BLOCKCHAIN™ IN HEALTHCARE TODAY

ORIGINAL RESEARCH

Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work

Abylay Satybaldy[1] MSc; Anton Hasselgren[2] MSc; and Mariusz Nowostawski[1] PhD

[1]Computer Science Department, Norwegian University of Science and Technology, Norway; [2]Department of Neuromedicine and Movement Science, Norwegian University of Science and Technology, Norway

Correspondence: Anton Hasselgren, Email: anton.hasselgren@ntnu.no

Keywords: blockchain, decentralized identity, virtual healthcare, identity management

Abstract

Background: The increasing use of various online services requires an efficient digital identity management (DIM) approach. Unfortunately, the original Internet protocols were not designed with built-in identity management, which creates challenges related to privacy, security, and usability. There is an increasing societal concern regarding the management of these sensitive data, access to it, and where it is stored. Blockchain technology can potentially offer a secure solution to address these issues in a decentralized manner without centralized authority. This is important for e-health services where the patient and the healthcare provider often are required to prove their identity. Blockchain technology can be utilized for creating digital identities and making its management easier, thus giving a higher degree of control to the user than what current solutions offer. It can be used to create a digital identity on the blockchain, making it easier for individuals and entities to manage, giving them greater control over who has their personal information and how they handle it. In addition, it might be utilized to create a higher degree of trust and security for e-health applications.
Objective: The aim of this research work was to review the state-of-the- art regarding blockchain-based decentralized identity management for healthcare applications. Based on this summary, we provide a viewpoint on how blockchain-based decentralized identity frameworks might be utilized for virtualized healthcare applications.
Methods: This research study applied a scoping, semi-systematic review approach to summarize the state-of-the-art. Included identity management systems were evaluated based on seven criteria: autonomy, authority, availability, approval, confidentiality, tenacity, and Interoperability.
Results: Seven blockchain-based identity management systems were included and evaluated in this work: these include solutions built with Ethereum, Hyperledger Indy, Hyperledger Fabric, Hedera, and Sovrin blockchains.
Conclusions: DIM is crucial for virtual health care. Decentralized identity management for healthcare purposes is currently being explored in both academia and the private sector. More work is needed with the aim of improving the efficiency of current DIM solutions and to fully understand what technical frameworks are best suited for e-health applications.

Received: December 9, 2021; Revised: December 12, 2021; Accepted: December 21, 2021; Published: March 22, 2022

Introduction

Blockchain and decentralized technologies have seen increased applications in the healthcare sector. Many of the inherited properties of blockchain technology have the potential to mitigate some of the current issues with health information systems (1, 2) and, equip a new, digital focused health care system, as an example. healthcare 4.0 (3). The identity management is a crucial part in most healthcare applications; patients need to prove that they are who they say they are and the same for medical professionals. To take a full advantage of the decentralized technologies, a digital identity management (DIM) approach should also be considered to move from current centralized solutions to decentralized or self-sovereign systems. Many decentralized healthcare applications lose its core value proposition when it needs to be tied to a

Table 1. Criteria for identity management in healthcare

Criteria	Abstract
Autonomy	Is the identifier independent from identity vendors? Identifiers must be independent of any identity provider or a central governor.
Authority	Can the individual have full control of his identity? Individuals must have complete power to manage their identities.
Availability	Can an individual have full access to his or her own data? Individuals must have full permission to gain access to their own data anytime anywhere.
Approval	Can the individual voluntarily approve the use of his identity? Individuals must voluntarily agree and approve requests before using their identity.
Confidentiality	Can the individual provide his identity with minimal disclosure of data? Individuals should share only the needed credentials with a minimal disclosure.
Tenacity	Can the identity live with the individual as long as possible? Individuals' identities must be persistent as long as possible.
Interoperability	Can the individual identity exchange data with any system or service globally? Individual Identities should be universal and widely used by any entities.

Source: Adopted from Bouras et al. (5).

centralized identity system, physical or digital. Therefore, there is a need to further explore how a decentralized identity management system could work and benefit the healthcare sector in a digital transformed system. The aim of this research work was to summarize the state-of-the-art regarding blockchain-based decentralized identity management systems for healthcare applications. Based on this summary, we provide a viewpoint on how blockchain-based decentralized identity frameworks could be utilized for healthcare applications and guide developers and researchers within this area.

Method

This research study has applied a scoping, semi-systematic review approach to summarize the state-of-the-art. The search was carried out mainly using the snowball method (4) with initial search in MEDLINE, Scopus and Google Scholar where the free text search terms: 'healthcare' OR 'e-health', were combined with the terms 'decentralized identity' OR 'blockchain' OR 'self-sovereign identity' using the Boolean operator AND. Inclusion of systems were based on how well the authors and developers had described their solutions and, to get a wide input, some diversification between the different systems was preferred. The review and the search were not meant to be comprehensive but will nevertheless provide an important summary and evaluation. As shown in Table 1, the criteria proposed by Boaras et al. (5) were adopted to evaluate the different decentralized identity management systems presented in the academic and gray literature.

Background

Blockchain

Public blockchain technology is a recent breakthrough of trusted computing without centralized authority in an open-networked system. Blockchain is a broad term for a collection of technologies that offer immutable ledgers that are replicated and synchronized over a large number of nodes. The data consistency is achieved by a special mechanism that makes the additions to the ledger agreed upon by consensus in the network. The main advantage or innovation of blockchains is the ability to achieve consensus and data consistency in the presence of certain number of malicious nodes, thus, enabling the system to operate in semi-trusted environments while maintaining security and trust of the ledger data. The public permissionless blockchains are also characterized by the absence of central administrators, eliminating the need for a trusted third party. Originally invented as the underlying infrastructure of Bitcoin (6), blockchain's potential application has reached far beyond cryptocurrency and financial assets. As the technology gained wider recognition in recent years, there have been a flurry of advancements, new use cases, and applications, including in health care (7).

Blockchain technology solves the decentralized governance over the data, and the elimination of trusted third party in maintaining consistency of data. Because of that, blockchain technology has the potential to transform and disrupt the digital society by enabling disintermediated digital platforms that have not been seen before. Since the dawn of the Internet, we have faced identity management challenges related to privacy, security, and usability. The increasing everyday usage of various online services requires an efficient DIM approach. Blockchain ledgers offer the ability to publish certain proofs or data snapshots needed for verification of digital identity attributes and credentials.

Identity

This study uses (8) the definition of identity as '*The set of known values or attributes that characterizes, identifies, or describes an entity*'. A person has several attributes, such as a name, birth date, and citizenship, which establish his or her identity in the real world. We may just use our first name or nickname among a group of friends, whereas

Citation: Blockchain in Healthcare Today 2022, **5**: 195 - http://dx.doi.org/10.30953/bhty.v5.195

within the work environment it might be necessary to use our full name. Identity also includes a set of identifiers, such as national identification number and driver's license number, which are linked to corresponding credentials. These identifiers are usually unique and issued by governmental institutions. Digital identity is a relevant concept in the digital world. A digital identity is a set of verified identifiers, digital attributes, and credentials for the digital world, similar to a person's identity in the real world (9).

Identity Management

Identity management is issuance, maintenance, and revocation of digital identifiers and credentials in applications, systems, and networks. *Identity management system* is a set of technologies and processes that can be used for identity management (9).

Traditional Identity Management

The Internet was not initially made with identity and digital credentials in mind. These aspects are something that has come after the Internet has evolved to become a medium for finance, commerce, e-health, and other broad range of services in the digital world. The traditional solutions, often based on a siloed, walled garden approach, result in privacy, security, and interoperability issues. The most conventional method for user management in online services today continues to be the use of traditional localized register of users. The end user signs up directly on the website, and the service provider creates a unique identifier and credential that is bundled together. The user can 'claim' this through identifier/password pair, provided as a form of identification. In this model, both the user and the service provider face several challenges. With the large number of online services an average person uses today, users must manage an increasingly large number of passwords, which is a daunting task. Due to this complexity, some users re-use the same password on multiple services, which leads to increased security risks. A leak of password from one of the users' online accounts results in a substantial risk of compromise of all accounts.

The second most used method is federated identity management. Most well-known federated identity schemes rely on a third-party identity provider (IdP) to broker identification using protocols, such as SAML (10), OpenID Connect (11), and OAuth (12). The user can then access multiple services using the single account. However, these centralized aggregators represent technologically a single point of control and a single point of failure. Typically, most of the service providers rely on centralized databases, which are in charge of storing the large amount of user data that could be potentially hacked by a malicious third party. The other risk is that the credential issued by the identity provider, for example, the Facebook account, can be locked by Facebook at any time, and the ability for the user to claim the credential is compromised. The credential is not stored or managed by the user, but rather, entirely controlled by the identity provider. Moreover, this model facilitates the tracking as the identity provider has access to information on what services the user is accessing and when. The results of surveys (13–15) revealed that the federated identity solution users are feeling 'lack of control' over their data and would like to control personal data themselves.

Decentralized Identity Management

Decentralized identity management is an alternative way of thinking and structuring the entire identity management workflows, which offers an improved mechanisms for verifying and authenticating users. It is a new architecture for privacy preserving and user-centric identity management. In this model, the user controls their identity data and interacts directly with the service providers – without relying on a trusted third party. The blockchain serves as a global registry for the decentralized public key infrastructure (DPKI) that provides the mapping of keys to the decentralized identifiers (DIDs).

Self-sovereign identity (SSI) is often used in synonym with decentralized identity management approaches. By combining the Martin H. Weik's definition of identity (8) and Peter de Marneffe's principles for self-sovereignty (16), we can describe SSI in its simplest form as *a digital representation of the individuals' characteristics, description, and identifiers where no government, or organization, can violate our right to choose our level of privacy or celebrity with our identity attributes*. Subsequently, Christopher Allen has defined the 10 principles of the SSI model (17). The SSI model aims to avoid a single point of dependency and allows individuals to take ownership of their digital identities. In SSI, there is no central authority, so users hold their own digital keys and have full control over their personal information. This information is typically carried around by the user in the digital identity wallet on his or her mobile device. The concept of SSI is becoming the next stage in the evolution of identity management systems. Various SSI systems exist, which provide solutions using a distributed ledger technology. Evernym (18), SertoID (19), and ION (20) are some examples of identity projects that are working on decentralized identity platforms. However, these sophisticated solutions are still at an early stage, where more discussions, validations, and investigations are needed (21).

SSI Standards

SSI is work in progress, which includes the work on standards for SSI. There are different groups and standardization agencies working to develop new standards, frameworks, and protocols, which could be the base of the SSI architecture. These efforts come from organizations like the Decentralized Identity Foundation (DIF), the European Blockchain Services Infrastructure, the Internet Engineering Task Force, IEEE, NIST, ISO, Sovrin

Foundation, OASIS, and the World Wide Web Consortium (W3C) (22). Until now, the two fundamental base standards for SSI are as follows: DIDs (23) and verifiable credentials (VCs) (24). DID is a new type of digital identifier that should be globally unique, persistent, and not requiring centralized registration authority. Its core architecture, data model, and syntax are standardized and developed by W3C DID Working Group. VC is a secure, tamper-evident digital credential that can be cryptographically verified. The W3C Credentials Community Group defines the issuance, storage, presentation, and verification of digital VCs. Moreover, DIF has several working groups that focus on authentication, secure data storage, and peer-to-peer communication in the context of SSI (25).

Privacy Properties

To protect their privacy, individuals must be empowered to control their own digital identities and personal data. Blockchains provide a promising operational environment for the trend of SSI, characterized by transformation from a non-user controlled centralized model to a fully user-controlled decentralized model.

Unlinkability. Before decentralized identity management, privacy preserving was incomplete due to the existence of centralized identity authorities. Service providers and users need to grant full trust to their identity providers. In other words, centralized identity providers could see activities between users and ser-vice providers, which compromises the identity information privacy.

Decentralized data storage. A decentralized identity model empowers users to 'bring their own storage' and give them control of their own information. This approach provides a privacy-respecting mechanism for storing, indexing, and retrieving data with a storage provider. Removing the need for dealing with storage infrastructure (instead leaving it to a specialist service provider that is chosen by the user) allows developers to focus on the functionality of their application. It reduces the compliance burden of managing customers' personal data in services.

User control and consent. In this new digital identity ecosystem, individuals (or entities) have full control over their digital credentials and attributes. Users can add, remove, and share digital credentials at their own discretion. Moreover, users can have one or more identifiers and can present credentials relating to those identifiers without having to go through an intermediary. Credentials made about a user can be self-asserted or asserted by a third-party whose authenticity can be independently verified by a relying party. All the credentials and personal identity information can be easily retrieved by the user when needed (21).

Security Properties

No single point of failure. The aggregation of personal data in one centrally controlled data storage brings an enormous risk of data breaches. The latest evidence of such data breaches are seen in Twitter (26), Equifax (27), Cambridge Analytica (28), and First American Financial (29) cases where the identity information of millions of individuals was exposed. Some of the data leaks are through hacks, but some are through design flaws of the data flows in the systems. Under the SSI model, identities must not be held by a single third-party entity.

Encrypted data vaults. As it is declared in the specification by DIF, the priority is to ensure the privacy of an entity's data so that it cannot be accessed by unauthorized parties, including the storage provider. The storage provider can not view, aggregate, analyze, or resell the data. To achieve this, the data must be encrypted while it is both at rest (on a storage system) and in transit (being sent over a network). This method also ensures that application data are portable and protected from storage provider data breaches (25).

Decentralized Identity Management for Digital Healthcare Applications

Healthcare information systems (HIS) contain medical-related data of patients that should be considered highly private. When health care is delivered both physically and digitally, it is equally important to protect the digital identity as the physical for patients in a HIS. Several blockchain-based applications and concepts for health care have been proposed (7). The digital transformation of the healthcare sector can be considered to decentralize the industry by its core; patients are generating more and more data from different personal devices, have the opportunity to receive healthcare services from a growing set of virtual healthcare providers, and medicines can now often be ordered from a variety of online pharmacies. This creates the need for patients to have the ability to digitally identify themselves more often and with more stakeholders, also outside their regular jurisdiction area (30).

In this review, we evaluate seven representative proposals for healthcare and their approach to deal with identity management. We selected these systems because they provide technical documentation, reports, and proof of concepts with the most technical details of their designs. This sample is meant to serve as an example and is not intended to be a comprehensive review of all published research in the area. By choosing seven examples with different approaches, we illustrate how identity management is tackled in a decentralized healthcare environment in the forefront of academic research and in the private sector. It is crucial to be able to verify a patient's identity and a healthcare providers' identity to deliver safe health services. This is as important in a digital environment as it is in a physical environment.

Related Work

To our knowledge, there are no more than two published papers that present a review of decentralized identity in

Citation: Blockchain in Healthcare Today 2022, **5**: 195 - http://dx.doi.org/10.30953/bhty.v5.195

health care with blockchain or distributed ledgers technology (DTL) (5, 31). These two papers highlight the need for decentralized identity management for several of use cases in the healthcare sector, in particular in e-health. Although these two publications provide insights into the topic, there is a need for further exploring how blockchain-based identity management fit in a healthcare context, especially in a virtual healthcare context. The contribution of this work is to analyze the current state-of-the-art of decentralized identity management concepts and frameworks presented in academic literature and from the industry. Furthermore, the paper summarizes how identity is managed in blockchain-based healthcare concepts in the literature. Finally, our work provides guidance for future decentralized identity systems for healthcareapplications and explores the fit of the state-of-art concepts for this purpose.

State-of-the-art in Peer-reviewed Literature

Medilinker (32) proposes a system built with Hyperledger Indy for the identity management, and Hyperledger Aeris was used as an application programming interface (API) to connect Indy's identity management features to personalized encrypted digital wallets of the users. The digital wallets hold by the patients contain private keys that control consent and personal data, including identity verifications. No personal data were stored on the blockchain. With given consent from the patients, through their digital wallets, data can be shared on chain. The consent is given using the private key, which is stored in the digital wallet. Hyperledger Indy was used with the motivation that it supports World Wide Web Consortium (W3C) standards, DIDs that provides full autonomy to users over their data, and has an active and supportive developer community.

Mikula and Jacobsen (33) presents a system for identity and access management using blockchain technology to support authentication and authorization of entities in a EHR system. The proof of concept was implemented using Hyperledger Fabric, and basic authentication and authorization operations such as registration, login, grant/revoke permissions, and update of the system were implemented. The system uses traditional front-end and back-end technologies for most parts of the system, the authentications and authorizations are vali dated through the blockchain ledger. The authors concluded that their system, implemented on the consortium blockchain Hyperledger Fabric, could scale and handle data from all the physician in Denmark, assuming that Hyperledger Fabric reaches its performance goal of 100.000 transactions per second in 15 nodes consortium.

In the article by Sharm et al. (34), the authors propose a novel healthcare framework using Inter Planetary File System and smart contracts for storage and access control of EHRs and other medical documents in the context of India's National Health Scheme. They utilized zero-knowledge proofs (ZKP) as an authentication mechanism in the proposed system to enable access to EHR in a privacy-preserving manner with the objective of increasing interoperability within the healthcare system. In the concept, the citizens of India who are entitled health instance coverage under the Prime Minister's, People's Health Scheme (PM-JAY) scheme (around 500 million individuals) can get access to a unique health ID controlled by a set of private/public keys. Biometrics is utilized together with national ID proofs to get access to the health ID at a service desk in any hospital. The individual is checked for eligibility in the PM-JAY scheme database through the service desk. If eligible, an e-card with the private key is issued to the individual. Together with a six-digit password this serves as a proof of eligibility of health services that can be used at any health providers in India.

The Health-ID solution presented by Javed et al. (35) runs on a consortium network based on the Ethereum blockchain. A consortium of healthcare regulators will manage the blockchain. An authority node is responsible for validating new blocks on the chain. The majority of the consortium decides the authority node. Their ID management systems have both patients and healthcare providers as users. The solutions require the patients to initially verify their identity using passports, national identity cards, or driving licenses. The healthcare providers are requested to use their practice license for the same, initial verification process. The identity owner can choose what kind of storage system to use for his or her identity attributes, and these can be either centralized systems or decentralized systems. The system tokenizes the identities of the participants, and the tokens are signed by healthcare regulators to verify the authenticity. The attributes of the identities are indexed on the blockchain.

State-of-the-art Developments in Practice

The Sovrin Foundation aims to standardize and build an infrastructure for SSI using blockchain as storage for decentralized identities. The Sovrin network is a public-permissioned blockchain that has been designed specifically for identity. Sovrin was one of the first projects that integrated and provided full support for VCs and DIDs. Moreover, a user can generate pairwise-pseudonymous DIDs (36) and public keys for every relationship, which makes each identifier unlinkable and protects his or her privacy. The credential exchange mechanism supports the selective disclosure based on an advanced privacy-enhancing technique known as a ZKP (37). To avoid security and privacy concerns, no private data, even in encrypted form, are stored on the Sovrin ledger.

The project was launched in 2017, and the open source code base was transferred to the Linux Foundation to become the Hyperledger Indy (38). The net-work relies on nodes called *Stewards* to achieve global consensus. The *Stewards* are approved by the non-profit Sovrin Foundation with a board

of 12 trustees. Truu (39) is one of the Sovrin Stewards that utilizes the Sovrin technology to create a portable, trusted digital ID for healthcare professionals in the UK. The company is collaborating with National Health Service (NHS) to transform the way healthcare organizations in the UK verify staff identities, qualifications, and certifications. MediBloc is developing a blockchain-based health information platform that provides patient-centric and reliable health information. Panacea is a public blockchain optimized for health data, developed by MediBloc to provide a tamper-proof, high-performance data ecosystem. Panacea blockchain relies on Delegated Proof of Stake consensus mechanism with the Practical Byzantine Fault Tolerance algorithm, which enables block validators, that are decided by votes of network participants, to create new blocks at a high speed. The Panacea Governance Council is responsible for making major technology and business decisions on the Panacea project (40).

In the MediBloc platform, health data providers can issue VCs with DID to patients. The integrity of the credential can be verified by anyone with the DID document on Panacea. The health data are managed only by the patient, and storage of the data is with the same user. The health data are stored in the form of Merkle tree, and the root hash of Merkle tree is recorded on the Panacea blockchain. The main benefit of Merkle tree method is that the users can share parts of the data while guaranteeing its integrity (41). It enables the selective disclosure of personal data. Other services that utilize a different data format can still be integrated into MediBloc through 'Merklizing' the data, and MediBloc provides software tools and guides. The platform has been used by several partner hospitals in South Korea, including Good Moonhwa Hospital, Yongin Severance Hospital, and Eunseong Medical Foundation (42, 43).

Hedera is a public distributed ledger for building and deploying decentralized applications and microservices. The network is made up of permissioned nodes run by the Hedera Governing Council, which consists of various organizations and enterprises representing industry, academia, and non-profits globally. The major software changes and business decisions are governed by council members. The Hashgraph consensus algorithm enables distributed consensus on the public Hedera ledger. The Hashgraph technology relies on the 'gossip about gossip' protocol where all nodes on the network 'gossip' about transactions to construct directed acyclic graphs (DAGs). Unlike a blockchain, DAGs time-sequence transactions without bundling them into blocks. 'Gossip' messages contain transactions, a timestamp, cryptographic hashes of two previous events and a digital signature. This enables Hashgraph to form an asynchronous Byzantine Fault-tolerant (aBFT) consensus algorithm (44).

Hedera provides developers with the tools to issue, verify, and revoke identity credentials for subjects and devices in a standards-based and privacy-respecting manner. Hedera's credentials follow the DIDs and VC standards, which are under development at the W3C. Credentials and related sensitive metadata are not stored on the Hedera main net. Currently, Hedera is being used for patient record management and health status verifications by Safe Health Systems and NHS (45).

Discussion

The digital transformation has reached the healthcare sector, and more and more health services are delivered virtually, across jurisdictions and by an increasing amount of providers. To verify one's identity as a patient (and healthcare professional) has always been important and is perhaps even more important when care is given virtually. Although many countries have implemented systems for national digital IDs, there are practical and theoretical challenges with such systems. The identity of an individual belongs to that person, and to be able to verify that such be considered a right, and not a privilege.

Blockchain technology has provided us with tools to decentralize applications that previously required a trusted third party. These new solutions and technologies present an opportunity to rethink how we manage identities and personal information digitally. SSI solutions provide the *identity owner* with full control over their identity and the ability to selectively disclose parts of that data, while keeping other parts hidden.

DIM solutions are currently under development and are evolving at a high pace. More research is needed to provide a deeper understanding of their functionalities and their role in e-health. The evaluation in 'Decentralized identity management for digital healthcare applications' section and its accompanying Tables 2 and 3 provide an overview of the current state of the decentralized identity landscape in healthcare sector. This review shows that different technical solutions are used, with different approaches to the utilization of blockchains. All the compared decentralized identity systems in 'Decentralized identity management for digital healthcare applications' section aim to give more control to patients over their identity data, and they also embrace the need for transparency and trust by providing the source code available for review. The study also reveals some unsolved challenges in developing decentralized identity solutions for healthcare applications.

Key Management

Control over user's cryptographic keys, as well as the rest of the contents of digital wallet such as credentials, is probably the single most critical element of the DIM architecture. While traditional identity management models provide a key management protocol that rely on a trusted third party, in the context of the DIM model, the responsibility of key management is assigned to the identity owners themselves. As the users are notorious for losing passwords and mobile

Citation: Blockchain in Healthcare Today 2022, **5**: 195 - http://dx.doi.org/10.30953/bhty.v5.195

Table 2. Summary of DIM solutions

DIM solutions	Distributed Ledger Technology	Privacy & Data minimisation	Identifiers & Authentication mechanism	Data Management	Open source	Scalable	Data market	Mobile friendly	Proof of concept
Sovrin Foundation	Public-permissioned Sovrin blockchain	Pairwise identifiers; Selective disclosure using VCs; No private information on Sovrin.	Based on DIDs and their associated verification keys.	Cloud + local storage	+	+	-	+	+
Hedera	Public distributed ledger Hedera Hashgraph (DAG)	Credentials or any related metadata is not stored on the nodes of the Hedera mainnet.	Based on DIDs and their associated verification keys.	Cloud + local storage	+	+	-	-	+
MediBloc	Public Panacea blockchain (DPoS)	Data minisation is implemented by Merkle proof and root hash.	Based on DIDs and their associated verification keys in DID document onPanacea.	Merkle tree root as key. Key-value database (mobile device)	+	+	+	+	+
Mikula & Jacobsen	Consortium Hyperledger Fabric blockchain	Users can grant permissions and revoke when needed. But medical identity and PIN of a patient is stored in blockchain.	The Auth- server authenticates and authorizes the user by querying the blockchain network.	Blockchain + SQL database	+	+	-	-	+
Health-ID	Consortium Ethereum blockchain	Hash of the identity attributes are stored on the blockchain.	Identifiers and attributes stored in a JSON Web Token. Smart contracts are used to authenticate users.	Blockchain + cloud storage (Dropbox, IPFS)	+	+	-	-	+
MediLinker	Hyperledger Indy and Hyperleder Aries, public permissioned blockchain	Users give consent for data sharing through their digital wallets.	The use of DIDs and digital wallets containing users private keys.	Blockchain + digital wallet	-	+	-	+	+
Sharma et al.	Public-permissionless Ethereum blockchain (PoW)	Privacy preserving identity verification using ZkSnarks. All the medical records are encrypted.	Authenticate users with existing national IDs using zero-knowledge proofs and E- cards.	IPFS and smart contracts	+	-	-	-	+

devices, the dependency on non-technical users to keep credentials safe comes with an undeniable risk. Creating a cost-efficient, usable, and secure management of identities is not an easy task. DIM requires effective innovative and well-analyzed solutions to support it.

Usability

Decentralized identity systems for healthcare applications should be designed to solve the challenges faced by the end users. We can see that the existing implementations primarily focus on the underlying technology and do not pay enough attention to the user interaction. Privacy implications for users and usable interface are crucial things when building new user-centric identity systems and need to be addressed by developers. The future decentralized identity schemes with an innovative technological underpinningbut developed with impractical end-user interaction are unlikely to create widespread uptake.

Interoperability

The results of this study show that there is still lack of a standardized implementation method for decentralized identity systems. The existing solutions have applied various methods of storage, authentication algorithms, encryption, and consent mechanisms. Due to the lack of a standardized implementation method, the evaluation and comparison of the existing solutions become challenging. However, as shown in Table 2, most of the reviewed solutions are based on W3C DIDs and VC specifications. These standards for SSI are under development and seek

Table 3. Evaluations of DIM solutions

DIM solutions	Autonomy	Authority	Availability	Approval	Confidentiality	Tenacity	Interoperability	Total
Evernym	2	2	2	3	3	1	1	14
Hedera	1	1	2	2	3	1	1	11
MediBloc	1	1	2	3	2	1	1	11
MedRec	1	1	3	3	2	2	1	13
Health-ID	1	2	2	3	3	2	1	14
Sharma et al.	2	1	3	3	3	2	2	16
Medilinker	3	2	3	3	3	3	2	19

to achieve a unified society with methods that allow communication across systems.

Scalability

Scalability challenges due to transaction throughput and latency of blockchain systems have for long time been known and recognized. In particular, the public permissionless blockchains, such as Bitcoin and Ethereum, face scalability restrictions due to high transactions costs and low throughput. There are various solutions offered for scalability of public permissionless blockchains, including layer 1 solutions (new networks such as Hedera or Solana) and layer 2 solutions that operate on top of the existing blockchains (such as Polygon and Arbitrum). Consortium or private blockchain usage can also address the scalability issues. All but one of the solutions summarized in this article use a consortium and/or private blockchain, which should enhance the scalability. Although you then need to accept a trade-off with decentralization since private and consortium blockchains are more centralized. Scalability is important to address for future work of DIM in health care.

The evaluation framework used in this article is recommended to be used by developers to ensure that their solution has a high degree of autonomy, authority, availability, approval, confidentiality, tenacity, and interoperability. The compliance to the listed criteria in Table 3 are not completely binary but rather a scale to which degree the criteria are met, the degree of compliance with a number from 0 to 3 where 0 is not at all complaint and 3 is highly compliant. Based on the outcomes and learnings from this study, the authors will develop a DIM system, tailored for a virtual healthcare environment, with the objective of improving what has been done previously.

Conclusion

In this article, we have reviewed the current state-of-the-art and presented the existing DIM solutions for healthcare applications. Based on the proposed criteria, we evaluated different DIM systems presented in the academic and gray literature.

Despite a wide variety of proposals for novel DIM for health care, current solutions are still limited. There exist open challenges related to privacy, usability, interoperability, and scalability that proposed systems are to address.

DIM is crucial for virtual health care as it offers novel features those traditional solutions lack. Decentralized identity management for healthcare applications is currently being explored in both the academy and the private sector. More work is needed with the aim to improve the efficiency of current mechanisms and to fully understand what technical frameworks are best suited for this particular use case.

Competing Interests

No conflict of interest reported.

Funding

This research study has been internally funded by the Norwegian University of Science and Technology.

Authors' Contributions

Abylay Satybaldy contributed to the conceptualization, methodology, writing, and original draft preparation of the article. Anton Hasselgren contributed to the conceptualization, methodology, visualization, writing, and original draft preparation of the article. Mariusz Nowostawski contributed with reviewing and supervision.

References

1. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In: Raj P, Deka GC, editors. Advances in computers. Vol. 111. Elsevier; 2018, pp. 1–41.
2. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography 2019; 3(1): 3. doi: 10.3390/cryptography3010003
3. Hasselgren A, Rensaa JAH, Kralevska K, Gligoroski D, Faxvaag A. Blockchain for increased trust in virtual health care: proof-of-concept study. J Med Internet Res 2021; 23(7): e28496. doi: 10.2196/28496
4. Biernacki P, Waldorf D. Snowball sampling: problems and techniques of chain referral sampling. Sociol Methods Res 1981; 10(2): 141–63. doi: 10.1177/004912418101000205
5. Bouras MA, Lu Q, Zhang F, Wan Y, Zhang T, Ning H. Distributed ledger technology for e-health identity privacy: state of the art and future perspective. Sensors 2020; 20(2): 483. doi: 10.3390/s20020483
6. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org; 2017. Available from: https://bitcoin.org/bitcoin.pdf [cited 19 August 2021].

7. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences – a scoping review. Int J Med Inform 2020; 134: 104040. doi: 10.1016/j.ijmedinf.2019.104040
8. Weik MH. Computer Science and Communications Dictionary. Boston, MA; Springer US; 2001. doi: 10.1007/1-4020-0613-6_8580
9. Ellingsen J. Self-sovereign identity systems: opportunities and challenges. Master's thesis, NTNU, 2019.
10. Hughes J, Maler E. Security Assertion Markup Language (SAML) v2.0 technical overview. OASIS SSTC Working Draft. 2005, pp. 29–38.
11. Sakimura N, Bradley D, de Mederiso B, Jones M, Jay E. Openid connect standard 1.0-draft 07. 2011.
12. Hardt D. The oauth 2.0 authorization framework. Tech. rep., RFC 6749, October 2012.
13. Mertens W, Rosemann M. Digital identity 3.0: the platform for the people. Working paper NO. 2. PWC Chair in Digital Economy. 2015. Avaiilable at: https://research.qut.edu.au/cde/wp-content/uploads/sites/279/2021/03/Digital-Identity-3.0-The-Platform-for-the-People.pdf
14. Satchell C, Shanks G, Howard S, Murphy J. Identity crisis: user perspectives on multiplicity and control in federated identity management. Behav Inf Technol 2011; 30(1): 51–62. doi: 10.1080/01449290801987292
15. Rose J, Rehse O, Rober B. The value of our digital identity. Boston Consulting Group; 2012. Available at: https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity
16. de Marneffe P. Vice laws and self-sovereignty. Crim Law Philos 2013; **7**(1): 29–41. doi: 10.1007/s11572-012-9157-x
17. Allen C. The path to self-sovereign identity. Available from: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html [cited 20 October 2021].
18. Evernym. The world's leading platform for verifiable credentials. Available from: https://www.evernym.com/ [cited 13 September 2021].
19. SertoID. Trust with control. Available from: https://www.serto.id/ [cited 13 September 2021].
20. ION. Layer 2 decentralized identifier network. Available from: https://identity.foundation/ion/ [cited 10 November 2021].
21. Satybaldy A, Nowostawski M, Ellingsen J. Self-sovereign identity systems. In: Friedewald M, Önen M, Lievens E, Krenn S, Fricker S, editors. IFIP International Summer School on Privacy and Identity Management. Springer; 2019, pp. 447–61.
22. López MA. Self-sovereign identity-the future of identity: self-sovereignity, digital wallets, and blockchain. Materials Today: Proceedings, 2019.
23. W3C Credential Community Group. Decentralized identifiers. Available from: https://www.w3.org/TR/did-core/ [cited 13 September 2021].
24. W3C. Verifiable credentials data model 1.0. Available from: https://www.w3.org/TR/vc-data-model/ [cited 20 June 2021].
25. DIF. Decentralized Identity Foundation. Available from: https://identity.foundation [cited 10 June 2021].
26. Iyengar R, CNN. Twitter accounts of Joe Biden, Barack Obama, Elon Musk, Bill Gates, and others apparently hacked. Available from: https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html [cited 15 July 2021].
27. Berghel H. Equifax and the latest round of identity theft roulette. Computer 2017; 50(12): 72–6. doi: 10.1109/MC.2017.4451227
28. Isaak J, Hanna MJ. User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer 2018; 51(8): 56–9. doi: 10.1109/MC.2018.3191268
29. Forbes. Understanding the first American financial data leak: how did it happen and what does it mean? Available from: https://bit.ly/3cmEKjJ [cited 12 May 2021].
30. Andersson T. The medical leadership challenge in healthcare is an identity challenge. Leadership in Health Services; 2015. Leadersh Health Serv (Bradf Engl). 2015;28(2):83–99. doi: 10.1108/LHS-04-2014-0032
31. Houtan B, Hafid AS, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access 2020; 8: 90478–94. doi: 10.1109/ACCESS.2020.2994090
32. Khurshid A, Holan C, Cowley C, Alexander J, Harrell DT, Usman M, et al. Designing and testing a blockchain application for patient identity management in healthcare. JAMIA Open 2021; 4(3): 1–8. doi: 10.1093/jamiaopen/ooaa073
33. Mikula T, Jacobsen RH. Identity and access management with blockchain in electronic healthcare records. In: 2018 21st Euromicro conference on digital system design (DSD); 2018 Aug 29–31, Prague, Czech Republic. IEEE; 2018, pp. 699–706.
34. Sharma B, Halder R, Singh J. Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. In: 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS); 2020 January 7-11, Bengaluru, India. IEEE; 2020, pp. 1–6.
35. Javed IT, Alharbi F, Bellaj B, Margaria T, Crespi N, Qureshi KN. Health-id: A blockchain-based decentralized identity management for remote healthcare. *Healthcare*. 2021;9:712. https://doi.org/10.3390/healthcare9060712.
36. W3C. Peer did method specification. Available from: https://openssi.github.io/peer-did-method-spec/ [cited 20 June 2020].
37. Sovrin Foundation. Sovrin: a protocol and token for self- sovereign identity and decentralized trust. 2018. Available from: https://sovrin.org/wp-content/uploads/Sovrin-Protocol- and-Token-White-Paper.pdf [cited 10 November 2021].
38. Linux Foundation. Hyperledger Indy project. Available from: https://www.hyperledger.org/projects/hyperledger-indy [cited 10 June 2021].
39. Truu. Trusted digital passports for healthcare professionals. Available from: https://truu.id/ [cited 15 October 2021].
40. Mediblock. Own your health data. It's rightfully yours. Available from: https://medibloc.com/en/ [cited 25 October 2021].
41. Mediblock. Medibloc techinical whitepaper. Available from: https://github.com/medibloc/whitepaper/blob/master/TechinicalWhitepaper_ENG.md/ [cited 25 October 2021].
42. Mediblock. Good Moonhwa Hospital. Available from: https://medium.com/medibloc/welcome-good-culture-hospital-44fb-1cb1a327 [cited 24 October 2021].
43. Mediblock. Yongin Severance Hospital. Available from: https://medium.com/medibloc/welcome-yongin-severance-hospital-c01ac5d64129 [cited 24 October 2021].
44. Hedera. Hashgraph consensus algorithm. Available from: https://docs.hedera.com/guides/core-concepts/hashgraph-consensus-algorithms [cited 20 October 2021].
45. Hedera. Hedera hashgraph for data integrity & authenticity. Available from: https://hedera.com/hh_safe-health-systems-case-study_201130.pdf [cited 20 October 2021].