IVBlock: A Blockchain-based Digital Identity Verification System

Pragyan Budhathoki, Gaurab Upreti, Manish Giri, Aayush Yadav, Shahid Noor
{budhathokp1, upretig1, girim1, yadava3}@mymail.nku.edu, noors2@nku.edu
School of Computing and Analytics
Northern Kentucky University

***Abstract*—In today's digital age, a key challenge is the need for secure and reliable identity verification. Traditional methods, often relying on centralized authorities, are vulnerable to data breaches, privacy concerns, and inefficiency. For example, the 2017 Equifax breach exposed the personal data of over 147 million individuals, highlighting the risks of centralized data storage. Similarly, traditional identity verification methods in banking often involve lengthy processes prone to human error and fraud. These methods pose risks such as identity theft and lack of user control over personal data; for instance, studies show that identity theft affected over 42 million individuals in the U.S. in 2021 alone, highlighting the critical need for improved security measures. Therefore, we need to design a robust security and highly scalable framework to effectively address user privacy concerns. To address these challenges, we propose a blockchain-based digital identity verification system that leverages the immutability and transparency of blockchain technology. Our research provides a comprehensive discussion on the system's architecture, implementation, and potential challenges, paving the way for secure and decentralized identity verification frameworks. Our framework enhances data security, ensures user privacy, and fosters trust between stakeholders. The experiment's results demonstrate significant improvements in efficiency and enhanced security compared to centralized solutions.**

***Keywords*-Digital identity verification, Blockchain technology, Data security, User privacy.**

I. Introduction

In today's digital world, the need for secure and efficient identity verification has become more critical than ever. Every day, people share sensitive personal information online—whether it's for banking, healthcare, education, or social networking. However, these systems are often vulnerable to data breaches, fraud, and identity theft. Cybercriminals have made centralized identity management systems, typically controlled by a single authority, their prime targets. According to the 2023 Identity Fraud Report by Javelin Strategy & Research, identity fraud continues to rise, with over 15 million U.S. citizens impacted in 2022 alone [1]. Furthermore, traditional methods such as passwords, social security numbers, and identity cards are increasingly insecure due to advances in hacking techniques and social engineering. Given the increasing frequency of data breaches and identity theft incidents, there is a pressing need to develop a more secure, privacy-preserving, and efficient identity verification solution [2].

Blockchain technology has emerged as a potential solution to these problems due to its unique attributes of decentralization, transparency, and immutability. Blockchain is a distributed ledger technology that enables secure, transparent, and immutable recordkeeping without relying on a central authority. It works with a system of nodes that verify transactions by using consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS). This makes sure that data that is recorded on the blockchain can't be changed [3]. Blockchain's decentralized nature is key to its ability to solve identity management problems. Blockchain enables users to retain control over their personal data and selectively share it with verified parties, in contrast to traditional client-server-based centralized models that store personal information in a single location, leaving it vulnerable to hacking. This decentralized approach eliminates the need for a trusted intermediary and significantly reduces the risk of data breaches and unauthorized access [4, 5]. Blockchain also uses advanced cryptographic techniques to protect the integrity of data, ensuring that only authorized parties can access or modify sensitive information [6]. By providing a secure, tamper-resistant, and transparent system for digital identity verification, blockchain can revolutionize identity management in various sectors, including finance, healthcare, and government services [7, 8].

Despite the great promise of blockchain for secure identity verification, current solutions face several challenges that require attention. Firstly, many blockchain-based identity systems still rely on a central authority for initial identity verification. For example, the Sovrin Network, one of the leading blockchain-based identity solutions, depends on trusted validators to establish user identities [9]. This contradicts the decentralized nature of blockchain and can introduce single points of failure. Secondly, scalability remains an issue in blockchain-based identity management systems. As the number of users and transactions increases, blockchain networks may experience delays and high transaction costs, especially in public blockchains like Ethereum [10]. Thirdly, privacy concerns arise when it comes to storing sensitive identity information on the blockchain. Although blockchain is known for its transparency and immutability, ensuring that personal data is only accessible to authorized parties without exposing it to the entire network remains a challenge. Solutions like zero-knowledge proofs and off-chain storage have been proposed to mitigate these issues, but they still face limitations in terms of user adoption and integration [11]. Lastly, regulatory compliance is a significant challenge for blockchain-based identity systems. As many countries have strict regulations regarding personal data, such as GDPR in the European Union, ensuring that blockchain-based identity systems comply with these regulations is a complicated task [7, 12]. These gaps in current solutions highlight the need for more efficient, scalable, and privacy-preserving blockchain-based identity systems.

In this paper, we propose a blockchain-based digital identity verification system that addresses the challenges mentioned above. Our system employs a hybrid approach, where users store their identity information off-chain, and the blockchain records only the cryptographic proofs of this data. This reduces the strain on the blockchain network and ensures the privacy of sensitive data. We can automate the verification process using smart contracts, guaranteeing secure identity verification independent of a central authority. Additionally, we incorporate a decentralized identity framework where users can retain full control over their data. This approach enhances privacy, scalability, and security compared to existing centralized systems. To further enhance security, our solution uses zero-knowledge proofs, ensuring that personal data is not exposed during verification while still allowing verifiable claims to be made [13]. We believe this approach provides a more secure, scalable, and user-centric solution for digital identity management.

We may need to address a few potential challenges in our proposed framework. One of the primary challenges is the issue of scalability. Blockchain networks, particularly public ones, often face difficulties handling a large volume of transactions, which could result in slow processing times and high fees. To mitigate this, our system will use a hybrid blockchain model that balances the benefits of decentralization with improved performance. Another challenge is ensuring the adoption of blockchain-based identity systems by both users and service providers. Despite its advantages, blockchain technology is still relatively new, and there may be resistance to adopting it due to a lack of understanding or trust. Moreover, regulatory compliance remains a concern, especially as governments and institutions continue to develop legal frameworks for blockchain. Ensuring that our system complies with existing privacy laws, such as GDPR, is critical to ensuring its long-term success. Finally, integrating blockchain-based identity solutions into existing infrastructure can be complex and may require significant investment from businesses and government entities [6,29]. Overcoming these challenges will be essential for the widespread adoption of blockchain-based identity verification systems.

We structure the remaining portions as outlined below. The motive for our effort is addressed in Section II. Related work is presented in Section III. Our design is delineated in Section IV, followed by an exhaustive operational model in Section V. Our experimental results are presented in Section VI, followed by our conclusions in Section VII.

II. Motivation

Identity verification has become a major concern in the digital world, especially with the increase in online services. Cyberattacks, hacking, and data breaches pose a significant threat to traditional identity systems, which store personal data in centralized databases. According to Javelin Strategy & Research (2020), identity fraud resulted in over $43 billion in losses, highlighting the security risks of centralized models [14]. These systems rely on intermediaries and central authorities to verify identities, which often leads to inefficiencies and trust issues. As a result, ensuring secure, user-controlled verification methods has become essential [15]. Failure to address these security and privacy concerns can lead to widespread financial losses, data misuse, and erosion of user trust in digital systems, making this problem critical to resolve.

Our project aims to address these challenges by utilizing blockchain technology to create a decentralized digital identity verification system. Blockchain provides a tamper-proof and transparent ledger, allowing users to control their data without relying on third parties. This decentralization mitigates the risks of data breaches and unauthorized access, making it a safer alternative to traditional systems [16]. By removing intermediaries and utilizing blockchain's inherent transparency, the system ensures that identity data remains secure, verifiable, and under the user's control [17]. Consider an example where an individual applies for an online loan. Sensitive documents like passports or social security numbers, submitted in a traditional system, pose risks of interception or fraud. Our blockchain-based system securely verifies the user's identity by storing data on the blockchain, preventing any tampering. The lender can verify this identity instantly through a smart contract, ensuring accuracy and reducing the potential for fraud. This streamlined process not only improves security but also minimizes operational delays and costs [18].

Our approach is novel because it combines blockchain's decentralized and immutable ledger with real-time verification through smart contracts, providing a solution that is more secure, efficient, and transparent than traditional systems [13].

III. Related Work

Researchers have extensively explored blockchain technology to address challenges in digital identity verification, particularly in mitigating issues like data breaches, identity theft, and lack of user control over personal information. Decentralized frameworks have been proposed to allow users to control their identity data, eliminating reliance on centralized authorities and enhancing security [15, 18]. Smart contract-based systems ensure privacy, enable secure identity authentication, and maintain data transparency and immutability. [19, 20]. Despite their potential, these systems face challenges such as scalability, integration with existing infrastructures, and regulatory compliance, requiring further research into optimization techniques and legal frameworks [21, 22].

Different sectors have investigated applications of blockchain technology. In cloud computing environments, decentralized identity management systems address security concerns associated with centralized systems by enabling secure and tamper-proof identity updates [19, 23]. The Internet of Things (IoT) benefits from blockchain-based identity management frameworks that ensure secure device identities and verified data transactions, though IoT device computational power remains a limitation. [15]. In the banking sector, decentralized systems combined with biometric authentication reduce fraud and enhance security, [24]. E-commerce platforms leverage blockchain for seamless and fraud-resistant user authentication, ensuring user control over personal data [25, 26]. Healthcare systems use blockchain to allow patients to control access to their medical data, improving privacy and access accuracy [27]. Online voting frameworks employ smart contracts for secure voter identity verification and vote recording, though scalability remains an issue for large-scale implementation. [28]. Government identity systems utilize blockchain for secure and efficient identity management, emphasizing transparency and auditability [22]. Blockchain also enhances security and operational efficiency in cross-border financial transactions by providing universal digital identities ([29]). Foundational studies have laid the groundwork for blockchain technology in digital identity management, identifying its potential to address security, privacy, and trust issues. [17].

Studies have identified several common drawbacks for blockchain-based identity solutions, despite their substantial benefits in terms of privacy, security, and transparency. Many of the systems proposed face issues related to the scalability of blockchain, especially when handling large volumes of transactions. [15, 26]. Integration with Legacy Systems Another recurring issue is the challenge of integrating blockchain solutions with existing centralized infrastructures, which may involve substantial upfront costs and technical complexity. [21]. Regulatory Compliance Several papers mention the difficulty of ensuring compliance with regulatory frameworks, particularly concerning data privacy laws such as GDPR ([22]). User Adoption The slow adoption of blockchain-based identity systems can be attributed to user unfamiliarity with the technology and the requirement for additional infrastructure, as noted by Ahmed et al. [18] and Vellaneda et al. [31].

IV. Conceptual Architecture

The architecture of the Blockchain-based Digital Identity Verification System is designed to provide a secure, decentralized, and transparent mechanism for managing digital identities. This system ensures that users retain control over their personal information while simultaneously enabling secure interactions with third-party services. The architecture is built on several interconnected components, each of which plays a critical role in enabling seamless and trustworthy identity verification. Figure 1 depicts a conceptual architecture of our model.

A. User Interface (UI)

The User Interface serves as the primary point of interaction for users who wish to manage and interact with their digital identities. Through the UI, users can create new identities, modify their existing data, and set privacy preferences. The UI interacts with the blockchain network to fetch verified identity details, ensuring that users can access their information in a secure and user-friendly manner.

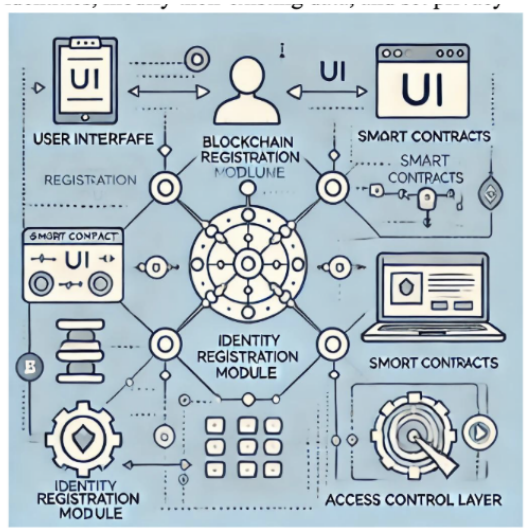

Fig. 1: Conceptual Architecture

B. Blockchain Network

The blockchain network is the backbone of the system, where all identity-related data is securely stored and managed. By utilizing a permissioned blockchain, the system ensures that only authorized entities can validate and record transactions related to identity verification. This approach minimizes the risk of unauthorized access and tampering. Each identity transaction—whether it's the creation, update, or verification of user data—results in a blockchain record, which cannot be altered once confirmed, ensuring the integrity and immutability of the data.

C. Smart Contracts

Smart contracts are used to automate identity-related processes, such as dentity verification, data validation, and access management. Once a user submits their identity information, the smart contract executes predefined rules to validate this data against trusted sources (e.g., government databases, biometric systems). This process reduces human intervention and ensures that identity verification is consistent, accurate, and compliant with privacy regulations. Smart contracts also ensure that users' consent is obtained before sharing their data with third-party services.

D. Identity Registration Module

The Identity Registration Module handles the initial process of creating a digital identity. When a user registers their information, this module hashes their personal details and stores them securely on the blockchain. The registration process may involve verifying the authenticity of the user's information using biometrics or government-issued identification. Once registered, the identity is securely linked to the user's private key, which ensures that only the user can modify or update their information.

E. Access Control Layer

The Access Control Layer governs who can access and view the user's identity data. This layer ensures that the user has full control over their personal information, enabling them to grant or revoke access to third-party applications and services. For instance, a user may allow a bank to verify their address but restrict a healthcare provider from accessing sensitive data such as their medical history. The access control layer is managed through cryptographic techniques that enforce privacy and security, ensuring that only authorized parties can access specific parts of the user's identity data.

The system operates in a manner that ensures security, transparency, and user control. When a user first interacts with the system, they provide personal information through the User Interface, which is then hashed and securely stored on the blockchain through the Identity Registration Module. If the user needs to verify their identity, they can request the Identity Verification Module to cross-check their information with trusted data sources. The verification process is automated via smart contracts, which validate the identity without requiring manual intervention. Once the identity is confirmed, users can grant or deny access to their data through the Access Control Layer, allowing third-party applications to authenticate users based on the verified identity.

In this architecture, blockchain technology provides several key advantages: immutability, transparency, and decentralization. The decentralized nature of the blockchain eliminates the need for a central authority, reducing the risk of data breaches and unauthorized access. Moreover, because the blockchain records are immutable, users can be assured that their data has not been tampered with, thus enhancing trust in the system.

The system's modularity allows for future scalability and the integration of additional services, such as multi-factor authentication or support for various types of biometric data. By incorporating blockchain, smart contracts, and oracles, this architecture offers a robust and efficient solution for digital identity management in an increasingly interconnected world.

V. Operational Model

The overall design follows a modular architecture that breaks down the system into distinct components, each responsible for handling a specific function. The system uses a hybrid approach combining blockchain's immutability for storing sensitive identity data and a user-friendly interface to enable seamless interaction. These components are: Identity Registration and Authentication: This component allows users to register their identity and authenticate themselves. It leverages blockchain to store encrypted personal information, ensuring data integrity and security.

A. Smart Contract for Verification

The blockchain will be used to deploy smart contracts that automate the verification process when a user attempts to authenticate. These contracts can validate user details like their identity, eligibility, and status.

B. User Interface

The front-end application is designed for both mobile and desktop users, offering a smooth interface for identity management, registration, and verification. It will allow users to securely upload their documents and interact with blockchain-based verification features.

C. Blockchain Network

The blockchain network will store identity data securely. It ensures decentralization and prevents unauthorized access to sensitive information. This network will also handle smart contract execution for verification. The core logic for verifying identity involves the use of smart contracts on the blockchain (algorithm 1. The process involves checking whether the user's identity data is stored in the blockchain and comparing it with the data submitted during the authentication attempt.

Algorithm 1: Smart Contract for Identity Verification

Input: $User\{Id, Name, DOB, GovtID\}$
Output: Verification result (approved or denied)
Retrieve user's identity U from blockchain ledger
if $User.Identity == null$ **then**
  return "User Not Registered"
end if
if $User.Id == U.Id \&\& User.Name == U.Name \&\& User.DOB == U.DOB \&\& User.GovtId == U.GovtId$ **then**
  return "Verification Successful"
end if
return "Verification Failed"

D. Protocols/Strategies

Several protocols and strategies are employed to ensure the security and efficiency of the system:

a) Identity Registration Protocol: The user's identity is first registered on the blockchain. This registration includes capturing encrypted personal data and submitting it to a smart contract for storage. The encryption ensures that the personal data is securely stored and can only be decrypted by authorized parties. The user is provided with a unique identifier that can be used for future authentication

b) Authentication Protocol: When a user attempts to authenticate, they provide their credentials, which are cross-checked against the data stored in the blockchain. Our algorithm (2) uses a zero-knowledge proof (ZKP) protocol to authenticate the user without revealing sensitive information, such as passwords or private keys. This enhances security by reducing the risk of data exposure.

Algorithm 2: Authentication Protocol using Zero-Knowledge Proof (ZKP)

Input: $User\{Id, Name, DOB, GovtID\}$
Output: Verification result (approved or denied)
Retrieve user's encrypted credentials identity EU from blockchain ledger
Generate a Zero-Knowledge Proof ZKP for the provided credential $User$
Submit the encrypted ZKP,EZKP to the blockchain for verification by the smart contract
if $EZKP == EU$ **then**
  return "Authentication Approved"
end if
return "Authentication Denied"

The Zero-Knowledge Proof as ensures that the user's credentials are verified without exposing any sensitive information to the system. It's a highly secure way to authenticate a user.

E. Smart Contract Execution Protocol

Smart contracts are responsible for automating the verification process. When a user submits their credentials, the smart contract is triggered to check if the identity matches the stored data. The contract logic handles the decision-making process, ensuring that verification is conducted securely and efficiently.

F. Data Integrity Protocol

Since blockchain inherently ensures data immutability, it is used to ensure the integrity of the identity data. Once stored, the data cannot be altered, reducing the risk of identity theft or fraud. Our proposed algorithm (algorithm 3) captures the essence of registering user data securely on the blockchain, where data is encrypted and stored under a unique identifier.

Algorithm 3: Identity Registration Protocol

Input: $User\{Id, Name, DOB, GovtID\}$
Output: Verification result (approved or denied)

```
Generate an encrypted user credentials EUSER from USER
Generate unique identifier UID for the user
Create a registration transaction RegT and submit to blockchain
Store the pair EUSER and UID on blockchain
Trigger smart contract to register the user on the blockchain
if transaction confirmation is received then
    return "Registration Successful"
end if
if transaction confirmation is failed then
    return "Registration Failed"
end if
```

G. App Interface Design

The app interface will be designed to provide a seamless and user-friendly experience. Upon opening the app, users will be greeted with a simple login screen where they can choose to either register or authenticate their identity.

a) Registration Screen: Users will be required to enter their personal information, such as their name, date of birth, and government-issued identification number. The app will then securely submit this data to the blockchain after encryption. A confirmation screen will inform the user once registration is successful.

b) Authentication Screen: Users who wish to authenticate their identity will enter the required credentials (e.g., name, birthdate, government ID). The system will communicate with the blockchain to verify the data and return the verification status (e.g., "Verification Successful" or "Failed").

c) Verification Status Screen: If the verification is successful, the user will be granted access to services. If the verification fails, the user will be informed, and they can try again or contact support.

d) Dashboard Screen: A secure dashboard will allow users to view their identity status, update their personal information, and manage their security settings.

H. Challenges in Design

While the system is designed to be highly secure, there are several challenges to address:

a) Scalability: Blockchain networks can sometimes face issues with scaling. As the number of users increases, the system must efficiently manage a large number of transactions and identity verifications without causing delays or failures.

b) User Adoption: Since blockchain is a relatively new technology, users might not be familiar with how it works. To solve this, the app must focus on providing a simple, intuitive interface to facilitate adoption among non-technical users

c) Regulatory Compliance: Depending on the region, digital identity verification systems must comply with various regulations such as GDPR. Ensuring compliance with these regulations while maintaining blockchain's immutable nature poses a challenge.

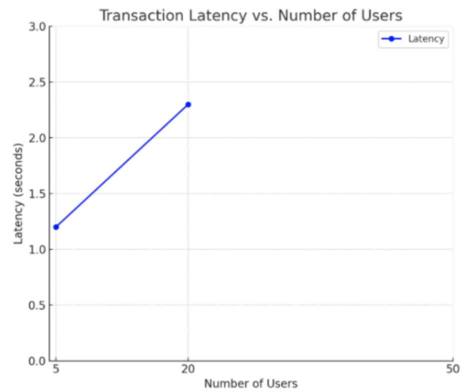

Fig. 2: Performance of Latency with No. of Users

This design and operational model lay out the foundation for the Blockchain-based Digital Identity Verification System. By employing blockchain for secure and immutable identity storage, smart contracts for automated verification, and a user-friendly interface, this system promises to offer a scalable, secure, and efficient solution to digital identity verification. Through this approach, we aim to tackle the issues of fraud, security, and inefficiency in traditional identity systems.

VI. Experimental Evaluation

The Blockchain-based Digital Identity Verification System was developed and tested using a robust experimental setup. The project utilized Solidity for smart contract development, while the front-end interface was designed using React to provide a user-friendly experience. Both Remix IDE and Visual Studio Code (VSCode) were used during the development phase for coding, debugging, and deploying the smart contracts. Node.js and Web3.js were employed for blockchain integration within the front-end application. Testing was conducted locally using Ganache, a blockchain simulator, to mimic real-world deployment conditions. User simulations were conducted with three groups representing low (5 users), medium (20 users), and high (50 users) network activity. Each group performed transactions, including user registration, identity verification, and identity updates, with 20 repetitions for each transaction type to ensure data reliability.

The experimental findings provided in figure 2 valuable insights into the system's performance and scalability. First, transaction latency was analyzed across different user loads. It was observed that the average latency remained low at 1.2 seconds for up to 20 users, increasing slightly to 2.3 seconds with 50 users. This increase reflects the natural delay in blockchain-based systems as network activity grows, yet the system maintained acceptable response times suitable for practical use. These results indicate that the system can efficiently scale with minimal impact on performance.

Second, the analysis of gas consumption (figure 3) revealed significant differences based on transaction types. User registration required the highest gas usage at approximately

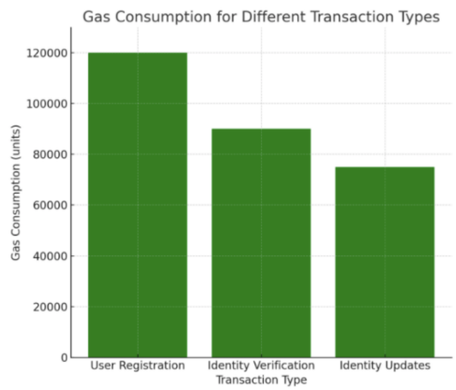

Fig. 3: Gas Consumption for Different Transactions

120,000 units per transaction due to the need to store extensive data on the blockchain. In contrast, identity verification and updates consumed 90,000 and 75,000 units, respectively, as they leveraged existing on-chain records. These findings suggest that while registration processes are more resource-intensive, they can be optimized for cost efficiency when scaling for larger user bases.

Lastly, the system demonstrated robust security throughout all experiments. The implementation of Zero-Knowledge Proofs effectively ensured that no sensitive user information was exposed, maintaining complete data confidentiality. Additionally, the immutable nature of the blockchain ledger prevented any tampering or unauthorized access, highlighting the system's ability to outperform traditional centralized identity verification methods. The combination of cryptographic techniques and blockchain's inherent security features reinforces the reliability of the proposed solution. Overall, the experimental results validate the system as a secure, scalable, and efficient alternative to conventional identity management solutions. Its readiness for deployment and ability to handle real-world challenges make it a promising approach for addressing existing gaps in digital identity verification.

VII. Conclusion

This research aimed to address the critical problem of securing and managing digital identities in a world increasingly reliant on online interactions. The centralized identity management systems commonly used today are prone to breaches, unauthorized access, and privacy violations. Our blockchain-based digital identity verification system offers a decentralized alternative that ensures data security, user privacy, and transparency by utilizing smart contracts and cryptographic protocols. By leveraging blockchain technology, the proposed solution eliminates the risks associated with centralized identity management systems, such as data breaches and unauthorized access. The blockchain-based digital identity verification system ensures user privacy, immutability, and secure data sharing through the use of cryptographic techniques and distributed ledger technology. The findings from the simulation and testing phases revealed that the system performs efficiently in verifying user identities, ensuring secure access to services, and providing a user-friendly interface. Future work aims to address these limitations by exploring layer-2 scaling solutions to reduce transaction costs and latency.

References

[1] V. Nehra, M. Aakarsh, H. Khanna, and N. Jindal, "Decentralized digital identity verification system using blockchain technology," in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*. IEEE, 2024, pp. 1–6.

[2] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, "Pbidm: Privacy-preserving blockchain-based identity management system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1524–1534, 2022.

[3] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, no. 2, p. 15, 2008.

[4] A.-C. Careja and N. Tapus, "Digital identity using blockchain technology," *Procedia Computer Science*, vol. 221, pp. 1074–1082, 2023.

[5] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied innovation*, vol. 2, no. 6-10, p. 71, 2016.

[6] 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, 2020.

[7] C.-T. Tsai, J.-L. Wu, Y.-T. Lin, and M. K.-C. Yeh, "Design and development of a blockchain-based secure scoring mechanism for online learning," *Educational Technology & Society*, vol. 25, no. 3, pp. 105–121, 2022.

[8] N. Balasubramaniam, "Blockchain based digital identity verification for social media," *Euroasia J. Math. Eng. Nat. Med. Sci.*, vol. 7, no. 8, pp. 202–209, 2020.

[9] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.

[10] X. Wang, X. Jiang, Y. Liu, J. Wang, and Y. Sun, "Data propagation for low latency blockchain systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3631–3644, 2022.

[11] P.-W. Chi, Y.-H. Lu, and A. Guan, "A privacy-preserving zero-knowledge proof for blockchain," *Ieee Access*, 2023.

[12] P. Hacker, I. Lianos, G. Dimitropoulos, and S. Eich, *Regulating blockchain: techno-social and legal challenges*. Oxford University Press, 2019.

[13] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[14] C. Ianzito, "Identity fraud cost americans $43 billion in 2023," https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html, 2023.

[15] Z. Yan, X. Zhao, Y. Liu, and X. R. Luo, "Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda," *Information & Management*, p. 104026, 2024.

[16] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, and J. Clark, "Bitcoin and cryptocurrency technologies (princeton university pres)," 2016.

[17] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[18] M. R. Ahmed, A. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113 436–113 481, 2022.

[19] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "Wip: A novel blockchain-based trust model for cloud identity management," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. IEEE, 2018, pp. 724–729.

[20] F. Sabrina, N. Li, and S. Sohail, "A blockchain based secure iot system using device identity management," *Sensors*, vol. 22, no. 19, p. 7535, 2022.

[21] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: a survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4-2, pp. 1735–1745, 2018.

[22] M. Kuperberg, S. Kemper, and C. Durak, "Blockchain usage for government-issued electronic ids: A survey," in *International Conference on Advanced Information Systems Engineering*. Springer, 2019, pp. 155–167.

[23] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers & Security*, vol. 99, p. 102050, 2020.

[24] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, and S.-M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," *Future Generation Computer Systems*, vol. 135, pp. 450–466, 2022.

[25] M. Aydar, S. Ayvaz, and S. C. Cetin, "Towards a blockchain based digital identity verification, record attestation and record sharing system," *arXiv preprint arXiv:1906.09791*, 2019.

[26] Ö. Doğan and H. Karacan, "A blockchain-based e-commerce reputation system built with verifiable credentials," *IEEE Access*, vol. 11, pp. 47 080–47 097, 2023.

[27] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021.

[28] P. R. Patil, D. Rout, and S. S. Mohite, "A survey of decentralized digital voting system using blockchain technology," in *International Conference on Data Science and Applications*. Springer, 2023, pp. 27–44.

[29] Z. Hongmei, "A cross-border e-commerce approach based on blockchain technology," *Mobile Information Systems*, vol. 2021, no. 1, p. 2006082, 2021.

[30] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and

verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.

[31] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.