A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records

Manoj T., Krishnamoorthi Makkithaya* and Narendra V G

Abstract: Over the past two decades, the fast pace of digitization in the healthcare ecosystem led to a phenomenal rise in the creation, storage and sharing of Electronic Health Records (EHRs) across the globe. However, the mechanism of authentication used for proving the identity of entities in EHRs is based on the identifiers issued by centralized identity providers (IDPs). It may lead to a single point of failure, loss of privacy and lack of interoperability. A new wave of decentralized identifiers (DIDs) and verifiable credentials (VCs) data modelled by blockchain has made it possible to achieve entity authentication in a decentralized manner. In this study, a blockchain-based framework with decentralized identifiers for patient authentication and consent management for EHR access using verifiable credentials is proposed. It describes the process of DID generation and authentication credential setup along with workflows for issuing and verifying credentials in the EHR ecosystem. The framework is implemented using Hyperledger Indy blockchain and Aries library. The study evaluates the performance of proposed workflows in terms of scalability, efficiency, resource utilization and conducts security analysis. Specifically, the outcome of this study can be used to realize the decentralized identity management and authentication in EHR systems.
Subjects: Computer Engineering; Computer Science (General); Communication Technology

Keywords: Electronic Health Records; Blockchain; Decentralized Identifiers; Entity Authentication; Verifiable Credentials; Hyperledger Aries; Hyperledger Indy

1. Introduction

In a civilized world, the identification of an entity (human, organization or a thing) is of paramount importance for performing the transactions or generating data in diversified domains such as finance, governance, healthcare, education, social networking, logistics, etc. With the help of an identifier, a claimant entity is able to prove to the verifying entity about its existence in a specific ecosystem. In the case of a human or organization, an identity provider (IDP) is involved in issuing an identity for availing the benefit of various services. When an entity uses these identifiers while operating with third parties, it may suffer from loss/theft of identity, masquerading/spoofing the identity, loss of privacy, interoperability. Besides this, the centralized management system controls most of these identifiers, which may lead to a single point of failure if it gets compromised.

The digitization movement in the 21st century fuelled by the penetration of the internet across the globe led to the conversion of paper-based records to digitized records. Even the healthcare sector has evolved itself over time to maintain patient’s health-related information in digitized records called Electronic Health Records (EHRs). Compared with the conventional paper-based system, EHRs offer ease of use, flexible record keeping and reduced operational costs (Greenhalgh et al., 2010). The sharing of health records with different stakeholder entities such as patients, physicians, researchers, insurers, etc., is very crucial in delivering a quality healthcare service (Yue et al., 2016). In India, Primary Health Centers (PHCs) offers healthcare services to the local population, and there is a need to adopt the EHR data models for public health. A health record is a systematic collection of health-related data about a patient. Whenever a patient visits a hospital, private clinic or PHC, a health record is generated. Even in electronic form, it is usually spread across multiple information systems, in different data formats and platforms (Azaria et al., 2016). These are the personal assets of patients containing valuable and critical information, and content sharing must rest with patients to preserve privacy. So, the authentication of entities sharing and accessing the EHRs becomes an area of interest in the process of conceiving a reliable healthcare system.

In the United States (US), all the healthcare ecosystem participants must comply with security and safety standards prescribed by HIPAA (Health Insurance Portability and Accountability Act) for collecting, storing and sharing EHRs. The EHR standards in India recommend the secure sharing of health records with minimal disclosure of patient identifiers (MoHFW India., 2016). According to a Cyber risk report by International Monetary Fund (IMF), around 1400 million data records have been breached using identity-based thefts as of 2020 (Adelmann et al., 2020). As per the practitioner’s report, the number of EHRs breached from 2005 to 2019 is at least 249.09 million. Out of that, in the last five years alone, approximately 157.40 million records were affected (Data Breaches, 2020). Most of the identity-related breaches are caused due to disclosure of sensitive information tied with identifiers, massive data collection and tracking enabled by the service providers. The principles promoted by the General Data Protection Regulation (GDPR; GDPR European Union, 2018) advocate entity controllable identifiers and minimum information collection to preserve privacy.

Recently, there has been a strong inclination from cybersecurity and standards developing communities such as the National Institute of Standards and Technology (NIST) to move towards decentralized identity management systems (O’Reilly et al., 2018). The blockchain has lived up to the true decentralization idea of distributed ledger technology. Its embracement has picked up momentum in the authentication of entities without a third party. However, most of the solutions proposed using blockchain depend upon centralized identifiers and smart contracts. Here the users are not in control of their identity, and smart contracts can increase the risk of vulnerability to attacks. It also poses a high risk of true identity being revealed in authentication or consent management for record sharing. The decentralized identifiers (DIDs) and verifiable credentials (VCs) based on
blockchain help resolve privacy issues in authentication and record sharing by proposing a user-centric control model for identity management. The interoperability across the services, processes and platforms are extremely difficult when the health records are spread across different service providers identified by multiple identifiers. A report by Healthcare IT News (Sullivan, 2018) states that in the USA, there are 16 other EHR vendors involved in offering services to a hospital. The globally unique identifiers like DIDs can achieve an open and interoperable EHR framework for the public health domain. The EHR should be open so that multiple stakeholders can contribute to health-related data, and interoperability leads to flexible data integration and record sharing.

The key objective of this research is to design a decentralized entity authentication framework based on decentralized identifiers and verifiable credentials with blockchain to realize entity controllable, privacy-preserving and interoperable identifier solution for EHRs. The motivation for choosing this research is that the multiple identifiers issued by centralized IDPs for entity authentication in EHRs are vulnerable to identity theft, privacy breaches very frequently, and the entity does not have control over the sensitive data. The key research contributions of this paper are:

- Firstly, we propose the blockchain-based entity authentication framework using decentralized identifiers and verifiable credentials model.
- A detailed process of DID generation and verifiable credential with required attributes is described along with methods for patient authentication and consent management for EHR access using VCs.
- We implement privacy-preserved credential issue-hold-verify workflows for patient authentication and patient-controlled consent management in EHRs using Hyperledger Indy blockchain and Aries library.
- Finally, we evaluate the performance of workflows in terms of scalability, efficiency, resource utilization and conduct its security analysis.

The remainder of this paper is organized into sections as follows: Section 2 describes the related work for entity authentication of EHRs and introduces to concepts related to blockchain, DIDs and VCs ecosystem, DID authentication, Section 3 describes the Blockchain DID-EHR framework with system architecture, DID generation and credential setup process, methods for patient authentication and consent management for EHR access using VCs, Section 4 details the implementation and evaluation of proposed workflows in the given framework, Section 5 focuses on the analysis of the framework, Section 6 concludes the paper with the brief about future work.

2. Background

2.1. Related work

2.1.1. Centralized identity management for entity authentication

In centralized identity management systems, a centralized IDPs will be responsible for issuing an identity (email id, phone number, government id, patient id) and are liable to maintain the trust factor associated with those identities. A well-established first line of defence in any identity mechanism is credential based. In the case of EHRs, as the privacy and security of the data records are vital, credential-based protection is a very trivial and flexible first-hand solution that is vulnerable to identity theft, spoofing attacks, and loss of privacy. In the case of multifactor authentication, it adds the additional layer of security to the existing credentials based authentication by the inclusion of secondary factors such as One Time Password (OTP), captchas, patterns or biometrics (Indu et al., 2018). Several studies on the two-factor authentication (Chaturvedi et al., 2017) and three-factor authentication (Renuka et al., 2019) have been conducted for authenticating the medical records. Despite
providing an additional layer of security, the multifactor authentication is prone to attacks such as identity theft, replay attack, phishing attack and DoS (Denial of Service) attack (Fernandes et al., 2014).

The authentication of entities can be achieved by binding centralized identifiers to cryptographically generated keys, signatures and certificates with the help of public key infrastructure (PKI). Some of the earlier studies that demonstrated the role of PKI in healthcare based authentication schemes includes multi-biometric key generation in cloud framework (Khan et al., 2014), Burrows-Abadi-Needham(BAN) logic combined with Elliptical Curve Cryptography (ECC; He & Wang, 2015), ECC and three-party key agreement (Odelu et al., 2015), random oracle model (Chatterjee et al., 2018) and centralized identifiers integrated with continuous biometric authentication in cloud (Farid et al., 2021). The primary issue with all the mechanisms associated with public key cryptography-based authentication is that identifier tied with the public key is controlled by either IDPs or service providers (SPs). The federated identity schemes such as OAuth, OpenID, and Security Assertion Markup Language (SAML) try to address identity silos created by multiple identifiers. The authentication schemes proposed by Bahga et al (Bahga & Madisetti, 2013) and Mandel et al., (Mandel et al., 2016) in the EHR environment makes use of SAML based Single Sign-On (SSO) method and Open ID Connect, respectively. Inspite of providing the relaxation from using multiple identifiers by federated identity mechanism, it suffers from the single point of failure problem, which could leave entities inaccessible to relying parties and also enable a service provider to breach the trust by masquerading as a user (Lesovre et al., 2019).

2.1.2. Decentralized identity management for entity authentication
The whole principle of decentralization is based on the simple idea that a transaction for a transfer of commodity/asset between two parties is approved through the consensus mechanism by the participating nodes. This transaction is recorded in an immutable distributed ledger. Blockchain is the first pragmatic distributed ledger protocol that pioneered the idea of decentralization into the financial transaction settlement. Later, the framework was generalized in the healthcare ecosystem by introducing programming capabilities using smart contracts. Yue et al. (2016) initiated the idea to adopt blockchain in the design of healthcare for decentralized identity management. MedRec (Azaria et al., 2016) is the first working prototype using blockchain for accessing the health records based on Ethereum smart contracts. Liang (2019) proposed a design for identity management and verification using blockchain technology to offer flexibility in health record access and enhanced protection for patient data. An efficient authentication mechanism for hospital networks based on blockchain was proposed by Yazdinejad et al. (2020) for the identification of distributed patients. Mubashar et al. (2021) designed a distributed hash table architecture based on IPFS and blockchain for the faster retrieval of health records.

A novel distributed architectures for EHRs based on Hyperledger fabric blockchain and conventional PKI were designed by Tanwar et al. (2020), Singh et al. (2021), and Nguyen et al. (2021). Similarly, Liang et al. (2017) and Mikula and Jacobsen (2018) achieved entity authentication through fabric environment. Some of the studies conducted on blockchain-based decentralized identity management using smart contracts for EHRs includes health-id for remote healthcare (Javed et al., 2021), identity-based authentication and key agreement (Lee & Yang, 2018) decentralized attribute-based signature technique Sun2018, Zero-Knowledge Proof (ZKP) mechanism (Hardjono & Pentland, 2019). The blockchain combined with public-key cryptography gives a powerful tool for authenticating entities with the help of smart contracts. However, it relies on the identifiers and rules dictated by the contracts and may be prone to correlation attacks. DID, also known as self-sovereign identifier (SSI) pioneered the movement and technology needed for realizing a globally unique, decentralized, cryptographically verifiable, contextual identifier with no registration authority that can be combined with blockchain for identity management to preserve the privacy of entities and ensure interoperability. The early efforts were taken by Sovrin foundation (Windle & Reed, 2018), Decentralized Identity Foundation (DIF) (Microsoft DIF Team, 2018), uPort (Lundkvist et al., 2017) in conceiving architecture and working model for decentralized identifiers. Lumedic Exchange (Nash, 2020) was the first company to demonstrate the network for the exchange of DID based credentials for healthcare.
For exchanging COVID-19 test and vaccination records, (Abid et al., 2021) proposed privacy preserved credential framework called Novidchain based on DIDs.

### 2.2. Preliminaries

#### 2.2.1. Blockchain and smart contracts

Blockchain is a peer-to-peer distributed ledger technology that is cryptographically secure, immutable, append-only that records, verifies, and updates the transactions among various parties via the consensus mechanism. The original idea of blockchain was pioneered by Stuart Haber and Scott Stornetta way back in 1991, where they outlined the use of a chain of cryptographically secured blocks for protecting the integrity and privacy of information in digital documents (Haber & Stornetta, 1991). Many related concepts such as “digicash”, “anonymous transactions”, “online shopping without bank”, “peppercoin” were on similar lines of blockchain. Still, most of them didn’t see much success due to a lack of commercial viability. Satish Nakamoto obtained the first breakthrough for the transaction of cryptocurrency named Bitcoin in a distributed and tamper proof manner (Nakamoto, 2008). The blockchain can be classified into three types, namely public blockchain, permissioned/consortium blockchain and private blockchain, depending upon who owns the distributed ledger and permission to update it (Salah et al., 2019). Some of the noteworthy blockchain platforms are Ethereum, Hyperledger, Multichain, Corda and Openchain. It is the synergy of many existing technologies such as distributed systems, peer-to-peer protocols, cryptography, consensus mechanisms and game theory. Hyperledger Indy is the permissioned and purpose-built identity-based blockchain initiated by the Sovrin foundation as the umbrella project under Linux foundation’s Hyperledger blockchain project (Windley, 2017). Indy is characterized by features such as support for decentralized identifiers and verifiable credentials, privacy preserved credential exchange, selective disclosure using zero-knowledge proofs (ZKPs), encrypted peer to peer connections, resistant to correlation attacks.

In 1990s, computer scientist named Nick Szabo mooted the idea of smart contract, where he proposed it as a set of digital promises to which transacting parties will be committed (Szabo, 1996). However, the true potential of smart contracts was not realized until the emergence of blockchain technology and consensus mechanism, which made it is possible to implement the smart contract in its true essence. Smart contracts have the characteristics of being verifiable and recordable on a blockchain, enforceable among anonymous nodes without third-party intervention and triggerable according to the predefined clauses (Wang et al., 2019). As Indy focuses on establishing the contextual identity relationship between transacting entities, it does not support any smart contracts.

#### 2.2.2. Decentralized identifiers and verifiable credentials

Decentralized Identifiers (DIDs) are a new kind of globally unique, portable and cryptographically verifiable identifier that does not rely on any centralized authority and can never be taken away (Hughes et al., 2019). The DIDs are characterized by four core properties: permanent/persistent, resolvable, decentralized, and verifiable cryptographically. The DIDs can be assigned to any entity such as human, organization or thing. Currently, efforts are done by W3C DID working group for standardizing the DIDs. The format of DID is somewhat similar to the Uniform Resource Name (URN) so that it can be adapted to work with multiple blockchain. The DID is composed of three components, namely Schema, DID method and DID method specification, as shown in Figure 1.

At a functional level, the significance of DIDs does not come from the identifier alone. Still, it depends upon how it is used by the applications designed to adopt that particular type of identifier. The DID holder and controller can be the same entity or a different one. A typical DID document comprises six optional components: id, which denotes DID, one or more public keys, authentication info, proof or signature of the DID holder, service endpoints, and metadata. The DID document is formatted in a Javascript Object Notation-Linked Data (JSON-LD) document style, and minimal DID document for any holder looks like as shown in Figure 2.
A Verifiable Credentials (VCs) is a digital attestation of identity owner using a tamper-evident credential whose authorship can be verified cryptographically (Sporny et al., 2019). The ecosystem of VCs introduces different roles for the entities such as subject (an entity about which claims are made), issuer (an entity that asserts the claims made about the subject), holder (an entity which possess the VCs), verifier (an entity which verifies the claims made about subject), verifiable data registry (a system which mediates creation and verification of keys, identifier and other relevant data) as depicted in Figure 3. The entity holding the VCs can prove to the verifying entity that it holds specific characteristics/attributes by generating the verifiable presentations and sharing them with the verifier. For instance, a citizen having VCs regarding a valid citizenship id issued by an authorized government body can share verifiable presentations with potential service providers like educators, hospitals, and banks to verify the claims. Specifically, the issuers ascertain the claims made regarding the subject before issuing the VCs. However, the verifiers draw their inferences regarding the credibility of the received credential.

2.2.3. DID authentication and decentralized key management system
DID Authentication (DID Auth) is a mechanism to realize that DID is in the control of the identity owner and prove it to the relying party with the help of different components like web browsers, mobile agents, device agents and other agents. The DID document’s “authentication” component helps demonstrate that DID is controlled by the entity that holds it. As an entity is in control of its identity, leveraging its privacy in a transaction with other parties becomes easy. DID Auth works on the principle of a challenge-response mechanism where the identity owner and relying party can mutually authenticate and establish a reliable communication channel. DID Auth and VCs exchange between transacting parties is entirely separate. Once the DID Auth process is accomplished between the transacting parties, the VCs exchange and verification protocol can be executed on top of DID Auth.

The management of keys and DIDs are the primary area of focus in decentralized identity management. The decentralized key management system (DKMS) inverts a basic idea of a traditional PKI system where centralized certificate authorities (CAs) issue digital certificates. With DKMS in place, the basis of trust for all stakeholders is any DID-based blockchain or distributed ledger. DKMS is an emerging open standard applicable to the wallets storing DIDs and private keys and to the agents that read/write from the wallets. The key idea of DKMS is to standardize the wallets storing confidential and crucial information and preserve privacy. The DKMS wallet comprises DIDs, private keys, endpoints, credentials, link secrets and tokens. A robust critical recovery method like offline recovery and social recovery is supported in DKMS.

3. Blockchain DID-EHR framework

3.1. System architecture
The system architecture for the blockchain based decentralized identifiers for entity authentication in EHRs is shown in Figure 4.

The data producers are the patients whose health records will be stored digitally in data storage entities located at hospitals, PHCs, private medical practitioners, personal healthcare systems, etc. Initially, when the patient (entity) gets admitted to the healthcare ecosystem to access the health services, authentication takes place with the help of DIDs and VCs to verify the identity. For their
own purposes, the content-rich EHRs are in demand to be accessed by various data consumers like medical researchers, health insurers, government agencies, statistics authorities, etc. VCs are exchanged between data consumers and patients to maintain the control of EHRs with patients rather than centralized authorities and share EHRs in a privacy preserved manner. As DIDs are globally unique and cryptographically resolvable persistent identifier, the interoperability is seamlessly achieved among the different EHR services. The underlying blockchain network acts as a distributed ledger to store the transactions related to identity management in terms of holding the public DIDs, keys, credential definitions, schemas and revocation registries.

3.2. DID generation and credential setup

In the general setup of entity authentication of patients and access to EHR, four actors are identified, namely Government Agency (provides valid identity proof), Patient (data producer), Healthcare Provider (data storage) and Medical Researchers/Insurers (data consumers). The source of trust is established with distributed ledger technology (blockchain) across the network of actors. The Hyperledger Indy blockchain technology built around the DIDs is used as a distributed ledger for decentralized DID generation and credential setup.

3.2.1. Stewards, actors and DID generation

The Hyperledger Indy uses two types of DIDs in their ecosystem. The first type is Verinym which determines the owner’s legal identity known to the ledger and visible to everyone. The second one is Pseudonym (blinded identifier), which is used in the context of ongoing digital connection between the parties to maintain privacy. Specifically, if a pseudonym is used to establish one digital relationship, it is called pairwise-unique identifier or peer-DID.

Stewards are the entities that can read and write to the permissioned indy ledger and run the validator nodes. They are the first actors to join the indy blockchain network. Stewards are responsible for defining the governance model and maintaining the credibility and level of trust in permissioned blockchain networks. In India, the Ministry of Health and Family Welfare (MoHFW) is entitled to formulate health policies and standards. So, for the EHR governance model MoHFW
department can be a steward to initiate and maintain the network. Stewards add the other actors (Government Agency, Healthcare provider) into a network and define their roles.

The pairwise-unique DID identifiers are generated for unique digital connections between two parties during the actors onboarding process. For instance, a pairwise-unique DID can be used for the interaction between the Patient and Healthcare Provider. The generation of pairwise-unique DID leads to the creation of verifying key, signing key and a DID. The verifying key and DID are public information recorded on the ledger, whereas the signing key is privately stored on a wallet. For the interaction with the ledger, another type of DID named Verinym needs to be used with the role of Trust Anchor. The steward onboards the Government Agency and Healthcare Provider as actors. The newly onboarded actors generate verifying key, signing key, and a new DID used as Verinym in a ledger. On receiving the communication of new DID record from actors, the steward will record the verifying key and DID to a ledger and grant the role of Trust Anchor as illustrated in Figure 5. On being accorded with the Trust Anchor role, the Government Agency and Healthcare Provider becomes fully functional to act on a ledger.

3.2.2. Credential setup
The overview of credential setup for patient authentication and EHR access is depicted in Figure 6.

The Government Agency can design a schema for issuing credentials for valid identity documents like Social Security Number (SSN) or Aadhar number. The attributes of a person considered for identity proof schema is shown in Figure 7. The credential definition is created by the issuer (Govt. Agency) utilizing the schema for offering VCs as a proof of identity for a person.

Similarly, for providing privacy preserved consent management for EHR access, a consortium on behalf of healthcare providers can design a schema for issuing credentials to researchers/insurers. Figure 8 provides the details of attributes related to a researcher utilized for EHR access schema. A particular issuer (Healthcare Provider) can later create credential definition following available schema and offer the VCs to access EHRs.
Figure 5. Steward onboarding and assigning actors with trust anchor role.

Figure 6. Credential setup for patient authentication and EHR access.

Figure 7. Attributes for identity proof schema.
3.3. Patient authentication using verifiable credentials

For the patient authentication in the EHR ecosystem with verifiable credentials following method is designed. The sequence of messages shared among issuer, holder and verifier during identity credential and identity proof exchange is detailed in Figure 9.

Step 1: Identification of the actors with specified roles

Issuer—Government Agency; Holder—Patient; Verifier—Healthcare Provider
Figure 10. Illustration of patient controlled consent management for EHR access using VCs.

Step 2: Offer-Request-Issuance at Issuer Side

a) **Credential Offer**: A Government Agency offers an identity-based credential to a Patient.

b) **Credential Request with Blinded Link Secret**: The Patient will retrieve the credential definition from ledger and generate identity credential request along with link secret to Government Agency.

c) **Credential Issuance connected to Blinded Link Secret**: The verifiable credential will be created by filling in the values in identity proof schema and adding proof connected to link secret and provided to Patient to be stored in wallet for future use.

Step 3: Offer-Request-Issuance at Verifier Side

| Table 1. Description of nodes used in experimentation |
|-----------------------------|----------------|----------------|----------------|----------------|
| Type of Node  | Processor Type | CPU Speed(GHz) | Operating System | Make and Model |
| Desktop        | 64-bit          | 3              | Ubuntu 20.04     | Lenovo V310z-All-in-One |
| Desktop        | 64-bit          | 3              | Ubuntu 20.04     | Lenovo V310z-All-in-One |
| Laptop         | 64-bit          | 2.20           | Ubuntu 20.04     | Lenovo Ideapad-110-15ACL |
a) **Proof Offer**: Patient tries to prove the identity to EHR systems, through proof offer to the Healthcare Provider.

b) **Proof Request**: After extracting the credential definition’s necessary attributes, the proof request is sent to the Patient by the Healthcare Provider.

---

**Table 2. Details of tools used in the experimentation**

| Tools                  | Description                                                                 |
|------------------------|-----------------------------------------------------------------------------|
| Docker Community Edition | Docker is used for getting all libraries and packages required for experimentation and avoid inconsistencies between the systems. |
| Hyperledger Indy       | It is the permissioned blockchain used for identity management and the indy ledger provided by bcgov in the form of von-network is used in setting up blockchain network locally. |
| Hyperledger Aries ACA-Py | Aries Cloud Agent Python library is used for issuing, storing and verifying the credentials in a non-mobile environment. |
| REST APIs              | Representational state APIs are used for exchanging the credentials between two end-points of Aries agents. |

---

**Figure 11. NYM, ATTRIB, SCHEMA and CRED_DEF ledger transactions for workflow 1.**

(a) NYM Transaction  
(b) ATTRIB Transaction  
(c) SCHEMA Transaction  
(d) CRED_DEF Transaction  

---

**Retrieval Information:**

- **Source:** T et al., Cogent Engineering (2022), 9: 2035134  
  https://doi.org/10.1080/23311916.2022.2035134  
  Page 12 of 23
c) **Proof Presentation**: The Patient will retrieve the VC from the wallet and presents the proof to the Healthcare Provider.

d) **Proof Verification**: The Healthcare Provider will verify that proof of identity is provided by valid Government Agency by matching it against the public key of the issuer in the blockchain.

### 3.4. Patient controlled consent management for ehr access using verifiable credentials

For patient-controlled consent management of EHRs using verifiable credentials following method is designed. The sequence of messages shared among issuer, holder and verifier during EHR access credential and EHR access proof exchange is detailed in Figure 10.

**Step 1: Identification of the actors with specified roles**

**Issuer**—Healthcare Provider; **Holder**—Researcher/Insurer; **Verifier**—Patient

**Step 2: Offer-Request-Issuance at Issuer Side**

a) **Credential Offer**: The Healthcare Provider offers an EHR access credential to a Researcher/Insurer.

b) **Credential Request with Blinded Link Secret**: The Researcher/Insurer will extract required credential definition from the ledger and add an EHR access credential request with link secret to Healthcare Provider.
c) **Credential Issuance connected to Blinded Link Secret**: The Healthcare Provider will generate necessary values for EHR access schema, proofs combined with link secret and issue a VC to the Researcher/Insurer.

**Step 3: Offer-Request-Issuance at Verifier Side**

a) **Proof Offer**: A proof offer will be generated whenever necessary for the researcher/insurer to access the EHR of a particular Patient.

b) **Proof Request**: In response, after looking up required attributes from credential definition, a proof request will be created by Patient to the Researcher/Insurer.

---

| Table 3. Average time duration for issuing and verifying credential in workflow 1 |
|---|---|---|
| No. of Credentials | Govt. Agency and Patient | Patient and Hospital |
|---|---|---|
| 50 | 0.75 | 0.38 |
| 100 | 0.74 | 0.38 |
| 150 | 0.79 | 0.41 |
| 200 | 0.77 | 0.43 |
| 250 | 0.79 | 0.47 |
| 300 | 0.80 | 0.47 |
| 350 | 0.79 | 0.41 |
| 400 | 0.82 | 0.47 |

| Table 4. Average time duration for issuing and verifying credential in workflow 2 |
|---|---|---|
| No. of Credentials | Hospital and Researcher | Researcher and Patient |
|---|---|---|
| 50 | 0.79 | 0.42 |
| 100 | 0.88 | 0.45 |
| 150 | 0.96 | 0.45 |
| 200 | 0.98 | 0.44 |
| 250 | 0.88 | 0.45 |
| 300 | 0.87 | 0.48 |
| 350 | 0.85 | 0.47 |
| 400 | 0.85 | 0.46 |

| Table 5. Comparison of resource utilization metrics with workflow 1 |
|---|---|---|---|
| | Memory (Avg) | CPU (Avg) | Network Input (Avg) |
| SoA1 | 207.5 MB | 27.70% | 6.6 MB |
| SoA2 | 200.3 MB | 3.03% | 3.3 MB |
| Our Workflow 1 | 98.3 MB | 5.24% | 8.1 KB |
| | | | Network Output (Avg) |
| | | | 713.36 KB |
c) **Proof Presentation:** The Researcher/Insurer will present the required VC from the wallet as proof to the Patient for verification.

d) **Proof Verification:** The Patient will verify that proof of EHR access issued by a specific Healthcare Provider through the public key obtained from the blockchain.
4. Implementation and evaluation

4.1. Experimental setup
The verifiable credentials model for patient authentication and consent management for EHR access using DIDs is realized using a Python-based Hyperledger Aries Cloud Agent (ACA; Hyperledger Aries CloudAgent Python, 2020) enabled with Hyperledger Indy blockchain locally running validator nodes in the form of von-network. The Aries ACA-Py agent is configured on two desktop machines and one laptop with the docker on Ubuntu 20.04 operating system connected using 1000 Mbps Ethernet cable to perform the experimentation of exchanging messages, issuing, storing and verifying credentials by the respective agents in the EHR environment. The description of the nodes and tools used in the experiment is detailed in Tables 1 and 2. The implementation of
patient authentication and consent management for EHR access is conducted on non-mobile agents considering the following two workflows:

**Workflow 1**: A Patient named "ABC" is requesting for identity credential from the Government Agency and plans to present the same identity credential as proof to the Hospital to avail services.

**Workflow 2**: A Researcher named "XYZ" requesting an EHR access credential from the Hospital and is willing to present the same access credential to the Patient (ABC) to retrieve their health records.

### 4.2. Experimental results

#### 4.2.1. Blockchain/ledger transactions

In Hyperledger Indy all the transactions are stored in a distributed ledger based on a Merkle tree. There are multiple ledgers which are categorized as pool ledger (network configuration transactions), config ledger (network upgrade transactions) and domain ledger (application and domain specific transactions). The transactions related to workflows 1 and 2 described in this study are recorded in the domain ledger. The key transactions maintained in the domain ledger are NYM, ATTRIB, SCHEMA and CRED_DEF. NYM transaction is used to create a Verinym identifier (DID known to the ledger) and corresponding record. The major components of this transaction block are target DID or Verinym identifier encoded in base58 string format, role of the agent (Steward, Trustee, Endorser or Common user), base58 encoded verification key. To add an attribute value to

| Table 6. Comparison of resource utilization metrics with workflow 2 |
|---------------------------------------------------------------|
| **Memory (Avg)** | **CPU (Avg)** | **Network Input (Avg)** | **Network Output (Avg)** |
| SoA1             | 206.0 MB      | 28.93%                  | 6.6 MB                  | 3.6 MB                  |
| SoA2             | 156.6 MB      | 3.04%                   | 3.3 MB                  | 2.2 MB                  |
| Our Workflow 2   | 99.4 MB       | 6.41%                   | 30.67 KB                | 1040.8 KB               |

| Table 7. Qualitative comparison with state-of-the-art |
|-------------------------------------------------------|
| **Features of Identifiers Used in Authentication** |
| **User Controllability** | **Privacy Preserved** | **Interoperability** | **Persistence** | **Use of Smart Contract** |
| Abid et al., (Abid et al., 2021) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Javed et al., (Javed et al., 2021) | ✓ | ✓ | × | × | ✓ |
| Nguyen et al., (Nguyen et al., 2021) | × | ✓ | × | × | ✓ |
| Singh et al., (Singh et al., 2021) | × | ✓ | × | × | ✓ |
| Tanwar et al., (Tanwar et al., 2020) | × | ✓ | × | × | ✓ |
| Yazdinejad et al., (Yazdinejad et al., 2020) | × | ✓ | × | × | × |
| Our Approach | ✓ | ✓ | ✓ | ✓ | × |
NYM record domain ledger makes use of ATTRIB transaction. Information such as target DID and attribute data is included in this transaction. SCHEMA transaction generates a template with the required attributes for issuing a credential to the user/holder. The fields such as signature type, tag and attributes constitute the information for this transaction. Workflow 1 generates an Identity proof schema and workflow 2 generates an EHR access schema. On the request of a specific user/holder, the CRED_DEF transaction defines a credential with the user-specific values inserted into the schema in the form of public keys that can be verified without revealing the holder’s identity. This transaction is made up of fields namely signature type, tag and attribute values. Figures 11 and 12 show all four transactions in action during workflow 1 and workflow 2, respectively.

4.2.2. Credential issue, hold and verify for workflows 1 and 2

Step 1: Initially, agents representing the actors in Workflow 1 (i.e., Govt. Agency, Patient, Hospital) and Workflow 2 (Hospital, Researcher, Patient) are connected with the help of Quick Response (QR) code invite.

Step 2: The Government Agency registers an identity proof schema definition to the indy ledger as shown in Figure 13a.

Step 3: The request for the identity proof credential from a Patient agent (ABC) is accepted and validated by Government Agency, and the credential is issued to them, as shown in Figure 13b.

Step 4: The Hospital agent requests the Patient agent (ABC) to prove its identity with the help of “Aadhar Number”, “Name” and “Date of Birth” as the attributes. In response, the identity proof credential produced by Patient agent (ABC) is verified through public keys of the issuer by the Hospital agent, as shown in Figure 13c.

Step 5: The Hospital agent issues an EHR access schema definition to the indy ledger as shown in Figure 13d.
Step 6: Now, when a Researcher agent (XYZ) is interested in accessing an EHR of the Patient(ABC), a specific access credential request is made to the Hospital agent. On meeting a particular hospital's ethical guidelines, it is issued to the Researcher agent (XYZ), as shown in Figure 13e.

Step 7: Finally, a Researcher agent (XYZ) presents EHR access credential proof in the form of "Researcher ID", "Researcher Name", "Accessible EHR ID", "Approving Authority", "Date of Approval" attributes to the Patient agent(ABC) to get access to the EHR as shown in Figure 13f.

4.3. Performance evaluation

4.3.1. Scalability and efficiency
The performance of workflows 1 and 2 implemented on Hyperledger Indy blockchain and Aries library is evaluated in terms of time duration for issuing and verifying the credentials in the EHR ecosystem. The experiment is conducted to issue and verify the different credentials to test workflows 1 and 2's scalability. The time duration to issue and verify a different identity credentials in workflow 1 is graphically exhibited in Figure 14. Similarly, the time duration to issue and verify various EHR access credentials in workflow 2 is shown in Figure 15. From these graphs, we can infer that the time duration for issuing and verifying credentials increases linearly as the number of credentials are increased. Thus, the proposed method in both workflows offers flexibility and can be seamlessly scaled to a higher number of transactions.

To measure the efficiency of issuing and verifying credentials, average time duration per credential issue and verification during workflows 1 and 2 are computed and listed in Tables 3 and 4. The average time duration per credential issue ranges between 0.74 seconds to 0.82 in the case of workflow 1 and 0.79 s to 0.98 s in workflow 2. In the same way, the average time duration per credential verify ranges between 0.38 s to 0.47 s in the case of workflow 1 and 0.42 s to 0.48 s in the case of workflow 2. The average time taken for credential verification is almost half of the credential issuance. The obtained results show that with decentralized solution in place, the average time taken for issuing and verifying a credential is within a second, which is very optimal.

4.3.2. Resource utilization
The performance metrics such as CPU usage, memory usage, network input and network output are used to evaluate resources utilized by the Government Agency, Patient and Hospital agents in the workflow1 and Hospital, Researcher and Patient agents in workflow 2. In this work, we have compared the resource utilization metrics of Hospital agent in workflow 1 and Patient agent in workflow 2 with the resource utilization of state-of-art mechanisms mentioned in SoA1 (Tanwar et al., 2020) and SoA2 (Singh et al., 2021), which is shown in Tables 5 and 6, respectively. Both workflows 1 and 2 performed better than SoA1 and SoA2 in terms of average memory consumption and network utilization (input and output). In terms of average CPU usage, the performance of workflows 1 and 2 is better than SoA1. However, in the case of SoA 2, average CPU consumption is slightly better than our workflows. The observations made for maximum resource utilization of all agents in workflows 1 and 2 are graphically represented in Figures 16 and 17, respectively. The results show that the verifier agent’s maximum CPU and memory in workflows 1 and 2 are lower than credential issuing agents. Even the data consumed by verifier agents in both the workflows from the network are very minimal. As the EHR environment involves verification of credentials as frequent transactions, workflows 1 and 2 provide an efficient and optimized solution.

5. Analysis

5.1. Qualitative comparison
In this section, proposed approach for identity management and authentication is compared with the state-of-the-art decentralized blockchain-based authentication systems based on the expected features of identifiers as described in Allen (2016). They include features like user controllability, minimal
disclosure of identities (privacy-preserving), interoperability, persistence and use of smart contracts as shown in Table 7. User controllability refers to fact that users have complete control over their identity without any dependency upon centralized systems. To preserve the privacy, the attributes related to identifier has to be disclosed as minimal as possible. Interoperability of identifiers helps in achieving the flexible and easy transition among various types of EHR systems. Persistence deals with fact that identifiers must be long-lived and should not be taken easily. The existing systems proposed by Nguyen et al. (2021), Singh et al. (2021), Tanwar et al. (2020), and Yazdinejad et al. (2020) make use of identifiers like patient id, hospital id issued by central administrators for authentication, which suffers from lack of user control, interoperability and persistence. The authentication scheme designed by Javed et al. (2021) tries to achieve the user-controlled decentralized identity but it fails in attaining interoperability and persistence as it associates the identifier with smart contracts. Similarly, work demonstrated by Abid et al. (2021) scores well in achieving the user control, privacy, interoperability and persistence, yet its association with smart contracts makes independent existence of identifiers quite challenging. Our proposed approach offers user-controlled, privacy preserved, interoperable and persistent decentralized identifiers for authentication without any overhead of smart contracts vulnerable to security threats.

5.2. Security analysis
This section conducts a security analysis of decentralized identifiers used for patient authentication and consent management of EHR access. The identity theft and Sybil attacks are restricted to a minimum in the case of decentralized identifiers, as users are in charge of their identity. The selective disclosure of identity and contextual identity relationships ensures that leakage and correlation attacks won’t occur. The option for flexible key rotation is available in decentralized identifiers that generate a new DID document and establish a self-controlled identifier trust that follows best cryptography practices. The privacy preserved sharing and verification of credentials using ZKP does not disclose the identity of the credential holder to any third party and not even to the verifier. As decentralized identifiers are unique, persistent, cryptographically verifiable global identifiers, they can be flexibly and seamlessly integrated with EHRs operating in different domains.

Generally, the smart contracts used in blockchain are prone to multiple security issues such as abnormal contracts, programming vulnerabilities in contracts, unsafe external data. Besides that, when an identity solution is implemented using smart contracts, the independent existence of the identity related to the user is violated. The solution designed by us does not make use of any smart contracts for identity management and avoids its vulnerabilities.

6. Conclusion and future work
The healthcare records are sensitive and require high security against data breaches and privacy-based disclosure during its collection and sharing. This study proposes a blockchain-based framework for entity authentication and privacy preserved consent management for EHR access using DIDs and VCs. The decentralized feature of the framework does not delegate control to a few centralized IDPs to authenticate and authorise access to sensitive health records. The integration of decentralized identifiers with verifiable credentials data model leverages the patient’s privacy in consent management for record access. The interoperability is easily realized as decentralized identifiers break the identity silos and plumbing required for a wide variety of EHR ecosystems.

The entire process of DID generation and credential setup is discussed in detail. The issue-hold-verify workflows defined for the patient authentication and consent management for EHR access is implemented using Hyperledger Aries and Indy framework for non-mobile agents. In our implementation, no private information related to the identity of patients or healthcare records is stored in the blockchain. Only publicly visible items such as public DIDs, schemas and credential definition are shown. The individual entities such as patients, researchers use peer DIDs instead of public DIDs, which helps them create contextual relationships with public entities such as hospitals and government agencies.
The performance evaluation of workflows is conducted w.r.t. its scalability, efficiency and resource utilization. The evaluation results show that the proposed approach is highly scalable and efficient in terms of time consumption for issuing and verifying the credentials. The further reduction in time duration can be achieved with the enhancements to credential exchange formats. Our approach proved to be better than existing systems as far as resource utilization like CPU, memory and network. A qualitative comparison of different existing identity management schemes with our approach is made based on expected features of decentralized identifiers. The security analysis shows that implemented workflows are resistant to data breaches, correlation, and information leakage attacks. Future work intends to implement the proposed framework in Hyperledger Aries and Indy for mobile agents and integrate it with real-time identity management and authentication mechanisms. We are also interested in fusing the machine learning algorithms to understand the pattern and behaviour of EHR record sharing for medical research or insurance purposes.

Funding
The authors received no direct funding for this research.

Author details
Manoj T1
ORCID ID: http://orcid.org/0000-0002-5472-2418
Krishnamoorthi Makkithaya1
E-mail: k.moothi@manipal.edu
Narendra V G1
ORCID ID: http://orcid.org/0000-0002-6239-0056
1 Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India.

Citation information
Cite this article as: A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records, Manoj T, Krishnamoorthi Makkithaya & Narendra V G, Cogent Engineering (2022), 9: 2035134.

Note
1. A blinded link secret is a large random number that helps: the holder prove that a credential is indeed issued to them. It is a cryptographic commitment that is blinded and included in the signature of the issuer so that holder can prove the knowledge of a secret without disclosing it.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Author statement
In healthcare information systems, the data flow among different stakeholders in the value chain matters for decision making. For the application of modern-day machine intelligence, trust in the data sources is paramount to preserve transparency. So, our research group mainly focuses on synergizing the Blockchain, AI and Machine Learning for enabling trust attributes in information systems. The study on “A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records” aims to achieve user-controlled, privacy-preserving authentication and consent management for EHRs using blockchain-based self-sovereign identity principles. The key idea of decentralized digital identity management can be used in any application domain. Verifiable credentials can be issued and verified in a privacy-preserved way without relying on centralized authorities.

References
Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). Novidchain: Blockchain-based privacy-preserving platform for covid-19 test/vaccine certificates (pp. 1–27). Software Practice & Experience. https://doi.org/10.1002/spe.2983
Adelmann, F., Elliott, J. A., Ergen, I., Gaidosch, T., Jenkinson, N., & Khioaonong, T., … others (2020). Cyber risk and financial stability: It's a small world after all (Tech. Rep.). International Monetary Fund.
Allen, C. (2016). The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed:11.01.2022)
Azaria, A., Eklblad, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International conference on open and big data. IEEE: OBD, 25–30. https://doi.org/10.1109/OBD.2016.11
Bahga, A., & Madisetti, V. K. (2013). A cloud-based approach for interoperable electronic health records (ehrs). IEEE Journal of Biomedical and Health Informatics, 17(S), 894–906. https://doi.org/10.1109/JBHI.2013.2257818
Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., & Vasilakos, A. V. (2018). Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment. IEEE Transactions on Dependable and Secure Computing, 15(5), 824–839. https://doi.org/10.1109/TDSC.2016.2616876
Chaturvedi, A., Mishra, D., & Mukhopadhyay, S. (2017). An enhanced dynamic id-based authentication scheme for telecare medical information systems. Journal of King Saud University Computer and Information Sciences, 29(1), 54–62. https://doi.org/10.1016/j.jksuci.2014.12.007

Data Breaches. (2020). https://privacyrights.org/data-breaches (accessed:10.05.2021)
Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised iot and cloud computing-based healthcare services. Sensors, 21 (2), 552. https://doi.org/10.3390/s21020552.
Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V. P., Freire, M. M., & Incio, P. R. M. (2016). Security issues in cloud environments: A survey. International Journal of Information Security, 15(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7
GDPR European Union. (2018). General Data Protection Regulation. https://gdpr-info.eu/ (accessed:10.05.2021)
Greenhalgh, T., Hinder, S., Stramer, K., Braton, T., & Russell, J. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: Case study of HealthSpace. Bmj, 341. https://doi.org/10.1136/bmj.c5814
Haber, S., & Stornetta, S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99–111. https://doi.org/10.1007/BF00196791
Hardjono, T., & Pentland, A. (2019). Verifiable anonymous identities and access control in permissioned blockchains. arXiv preprint arXiv:1903.04584. https://arxiv.org/pdf/1903.04584

He, D., & Wang, D. (2015). Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal, 9(3), 816–823. https://doi.org/10.1109/JSTY.2014.2301517

Hughes, A., Sporny, M., & Reed, D. (2019). A Primer for Decentralized Identifiers—An Introduction to self-administered identifiers for curious people (W3C Credentials community group). https://w3c-ccg.github.io/did-primer/ (accessed: 11.05.2021)

Hyperledger Aries Cloudagent Python. (2020). 34. https://github.com/hyperledger/aries-cloudagent-python (accessed: 20.07.2021)

Mikula, T., & Jacobsen, R. H. (2019). Identity and access management with blockchain in electronic healthcare records. In 2018 21st Euromicro conference on digital system design (dss), IEEE. (699–706).

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. An International Journal, 21(4), 574–588. https://doi.org/10.1016/j.jestech.2018.05.010

Javed, I. T., Alharbi, F., Bellaj, B., Margoria, T., Crespi, N., & Qureshi, K. N. (2021). Health-id: A blockchain-based decentralized identity management for remote healthcare. Healthcare, 9 (6), 712. https://doi.org/10.3390/healthcare9060712

Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A cloud-based framework for security and patients’ data privacy using wireless body area networks. Computers Science Procedia, 34, 511–517. https://doi.org/10.1016/j.proced.2014.07.058

Lee, S.-H., & Yang, C. (2019). Fingerprint analysis management system using microscopy sensor and blockchain technology. International Journal of Distributed Sensor Networks, 14(3), 155014771876074. https://doi.org/10.1177/1550147718760744

Lesavre, L., Varin, P., Meil, P., Davidson, M., & Shook, J. (2019). A taxonomic approach to understanding emerging blockchain identity management systems. arXiv preprint, arXiv, 1908.00929. https://arxiv.org/ftp/arxiv/papers/1908/190800929.pdf

Liang, Y. (2019). Identity verification and management of electronic health records with blockchain technology. In 2019 ieee international conference on healthcare informatics (ihci), IEEE, (pp. 1–3).

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 ieee 28th annual international symposium on personal, indoor, and mobile radio communications (pimrc), IEEE, (pp. 1–5)

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Seno, M. (2017). Uport: A platform for self-sovereign identity. https://whitepaper.uport.me/uPort whitepaper DRAFT20170221.pdf (accessed: 26.10.2021)

Mandel, J. C., Kreda, D. A., Mondi, K., Kohane, I., & Ramoni, R. (2016). Smart on fhir: A standards-based, interoperable apps platform for electronic health records. Journal of the American Medical Informatics AssociationJAMIA, 23(5), 899–908. https://doi.org/10.1093/jamiaocv189

MohFW India. (2016). Electronic Health Standards ForIndia. https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf (accessed: 26.10.2021)

Mubashar, A., Asghar, K., Javed, A., Rizwan, M., Srivastava, G., Gadekallu, T., & Shabbir, M. (2021). Storage and proximity management for centralized personal health records using an ipsfs-based optimization algorithm. Journal of Circuits Systemsand Computers, 31(2), 2250010. https://doi.org/10.1142/S0218126622500104

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf

Nash, M. (2020). Introducing lumedconnect. https://www.lumedic.io/ perspectives/introducing-lumedic-connect (accessed: 26.10.2021)

Nquyen, D. C., Pathiranar, P. N., Ding, M., & Seneviratne, A. (2021). Bedgearch: A decentralized architecture for edge-based iomt networks using blockchain. IEEE Internet of Things Journal, 8(14), 11743–11757. https://doi.org/10.1109/JIOT.2021.3058953

O’Reilly, P. D., Rigopoulos, K. G., Witte, G. A., & Feldman, L. (2018). NIST/ITI cybersecurity program annual report 2019 (Tech. Rep.). NIST. https://doi.org/10.6028/NIST.SP.800-211

Odelu, V., Das, A. K., & Goswami, A. (2015). An efficient biometric-based privacy-preserving three-party authentication with key agreement protocol using smart cards. Security and Communication Networks, 8(18), 4136–4156. https://doi.org/10.1002/sec.1330

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., & Holt, J. (2020). Decentralized identifiers (dids) v1.0. Draft Community Group Report. https://www.w3.org/TR/2019/WD-did-core-20191107/

Renuka, K., Kumari, S., & Li, X. (2019). Design of a secure three-factor authentication scheme for smart healthcare. Journal of Medical Systems, 43 (5), 133. https://doi.org/10.1007/s10916-019-1251-3

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for ai: Review and open research challenges. IEEE Access, 7, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507

Singh, A. P., Pradhan, N. R., Luhach, A. K., Agnihotri, S., Jhanjhi, N. Z., Verma, S., … Roy, D. S. (2021). A novel patient-centric architectural framework for blockchain-enabled healthcare applications. IEEE Transactions on Industrial Informatics, 17(8), 5779–5789. https://doi.org/10.1109/TII.2020.3037889

Sporny, M., Longley, D., & Chadwick, D. (2019). Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web. W3C. https://www.w3.org/TR/ Verifiable-Credentials-Draft/what-is-a-verifiable-credential (accessed: 11.05.2021)

Sullivan, T. (2018). Why ehr data interoperability is such a mess in 3 charts. https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts (accessed: 26.10.2021)

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. of EXTROPY: The Journal of Transhumanist Thought 16, 18(2).

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/10.1016/j.isac.2019.102407.

Team, M. D. I. F. (2018). Decentralized identity- own and control your identity. Microsoft. https://query.prod.cms.cms.microsoft.com/cms/api/opi/cms/Re2DjY (accessed: 26.10.2021)

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Transactions on Systems. Man and Cybernetics Systems, 49(11), 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123
Windley, P. (2017). Hyperledger Welcomes Project Indy. Hyperledger Project. https://github.com/hyperledger/aries-cloudagent-python (accessed: 20.07.2021)

Windley, P., & Reed, D. (2018). Sovrin: A protocol and token for self-sovereign identity and decentralized trust. Whitepaper the Sovrin Foundation. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, -K.-K. R., & Aledhari, M. (2020). Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE Journal of Biomedical and Health Informatics, 24(8), 2146–2156. https://doi.org/10.1109/JBHI.2020.2969648

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 1–8. https://doi.org/10.1007/s10916-016-0574-6