Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Self-sovereign identity for healthcare using blockchain

Mohammed Shuaib [a,b], Shadab Alam [b,*], Mohammad Shabbir Alam [b], Mohammad Shahnawaz Nasir [b]

[a] *Razak Faculty of Technology and Informatics, University Teknologi Malaysia, Malaysia*
[b] *Department of Computer Science, College of CS & IT, Jazan University, Jazan, Saudi Arabia*

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Self-sovereign identity
Blockchain
EHR
Security
Privacy
Healthcare

ABSTRACT

Secure and reliable identity is essential for identifying a user accurately and providing services. The traditional centralized identity systems have several security weaknesses and do not support user control. Self-sovereign identity (SSI) has been proposed to provide user control and secure identity model. User record privacy and security is a critical factor for any healthcare information system. Healthcare is also a domain where SSI solutions can counter patient information privacy and security threats. This paper reviews the applicability of blockchain-based SSI solution in healthcare, their advantages and requirements. It further provides a model use case for demonstrating the SSI application in healthcare.

Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

1. Introduction

Blockchain is a trustless, decentralized security model. Under this model, users will verify transactions that are currently taking place. Users will form a scalable, decentralized network to allow transactions between anonymous parties. And there's a way to detect fraud. Consequently, protection is provided in a decentralized manner, and a stable network is provided without any middleman's involvement. Initial implementations of the distributed ledger model are public blockchains such as Bitcoin and alternative cryptocurrencies like Litecoin. Bitcoin uses distributed ledger technology (DLT) for a decentralized payment system. It addresses dual-spending issues using proof-of-work (PoW) consensus mechanism [1,2].Fig. 1.Fig. 2.

The primary motivation behind blockchain adoption against the client–server model is to provide reliability, stability, timeliness and productivity in a legal system primarily due to its decentralized and distributed existence and the absence of intermediaries. Blockchain technology is still in the early stages of the research. The number of studies dedicated to the applications of blockchain technology is growing dramatically [3]. Technology may be called a technical hype: the latest state-of-the-art technology has only hit the hype cycle's height [4]. As such, many technologies and applications have been found. Healthcare is an area that has always come up with health-focused ideas to solve healthcare challenges [5,6]. There are a variety of stakeholders in the healthcare system, including hospitals, insurance providers and patients. It is easy for health authorities to access patient information. In the traditional model, medical information for patients is maintained in protected data centres. Conversely, due to the diversity of digital data and the high proportion of health data generation sources, big data in healthcare is growing.

Currently, hospitals use Health Information Systems to register, share and interpret health information. As sources such as wearable devices and mobile devices have appeared, combining patient data with this form of digital identity poses new problems [3,5,6]. These problems include compliance with the regulations, exchange and review of health data, effective and reliable sharing.

Health information systems contain extremely confidential personal information about the patient. Self-sovereign identity enables patients to have full power over their identity and the existence of information. Nowadays, the digital and physical world has become so interconnected that the self-sovereign identity is as important as physical identity.

The authentication and authorization process for individuals and organizations is a major recurring factor in blockchain applications – as explored by the Techruption [7] had the most successful project, for example, Self-sovereignty identity for healthcare allows a patient to control all aspects of their identity. A blockchain-based identity platform can be useful for various applications and in different environments [8].

Current technology does not allow for efficient processing of patient digital information while maintaining patients' privacy

[*] Corresponding author.
E-mail address: s4shadab@gmail.com (S. Alam).

https://doi.org/10.1016/j.matpr.2021.03.083
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

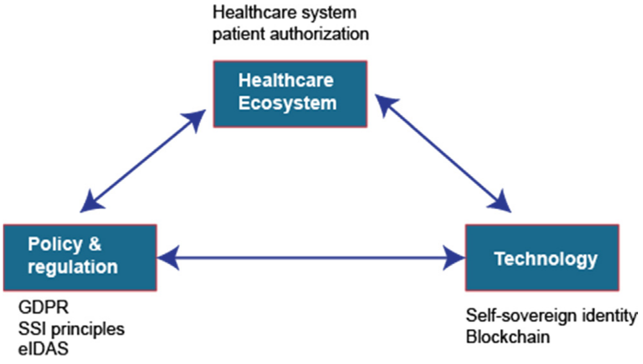

Fig. 1. Self-Sovereign identity framework for healthcare.

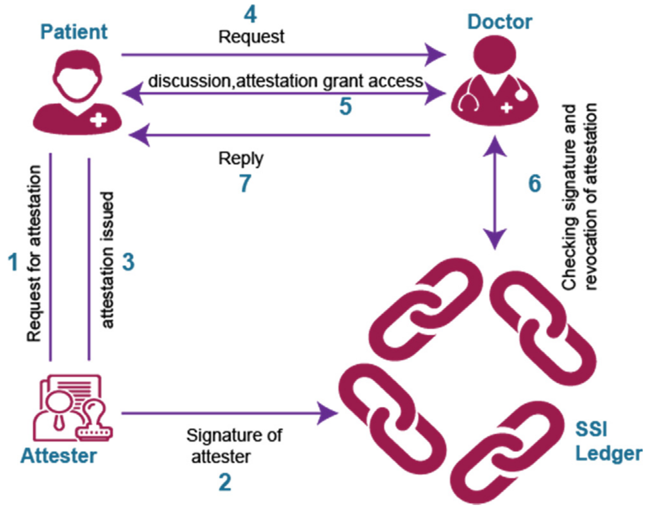

Fig. 2. Workings of the SSI framework with attestations.

and security [9,10]. In traditional centralized models, the privacy of patients is protected by healthcare service providers [11–14]. To obtain access to services, the patient must trust the healthcare service providers [15,16]. Traditional centralized models have many drawbacks, like data potentially lost due to hardware or device malfunctions. Besides, if anyone breaches or alters the patient information, patients will not track or restore the changes to their records. Healthcare providers are involved in the data transfer from one centre to another [17].

In this regard, blockchain-based self-sovereign identity system for healthcare would allow patients to regain control of their own information. And provide security of patient information [18].

Blockchain technology's capabilities make it the best suitable for implementing the functionalities required to implement a standardized, interoperable healthcare ecosystem. Irrespective of who gathers healthcare information, the patient is at the centre of the self-sovereign identity ecosystem and chooses to share their information and comply with European Union regulations related to privacy [19,20].

The organization of the paper is as follows. Section II provide a literature survey of the related field and basic concepts. Section III reviews the SSI requirements in healthcare, and section IV presents a blockchain-based SSI framework for healthcare. Section V presents a use case of SSI application in healthcare, and finally, section VI concludes the chapter.

2. Literature survey

Possessing a legal identity can help non-documented migrants access health facilities and other support schemes during a pandemic or emergency period. It helps governments identify the weaker section of society who are most vulnerable to such pandemic situations to counter the pandemic and support the population by uniquely identifying and tracking them.

There are a limited number of studies on the implementation of blockchain-based Self-sovereign identity system in healthcare [17,19,21–24]. These research works have been outlined in Table 1. The paper [19] demonstrate the four different aspects of BC applications in healthcare focused on (1) security, (2) interoperability, (3) data sharing, and mobility. McGhin et al. [19] have chosen similar works concentrating on wireless, Internet of things, mobile health, and science. Paper [17] examines the basic study of identity and access control systems (IAM). The paper describes the basic elements for a BC-based identity management framework, including accessibility, compliance, regulation, incorporation, and standardization. Nevertheless, it does not address healthcare-related issues such as doctors, patients, researchers, medical and clinical research facilities, and in- insurance providers. Paper [21] explores ways to solve obstacles when building identity management systems for the IoT. They compare existing identity management systems, including decentralized authentication, domain name service (DNS), blockchain infrastructure, safeguarding personal privacy, etc. However, the paper does not entirely address the complexities of developing Electronic Health Records (EHR) and Patient Health Records (PHR), that are the building blocks of the Internet of Healthcare Things (IoHT) [24]. However, the survey only covers those working within the organization and management area [23].

A questionnaire-based survey was conducted by [23] among medical doctors and patients concerning their blockchain preferences for the management and processing medical information. Their results suggest that the use of BC is more favourable for patients than for medical experts. However, [23] does not address either the medical information management system, but instead discusses the patient's perspective.

2.1. Basic concepts

1) *Digital identity:* Identity is a set of characteristics that belong to a single individual [31] The digital identity includes knowledge about an individual used by computers as an external agent. Another definition of digital identity is an online or networked identity that an individual, organization or electronic device adopts or asserts in cyberspace [32].
2) *Authentication:* Authentication is built using authentication factors that indicate that someone he says is now at the end of the connection channel. Three factors can be used to authenticate an identity.

Table 1
Review of available BC-SSI solution.

Ref	BC-SSI solutions	Distributed technology	Data management & privacy
[25]	MEDIBLOC	DPoS and QRC20 Token	Markel tree & Key-value DB
[26]	ScriptDrop	PoS & ERC20 token	Permissioned hyper ledger fabric
[27]	HealthWizz	PoS & ERC20 token	Local or Cloud storage
[28]	Dentacoin	PoS & ERC20 token ethereum	Public ledger
[29]	MedRec	PoS	SQLite
[30]	Gem	GemOS specialized platform	Compatible with multiple storage methods

First, Information factors: like a password; Second, possession factors include smartcards, hardware keys, etc. lastly, being/inherence factors, for instance, biometrics [33].

3) *Authorization:* Authorization consists of providing ac- cess to services to those that have been authenticated. Au- authorization relies on authentication since access is determined based on one or more verified attributes [34].
4) *Digital trust:* Trust is something that characterizes every interaction and transaction. New modern industry patterns unexpectedly put together a wide variety of people, businesses, products and algorithms on a large scale. It creates the need to make immediate trust so that it can be realized. Regular confidence models are not adequate to describe emerging digital identities.
5) *Self-sovereign identity:* Self-Sovereign Identity (SSI) supports users' full control of personal identity information (PII) across various authorities. However, there is no consensus about what the SSI is. Allan attempts to demarcate SSI by introducing ten concepts unique to it [35]. These principles are outlined in Table 2.

The SSI is usually used for electronic transactions to promote (business). A general form is that to use the service, a service provider requires an end-user. To use the service, he should show his attributes [36]. The service provider is a relying party requiring an attestation request: it requires end-user information to comply with business rules and ensure that it profits from the transaction. It needs users to acquire the desired credentials, whether they are stored on their phone, in a public blockchain. He third party is the Issuer of Attestation, who issues the appropriate missing credentials [18,37–39].

The SSI is constructed based on claims. An attestation is a series of statements relating to the validity of another collection of arguments. The original set of claims may also be considered an argument. The recipient of the attestation should be able to affirm the dedication of the certifier to the allegations. Therefore, the dedication should be in the form of a digital signature in a blockchain or a data pointer. Node recognition in the network takes place through the use of decentralized identifiers (DID) [40–43]. A DID is essential for interacting with the network and doing transactions [44] . It is the number/name/string that you identify someone. A Cryptographic Identifier (CID) is a cryptography key connected to a private key [45].

3. Requirements of SSI adoption in healthcare

Several factors influence the adoption or acceptance of a new solution in any domain. There are some specific requirements for adopting SSI in the field of healthcare. These requirements have been summarized in Table 3 given below.

Table 2
Principles of SSI.

SSI Principle	Description
Access	Users need to have access to their own records.
Existence	Users must have an independent life.
Control	Users should regulate their identity.
Persistence	Long-lived identities must be established.
Transparency	Systems and algorithms should be transparent
Interoperability	Identities should be used as broadly as possible.
Portability	Identity information and services must be transportable.

Table 3
Requirements for adopting SSI in healthcare.

Requirements	**Explanation**
Trust	- provide Integrity and control
Transparency	- Contracts through blockchain - No secret transmission of knowledge.
Ease of use	- Easy for patients - Easier for healthcare provides - Complex structures are not appropriate. - Not a lot of work all of a sudden, - Supportable - More effective
Security	- Provide recovery in case of Losing personal keys - No access to unwanted intruders
Rights and access	- provide service for maintenance - manage corrections - provide Tracking
Compliance	- provide services in compliance with regulation
Added value	- provide additional features
Efficiency	- No redundancy
Awareness	- Control by a patient over their PII - Give Significance of data sharing of personal information
Patient-centred	- Support Monitoring by patients

4. Blockchain-based SSI framework for healthcare

Blockchain's inherent qualities give many socio-economic health benefits: trusted intermediaries become redundant, and transaction costs can be reduced. Blockchain technology is providing a modern digital identity storage network. Also, with blockchain-based SSI, shared data is modified almost in real-time, and the patient can have more control over his or her own data [46–48]. Further Table 4 presents the advantages of using SSI in healthcare.

The various factors of Self-sovereign identity-based healthcare framework are discussed in the following points.

4.1. Healthcare system

Healthcare system complexity doesn't really encourage new innovation. A more structured approach to experiments and implementations in relatively closed, risk-free environments is appropriate instead of a top-down reversal of existing frameworks.

4.2. Perception

In the field of healthcare, understanding the issue by actors is also not helpful. From the healthcare providers' point of view, there is no sense of urgency concerning the current IT technology and patients' personal data. Aspects such as red tape and data silos can improve; however, risks to personal data records in healthcare

Table 4
Advantages of SSI adoption in healthcare.

Advantage	**Explanation**
Patient control	• Explicit consent by the patient • Provide care as per the patient needs
Time slots	• Data is not needed all the time
New links for providers	• Data request • Medications
Service	• Patient services
Less risk	• Minimal data incorporated • Minimized data coupling
Compliance	• Compliance with legal regulations
Low maintenance	• Reduced costs • Automatic update of records
Data available for research	• Assessing treatment quality

privacy are considered relatively low. Therefore, it seems necessary to incorporate a new approach to increase the understanding of providers and patients. Healthcare providers are not commonly told about the implications and the specifics of the GDPR. As problems with the current situation are not fully understood. To inspire healthcare providers like doctors, a new system could, first and foremost, provide an added advantage in terms of usability.

Identification does not appear to be a top priority for patients either. It is not listed in the healthcare list of quality indicators. However, the blockchain experts surveyed anticipate positive growth for self-sovereign identity in healthcare, and the government also seems eager to participate.

5. Use case

An example of a patient (the end-user) who needs to classify himself while going to the doctor demonstrates Self-Sovereign Identity's functioning based on attestation [49]. The patient must have some identifying documents to recognize and prove that they are covered to receive care from the healthcare provider or doctor. The doctor has decided that he must trust the patient and provide him with a recognized health insurance provider certification.

1) Firstly the patient needs the health insurance company to attest the insurance. For instance, SA is a health insurance company which act as an attestation issuer. So the patient will send the digital singed attestation request to the health insurance company
2) The SA health insurance attester verifies the digitally signed attestation of the patient. To verify that his attestations are authentic, he places his signature on the public blockchain for use by others.
3) The attestation received contains the signature of the attester which is sent for the patient's use.
4) The patient demands services like access to dental services from the doctor.
5) The doctor can only grant this access if such verified claims such as the policy plan and verification of personal information. Therefore the doctor may request the patient to provide credentials.
6) When the doctor receives the patient's credentials, he will verify the credentials' validity through the public ledger.
7) Based on the credentials' validation, the healthcare provider can access or deny the services.

6. Conclusion

The Self-sovereign identity is based on a set of principles that need to be satisfied. As such, various implementations are possible, but as of now, blockchain is commonly used to grant individuals true power over their own identification. It will generate data access and data ownership models. Blockchain implementations aren't widely accepted, with the only Bitcoin having an important user base. There are some general identification implementations, also in the production process or roll-out. But they're not yet optimized for healthcare applications. Estonia, however, made its health data available with a blockchain mechanism.

The self-sovereign identity will definitely boost compliance with current regulations and alter data processing paradigms in healthcare by providing patient to control identity information. It will help the healthcare service provider to become more service-oriented and develop their products or applications. It seems that self-sovereign identities can be applied cost-effectively, as they can altogether remove inefficient onboarding operations and quickly provide data access and authentication.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Bitcoin.org, "Bitcoin - Open source P2P money," 2013. https://bitcoin.org/en/ (accessed Jan. 22, 2021).

[2] C. Vine, "Proof of Work Colony," CoinDesk, Jun. 05, 2016. https://en.bitcoin.it/wiki/Proof_of_work (accessed Jan. 22, 2021).

[3] M. Westerlund and N. Kratzke, "Towards Distributed Clouds: A Review About the Evolution of Centralized Cloud Computing, Distributed Ledger Technologies, and A Foresight on Unifying Opportunities and Security Implications," in: 2018 International Conference on High Performance Computing & Simulation (HPCS), Jul. 2018, pp. 655–663, doi: 10.1109/HPCS.2018.00108.

[4] Gartner, "Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage," Gartner's 2016 Hype Cycles Highlight Digit. Bus. Ecosyst., no. August, p. 1, Sep. 2016, Accessed: Jan. 22, 2021. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2016-08-16-gartners-2016-hype-cycle-for-emerging-technologies-identifies-three-key-trends-that-organizations-must-track-to-gain-competitive-advantage.

[5] Philipp Sandner and Daniel Hofelmann, "Decision-making aid for the use of blockchain technologies in companies: Four frameworks in comparison | by Philipp Sandner | medium," Aareal, Apr. 05, 2019. https://philippsandner.medium.com/entscheidungshilfe-für-den-einsatz-von-blockchain-technologien-in-unternehmen-vier-frameworks-im-fa7b5a9a0bc5 (accessed Jan. 22, 2021).

[6] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and Big Data to Transform the Healthcare," in: Proceedings of the International Conference on Data Processing and Applications - ICDPA 2018, May 2018, pp. 62–68, doi: 10.1145/3224207.3224220.

[7] Brightlands, "Brightlands Smart Services Campus," 2018. https://www.brightlands.com/en/brightlands-smart-services-campus/brightlands-techruption#about (accessed Jan. 22, 2021).

[8] M. Shuaib, S. Alam, S.M. Daud, Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme, Springer, Singapore, 2021, pp. 3–10.

[9] S. T. Siddiqui, S. Alam, M. Shuaib, and A. Gupta, "Cloud Computing Security using Blockchain," J. Emerg. Technol. Innov. Res., 6(6), pp. 791–794, 2019, [Online]. Available: www.jetir.org.

[10] M. Shuaib, S. M. Daud, S. Alam, and W. Z. Khan, "Blockchain-based framework for secure and reliable land registry system," TELKOMNIKA (Telecommunication Comput. Electron. Control., 18(5), p. 2560, Oct. 2020, doi: 10.12928/telkomnika.v18i5.15787.

[11] S.T. Siddiqui, S. Alam, R. Ahmad, M. Shuaib, Security threats, attacks, and possible countermeasures in internet of things, in: Lecture Notes in Networks and Systems, Springer, 2020, pp. 35–46.

[12] S. Alam, M. Shuaib, and A. Samad, "A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing," in: Lecture Notes in Networks and Systems, vol. 55, 2019, pp. 231–240.

[13] S. Tabrez Siddiqui, M. Shuaib, A. Kumar Gupta, and S. Alam, "Implementing Blockchain Technology: Way to Avoid Evasive Threats to Information Security on Cloud," in: 2020 International Conference on Computing and Information Technology (ICCIT-1441), Sep. 2020, no. October, pp. 1–5, doi: 10.1109/ICCIT-144147971.2020.9213798.

[14] S. Abdus, A. Shadab, S. Mohammed, and B. Mohammad.Ubaidullah, "Internet of Vehicles (IoV) Requirements, Attacks and Countermeasures," in: 5 Int. Conf. "Co mputing Sustain. Glob. Dev., no. March, pp. 4037–4040, 2018.

[15] Bahar Houtan, Abdelhakim Senhaji Hafid, Dimitrios Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494, https://doi.org/10.1109/ACCESS.2020.2994090.

[16] A. Samad, M. Shuaib, and M. Rizwan Beg, "Monitoring of Military Base Station using Flooding and ACO Technique: An Efficient Approach," Int. J. Comput. Netw. Inf. Secur., 9(12), pp. 36–44, Dec. 2017, doi: 10.5815/ijcnis.2017.12.05.

[17] Michael Kuperberg, Blockchain-based identity management: a survey from the enterprise and ecosystem perspective, IEEE Trans. Eng. Manag. 67 (4) (2020) 1008–1027, https://doi.org/10.1109/TEM.2019.2926471.

[18] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology," arxiv.org, pp. 1–8, Apr. 2019, Accessed: Apr. 13, 2020. [Online]. Available: http://arxiv.org/abs/1904.12816.

[19] T. McGhin, K.K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: research challenges and opportunities, J. Netw. Comput. Appl. 135 (February) (2019) 62–75, https://doi.org/10.1016/j.jnca.2019.02.027.

[20] Toshendra kumar sharma, "Widespread Adoption of Self-Sovereign Identity in the Wake of COVID-19," Blockchain Council, 2021. https://www.blockchain-council.org/blockchain/widespread-adoption-of-self-sovereign-identity-in-the-wake-of-covid-19/ (accessed Jan. 14, 2021).

[21] X. Zhu and Y. Badr, "A Survey on Blockchain-Based Identity Management Systems for the Internet of Things," in: 2018 IEEE International Conference on

Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Jul. 2018, pp. 1568–1573, doi: 10.1109/Cybermatics_2018.2018.00263.

[22] D.V. Dimitrov, Blockchain applications for healthcare data management, Healthc. Inform. Res. 25 (1) (2019) 51–56, https://doi.org/10.4258/hir.2019.25.1.51.

[23] Y.S. Hau, J.M. Lee, J. Park, M.C. Chang, Attitudes toward blockchain technology in managing medical information: survey study, J. Med. Internet Res. 21 (12) (2019), https://doi.org/10.2196/15870 e15870.

[24] Tanvi Garg, Navid Kagalwalla, Prathamesh Churi, Ambika Pawar, Sanjay Deshmukh, A survey on security and privacy issues in IoV, Int. J. Electr. Comput. Eng. 10 (5) (2020) 5409, https://doi.org/10.11591/ijece:v10i5.pp5409-5419.

[25] Hyun Wook Han, "Medibloc suggests innovative paradigm to healthcare industry by developing a patient-centric healthcare data solution to make everyone's life healthier," Medibloc, Jun. 17, 2019. https://medibloc.org/en (accessed Jan. 22, 2021).

[26] N. E. W. Way, O. F. Leveraging, and M. Adherence, "Blockchains and Pharmacies: a New Way of Leveraging Medication Adherence," Intell. HQ, pp. 1–8, Mar. 2018, Accessed: Jan. 22, 2021. [Online]. Available: https://www.intelligenthq.com/blockchains-and-pharmacies-a-new-way-of-leveraging-medication-adherence/.

[27] Health Wizz, "Health Wizz — Mobile Application," Health Wizz, Feb. 2019. https://www.healthwizz.com/ (accessed Jan. 22, 2021).

[28] T. Wu, "Dentacoin: The Blockchain Solution for the Global Dental Industry," p. 37, 2017, Accessed: Jan. 22, 2021. [Online]. Available: https://dentacoin.com/%0Ahttps://dentacoin.com/web/white-paper/Whitepaper-en1.pdf.

[29] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in: 2016 2nd International Conference on Open and Big Data (OBD), Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[30] Health Gem, "Health," GemOS, 2018. https://enterprise.gem.co/health/ (accessed Jan. 22, 2021).

[31] ISO, "ISO/IEC24760-1: Information technology — Security techniques — A framework for identity management —." pp. 1–20, Dec. 2011, Accessed: Jan. 22, 2021. [Online]. Available: https://www.iso.org/standard/57914.html.

[32] M. Shuaib, S. Alam, S. Mohd, and S. Ahmad, "Blockchain-Based Initiatives in Social Security Sector," in: EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD), 2020, p. 8.

[33] F. Gaehtgens and A. Allan, "Digital Trust — Redefining Trust for the Digital Era," 2017. Accessed: Jan. 22, 2021. [Online]. Available: https://www.gartner.com/en/doc/3735817-digital-trust-redefining-trust-for-the-digital-era-a-gartner-trend-insight-report.

[34] M. Shuaib, A. Samad, S. Alam, and S. T. Siddiqui, "Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organizations," in: Advances in Intelligent Systems and Computing, vol. 904, 2019, pp. 387–399.

[35] Christopher Allen, "The path to self-sovereign identity," Coin Desk, Apr. 25, 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed May 18, 2020).

[36] S. Alam, S. T. Siddiqui, A. Ahmad, R. Ahmad, and M. Shuaib, "Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges," in: Lecture Notes in Networks and Systems, vol. 94, 2020, pp. 119–126.

[37] A. Abraham, "Whitepaper Self-Sovereign Identity," pp. 1–39, 2017.

[38] P. S. Hannigan, "Self-Sovereign Identity in Digitalized Border Security," 2019. Accessed: May 14, 2020. [Online]. Available: https://www.researchgate.net/profile/Paul_Hannigan3/project/Self-Sovereign-Identity-for-Digitalizing-Border-Security/attachment/5e4038a6cfe4a740247f6c9e/AS:856710507929600@1581267110381/download/MSc+Dissertation.pdf?context=ProjectUpdatesLog.

[39] M. Allende López, Self-sovereign identity: the future of identity: self-sovereignity, Digital Wallets, and Blockchain, Inter-American Development Bank, 2020.

[40] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized Identifiers (DIDs) v1.0," 2019. Accessed: Aug. 19, 2020. [Online]. Available: https://w3c.github.io/did-core/.

[41] C. Allen et al., "Decentralized Public Key Infrastructure A White Paper from Rebooting the Web of Trust by (alphabetical by last name)," 2015.

[42] András Lux et al., "Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials," in: 2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), Jun. 2020, pp. 71–78, doi: 10.1109/BRAINS49436.2020.9223292.

[43] D. Reed, M. Sporny, D. Longley, and C. Allen, "Decentralized Identifiers (DIDs) v0. 11: Data Model and Syntaxes for Decentralized Identifiers," 2019.

[44] S. T. Siddiqui, M. Shuaib, and B. Mohammad.Ubaidullah, "Web Based Requirements Management Tools for Software Development: A Study," in: Proc. 12th INDIACom; INDIACom-2018; IEEE, no. February 2019, pp. 10–15, 2018.

[45] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2018, pp. 1–5, https://doi.org/10.1109/PIMRC.2017.8292361.

[46] R. J. Krawiec et al., "Blockchain: opportunities for health care," ComputerWeekly.com, p. 14, 2016, [Online]. Available: https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html.

[47] R. Krawiec et al., "Blockchain: Opportunities for Health Care," 2016.

[48] S.T. Siddiqui, R. Ahmad, M. Shuaib, S. Alam, Blockchain security threats, attacks and countermeasures, Adv. Intelligent Syst. Comput. 1097 (2020) 51–62, https://doi.org/10.1007/978-981-15-1518-7_5.

[49] J. Schouten, "Opportunities for Blockchain- Based Identity in Healthcare," Master thesis, 2017.