Customer Identity Management in Health Insurance with Blockchain Technology: A Literature Review

Matthias Pohl[a], Hannah Giegold, Christian Haertel[b], Daniel Staegemann[c] and Klaus Turowski[d]
MRCC VLBA, Faculty of Computer Science, Otto von Guericke University, Magdeburg, Germany
{*firstname.lastname*}*@ovgu.de*

Keywords: Customer Identity Management, Blockchain, Health Insurance, Access Management.

Abstract: Customer identity management systems are an important part of the IT infrastructure of health insurance companies. However, the current systems face challenges due to the centralized system architecture, display disadvantages in identity verification, and pose security risks for customer data. Since blockchain systems are often mentioned as a solution, the goal of this paper is to examine how blockchain-based identity management can improve this particular process of identity management in the health insurance industry. Therefore, a systematic literature review was conducted, covering the challenges of centralized systems, a solution to the problem through decentralized systems, and possible designs and approaches of blockchain identity management systems. This revealed that current systems face problems in identity verification, authentication, user experience, data storage, data security, and data control. In addition to that, it was found that decentralized systems can solve many of those challenges. They facilitate the know-your-customer process for customers and companies, increase data security, create a trusting relationship between the customer and the company, and give customers control over their data. Thus, the use of a decentralized identity management system for the insurance industry is associated with advantages and has great potential to improve the current identity management process.

1 INTRODUCTION

As digitization progresses, our technology continues to evolve and ensures that our everyday lives are increasingly being shaped by the use of digital services and processes, as shown by the Global Digital Sentiment Survey 2022 by McKinsey & Company, in which 70% of respondents used these services (McKinsey & Company, 2022). Due to fierce competition, companies are under pressure to offer their customers an excellent user experience (UX) to retain them in the long term and attract new customers. In addition to the ease of use of the systems, providers must ensure that the stored customer data is securely protected and offer suitable customer identification and authentication. The latter is of central importance, since according to the Global Identity & Fraud Report, identity theft is one of the greatest risks within the virtual world (Experian Information Solutions, 2022). According to the Modern Bank Heist 3.0, the Banking, Financial Services and Insurance (BFSI) sector is one of the most popular targets for cybercriminals and in 2020 80% of respondents reported an increase in attacks compared to previous year (Kellermann and Murphy, 2020). The reason for this is the large amount of valuable data, which includes the personal and financial information of customers (European Insurance and Occupational Pensions Authority, 2021). As a result, companies in the insurance environment need to ensure proper customer identity and access management (CIAM) to meet the growing challenges. However, currently deployed systems face problems such as vulnerabilities in authentication and verification methods, obstacles due to centralized system architectures, high risk of cyberattacks, and drawbacks for UX (Mulaji et al., 2021). Due to these challenges, it is significant to investigate new alternatives. In this regard, blockchain technology has the potential to transform identity management processes in the insurance industry. The use of this technology is not yet widespread in the sector, but its use offers the opportunity to reduce costs, increase process efficiency, facilitate new customer verifica-

[a] https://orcid.org/0000-0002-6241-7675
[b] https://orcid.org/0009-0001-4904-5643
[c] https://orcid.org/0000-0001-9957-1003
[d] https://orcid.org/0000-0002-4388-8914

Pohl, M., Giegold, H., Haertel, C., Staegemann, D. and Turowski, K.
Customer Identity Management in Health Insurance with Blockchain Technology: A Literature Review.
DOI: 10.5220/0012575200003657

In *Proceedings of the 17th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2024) - Volume 2*, pages 803-811
ISBN: 978-989-758-688-0; ISSN: 2184-4305

tion, and increase trust and transparency among the parties involved. In addition, the use of blockchain facilitate the detection and prevention insurance fraud (European Insurance and Occupational Pensions Authority., 2021).

Several studies have examined the role of blockchain in identity management and insurance. One study highlights how blockchain and other digital technologies can revolutionize the insurance industry, emphasizing their potential for customer-centric services and cost reduction, but also noting challenges in replacing legacy systems (Eckert and Osterrieder, 2020). Another study uses a SWOT analysis to assess benefits and drawbacks of blockchain in insurance, suggesting its potential to streamline processes yet acknowledging the need for further development (Gatteschi et al., 2018). Research in the BFSI sector focuses on the significance and transformative impact of blockchain in identity management, particularly highlighting the promise of the Zero-Knowledge-Proof technology (ZKP) (Akram and Sen, 2022). A comprehensive literature review and various investigations into blockchain-based identity management systems reveal their potential to overcome traditional system limitations but indicate that blockchain technology still lags in implementation and efficacy compared to existing solutions (Ahmed et al., 2022, Kuperberg, 2020). Lastly, a study on the practicality of blockchain for organizational identity management suggests it holds promise but is still in a developmental phase, with proper planning needed for effective implementation (Mulaji et al., 2021). Compared to existing studies, the paper at hand focuses on identity management and verification in the insurance environment. In order to clarify the objectives of future research, the following research question (RQ) will be answered:

RQ: *How does the current research landscape of academic and commercial Blockchain solutions for identity management look like?*

To answer the research question, this introduction to the research topic is followed by a detailed explanation of the research methodology, focusing on the structured literature review process. The results section (Sec. 3) presents a comprehensive overview of academic and commercial solutions identified in the literature review. Finally, the paper offers a comparative analysis of these solutions from technical and process perspectives, culminating in a conclusion that summarizes key findings and suggests directions for future research.

2 METHODOLOGY

This section describes the procedure of the systematic literature search. It includes the selected databases, search terms, the inclusion and exclusion criteria, as well as a presentation of the search results and the search process. In general, we follow the approach of vom Brocke et al. Brocke et al. (2009). After defining the review scope (I) in section 1, we conceptualize the topic (II) of the literature review in subsection 2.1.Subsequently, the search process (III) can be started, which is described in subsection 2.3. The results are compiled and analyzed in sections 3 and 4 (IV). Finally, the summary of results provides an outlook on the research agenda (V).

The search process is conducted on the scientific literature databases of ACM, IEEE, Scopus, Springer Link, and Web of Science. These databases were chosen for searching as they cover an extensive collection of literature in the necessary subject areas.

2.1 Search Terms

For the systematic literature review, search terms were formed, which were composed of different topic-related terms. The terms were derived based on the title, objective, and research question and divided into the four components ”blockchain”, ”customers”, ”identity management”, and ”insurance”. The formation was done with the help of the Boolean operators ”AND” between the components to limit the search results and ”OR” between the basic terms to consider synonyms during a search. Furthermore, parts of the expressions of the identity check were combined with terms from the component ”customers” to reduce the results of the search and to specify the generic terms. In addition, the wildcard operator (*) was used to include variations of the individual terms in the search. The search terms are constructed with the following concepts:

- **Blockchain:** blockchain, blockchain-technology, blockchain-based, distributed ledger, DLT
- **Customers:** customer, user
- **Identity Management:** identity, identification, identity verification, identity authentication, identity management, access management, CIAM, self-sovereign identity, SSI, decentralized identity, KYC
- **Insurance:** insurance, BFSI

2.2 Inclusion and Exclusion Criteria

For the systematic literature search, inclusion and exclusion criteria were determined to assess the literature found in terms of its suitability and relevance. The search was limited to publications in English and German. In addition, only conference papers and journal articles were considered due to being peer-reviewed. In addition, exclusion will occur if the proposed IDM solution is not a blockchain-based system. Further, papers will be excluded that do not focus on or consider IDM systems and papers that especially focus on the legal topic of the systems. Additionally, entries will not be considered if their environment and the IDM are not in the enterprise, BFSI, general systems, cloud, Internet of Things, customer, or public sectors.

2.3 Literature Search Results

During the systematic literature search, a total of 2,090 hits were obtained using the databases by applying the search restrictions (Sec. 2.1). After duplicates were removed, 1,545 entries remained. Subsequently, the title and abstract were evaluated for relevance with the addition of the inclusion and exclusion criteria of the topic and setting. Thus, the total number was reduced to 370 entries. In addition to this, a further 15 entries were removed because of unavailability of the full text. After the pre-selection, the remaining entries were subjected to a full-text review. The elimination was based on the criteria of language, availability, environment, and subject matter. Four papers were eliminated because the full text was only available in Chinese. 20 other papers were sorted out because they had a supply chain (4), energy sector (5), smart city (4), or other (7) environment. Thematically, a total of 248 entries were removed. 147 articles were sorted out because they had an inappropriate subject focus. Instead of an IDM system, the focus was on specific advances (e.g., data storage, data sharing, contact tracking), technologies (e.g., blockchain, Inter Planetary File System, ZKP), or financial applications and payment systems. 91 papers were eliminated because the proprietary solution presented was not a blockchain-based IDM system, and seven publications were excluded because they had a strong focus on blockchain or the legal framework of the systems. After the review, 83 submissions remained. These were divided into the groups ”own blockchain IDM solution” (50 entries) and ”other literature” (33 entries). Group one was used for the selection of blockchain-based systems in Section 3. For the second group, an additional look was taken to see, which papers dealt with a tabular comparison of blockchain-based IDM solutions. The comparison criteria for Section 4 were derived from the remaining 14 papers. Companies within this industry and their IDM systems were investigated independently. In addition, studies and articles from insurance trade magazines were included. To provide a comprehensive analysis of blockchain IDM systems, commercial solutions were examined to amend the scientific literature research. This analysis was based on published white papers, documentations, and entries on company websites.

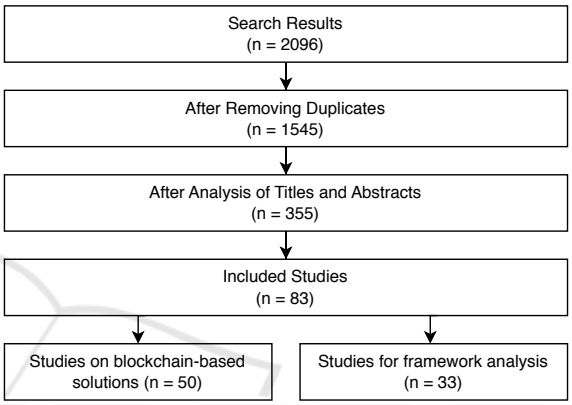

Figure 1: Overview of literature selection process.

3 BLOCKCHAIN IDENTITY MANAGEMENT SOLUTIONS

In the following, various blockchain identity management solutions are examined. The first subsection gives an insight into proposed approaches from the scientific literature and the second section delves into commercial solutions.

3.1 Academic Solutions

From the literature review, 50 proposals emerged, which were reviewed using an additional selection process, thus reduced to eight solutions. This process centered on determining if the proposal addresses a general identity management system or specific individual processes. Emphasis is placed on identifying publications that propose self-sovereign identity (SSI) systems, with a focus on papers that adhere to SSI principles and describe identity management or Know Your Customer (KYC) processes. To ensure relevance, papers lacking citations or use cases in general identity management, BFSI, or cloud computing are excluded from further analysis (see Table 1).

Table 1: Overview on solutions from academic literature.

Ref	BP	BT	C	I	S
Soltani et al. (2021)	Hyperledger Indy	public, permissioned	Plenum	n	off
Chen et al. (2021)	Hyperledger Fabric	consortium	Kafka-Consensus	y	off
Liao et al. (2022)	Ethereum	consortium	Proof-of-Authority	y	off
Bandara et al. (2022)	Rahasak	permissioned	Kafka-Consensus	y	off
Otta and Panda (2022)	Ethereum	-	Proof-of- Work	y	off
Schlatt et al. (2022)	-	-	-	n	off
Abraham et al. (2021)	-	permissioned	-	y	off
Hong and Kim (2020)	Ethereum	-	-	y	on

3.2 Commercial Solutions

The following section contains the analysis of existing blockchain-based IDM solutions. Based on the "KuppingerCole Market Compass Decentralized Identity: Blockchain ID & SSI Solutions" (Bailey, 2020), the solutions mentioned therein were considered. In a further selection process, the solutions were reduced to five products, as the solutions eliminated did not have sufficient documentation or were in the development or test phase at the time of the review. Exclusion due to a lack of documentation relates to the KYC systems Authenteq and KnowMeNow. The identity solution ShoCard was taken over by Ping Identity and integrated into their product PingOne Neo (Bailey, 2020), whiich is currently in its test phase. The two uPort products Serto Identity and Veramo as well as the Cambridge Blockchain are only in beta status or development and are eliminated for closer examination. Thus, only five selected solutions are considered for comparison (see Table 2).

4 SELF-SOVEREIGN IDENTITY MANAGEMENT SYSTEMS

The following section examines the extent to which self-sovereign identity management systems can have the potential for improving identity management.

4.1 General Perspective

Decentralized identity management systems provide a secure and trusted method for identity verification and management (Akram and Sen, 2022). They are considered as problem solvers of centralized systems (Panait et al., 2020). With their advantageous system architecture, they ensure that personal customer data is no longer stored centrally at an instance, but decentrally at the users themselves. The elimination of the central authority shifts the balance of power in favor of the customer and balances the previously asymmetrical trust relationship (Panait et al., 2020). When using digital services, the user can decide independently, which data should be shared with the service provider (Nuggets Ltd, 2017) and disclosure of the customer's personal data is only possible with their consent. In addition, the independence from central organizations ensures that the existence and functionality of users' digital identities are not dependent on them (SelfKEy DAO, 2023). The user can select partial information from their Verifiable Credentials (VC), which ensures that the organization only receives the data it needs to verify the user. Using cryptographic techniques such as ZKP and data minimization, the user data privacy can also be increased and legal regulations such as the GDPR are easier to comply with (SelfKEy DAO, 2023). Increased data security is also the result of having centralized data servers, which mitigates the risk from data leaks (Mulaji et al., 2021). If fraudsters want to steal an identity of a user, they must be in possession of their cryptographic key pair to prove that they are the owner of the stolen VC (Dock Labs AG, 2023). However, since the customer data and private keys are usually stored in their own SSI wallets, they must have malicious actors to penetrate each user wallet. Consequently, the chance of identity theft is reduced (Panait et al., 2020). Another advantage is the increased resilience to a Single-Point-of-Failure (SPOF) compared to the centralized systems due to disintermediation and decentralization (Mulaji et al., 2021). Common standards and protocols such as Decentralized Identifiers (DID) provide interoperability among SSI-systems and an improved UX. They allow data to be transferred efficiently and more easily between systems without compromising user security, control rights, and privacy (SelfKey Foundation, 2017). Moreover, they allow the user to use the same digital identity for different applications or services. Thus, the management of digital identities becomes easier (SelfKey Foundation, 2023). The insecure password login method of centralized systems

Table 2: Overview on commercial solutions.

Name	BP	BT	C	Year	Costs	S	OS
BlockID	Ethereum	private, permissioned	Proof-of-Authority	2018	y	on	n
Civic	Solana	public	Proof-of-Stake, Proof-of-History	2015	y	off	n
Evernym	Sovrin	public, permissioned	Plenum	2013	y/n	off	y
Nuggets	Ethereum	public	-	2017	y	off	n
SelfKey	Ethereum	public	Proof-of-Authority	2017	n	off	y

is replaced by a passwordless method, the decentral identifier, in the SSI-IDM. Moreover, cryptographic verification mechanisms of DID increase the security of user authentication compared to passwords (SelfKEy DAO, 2023). Through digital signatures, users can prove the integrity and authenticity of the transmitted data and be verified as the unique owner of the digital identity (Dock Labs AG, 2023). Further, the use of the trusted certificates and SSI solution ensures that insurance fraud can be better detected or even prevented (Eckert and Osterrieder, 2020). Besides the above point, the use of cryptography and VC supports fast and easy verification of new customers and guarantees the validity and integrity. The SSI system can speed up the process because the verifier can check the data of customers in real-time without contacting the issuer of the information. In finance, this can reduce the onboarding process for new customers from an average of one to three months to a few days or hours (SelfKEy DAO, 2023). The use of digital signatures enhances security by allowing precise verification of the issuer of the data and the intended recipient, thereby making it more challenging to manipulate, steal, or create false identity data (Dock Labs AG, 2023). In addition, the use of blockchain as a trusted data registry ensures that the stored data is difficult to change or manipulate (Mulaji et al., 2021) and the origin of incorrect data can be determined (Nuggets Ltd, 2017). The SSI system reduces the number of KYC processes for new customers to one verification, as companies can share customer data from the decentralized ledger across corporate domains (Akram and Sen, 2022, Eckert and Osterrieder, 2020, Nuggets Ltd, 2017). The user can use the VC received with other companies that also require a KYC check (Dock Labs AG, 2023). In addition to saving time, shared customer verification saves companies financial budgets (Nuggets Ltd, 2017). A further reduction in expenses results from the fact that companies no longer need to store, protect, and manage sensitive data of users and passwords (Mulaji et al., 2021). In addition, customer SSI self-management ensures a reduction in customer service expenses as data can be changed and updated synchronously across all services (Dock Labs AG, 2023, SelfKEy DAO, 2023). The use of a decentralized management system can improve the relationship between a company and its customers and help build a two-way trust through mutual authentication. By using SSI agents as intermediaries between the two parties, both agents can share VCs with each other and verify that they are valid. If one party's VC proves to be invalid, the agents can inform their owners and terminate the connection to protect users from phishing sites (SelfKEy DAO, 2023). In summary, the use of an SSI system provides clients with more convenience, security, and privacy than a centralized IDM (SelfKEy DAO, 2023).

4.2 Potentials of Blockchain Identity Management Solutions

The analysis of the 13 solutions shows that the use of a blockchain-based identity management in the insurance environment can solve challenges of centralized systems and realize the majority, of the elaborated advantages. The evaluation criteria include aspects like decentralized data storage, user-centric data sovereignty, independence from central authorities, the application of cryptographic security measures, and the management of private keys by users themselves. In addition, we checked on an increased resistance to a SPOF, a portable identity, a reusable KYC-VC as well as a passwordless login, and whether the first identity check is performed with VC (see Table 3). The results of the analysis show that all but one of the systems allow decentralized storage of user identity data and ensure that no single entity or central system has complete control over customer data. In all of the solutions examined, the user bears responsibility for their data, can access it via their wallet, and can easily manage or change it. In addition, all solutions confirm the advantage that data sharing is only possible with the explicit consent of the customer and can be done selectively. The analysis also shows that the use of SSI systems provides an increased resistance to SPOF. This is ensured by the decentralized structure of the blockchain used in all systems, which stores information regarding identity distributed across multiple nodes and enables secure data exchange across enterprise domains. The increased resilience is supported by the use of decentralized login procedures

Table 3: Comparison of SSI solutions with an analysis framework adapted from scientific literature.

Name	DS	SM	DT	U	SD	DID	VC	SP	LS	ZKP	S	W	AS	PI	PL	IP1	KYC1	DU
KYC2	Y	Y	Y	N	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	-	N	Y	N
SSI-Chain	Y	Y	Y	N	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-	N
BIMAC	N	Y	Y	N	Y	Y	-	Y	-	-	Y	Y	Y	Y	Y	-	Y	P
Casper	Y	Y	Y	N	Y	Y	-	Y	-	Y	Y	Y	Y	Y	N	N	Y	N
Otta et al.	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y	Y	Y	Y	-	N
Schlatt et al.	Y	Y	Y	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	Y	P
Abraham et al.	Y	Y	Y	N	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-	N
Vault-Point	Y	Y	Y	Y	Y	-	-	Y	-	-	Y	P	Y	Y	Y	N	-	N
BlockID	Y	Y	Y	N	Y	Y	Y	Y	-	-	Y	Y	Y	Y	Y	N	Y	N
Civic	Y	Y	Y	P	Y	Y	Y	Y	-	-	Y	P	Y	Y	Y	N	Y	N
Evernym	Y	Y	Y	N	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	P	Y	N
Nuggets	Y	Y	Y	P	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	N	Y	N
SelfKey	Y	Y	Y	N	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	N	Y	N

DS: decentralized data storage, **SM:** self-management, **DT:** data sharing through user consent, **U:** independence from central instance, **SD:** selective data forwarding, **DID:** decentralized identifier, **VC:** verifiable credentials, **SP:** key pair, **LS:** link secret, **ZKP:** zero-knowledge proof, **S:** private key on customer device, **W:** Resistance to SPOF, **AS:** use of general standards, **PI:** portable identity, **PL:** passwordless login, **IP1:** initial identity check with verifiable credentials, **KYC1:** one-off KYC check, **DU:** storage of all sensitive customer data at the company (**Y**: Yes, **N**: No, **P**: Partly)

and general standards. Additionally, the interoperability among solutions reduces the risk of being dependent on a particular system. However, complete exclusion of a SPOF does not occur as the VaultPoint and Civic solutions demonstrate. Each system allows the customer to have a portable identity and eleven of the analysed systems use a passwordless login. The decentralized login used by the majority, using DIDs or the cell phone as an authentication device, confirms the replacement of the traditional username/password method. Protected by cryptographic measures, it leads to more security, convenience, and an improved UX. Some of the anaylzed solutions show that this can be increased by simply updating all accounts via the wallet and automatically filling out forms. In addition, individual systems offer users to monetize their own data and deposit them with a real value. Another benefit reinforced by the research are the time and cost savings for identity verification processes that are possible with the use of SSI systems. The majority of solutions allow the customer to go through the full KYC verification process only once. They can use the issued VC or token to identify themself at other service providers. In addition to cost savings in the KYC process, the analysis shows a reduction in spending due to the elimination of securing sensitive data on company servers. A deviation only occurs in two of the examined solutions, where storage in case of suspicion or central storage of customer data on bank servers is mentioned. All solutions use cryptographic measures. They reduce the dangers of identity verification through VCs and DIDs and provide more security and privacy to the user through the use of ZKPs, link secrets, and cryptographic key pairs. Scenario analyses of the solutions also show that the SSI systems provide increased security against data theft as this is more costly compared to central databases. Private keys of customers are stored on private devices in all system architectures. The blockchain as a trustworthy data registry and reputation system acts as a bilateral communication channels, with mutual authentication, zero trust, VC as well as tokens, thus the trust is increased between the different parties. However, a complete independence from central instances and improvements for identity verification cannot be fully realized. The first point is influenced in the systems by the architecture of the blockchain, the used consensus mechanism, or the initial identity verification. Seven solutions use permissions, consortium, or private blockchain, which provide clients with greater independence than centralized systems, but network access and participant rights are still controlled by one or more central entities and are thus not fully decentralized. Moreover, consensus mechanisms such as proof-of-authority ensure that users are dependent on a central authority and must trust the validators (Malhotra et al., 2022). Benefits from using VC for initial verification cannot be realized in seven cases. In these solutions, the initial identity verification in the SSI ecosystem takes place without VC and relies on the procedures already used in the centralized solutions. In the study, only three of the identity management solutions examined use VC for initial verification, while two others offer both VC and alternative methods. However, the identity verification process in seven of the systems is vulnerable to tampered evidence as they depend on trusted entities for the verification and issuance of VC. Regarding the introduction of these systems, high security requirements for digital wallets (Bach, 2021) and the need for special-

ized terminals to store cryptographic keys are further challenges. A lack of awareness and lack of or incorrect knowledge of people about the new technology can lead to difficulties in adopting it (SelfKey Foundation, 2023). In addition, the UX may suffer if system operations are too complex or new to users. The user trades control for convenience (Preukschat and Reed, 2021) and faces extra work as they are responsible for managing, backing up, and protecting their own data (SelfKey Foundation, 2023). There is also a risk of consent fatigue if the customer has to manage too many requests (Soltani et al., 2021). Insurance companies face the problem of integrating the new systems into their existing IT infrastructure. Although the majority of the analyzed market solutions are white-labeled products that are easy to integrate with the help of documentation, the IT department of the insurer still needs the technical know-how and skills to understand and develop the code (Eckert and Osterrieder, 2020). In addition, the redesign of the IT landscape might necessitate large investments (SelfKey Foundation, 2023). Further, for the utilization of blockchain-based systems, both customers and companies must obtain the appropriate currency to facilitate payment for transactions and services (1Kosmos Inc., 2023). The adoption of blockchain technology and decentralized storage in systems faces several challenges. Scalability issues and limitations in storage space are significant concerns (SelfKey Foundation, 2023). The choice of consensus mechanism can affect system performance, resource usage, and may result in less decentralization. Data storage methods also present difficulties as on-chain storage hampers scalability and system speed, and raises issues regarding the right to be forgotten, as personal data could remain permanently on the ledger. Off-chain storage, on the other hand, is susceptible to corruption and tampering (Nuggets Ltd, 2017). Additionally, user access to data is dependent on private keys. Losing these keys poses a risk, although recovery solutions like BIP39 exist, they are not foolproof, and losing recovery phrases means losing access to private data (Soltani et al., 2021). Furthermore, authentication with Decentralized Identifiers (DIDs) has been found to be more time-consuming than traditional password methods. Finally, uncertainties and lack of guidelines in the legal and regulatory environment complicate the diffusion of systems in the insurance sector and the verification of documents (Eckert and Osterrieder, 2020). Despite these challenges, the use of SSI systems offers many benefits to the insurance industry and its customers and can overcome the majority of the challenges of centralized IDM systems. However, two issues cannot yet be fully answered and, in conjunction with SSI systems' native challenges, continuous development of the technology is needed to solve these problems.

5 CONCLUSION

This research explored how blockchain could enhance customer identity management in the insurance industry. It highlights that current systems are centralized, posing risks like data breaches and limited user control. The study suggests that blockchain-based SSI systems could offer improvements by decentralizing data management and enhancing security and user autonomy. However, SSI systems also have limitations, such as partial decentralization and similar vulnerabilities in identity verification. Future work should include an in-depth security evaluation of blockchain-based self-sovereign identity systems. This would involve assessing their resilience to cyber threats, data integrity, and privacy safeguards. Analyzing how these systems conform to established security principles would be crucial (Allen, 2016). Expanding the research to include insurance companies on a global scale, particularly in Europe and other regions, would provide a more comprehensive understanding of identity management practices. This broader perspective could highlight regional differences and similarities, offering a more nuanced view of the challenges and opportunities in adopting blockchain technology for identity management. Investigating a variety of other SSI and Decentralized Trust Infrastructure systems could enrich the understanding of the landscape. This exploration should aim to assess different models and architectures, comparing their effectiveness, user-friendliness, and scalability. The study should expand its criteria catalog to encompass emerging attributes and technologies. This would involve exploring new blockchain features, advancements in encryption, and evolving regulatory requirements. Such an extension would ensure that the analysis remains relevant and comprehensive in the rapidly evolving field of digital identity management. A further critical area for future research is the practical implementation of SSI systems in the insurance industry. This includes pilot studies or case studies demonstrating real-world applications and challenges. Investigating the gap between theoretical benefits and actual outcomes in these implementations would provide valuable insights into the feasibility and effectiveness of SSI systems in a real-world setting. Besides, the development of a further fully comprehensive approach to SSI-IDM using blockchain technology (Pohl et al., 2020) and the modeling of integration into organiza-

tional processes (Pohl et al., 2023) can be pursued. Finally, understanding the factors that influence user acceptance and adoption of these systems is essential. Future studies should explore the societal, behavioral, and technological barriers to the widespread adoption of blockchain-based identity management solutions.

REFERENCES

1Kosmos Inc. (2023). 1Kosmos Authenticators.

Abraham, A., More, S., Rabensteiner, C., and Hörandner, F. (2021). Revocable and Offline-Verifiable Self-Sovereign Identities. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1020–1027.

Ahmed, M. R., Islam, A. K. M. M., Shatabda, S., and Islam, S. (2022). Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access*, 10:113436–113481.

Akram, M. and Sen, A. (2022). A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof. In *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, pages 1295–1299.

Allen, C. (2016). The Path to Self-Sovereign Identity.

Bach, N. (2021). Dezentrale Identifikatoren (DIDs): Die nächste PID-Evolution: selbstsouverän, datenschutzfreundlich, dezentral. *o-bib. Das offene Bibliotheksjournal / Herausgeber VDB*, 8(4):1–20 Seiten.

Bailey, A. (2020). Decentralized Identity: Blockchain ID & Self-Sovereign Identity Solutions.

Bandara, E., Shetty, S., Mukkamala, R., Liang, X., Foytik, P., Ranasinghe, N., and De Zoysa, K. (2022). Casper: a blockchain-based system for efficient and secure customer credential verification. *Journal of Banking and Financial Technology*, 6(1):43–62.

Brocke, J. v., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., and Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *ECIS 2009 Proceedings*.

Chen, Y., Liu, C., Wang, Y., and Wang, Y. (2021). A Self-Sovereign Decentralized Identity Platform Based on Blockchain. In *2021 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–7.

Dock Labs AG (2023). Blockchain Identity Management: Complete Guide 2023.

Eckert, C. and Osterrieder, K. (2020). How digitalization affects insurance companies: overview and use cases of digital technologies. *Zeitschrift für die gesamte Versicherungswissenschaft*, 109(5):333–360.

European Insurance and Occupational Pensions Authority (2021). Cyber-Risiken: Was sind die Auswirkungen auf die Versicherungsbranche? (ARTIKEL15).

European Insurance and Occupational Pensions Authority. (2021). *Discussion paper on blockchain and smart contracts in insurance.* Publications Office, LU.

Experian Information Solutions, I. (2022). 2022 Global Identity and Fraud Report. Technical report.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., and Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, 10(2).

Hong, S. and Kim, H. (2020). VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0. *ELECTRONICS*, 9(8).

Kellermann, T. and Murphy, R. (2020). Modern Bank Heists 3.0. Technical report, VMware.

Kuperberg, M. (2020). Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Transactions on Engineering Management*, 67(4):1008–1027.

Liao, C., Guan, X., Cheng, J., and Yuan, S. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems - The International Journal of EScience*, 135:450–466.

Malhotra, D., Saini, P., and Singh, A. (2022). How Blockchain Can Automate KYC: Systematic Review. *WIRELESS PERSONAL COMMUNICATIONS*, 122(2):1987–2021.

McKinsey & Company (2022). Digital Sentiment Survey 2022: Deutsche Verbraucher:innen werden zunehmend digitaler.

Mulaji, S. S. M., Roodt, S. S., and Zhang, Y. (2021). The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis. *Sec. and Commun. Netw.*, 2021.

Nuggets Ltd (2017). Nuggets White Paper V18.

Otta, S. P. and Panda, S. (2022). Decentralized Identity and Access Management of Cloud for Security as a Service. In *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pages 299–303.

Panait, A.-E., Olimid, R., and Stefanescu, A. (2020). Identity management on blockchain – Privacy and security aspects. *Proceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science*, 21(1):45–52.

Pohl, M., Degenkolbe, R., Staegemann, D., and Turowski, K. (2020). Towards a blockchain technology framework–literature review on components in blockchain implementations. In *ACIS 2020 Proceedings*. Association for Information Systems.

Pohl, M., Degenkolbe, R., Staegemann, D. G., and Turowski, K. (2023). Decentralised autonomous management of an association through smart contracts according to german legislation. In *ICEIS (1) 2023*.

Preukschat, A. and Reed, D. (2021). *Self-sovereign identity: decentralized digital identity and verifiable credentials*. Manning, Shelter Island.

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2022). Designing a Framework for Digital KYC Processes

Built on Blockchain-Based Self-Sovereign Identity. *INFORMATION & MANAGEMENT*, 59(7).

SelfKEy DAO (2023). SelfKey DAO Whitepaper EN.

SelfKey Foundation (2017). SelkKey.

SelfKey Foundation (2023). Login with SelfKey · Developers.

Soltani, R., Nguyen, U. T., An, A., and Galdi, C. (2021). A Survey of Self-Sovereign Identity Ecosystem. *Sec. and Commun. Netw.*, 2021.