International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

BLOCKCHAIN-BASED IDENTITY VERIFICATION (DECENTRALIZED IDENTITY VERIFICATION)

Sri Kanth Mandru
Mandrusrikanth9@gmail.com

Abstract

The paper presents decentralized systems for identity verification based on a promising technology like blockchain, and its disruptive capabilities are discussed. It, therefore, implies that there must be a better, more efficient, effective, and secure way of identifying people than through centralized identification systems because of the problems faced, such as insecurity and invasion of privacy. Another critical characteristic of a blockchain type of data availability is that it is decentralized, immutable, and protected by cryptography, and its use gives its owners more data control. The paper's findings show more control over the persona, lower operational costs, and lower chances of fraud when the identity is created on blockchain technology. The potential expected effects include increased confidence levels in making online contacts, where many activities are eased out through different sectors of the economy and the building blocks of a solid and people-focused digital economy put in place.

Keywords: Blockchain, Decentralized identity, Identity verification, Attestation

I. INTRODUCTION

The usefulness of every Internet-related business and communication depends on processes verifying the parties' identity. However, they are also accompanied by certain disadvantages from constructing and maintaining centralized conventional systems. This makes the sharable databases open to hacker attacks, and the user may lose valuable information, diminishing their confidence in the system. Also, it requires other costly and time-consuming verification processes in most cases, which can be very uneconomical and unpalatable to users. That is why applying such a distributed verification system as blockchain can be considered promising [1]. That is why decentralization, immutability, and some peculiarities of cryptography applications in blockchain introduce a solution for Digital Identity management.

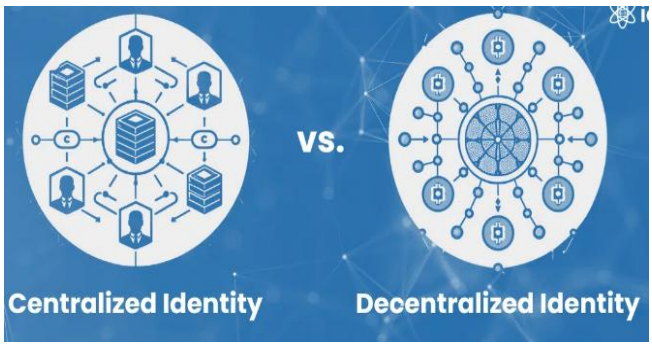

Figure 1: Centralized vs. Decentralized Identity [1].

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

In this regard, the blockchain is beneficial in that it is connected with the very essence of how it functions. The principle of consensus is designed to remove intermediaries and provide secure, private transactions directly between users while returning the sovereignty over it to the users.

This research proposes an analysis of the possibilities of the identity verification system using blockchain. The article further elaborates on how this technology, which is still relatively unknown to the public and the media, can increase data protection and liberate processes from misunderstanding and failings of centralization [2]. These will include the current adoption scenarios, trends in technology, the effects on society, and overall impacts in different sectors. Accordingly, our study aims to share an understanding of how blockchain may shift identity management practices by focusing on such areas and helping to create a safer environment where people can perform operations on the Internet.

II. PROBLEM STATEMENT

Several problems reduce the efficiency and reliability of the traditional ways of identity proving with some risks, including security risks where some security issues have been noted. This is a vulnerability that hackers would go for because a lot of information is put in large centralized servers [3]. As it is evident, forms of fraud and scams, such as Identity theft, have made people so much more vulnerable due to occurrences like the Equifax hack.

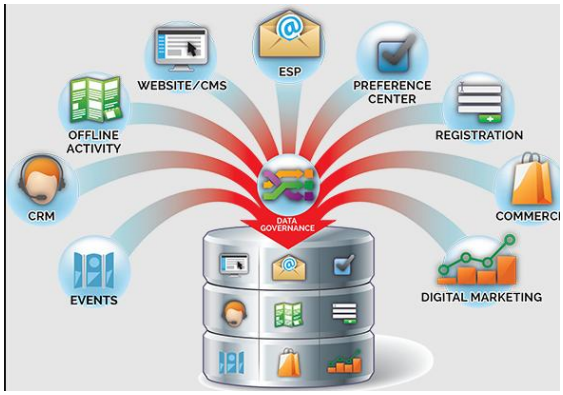

Figure 2: Vulnerabilities of Centralized Database [3].

The current systems are also not distinguishable from many problems about privacy. Increasingly, a paradigmatic centralized agency of this kind acquires and stores vast quantities of personal data; as such, the Twin Dilemmas of data abuse and use consent arise again. The problem, therefore, stems from the outcome where all information is concentrated and the kind of exposure people will be put into positions that make them vulnerable and, thus, prone to exploitative situations.
Another effect is that the country's economy is centrally controlled by one or more central people or companies. This is because users employ the services of these companies for identity management and verifications, and therefore, there is always the element of risk. That, especially when these agencies were unclear or inefficient, may have caused these delays [4]. Excessive spending and poor output worsen if the situation is not bad enough. Of course, there is an inherent downside to conventional online identity verification solutions based on documents and other forms of physically administered biometric tests: the approach can raise operating costs and slow

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

down time. Such inefficiencies are more apparent and expensive, and organizations need to create identities to fit the rules, which is evident in the financial sector. Some of these difficulties are highlighted below. As discussed above, Equifax, in the year 2017, faced a data breach in which it was invaded, and the identity of approximately 147 million customers was put at risk [5]. The Facebook data scandal could be another excellent example of how centralized corporate structures take advantage of users' information and why privacy is an issue. These cases prove that decentralization must be improved, and the identity verification system is even more secure when using blockchain, so the discussion moves on.

III. SOLUTION

A. Blockchain-Based Identity Verification

Analyzing the main principles of blockchain, such as decentralization, non-interference, and consensus mechanisms, it is possible to conclude that the given technology satisfactorily solves the existing identification problems at the current level of its development. This minimizes the tendency for failure in the various entities in a network and makes the system more robust since there is central control of the whole network in a star topology.

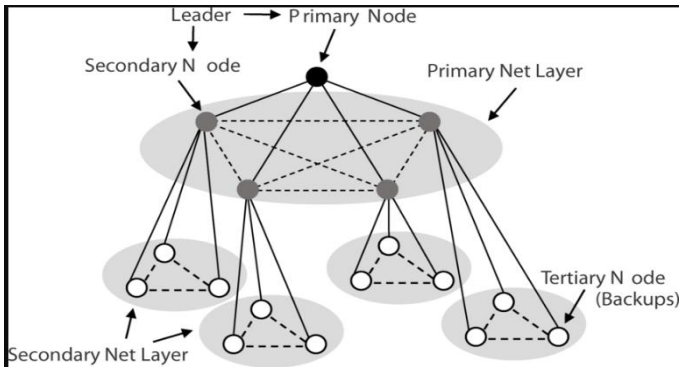

Figure 3: Structure of consensus mechanism [5]

B. Types of blockchains

Some of the various forms blockchains may take include consortium or permissioned, private, and public. Ethereum, Bitcoin, and all the above flows are implemented in open blockchains that allow anyone to observe all the transactions.

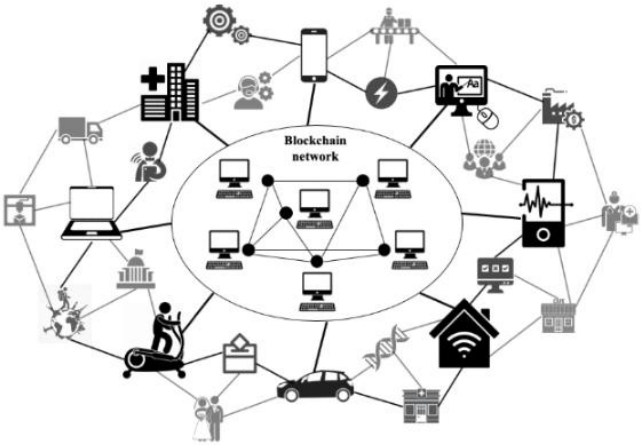

Figure 4: Blockchain with the decentralization [6].

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

Private blockchains give customers more privacy since they can be created with restricted accessibility to specific participants. Consortium blockchains refer to hybrid ledgers, which are regulated whereby the degree of control and openness are midway between fully public and fully private. Several organizations run them. The following are some organizations that operate these centers.

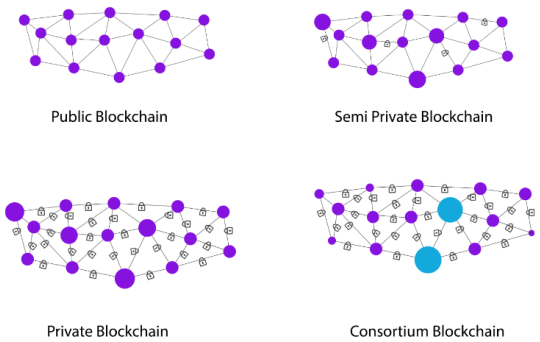

Figure 5: Types of Blockchain Technology [6].

Blockchain removes existing problems with centralized identification methods and leverages decentralized attestation, improved security, and the ultimate authority of end-users. Cryptography procedures like Public Key and Private Key are among the most widely used security standards that guarantee identification data cannot be accessed or viewed by unauthorized individuals. This means that instead of services getting users to give out what they desire and their identities, it will be up to the users to determine what they want to share and with whom, which reduces privacy invasion and the possibility of users being taken advantage of.

C. The technical architecture of a blockchain-based identity verification system

The components that form a technical implementation of a blockchain-based identity verification system include verified credentials, intelligent contracts, and DIDs [7]. Smart contracts are digital contracts in which the contract terms are encoded on a blockchain; such contracts are fully automated and do not involve third parties.

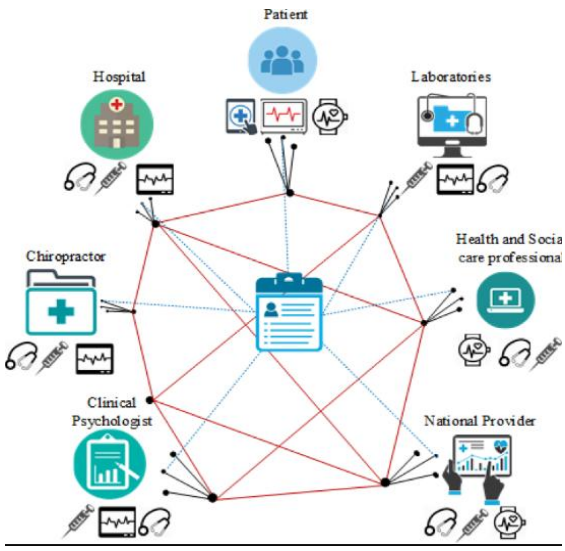

Figure 6: Blockchain architecture for the e-ID system [7].

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

DID is a unique identification number that allows people to own and control their unique identity on the Internet without relying on a superuser [8]. The type of credentials that may, in turn, be guaranteed through cryptography to ascertain that the assertion of identification data is genuine and that the data has not been tampered with is known as verifiable credentials.

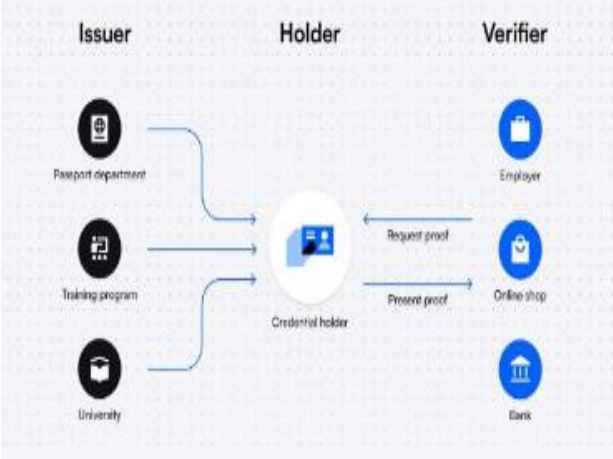

Figure 7: Blockchain-Based Certificate Verification System [9].

By implementing the above elements, blockchain-based identity verification solutions mitigate the nuisances and inconveniences associated with current identity verification procedures and provide a more personal, secure, and quick method than traditional methods.

IV. USES

Blockchain in business identity verification suits various industries and significantly advances existing solutions. It enriches interacting with a client from the financial services sector by safely identifying, minimizing the risk, and complying with the KYC and AML standards. For instance, the Swiss-based financial service firm UBS conducted research on the usage of blockchain technology in the identification process to increase security and make all the processes faster Maybe there is a sense of managing patient identification issues more privately and securely in healthcare. Blockchain offers higher levels of data and patient privacy since it makes medical records more effective and accessible to the appropriate people [10]. Therefore, the use of blockchain technology, if properly embraced, has the potential to revolutionize the provision of healthcare solutions.

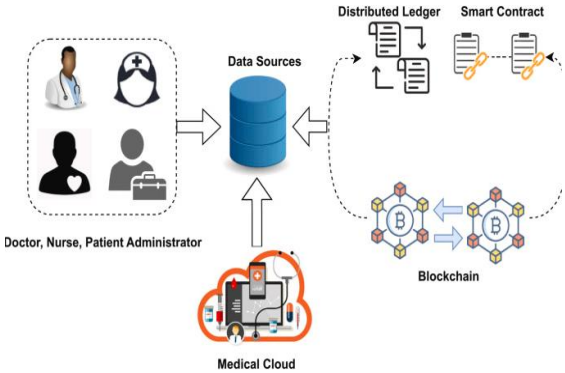

Figure 8: Blockchain for healthcare systems [10].

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

Blockchain can help government agencies safely and openly manage citizens. This includes digital voting systems where, through blockchain, vote gerrymanders, voter identification, and authentication are assured, reducing fraud levels and increasing people's support in political processes. Zug, a town in Switzerland, also dubbed the 'Cr'pto Valley,' has trialed an electronic election via the blockchain. In education, it can be applied to verify the authenticity of academic certificates to minimize forging cases and make ascertaining the certificates easier [11]. The Digital Diploma project implemented by MIT guarantees the sustainability and credibility of academic data using blockchain certificates.

Regarding application or implementation, the technology can be used to verify the users' entities in trading activities through blockchain technology, which most trading companies use to reduce the chances of fraud and build trust between buyers and sellers. For example, Alibaba has recently initiated an anti-counterfeit application of the blockchain project, which can show user and product identification through the blockchain platform. Blockchain outperforms traditional solutions because we observe how decentralized technology allows users to manage their data when verifying identities. In light of this, the following advantages prepare the stage for blockchain to become a disruptive technology in different industries.

V. IMPACT

A. Benefits of Decentralized Identity Verification

Industries use blockchain to decentralize data, encryption, and digital storage, enhancing security and privacy. This means that personal data must be transmitted and encrypted. Thus, the data cannot be easily hacked or duplicated by an unauthorized person and helps to reduce cases of theft, among others. The users retain the ownership of submitted information throughout the process by only providing the ID fields for a unique identification process while leaving out the other fields that may hold sensitive information. The blockchain system reduces emulation, fraud, and identity theft since it does not include middle agents and controlling organizations [12]. Hence, the chronicity of records also ensures that documents cannot be forged; this gives people more confidence in online deals since it is impossible for someone to pretend to be somebody else. It also aims to decentralize the identity verification process, which improves efficiency and, consequently, the observance of costs. The operations are efficient, and people and companies benefit when all the other procedures and paperwork are taken out. There is evidence that one of the leading performers enjoys a high appreciation of the power, and it can be noted that they are empowered to work in the position. This is an example of blockchain principles of self-sovereign identity, as these people are handed control over identity controls [13]. The operational tasks can be considered enabling value, for they make digital transactions more autonomous and reliable. The user can handle several accounts across different platforms by performing the tasks.

B. Potential Challenges and Risks

Another technical negative aspect of using blockchain networks is that such networks have specific restrictions regarding the number of transactions and the size of the corresponding networks [14]. Data protection laws, laws that demand identification, and jurisdictions are among the laws that lead to challenges during implementation. It has also been in the best interest of the generality of the application context that privacy should not be an absolute impediment to legal responsibilities. Consequently, for the blockchain to be mainstreamed, this paper aims to demonstrate how blockchain solutions can integrate with other systems. However, a persistent source of concern is

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

the specification of the reference models that could allow the integration and exchange between a minimum of two of the methods [15]. However, decentralized identity verification is fun and has cool features like increased security; fewer failed attempts, the taxpayer saved, and user autonomy. To enable the full potential of blockchain for identity verification, we need to analyze and solve three problems: integration, legal, and technology.

VI. SCOPE

- In recent years, due to growing concerns about data privacy and security, many sectors, such as health care, government, and even the finance and banking sectors, have considered using blockchain mainly for identity identification.
- There is a lack of similar large-scale studies, and most pilot studies and projects that have been conducted provide empirical evidence of applicability in real-world settings.
- It is still in its infancy due to technology and policy constraints for which its use has formally been relegated to such a state.
- It is expected that any future progress will be made with deploying blockchain technology for identity verification [16].

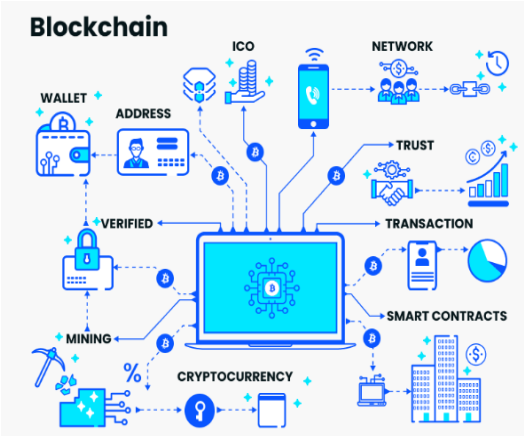

Figure 9: Impact of Blockchain on Fintech [16]

- This is why scalability and transaction rate optimizations occur through work on improving the blockchain architecture and the consensus algorithms in their pursuit of the same goal.
- User interface and cooperation solutions are also progressing, and such tools will enhance usability and compatibility with numerous platforms.

A. Integration with Other Emerging Technologies

- Actualization of AI, IoT, or blockchains in identity verification results in better opportunities.
- To avoid identity fraud, the AI system may check for any irregularities in the data stored within the blockchain [17].
- Blockchain is for the secure and efficient transfer of data since the IoT devices can recognize and communicate with each other through the blockchain.

International Journal of Core Engineering & Management
Volume-6, Issue-10, 2020 ISSN No: 2348-9510

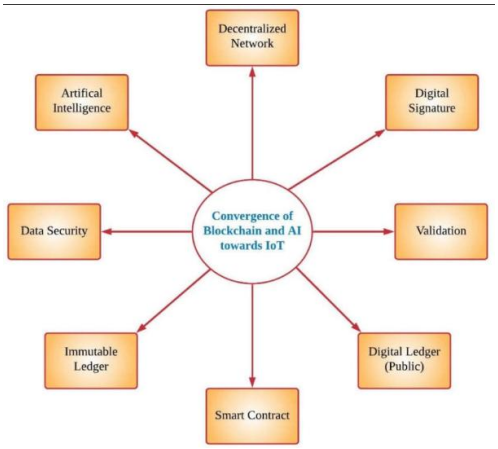

Figure 10: Integration of blockchain and Artificial Intelligence [18].

- The first focus area is the concept often referred to as scalability, With the advent of layer two solutions like state channel and side chains increasing transaction rate and throttling down the overcrowding of the main chain while retairetainingntralization [18].
- These are among the challenges under improvement in the current research and development to develop more consensus types and other practical ways of scaling off the chain.

B. Evolution of Standards and Frameworks

- Standardization activities are required to ensure that it can smoothly fit into the planned architecture and adhere to the policies laid down by the government in terms of rules and laws.
- The FOR is W3C and other agents that provide inputs towards developing standard specifications for DIDs and verified credentials to facilitate and encourage such massive use [19].
- These are also unfolding to establish governance and compliance guidelines to clear laws and protect the consumers.
- The potential application of the systems based on the blockchain for ID verification is in the new model of trust ownership of identity information [20].
- In achieving privacy, compliance makes the users powerful and also breaks down the operation cost in organizations due to enhanced security.
- To a great extent, broad use. The verification and management of identities in the upcoming years and decades and the appearance of such an application after the law changes are to be blockchain-regulated.

VII. CONCLUSION

- The principal problem of centralized identification systems is rooted in the fact that governments, corporations, or other authorities possessing power can abuse such control and manage access according to their preferences.
- Asolution that has been proposed as more feasible and effective is the blockchain identification solution.

- Previously, it has been demonstrated that due to decentralization, immunity, and cryptographic integrities, blockchain can improve data protection, minimization of fraudulence, and user control.
- These opportunities cover almost all fields, such as e-sales, telemedicine, administration, education, and financial services, proving the technology's vast popularity and significance.
- Technological advancement, regulation, and compatibility issues present risks; thus, the stakeholders must critically assess the pilot and partnerships.
- As for future development research, the attention is expected to follow the extension of the scalability prospects of blockchain, the improvement of the governance models for the systems, and the application of the idea to other technologies such as IoT and AI.
- The future combining of accumulated and enhanced technological advancement of the blockchain has emerged a new world of Identity and Trust management through creating more accessible, faster, and personalized digital interactions.

REFERENCES

1. S. E. Haddouti and M. D. E.-C. E. Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," Apr. 2019, doi: 10.1109/commnet.2019.8742375. Available: https://doi.org/10.1109/commnet.2019.8742375
2. A.Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-Based Identity Verification System," Oct. 2019, doi: 10.1109/icsengt.2019.8906403. Available: https://doi.org/10.1109/icsengt.2019.8906403
3. G. Malik, K. Parasrampuria, S. P. Reddy, and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Mar. 2019, doi: 10.1109/vitecon.2019.8899569. Available: https://doi.org/10.1109/vitecon.2019.8899569
4. A. A. Monrat, O. Schelen, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, vol. 7, pp. 117134–117151, Jan. 2019, doi: 10.1109/access.2019.2936094. Available: https://doi.org/10.1109/access.2019.2936094
5. S. Y. Lim et al., "Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey," International Journal on Advanced Science, Engineering and Information Technology/International Journal of Advanced Science, Engineering and Information Technology, vol. 8, no. 4–2, pp. 1735–1745, Sep. 2018, doi: 10.18517/ijaseit.8.4-2.6838. Available: https://doi.org/10.18517/ijaseit.8.4-2.6838
6. O. Avellaneda et al., "Decentralized Identity: Where Did It Come From and Where Is It Going?," IEEE Communications Standards Magazine, vol. 3, no. 4, pp. 10–13, Dec. 2019, doi: 10.1109/mcomstd.2019.9031542. Available: https://doi.org/10.1109/mcomstd.2019.9031542
7. D. Maldonado-Ruiz, J. Torres, and N. E. Madhoun, "3BI-ECC: a Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography," Sep. 2020, doi: 10.1109/brains49436.2020.9223300. Available: https://doi.org/10.1109/brains49436.2020.9223300
8. K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," Sep. 2020, doi: 10.1109/brains49436.2020.9223312. Available: https://doi.org/10.1109/brains49436.2020.9223312

9. Y. Li et al., "Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies," IEEE Network, vol. 33, no. 5, pp. 111–117, Sep. 2019, doi: 10.1109/mnet.2019.1800271. Available: https://doi.org/10.1109/mnet.2019.1800271
10. M. Kuperberg, "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/tem.2019.2926471. Available: https://doi.org/10.1109/tem.2019.2926471
11. Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," Journal of Network and Computer Applications, vol. 166, p. 102731, Sep. 2020, doi: 10.1016/j.jnca.2020.102731. Available: https://doi.org/10.1016/j.jnca.2020.102731
12. P. Yeoh, "Regulatory issues in blockchain technology," Journal of Financial Regulation and Compliance, vol. 25, no. 2, pp. 196–208, May 2017, doi: 10.1108/jfrc-08-2016-0068. Available: https://doi.org/10.1108/jfrc-08-2016-0068
13. M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060. Available: https://doi.org/10.1016/j.future.2019.02.060
14. V. Garcia-Font, "Blockchain: Opportunities and Challenges in the Educational Context," in Lecture Notes on data engineering and communications technologies, 2019, pp. 133–157. doi: 10.1007/978-3-030-29326-0_7. Available: https://doi.org/10.1007/978-3-030-29326-0_7
15. K. Pinter, D. Schmelz, R. Lamber, S. Strobl, and T. Grechenig, "Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms," in Lecture notes in business information processing, 2019, pp. 151–165. doi: 10.1007/978-3-030-30429-4_11. Available: https://doi.org/10.1007/978-3-030-30429-4_11
16. L. Argento et al., "ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability," Applied Sciences, vol. 11, no. 1, p. 165, Dec. 2020, doi: 10.3390/app11010165. Available: https://doi.org/10.3390/app11010165
17. W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography," Aug. 2019, doi: 10.1109/ccet48361.2019.8989361. Available: https://doi.org/10.1109/ccet48361.2019.8989361
18. M. Aydar and S. Ayvaz, "Towards a Blockchain based digital identity verification, record attestation and record sharing system," arXiv (Cornell University), Jan. 2019, doi: 10.48550/arxiv.1906.09791. Available: https://arxiv.org/abs/1906.09791
19. O. Dib and K. Toumi, "Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions," Annals of Emerging Technologies in Computing, vol. 4, no. 5, pp. 19–40, Dec. 2020, doi: 10.33166/aetic.2020.05.002. Available: https://doi.org/10.33166/aetic.2020.05.002
20. J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," IEEE Access, vol. 7, pp. 164908–164940, Jan. 2019, doi: 10.1109/access.2019.2950872. Available: https://doi.org/10.1109/access.2019.2950872