International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Check for updates

Analyzing the Role of Blockchain in Identity and Access Management Systems

Nikhil Ghadge [*]

Software Architect Okta.Inc, Software Engineering, San Francisco, CA, USA.

International Journal of Science and Research Archive, 2024, 12(01), 2249–2256

Publication history: Received on 24 April 2024; revised on 02 June 2024; accepted on 05 June 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.1.1019

Abstract

In today's digital world, protecting identities and securing access to sensitive data are crucial tasks. Traditional centralized Identity and Access Management (IAM) systems are vulnerable to data breaches and unauthorized intrusions. Blockchain technology has emerged as a promising solution to bolster IAM systems by decentralizing control and enhancing security measures.

This paper explores the integration of blockchain technology into IAM frameworks to address the shortcomings of centralized systems. It examines the fundamental principles of blockchain, highlighting its immutability, decentralization, and cryptographic security features. By leveraging these attributes, blockchain-based IAM systems offer a robust infrastructure for identity verification, authentication, and authorization processes.

Various use cases of blockchain in IAM are discussed, including self-sovereign identity, decentralized authentication protocols, and secure data sharing mechanisms. The paper elucidates how blockchain enhances trust and transparency in identity management, granting individuals greater control over their personal data while ensuring privacy and security. It also scrutinizes the challenges and considerations associated with implementing blockchain-based IAM solutions, such as scalability, interoperability, and regulatory compliance. Additionally, the paper explores potential future developments and trends in this evolving field, emphasizing the importance of collaboration between industry stakeholders and regulatory bodies to foster innovation while addressing security and privacy concerns.

In summary, this paper underscores the transformative potential of blockchain technology in fortifying IAM systems, leading to a more secure and resilient digital ecosystem.

Keywords: Identity and Access Management; Security; Blockchain; Identity theft; Artificial Intelligence

1. Introduction

1.1. Definition of Blockchain

Blockchain, in the context of Identity and Access Management (IAM) frameworks, refers to a decentralized, immutable digital ledger that securely records transactions across a distributed computing network. This innovation, rooted in the financial and digital domains, holds transformative potential to enhance security and fortify trust in IAM methodologies [1]. By harnessing structural narratological ontology alongside enterprise ontological systems, blockchain transcends traditional identity management frameworks and positions itself as a semantic web-based strategy for secure and efficient IAM approaches. The integration of blockchain technology into IAM frameworks heralds a paradigm shift towards a framework that embraces robustness, decentralization, and dependability for managing identities and access controls in the digital realm, thereby transforming the fundamental perceptions and implementations of security [2].

[*] Corresponding author: Nikhil Ghadge

1.2. Ease of Use Overview of IAM Systems

The domain of IAM systems, serving as essential conduits for securing resource and data access across vast networks, becomes increasingly complex with the expanding horizons brought by the Internet of Things (IoT). Traditional IAM architectures face challenges in accommodating the multitude of interconnected devices and provisions. It is suggested that a paradigm shift towards a device-centric orientation necessitates innovative modalities [3], including blockchain-infused IAM solutions like UniquID, to navigate the complexities inherent in centralized infrastructural topographies. Moreover, the growing trend towards frictionless authentication mechanisms highlights the imperative for IAM systems to exhibit adaptability across user environments while providing seamless yet secure entry points [4]. Organizations focused on enhancing both security and user experiences must embrace a panoramic understanding of IAM systems—one that inquires deeply into the dynamic and static aspects of technological landscapes and user requirements, amplifying the cardinality of resilient and scalable solutions like blockchain in the strategic deployment arteries of IAM.

1.3. Importance of Integrating Blockchain in IAM Systems

Integrating blockchain modalities into IAM ecosystems emerges as a pivotal endeavor, primarily in overcoming the complex challenges of security and fiduciary assurance. Inherently, the blockchain construct offers an advanced fortification archetype, pivoting around the sovereign characteristics of decentralization, thus bolstering the confidentiality, integrity, and availability of information within IAM schemata, congruent with the foundational doctrines of information safeguarding protocols. This confluence not only mitigates potential vulnerabilities related to unauthorized disclosure, alteration, and obliteration but also promotes transparency and procedural automation within identity oversight mechanisms. By employing the immutable and cryptographic quintessence of blockchain, IAM infrastructures are envisioned to lay a veritable foundation for fortified data reciprocation and consumer validation strategies. Moreover, the assimilation of blockchain within IAM infrastructures aligns with an expansive vision of propelling digital innovations across various sectors, including healthcare, finance, and government services, corroborated by exemplary deployments cataloged in relevant academic discourses [1][5].

2. Fundamentals of Blockchain Technology

2.1. Decentralization

In the domain of IAM frameworks, the principle of decentralization remains critically integral, especially as it intersects with the implementations of blockchain technology. Relevant research propounds the perspective that entrenching a decentralized architectural construct [6] within smart surveillance mechanisms intensifies security levels and sturdiness, primarily by bifurcating and decentralizing node operations, consequently subverting the construction of conventional single failure points and privacy intrusions. By encapsulating IAM functionalities into segregated microservice structures, combined with the utilization of blockchain for synchronized securement and access modulation, IAM infrastructures acquire assurances towards the incorruptibility of data storage articulations and decentralization-grounded [7], granular access controls. The adoption of decentralization within IAM infrastructures not only magnifies the fortitude of security and trustfulness but also subscribes earnestly to the core principles of blockchain technologies dedicated to cultivating secure, transparent, and efficient systemic frameworks.

2.2. Immutability

Delving into the essence of immutability within the blockchain framework illuminates its cardinal function in amplifying both efficacy and security dimensions of IAM landscapes. The underpinning architecture, encompassing a distributed ledger alongside cryptographic fortifications inherently pivotal to blockchain technologies, anchors the immutability paradigm robustly [8]. This tenet corroborates the principle that subsequent to data inscription on the blockchain, possibilities for alterations or interferences are ostensibly eradicated. This impenetrable characteristic emerges as quintessential within the terrain of IAM systems, as it ascertains the unassailability and consistencies of user identity markers, in conjunction with access entitlements meticulously catalogued on the blockchain. Blockchain technology ensures transparency and security in IAM systems by providing an incorruptible audit trail, preventing unauthorized tampering with sensitive data. This enhances data security and enables IAM infrastructures to manage identities and access privileges with precision and reliability across various sectors.

2.3. Consensus Mechanisms

In the domain of blockchain systems, particularly when examined through the prism of IAM frameworks, the role of consensus mechanisms is not just central but critical to the assurance of system integrity and security. Within scholarly discussions, it is underscored that an intrinsic aspect of blockchain's foundational technology is its reliance on a peer-to-peer network model. This model supports a decentralized validation process among nodes which, in turn, is pivotal in augmenting the reliability quotient of the entire network's architecture [9]. Furthermore, the inclusion of distributed databases alongside the deployment of asymmetric encryption techniques bolsters the transaction security within the blockchain, which is paramount in the protection of delicate identity and access-related data, characteristically found in IAM systems. Nevertheless, prevalent challenges still loom large in enhancing the efficiency and scalability of consensus mechanisms within the architectural confines of blockchain frameworks, as elaborated upon in discourses pertaining to learning analytics [9]. Despite the burgeoning potential of blockchain technology to engender transformative impacts across diverse sectors, including IAM systems, the intricacies involved in the efficacious implementation of robust consensus mechanisms demand heightened scholarly focus. This is crucial not only to amplify data privacy and security benchmarks within online educational ecosystems but also in broadening the scope to various other digital interactivities.

3. Challenges in Traditional IAM Systems

3.1. Centralized Data Storage

The entrenched paradigm of centralized data repositories has long underpinned the frameworks of IAM, yet stands at the cusp of obsolescence in the face of burgeoning phenomena such as the Internet of Things (IoT) and Data as a Service (DaaS) schemas. As elucidated [3], traditional IAM structures falter amidst the intricate multiplicity native to IoT devices and contemporary digital services, propelling a pivot toward frameworks that are simultaneously decentralized and robust in nature. The UniquID proposition of integrating blockchain methodologies provides a laudable pivot by obviating the dependency on quintessential centralized IAM constructions, thereby ensuring both scalability and fortified security protocols. DaaS aims to break away from traditional data localization constraints, enhancing data exchange and interoperability across cloud-based infrastructures [10]. Integrating blockchain into IAM systems has the potential to transform centralized storage into a more secure, efficient, and decentralized paradigm, meeting the needs of today's rapidly evolving digital landscape.

3.2. Single Point of Failure

The penetration of blockchain technology into IAM systems is perceived as an advantageous strategy for ameliorating the pivotal problem of single points of failure. In traditional IAM constructs, there exists a prevalent struggle to integrate a multitude of heterogeneous devices and syndicates of web-based services, precipitating architectural strata that might be cumbersome and adversely prone to lapses. This notion is fortified in expositions [3] that elucidate that the proliferation of the Internet of Things has catalyzed a paradigm shift towards device-centric interactions, thus necessitating a recalibration of IAM paradigms. Utilization of blockchain-oriented solutions, such as UniquID, ostensibly facilitates the circumvention of centralized IAM configurations, thereby propelling an enhancement in scalability and fortitude of IAM frameworks. Computational mechanism design offers valuable tools for analyzing decision-making in multiagent systems, helping to create robust IAM structures that can mitigate the risks of single points of failure [11]. Integrating these technological advancements into IAM systems enhances both security and continuity in access management processes, ultimately improving the effectiveness of IAM deployments in the digital age.

3.3. Security and Privacy Concerns

In the realm of IAM systems, especially with the rise of new technologies like the Internet of Things (IoT) and the widespread use of cloud computing, various challenges emerge that call for innovative solutions. Traditional IAM setups often struggle to address the complexities introduced by IoT and diverse online services, leading to cumbersome structures and vulnerable single points of failure. Blockchain-based approaches, such as the UniquID model, advocate for decentralized systems that promise enhanced scalability and resilience, overcoming limitations of centralized IAM frameworks [3]. Additionally, contemporary cryptographic methods play a crucial role in protecting sensitive data in cloud environments, where security, privacy, and reliability are paramount concerns [12]. Through the integration of cryptographic techniques and ongoing research efforts, cloud security is evolving to adapt to changing technological landscapes, emphasizing the need for robust security protocols and the preservation of privacy in IAM configurations.

4. Benefits of Integrating Blockchain in IAM Systems

4.1. Enhanced Security

With the incorporation of blockchain frameworks within IAM modalities, a paramount emphasis has been positioned on the augmentation of security protocols essential for the protection of critical data and assurance of data consistency. The assimilation of this blockchain apparatus within IAM matrices proposes an array of boons, encompassing decentralization, transparency, and automation of processes [1], whilst concurrently interfacing with the non-mutability attribute of blockchain, which instigates complexities regarding data privacy edicts, specifically in relation to the principles concerning the right to oblivion and non-disclosure [13]. To address these critical issues and enhance security in IAM systems, implementing specialized information security controls tailored for blockchain technologies is essential. Safeguarding the confidentiality, integrity, and availability of data assets, while mitigating security threats, is paramount. These tailored security measures for blockchain effectively prevent unauthorized access, tampering, or deletion of information, thereby strengthening the security framework within IAM networks. Continued development of innovative methodologies, as discussed in scholarly discussions, will further enhance the security of digital identities within blockchain infrastructures. This aligns with regulatory requirements and promotes the advancement of robust security measures within IAM frameworks.

4.2. Improved Data Integrity

The realm of IAM systems, integrating blockchain technology offers a promising avenue for enhancing data integrity measures. The inherent security and immutability of blockchain provide significant enhancements, bolstering the reliability of sensitive databases managed within these frameworks. This is particularly crucial in managing identities and access protocols, where the accuracy and dependability of data are paramount. Blockchain, renowned for its decentralization, transparency, and immutability, plays a fundamental role in safeguarding informational assets within IAM structures. Additionally, the development of novel information security controls tailored to blockchain's architecture is expected to effectively mitigate potential threats to data integrity. The integration of blockchain's robust security features within IAM domains not only strengthens data integrity but also supports the confidentiality and accessibility of informational assets, aligning with the broader objectives of IAM frameworks. As technological advancements reshape data management landscapes, the convergence of blockchain and IAM systems emerges as a compelling approach to authenticate heightened data integrity and secure access controls in an evolving digital era.

4.3. Increased Transparency

Transparency is a crucial aspect within Blockchain in IAM Systems. Technologies like blockchain play a significant role in enhancing transparency. An example of this is evident in agricultural sectors, where permissioned blockchains not only provide tamper-resistant functionalities but also integrate various designated services into a comprehensive solution, as documented in relevant literature [14]. Additionally, exploring the intricate corridors of a Health Data Marketplace (HDM) in the Norwegian e-health panorama, one cannot help but discern the salience of transparency [5]. This domain carefully tackles both the inherent limitations and the roles played by stakeholders, from Platform Operators to Legal Authorities, in orchestrating a health data exchange platform that appears seamless and ethically aligned. The deliberate integration of blockchain into IAM systems could similarly enhance transparency. This enhancement could potentially foster newfound trust and compliance in the often complex realm of data management practices.

5. Use Cases of Blockchain in IAM Systems

5.1. Self-Sovereign Identity

In digital identity management, the concept of self-sovereign identity marks a notable departure from traditional approaches, emphasizing individual autonomy over personal data. Leveraging blockchain in such models aims to create secure, immutable, and decentralized infrastructures, where individuals have sole control over their identity elements. Integrating this technology into IAM systems is expected to enhance both the security protocols for data and the transparency in identity-based transactions [2].

Scholarly discussions highlight the need for balance between technological advancements, organizational readiness, and environmental factors in identity management. Despite promising discussions, implementation faces challenges like interoperability issues and privacy concerns. However, the adoption of distributed identity management models within organizational frameworks suggests a shift towards more efficient, user-centric identity ecosystems. As digital identification evolves, embracing self-sovereign identity principles through blockchain technology could lead to significant reforms in IAM, reshaping global identity management mechanisms.

5.2. Access Control Management

In discussions surrounding IAM systems, a noticeable shift is underway due to the emergence of Internet of Things (IoT) technologies and the growing acceptance of blockchain methodologies. Traditional IAM frameworks face challenges stemming from IoT complexities and the diverse digital service federations [3]. Blockchain's decentralized nature has the potential to revolutionize access control management by enhancing security, transparency, and immutability. Leveraging blockchain attributes, organizations can overcome limitations of centralized IAM infrastructures, establishing robust, scalable solutions crucial for protecting informational assets' confidentiality, integrity, and availability. Integrating blockchain into existing IAM frameworks may drive the adoption of new security controls to mitigate risks, enhancing the sophistication of access control management in the ever-evolving digital landscape.

5.3. Identity Verification Processes

In the realm of blockchain-integrated IAM systems, particularly with the rise of Internet of Things (IoT) frameworks, there's been a notable shift in identity verification methodologies. Traditional IAM architectures are found lacking when confronted with the complexities of IoT components and federated digital platforms. This necessitates a move towards innovative paradigms like UniquID, a blockchain-based solution that promotes enhanced scalability and architectural robustness, diverging from centralized IAM models [3]. Furthermore, the combination of peer-to-peer cryptographic decentralization and advancements in zero-knowledge proof offers a promising avenue for credential management systems that prioritize privacy. This proposed system aligns credentials on-chain, following the W3C verifiable credential standard, demonstrating the potential of blockchain-enabled transparent paradigms while preserving user pseudonymity [15]. These advancements underscore the transformative impact of blockchain technology on enhancing the security and reliability of IAM infrastructures, marking the beginning of a new era in identity verification procedures.

6. Implementation Strategies for Blockchain in IAM Systems

6.1. Hybrid Models

In the complex landscape of applying blockchain to IAM Systems, the rise of hybrid models represents a significant approach to addressing interoperability challenges and evolving security vulnerabilities. Focusing on socio-technical issues emphasizes the need for innovative methodologies like hybrid constructs, which aim to improve interoperability while maintaining security within IAM frameworks [16]. These hybrid paradigms, combining various architectural strategies and remedial measures from different domains, help alleviate the complexities arising from the technological diversity inherent in IAM configurations. Additionally, discussions highlight the importance of robust governance structures and customized information security measures tailored to blockchain. By embedding blockchain principles, hybrid frameworks strengthen the confidentiality, integrity, and availability of informational assets, protecting IAM infrastructures from unauthorized access and tampering. Thus, the fusion of hybrid models and blockchain technology presents a promising opportunity to create resilient and secure IAM systems amidst the intertwined challenges of interoperability and security in the digital realm.

6.2. Access Control Management

Ensuring seamless interoperability between blockchain frameworks and traditional IAM systems is considered crucial in our current digital landscape. According to scholarly discussions, the integration of interoperability solutions can exacerbate existing challenges associated with combining different architectures. Additionally, the widespread adoption of blockchain across various sectors, alongside IAM implementations, highlights the need for robust security strategies to protect sensitive data [16].

To effectively integrate blockchain paradigms with existing IAM infrastructures, it's essential to bridge the gap between established norms and innovative blockchain techniques. Developing new information security measures tailored for blockchain applications enables organizations to mitigate risks while safeguarding the confidentiality, integrity, and availability of interconnected data. The adoption of interoperability, with a focus on security principles, is expected to enhance the functionality and trustworthiness of blockchain-infused IAM systems, fundamentally transforming digital identities and access management mechanisms.

6.3. Scalability Considerations

Exploring the intersection of Blockchain technology and IAM systems highlights the critical need for scalability. With blockchain being increasingly adopted across various sectors, robust scalability strategies become essential for IAM infrastructures. As organizations leverage blockchain for secure and decentralized identity management, scalability becomes crucial for accommodating growing transaction volumes and increasing user interactions.

Scholarly discussions on digital identity management emphasize the importance of flexible architectural frameworks and interoperable channels to facilitate seamless identity exchange across domains [17]. This highlights the relevance of scalability challenges within IAM ecosystems, underscoring the need for adaptable design paradigms capable of accommodating evolving user needs and expanding network scopes while ensuring integrity and security. Drawing insights from academic sources, IAM frameworks can embrace scalable approaches that align with the dynamic nature of blockchain integration dynamics, thereby avoiding potential bottlenecks and enhancing overall systemic efficiency.

7. Future Trends and Challenges

7.1. Regulatory Compliance

Navigating regulatory compliance in the utilization of blockchain within IAM systems is crucial for ensuring data integrity and protection. As institutions increasingly adopt blockchain paradigms in their IAM frameworks, adherence to regulatory frameworks becomes essential for safeguarding user privacy and ensuring data confidentiality.

Drawing insights from relevant legal judgments and potential legislative trends can inform compliant data exchange methods within IAM systems. Additionally, considering the concept of investment in watershed services (IWS) underscores the importance of directing investments towards nature-centric solutions while emphasizing the need for regulatory compliance to protect IAM systems from emerging threats [18]. Aligning IAM deployments with regulatory requirements, coupled with embracing innovative approaches from diverse industries, enables organizations to enhance their data security protocols while ensuring ethical and secure management of user identities [19].

7.2. Evolution of Blockchain Technology

In the context of modern technological advancement, blockchain technology stands out as a crucial innovation, extending beyond conventional financial transactions. Recent scholarly research highlights its increasing utilization in safety-critical cyber-physical systems, including autonomously navigated vehicles and smart power distribution networks. This adoption aims to address specific challenges while enhancing operational efficiency [20].

Moreover, blockchains are increasingly being utilized in identity governance and metadata archival processes, demonstrating a strategic approach to enhancing data security and privacy within blockchain infrastructures. This dual evolution emphasizes the dynamic nature of blockchain technology, where advancements in safety-critical systems intersect with the need for strengthened IAM solutions [21]. By intelligently integrating blockchain's foundational principles with the evolving landscape of digital identity protection, IAM systems can effectively harness blockchain's inherent security features to establish a foundation of trust, transparency, and operational efficiency in data management processes. This convergence illustrates the transformative potential of blockchain technology in enhancing security frameworks and functionality within complex digital ecosystems.

7.3. Integration with Emerging Technologies

The integration of blockchain technology with emerging innovations like machine learning and artificial intelligence holds significant potential to revolutionize IAM systems. Leveraging the capabilities of these cutting-edge technologies, IAM frameworks could improve security, authentication methods, and data protection [21].

Machine learning algorithms, for example, could enhance the accuracy and speed of monitoring bio-dynamic processes, thereby contributing to the development of more robust and efficient IAM solutions. Additionally, the application of machine learning in biosensors could increase sensitivity and selectivity, strengthening identity validation protocols within IAM systems. The adoption of these advanced technologies represents a comprehensive strategy for enhancing security and data management within IAM structures, leading organizations toward a digital ecosystem that is more inclusive and secure. As organizations navigate the complexities of technological advancement, the synergy between blockchain, machine learning, and artificial intelligence offers a transformative approach to fortifying IAM systems and safeguarding sensitive data.

8. Conclusion

8.1. Recap of the Importance of Blockchain in IAM Systems

Blockchain plays a foundational role in IAM frameworks, providing a secure and transparent platform for managing user identities and access privileges. Leveraging its decentralized nature, blockchain enhances security, privacy, and trust in digital interactions.

The integration of blockchain technology has the potential to mitigate compliance risks associated with cloud deployments, establishing a robust foundation for regulatory compliance. Furthermore, combining emerging technologies like artificial intelligence with blockchain within IAM systems strengthens authentication mechanisms and protects sensitive data [22]. Overall, blockchain's significance in IAM systems lies in its ability to revolutionize identity authentication processes, access management, and data protection, paving the way for resilient and efficient digital infrastructure for organizations.

8.2. Summary of Benefits and Challenges

Scholarly discussions emphasize the positive impacts of integrating supply chain analytics for small and medium enterprises (SMEs), such as improved transparency, cost reductions, and optimized resource allocation. However, several challenges hinder the successful implementation of such initiatives. These challenges include acquiring necessary resources, enhancing cognitive capabilities, and managing organizational transformations, which collectively pose significant obstacles for SMEs venturing into supply chain analytics projects.

Furthermore, discussions about the economic impacts of climate change highlight the need to transition to a less carbon-intensive economic model, emphasizing the importance of integrating environmental sustainability into supply chain operations. Given the evident benefits of analytics in supply chain management, SMEs must navigate through challenges while adapting to changing environmental conditions to maximize the benefits of such technological advancements.

8.3. Recommendations for Future Research

Undertaking scholarly research in the field of Blockchain for IAM Systems highlights the need for future investigations to enhance understanding of equity and access issues often overlooked by traditional study parameters. It is strongly suggested that future inquiries into IAM systems adopt an inclusivity-focused approach. Using qualitative methodologies to analyze the various factors influencing equity can provide a deeper understanding of the complex dynamics at play. Additionally, aligning research methodologies with standardized diagnostic criteria and improving methodological quality can facilitate the development of more effective and insightful solutions to address equity challenges within IAM infrastructures. By adopting a multidimensional analytical framework that considers strategies at both policy and individual levels, future scholarly endeavors in this area can effectively contribute to promoting equitable practices and expanding access within IAM systems.

Summarizing the reflections on the integration of blockchain technology into IAM frameworks brings forth several important considerations. Cross-disciplinary inquiries shed light on the significant impacts of avant-garde strategies on outcomes and educational achievements. Additionally, discussions around normative frameworks emphasize the need to reconcile conflicting intellectualizations to advance complex ideological constructs. These discussions highlight both challenges and opportunities in adopting blockchain within IAM infrastructures. By leveraging interdisciplinary insights and resolving normative conflicts thoughtfully, organizations can enhance cybersecurity defenses, improve user authentication methods, and streamline identity management operations. Therefore, a discerning and tactful deployment of blockchain innovations within IAM paradigms is crucial for optimizing their utilities and addressing accompanying ethical considerations effectively.

References

[1] S. S. Galazova and L. R. Magomaeva, “The Transformation of Traditional Banking Activity in Digital,” International Journal of Economics and Business Administration, vol. VII, no. Special Issue 2, pp. 41–51, Jan. 2019, doi: https://doi.org/10.35808/ijeba/369.

[2] Nicolae Sfetcu, Philosophy of Blockchain Technology - Ontologies. MultiMedia Publishing, 2019. doi: https://doi.org/10.58679/mm73548.

[3] A. Giaretta, S. Pepe, and N. Dragoni, “UniquID: A Quest to Reconcile Identity Access Management and the IoT,” Software Technology: Methods and Tools, pp. 237–251, 2019, doi: https://doi.org/10.1007/978-3-030-29852-4_20.

[4] Tim Van hamme et al., “Frictionless Authentication Systems: Emerging Trends, Research Challenges and Opportunities,” arXiv (Cornell University), Sep. 2017.

[5] M. Erdvik and K. Intaraphasuk, “Mapping the Path to a Health Data Marketplace in Norway: An Exploratory Case Study,” uia.brage.unit.no, 2023. https://hdl.handle.net/11250/3082720

[6] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, "A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology," IEEE Xplore, Sep. 01, 2018. https://ieeexplore.ieee.org/document/8656968

[7] R. Xu, X. Lin, Q. Dong, and Y. Chen, "Constructing Trustworthy and Safe Communities on a Blockchain-Enabled Social Credits System," Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Nov. 2018, doi: https://doi.org/10.1145/3286978.3287022.

[8] N. LeBlanc, "An Analysis and Enumeration of the Blockchain and Future Implications," Jan. 2020.

[9] D. Amo, D. Fonseca, M. Alier, F. J. García-Peñalvo, and M. J. Casañ, "Personal Data Broker Instead of Blockchain for Students' Data Privacy Assurance," Advances in Intelligent Systems and Computing, pp. 371–380, 2019, doi: https://doi.org/10.1007/978-3-030-16187-3_36.

[10] O. Terzo, P. Ruiu, E. Bucci, and F. Xhafa, "Data as a Service (DaaS) for Sharing and Processing of Large Data Collections in the Cloud," 2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, Jul. 2013, doi: https://doi.org/10.1109/cisis.2013.87.

[11] R. K. Dash, N. R. Jennings, and D. C. Parkes, "Computational-Mechanism Design: A Call to Arms," dspace.uohyd.ac.in, Nov. 2003, Available: https://dspace.uohyd.ac.in/handle/1/6227

[12] M. S. Kiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing," Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 5, pp. 731–760, Jun. 2016, doi: https://doi.org/10.1007/s12652-016-0385-0.

[13] I. Gutierrez-Aguero, S. Anguita, X. Larrucea, A. Gomez-Goiri, and B. Urquizu, "Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum," IEEE Access, vol. 9, pp. 108912–108923, 2021, doi: https://doi.org/10.1109/access.2021.3101302.

[14] F.-J. Ferrández-Pastor, J. Mora-Pascual, and D. Díaz-Lajara, "Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production," Journal of Industrial Information Integration, vol. 29, p. 100381, Sep. 2022, doi: https://doi.org/10.1016/j.jii.2022.100381.

[15] J. Heiss, R. Muth, F. Pallas, and S. Tai, "Non-disclosing Credential On-chaining for Blockchain-Based Decentralized Applications," Lecture notes in computer science, pp. 351–368, Jan. 2022, doi: https://doi.org/10.1007/978-3-031-20984-0_25.

[16] Rita, P. H. Valle, K. S. Santos, and E. Y. Nakagawa, "Systems Interoperability Types: A Tertiary Study," ACM computing surveys, Apr. 2024, doi: https://doi.org/10.1145/3659098.

[17] Anar Bazarhanova and K. Smolander, "The Review of Non-Technical Assumptions in Digital Identity Architectures," Proceedings of the ... Annual Hawaii International Conference on System Sciences, Jan. 2020, doi: https://doi.org/10.24251/hicss.2020.785.

[18] G. Bennett, C. Nathaniel, and A. Leonardi, Gaining Depth State of Watershed Investment 2014. Forest Trends Ecosystem Marketplace, 2014.

[19] N. Ghadge, "Enhancing threat detection in Identity and Access Management (IAM) systems," International Journal of Science and Research Archive, vol. 11, no. 2, pp. 2050–2057, 2024, doi: https://doi.org/10.30574/ijsra.2024.11.2.0761.

[20] C. Berger, B. Penzenstadler, and Olaf Drogehorn, "On using blockchains for safety-critical systems," arXiv (Cornell University), May 2018, doi: https://doi.org/10.1145/3196478.3196480.

[21] T. Faisal, N. T. Courtois, and Antoaneta Serguieva, "The Evolution of Embedding Metadata in Blockchain Transactions," Jul. 2018, doi: https://doi.org/10.1109/ijcnn.2018.8489377.

[22] T. Weber, A Generic Approach for the Automated Notarization of Cloud Configurations Using Blockchain-Based Trust. Springer Gabler Wiesbaden, 2023. doi: https://doi.org/10.1007/978-3-658-42844-0.