a blockchain or propose robust mechanisms for mitigating these risks.

The proposed framework may also have limited generalizability to diverse healthcare settings or contexts. Factors such as healthcare infrastructure, patient demographics, and regulatory environments may vary across different regions, affecting the applicability and effectiveness of the framework.

While the study briefly mentions ethical considerations such as patient consent and data ownership, it does not delve into deeper ethical implications, such as the potential for exploitation or discrimination based on health data. Further exploration of these ethical considerations is warranted.

Lastly, the study does not address resource constraints that healthcare organizations may face in implementing and maintaining a blockchain-based system. Factors such as financial resources, technical expertise, and organizational capacity may impact the feasibility and sustainability of the proposed framework.
Addressing these limitations will be essential for future research to advance the practical implementation and effectiveness of blockchain-based solutions in healthcare data management and exchange.

Conclusions

In conclusion, our conceptual framework offers potential solutions to significant challenges in health data management and exchange using blockchain technology. While our study acknowledges several limitations, it suggests avenues for improving healthcare data governance.

The framework's emphasis on patient empowerment, data security, and accessibility for research highlights its potential to enhance the healthcare ecosystem. By providing patients with greater control over their health data and ensuring secure and transparent data exchanges, the framework aligns with the evolving needs of modern healthcare systems.

However, it's essential to recognize the limitations identified, including the conceptual nature of the study, technical challenges associated with blockchain technology, and potential barriers to adoption and implementation in real-world healthcare settings.
Moving forward, further research is necessary to validate the proposed framework empirically and address the identified limitations. Collaboration among researchers, healthcare practitioners, policymakers, and technology experts will be vital in refining the framework and overcoming existing challenges.

While cautious optimism is warranted, we must approach the adoption of blockchain technology in healthcare with a clear understanding of its potential benefits and limitations. With continued research and collaboration, we can work towards developing practical solutions that enhance healthcare data management and ultimately improve patient care.

References

[1] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," *Computer Networks,* vol. 130, pp. 94-120, 2018.

[2] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *International journal of medical informatics,* vol. 148, p. 104399, 2021.

[3] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems,* vol. 42, no. 8, p. 140, 2018.

[4] Y. Ranjan *et al.*, "RADAR-base: open source mobile health platform for collecting, monitoring, and analyzing data using sensors, wearables, and mobile devices," *JMIR mHealth and uHealth,* vol. 7, no. 8, p. e11734, 2019.

[5] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE access,* vol. 7, pp. 61656-61669, 2019.

[6] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," *Array,* vol. 14, p. 100139, 2022.

[7] M. Macdonald, L. Liu-Thorrold, and R. Julien, "The blockchain: a comparison of platforms and their uses beyond bitcoin," *Work. Pap,* pp. 1-18, 2017.

[8] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association,* vol. 26, no. 5, pp. 462-478, 2019.

[9] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. Kayes, M. Alazab, and P. Watters, "A comparative analysis of distributed ledger technology platforms," *IEEE Access,* vol. 7, pp. 167930-167943, 2019.

[10] B. J. Oates, *Researching information systems and computing*. Thousand Oaks, Calif.: SAGE Publications, 2006.

[11] D. E. Avison, F. Lau, M. D. Myers, and P. A. Nielsen, "Action research," *Communications of the ACM,* vol. 42, no. 1, pp. 94-97, 1999.

[12] B. Somekh, *Action research*. McGraw-Hill Education (UK), 2005.

[13] S. Y. Jung, T. Kim, H. J. Hwang, and K. Hong, "Mechanism design of health care blockchain system token economy: development study based on simulated real-world scenarios," *Journal of Medical Internet Research,* vol. 23, no. 9, p. e26802, 2021.

[14] M. C. Ballandies, "To incentivize or not: Impact of blockchain-based cryptoeconomic tokens on human information sharing behavior," *IEEE Access,* vol. 10, pp. 74111-74130, 2022.

[15] A. B. Haque, A. Muniat, P. R. Ullah, and S. Mushsharat, "An automated approach towards smart healthcare with blockchain and smart contracts," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2021: IEEE, pp. 250-255.

[16] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in *Healthcare*, 2019, vol. 7, no. 2: MDPI, p. 56.

[17] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020: IEEE, pp. 310-317.

[18] M. Schnitzbauer, "Smart contracts in healthcare," *Digitalization in Healthcare: Implementing Innovation and Artificial Intelligence,* pp. 211-223, 2021.

[19] H. Wang, Z. Zheng, S. Xie, H.-N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services,* vol. 14, pp. 352-375, 10/12 2018, doi: 10.1504/IJWGS.2018.10016848.

[20] M. M. Queiroz and S. F. Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," *International Journal of Information Management,* vol. 46, pp. 70-82, 2019.

[21] V. Srivastava, T. Mahara, and P. Yadav, "An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks," *International Journal of Cognitive Computing in Engineering,* vol. 2, pp. 171-179, 2021/06/01/ 2021, doi: https://doi.org/10.1016/j.ijcce.2021.10.002.

This working paper is a result by group work in completion of DRL028

Molde University College
Specialized University in Logistics

HiMolde PhD

DRL028 Blockchain Applications in SCM

Credits: **5 ECTS**

Time: **27 – 31 May 2024**

The course covers fundamental concepts within blockchain technologies (BC) and their applications in supply chain management (SCM). Examples include historical perspectives, BC basics, basic cryptography, peer-to-peer transactions, BC structure, monetary policy and mining, forks and attacks, beyond bitcoin, Ethereum, smart contracts, and enterprise BCs.

Day 1 – May 27, 2024

Welcome & introduction (Bjorn, Anolan, Nitin, Arvind, Alok, Terje)

Each student presents him/her-self, thesis topic and motivation for blockchain (10 min each)

How to Use Publication to Advance Your Academic Career: An International Perspective! (Arvind)

It's All About Collaboration (Research Approaches) (Arvind)

Converting Your Research into a Paper for Publication! Present organization of groups (Alok, Arvind)

Lecture: Blockchain technology and SCM (by Nitin)

Blockchain-SCM Project: Ideas for seminar working paper (led by Alok)

Day 2 – May 28, 2024

Task 1, 2 and 3 Presentations with discussions (max 30 min for each)

Lecture: Blockchain technology and SCM (by Nitin)

Blockchain-SCM Project: Identify a research focus area & gap identification (led by Alok)

Day 3 – May 29, 2024

Task 4, 5 and 6 Presentations with discussions (max 30 min for each)

Lecture: Blockchain technology and SCM (by Nitin)

Blockchain-SCM Project: Research Approach/Method

Day 4 – May 30, 2024

Task 7 and 8 Presentations with discussions (max 30 min for each)

Lecture: Blockchain technology and SCM (by Nitin)

Lecturers presenting their research on Blockchain in SCM (15 min for each)

Blockchain-SCM Project: Working paper writing (led by Alok)

Day 5 – May 31, 2024

Blockchain-SCM Project: Working paper writing (led by Alok)

Blockchain-SCM Project: Presentation of working paper (by each PhD student)

Summing up

Faculty instructors

Nitin Vasant Kale, Professor of Information Technology Practice, University of Southern California, USA
Arvind Upadhyay, Professor of Operations, Logistics and SCM, London Metropolitan University, UK
Alok Mishra, Professor of Data Management & Software Engineering, NTNU, Norway
Bjørn Jæger, Professor of Informatics, Molde University College, Norway
Anolan Milanés, Associate Professor, Molde University College, Norway

Høgskolen i Molde
PO.Box 2110
N-6402 Molde
Norway
Tel.: +47 71 21 40 00
post@himolde.no
www.himolde.no