


# Identity and access management using distributed ledger technology: A survey

Fariba Ghaffari<sup>1,2</sup>  | Komal Gilani<sup>1,2</sup> | Emmanuel Bertin<sup>1,2</sup> | Noel Crespi<sup>2</sup>

<sup>1</sup>Orange Innovation, Caen, France

<sup>2</sup>IMT, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France

## Correspondence

Fariba Ghaffari and Emmanuel Bertin, IMT, Telecom SudParis, Institut Polytechnique de Paris, 91764 Palaiseau, France.

Email: fariba.ghaffari@orange.com; emmanuel.bertin@orange.com

## Summary

As the basic building block of any information security system, identity and access management (IAM) solutions play vital role in enterprise's security programmes. Providing centric solutions for IAM is inefficient in terms of having single point of failure, high cost, duplication and complexity to the users. Recently, emerging the distributed ledger technology (DLT) has attracted significant scientific interests in research areas like identity management, authentication and access control processes. In these contexts, Blockchain can offer greater data and rule confidentiality and integrity, as well as increasing the availability of the system by removing the single point of failure in the procedure. In this paper, we provide a comprehensive overview of the IAM solutions based on their basic components including identity management, authentication and access control. In the identity concept, we discuss about self-sovereign identity which enhances privacy and security of distributed digital identities by providing individual's consolidated digital identity and verified attributes for enabling them to utilize their ownership. To offer a clearer understanding of the state of the art, we propose taxonomy to categorize them based on their features. For the conclusion of the paper, we compare the existing methods based on proposed taxonomy. Also, considering the advantages and disadvantages of existing methods, we discussed about the possible future directions.

## 1 | INTRODUCTION

As information systems have dramatically increased the number of their users, identity management (IdM), authentication, and access control (AAC) have become critical factors in resource and information protection. The combination of these security solutions results in identity and access management (IAM) methods. The majority of existing IAM solutions are centralized which have become one of the most challenging security parts in the companies in order to protect user's privacy and have secure and compliant access to IT resources. As a brief explanation, the IAM framework connects multiple interdependent components, including an identities' database, a credential manager, an authentication server, a credential core, a resources database, a resource manager, an access policy engine, and a trust engine to provide information security.<sup>1</sup>

The importance of IAM solutions can be projected in IdM and access control components. To provide user-centric services, organizations assemble huge amounts of personal information. The collected data are further utilized for profiling, prediction, and economic growth. In existing IdMs, the management of identities and Personally Identifiable Information (PII) is controlled by Central Authorities (CA), and the user has little or no control over their data sharing and privacy. Furthermore, the collection of PII makes the service providers primary target of attacks and results in

security breaches and privacy exploitation.<sup>2</sup> The recent work to eliminate the central service providers is one unique digital identity that is build, managed and controlled by identity owner (i.e., the user).<sup>3</sup> Such identity that provides user centric data ownership is called Self-Sovereign Identity (SSI).

As part of IdM solutions, user authentication is developed in a variety of central solutions. For instance, many organizations have developed their authentication mechanism based on the OAuth protocol,<sup>4</sup> but the CA part remained intact. Digital identity authentication ensures that individuals are whom they claim to be in the online systems. The verification of the subject and protection of sensitive information is the key component of trustworthiness in the IdM. Users have to exchange their personal information (e.g., credentials, PII) with organizations in exchange or services. To overcome stealing, misusing, or manipulating these data in a central approach, service providers are required to provide multifactor authentications along with management of identities which further complicates the systems. Besides the central approach, federated instances provide access to multiple sites with the same credentials. However, the control and ownership of data remain in the hand of the identity service provider.

Different from IdM and authentication, access control is the process of granting or denying the access request of a subject (i.e., someone/something that wants to use a resource) to a specific object (i.e., resources that subject want to use it like network, data, application, service, etc.).<sup>5</sup> In other words, access control is a security technique that regulates who or what can do which action (e.g., use, read, write, execute, view) on specific resources in a computing environment.<sup>6</sup> This process mostly is done after successful authentication.

Combination of these components together with monitoring systems can define IAM solutions (see Figure 1). In order to achieve secure communication and access, IAM provides the following<sup>7</sup>: (1) identity provisioning, update, revocation and lookup as *IdM operations*.<sup>8</sup> (2) *access control* mechanisms to prevent unauthorized access to enterprise resources<sup>9</sup> and (3) *monitoring & logging* to store trace of access and logins.<sup>10</sup>

Recently, the introduction of Blockchain<sup>11</sup> and smart contracts<sup>12,13</sup> as extensions of distributed ledger technology (DLT) are changing different aspects of business models, management, and even IAM components, in different

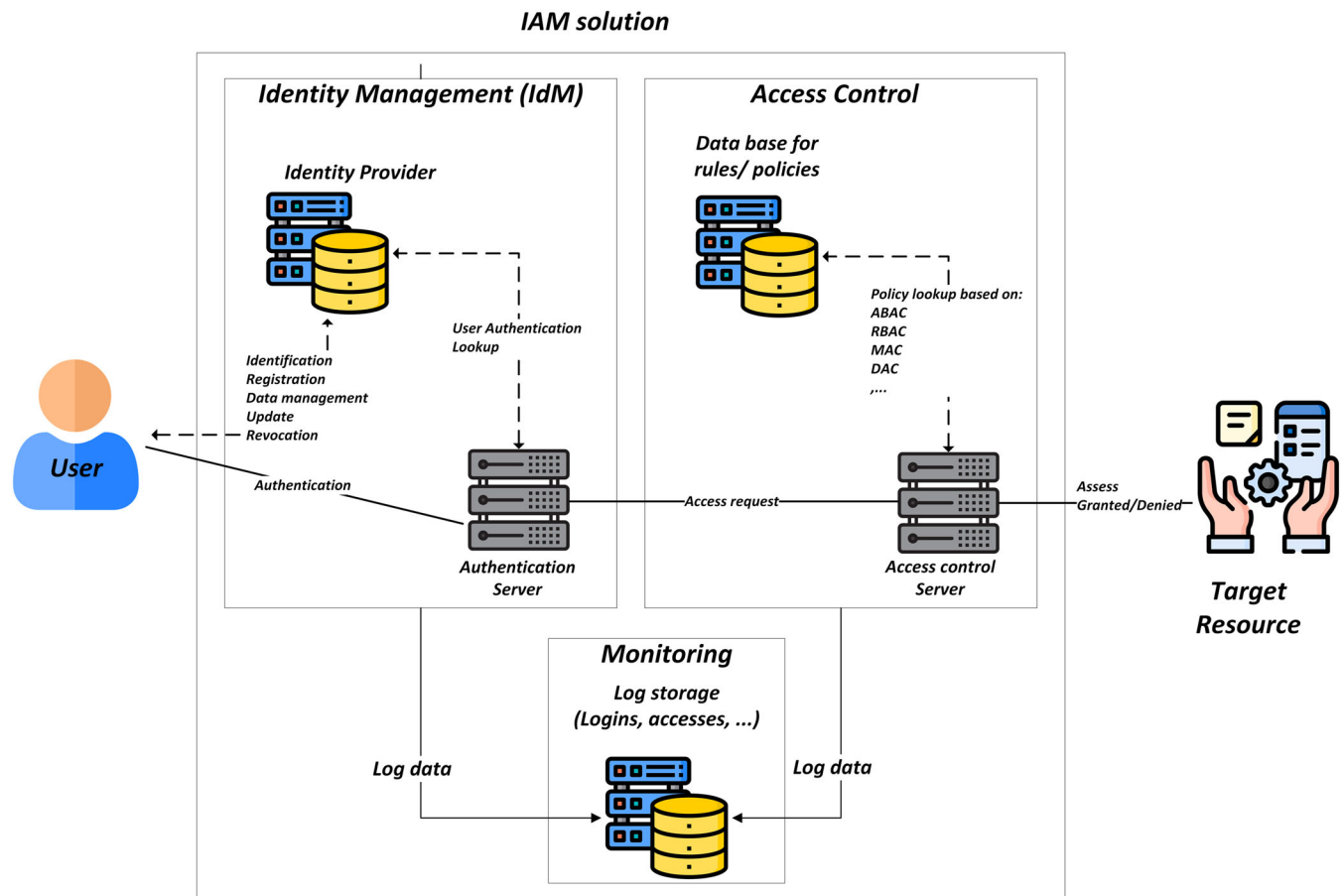


FIGURE 1 Components of identity and access management (IAM) solutions<sup>7</sup>

use-cases such as telecommunication, healthcare, Internet of Things (IoT) and smart cities. This technology is recognized as a tamper-resistant and transparent ledger. So, it can be used to bind the users with the claims they make, to prevent identity frauds in IdM. Moreover, its immutability, decentralized, traceability, and non-repudiation are the most attractive features for using this technology in the IAM process. The immutability of Blockchain can decrease the probability of fraud and access change in the system, while decentralized nature can remove the single point of failure and increase the network and systems tolerance and availability. On the other hand, non-repudiation can remove the possibility of access deny and traceability guarantees the possibility of tracking the user actions in the system. Besides the benefits of Blockchain for IAM solutions, there are several challenges which demand prime attention,<sup>14,15</sup> which are mainly user's privacy and system latency.

The rest of this paper is organized as follow: Section 2 briefly reviews IdM approaches, authentication, access control and DLT. Section 3 describes how Blockchain can transform IAM, and then the proposed taxonomy is depicted. Section 4 describes the current state of the art in separate components of IAM (i.e., IdM, access control and monitoring), as well as comprehensive solutions. Finally, Section 5 draws some conclusions about this taxonomic approach, with a summary of advantages and disadvantages of the current methods as well as recommendations for future directions and open problems.

## 2 | BACKGROUND

In this section, we describe the main background which is needed to best understand the rest of paper, including IdM, access control, authentication and a brief description of DLT (including Blockchain and smart contracts).

### 2.1 | Identity management

IdM is an administrative process to create and maintain user account to be used for authentication and identification in online services. It is required to simplify the user provisioning process and ensure that the legitimate users can have access to the services. The IdM system lifecycle comprises of four phases including *registration/identification*, *authentication*, *issuance* and *verification*. According to our interpretation, there are three types of IdM solutions:

- Central model: the central service provider stores the credentials and validate them to access the online services through their own authentication mechanism.<sup>16</sup> In simple central models, there is one identity provider for several service providers, but in Silo/isolated model, each service provider has its own identity provider.<sup>17</sup>
- Federated model: in this model, one of the service providers plays the role of an identity provider, who is responsible for creating, maintaining and authenticating users of several service providers.<sup>17,18</sup> The Facebook's and Google' Single Sign-On (SSO) are examples of federated entities.
- SSI: this type provides the ownership of data to user which can promote user's control on their data and transparency, by letting the owner of data to control the information without relying on third parties. Ten principles of SSI are existence, control, access, transparency, persistence, portability, interoperability, consent, minimization and protection.<sup>19</sup>

#### 2.1.1 | Attribute federation and verified claims in IdMs

From the security perspective, the anonymity of identity is affected by degree of link ability of personal data.<sup>20</sup> As digital identity is classified into different context (i.e., PII and non-PII), it is important to provide selective disclosure of PII. PII is defined as subset of information sufficient to identify the identity holder within set of subjects.<sup>21</sup> The regulation from standard bodies is currently practiced for data privacy and management around the world. For instance, General Data Protection Regulation (GDPR)<sup>22</sup> is enforced by European Union. One function that is fundamental to IdM is to distinguish one subject from another. In current IdM infrastructure, service providers need to identify users through claim verification or certain attributes of the user.

## 2.2 | Authentication

Authentication is a security mechanism for verifying the identity of a user, process or device, as a prerequisite to allowing access to resources in an information system. Traditional authentication methods and systems use a CA for assessing the request which could be the main single point of failure for a system.<sup>23</sup> There are four main authentication methods<sup>24</sup>:

- *Knowledge-based*: relies on knowledge about the users, such as their IDs and passwords;
- *Possession-based*: based on a user's possessions, including their credentials, RFID, etc.;
- *Inherence or biometric-based*: uses biometric features, like fingerprint, iris data, etc.<sup>25</sup>;
- *Multifactor*: combining two or more of the previous methods.

## 2.3 | Access control

Access control is a security technique that regulates who or what can perform an action on resources. The most well-known methods are listed below:

- Discretionary access control (DAC): this method considers owner-based administration of the objects. In other words, the owner of the object will define the access rules and policies over that. DAC is implemented by access control list or capability matrix (CapBAC).<sup>26,27</sup>
- Mandatory access control (MAC): this model is based on the classification of the objects and subjects. The subjects whose level is upper than the object can have access on it. The access decision in this method will be made by a CA.<sup>6,26,27</sup>
- Role-based access control (RBAC): this method manages the access of subjects based on their role within the system and on rules defining what kind of accesses is allowed to subjects in given roles. Due to the nature of this access control model, a limited number of roles can represent many users, and it becomes easier to audit which users have which kind of permissions and what permissions have been granted to a given user.<sup>26</sup>
- Attribute-based access control (ABAC): this method is a logical access control model which controls access to objects by evaluating some defined control rule or policy against the attributes of subject, object, actions and the environment relevant to a request. ABAC is useful for fine-grained access control.<sup>28</sup> In this method, subject attributes are related to identifiers that specify the subject who is demanding access to an information asset. Object attributes distinguish the resources that the subject want to access to them. The action that will be performed by the subject on object defines by action attributes. Environment attributes describe the environment identifying the context in which access is requested, for example, time and location.

## 2.4 | Distributed ledger technology

DLT is a general term for technologies that utilize replicated, shared and synchronized digital data between the users of private or public distributed computer networks located in multiple sites, geographies or institutions. Blockchain was introduced by Nakamoto in 2008.<sup>11,29</sup> It is a distributed, cryptographically secure, append-only, immutable, traceable and transparent technology that is updateable only via consensus among a majority of the existing peers on the network.<sup>30,31</sup> These features make Blockchain attractive as a decentralized consensus mechanism, since there is no CA for controlling the ledger. From an architectural perspective, Blockchain is a linked-list data structure that uses hash amount of previous blocks to create the link (see Figure 2). As well as the hash of its previous block, each block in a Blockchain consists of a set of transactions and their hash; it is these connections to the previous hashes that make a Blockchain immutable. After executing a consensus algorithm successfully in the network, new block will be added to the system. Widely used consensus algorithms include proof-of-work,<sup>32,33</sup> proof-of-stake<sup>34</sup> and Practical Byzantine Fault Tolerance.<sup>35</sup>

Introduced by Szabo in 1998,<sup>12</sup> smart contracts are defined as computerized transaction protocols that execute the terms of a contract on a Blockchain. Smart contracts are based on Blockchain and DLT. Some of the highlighted purposes of smart contracts are to satisfy common contractual conditions, minimize exceptions both malicious and

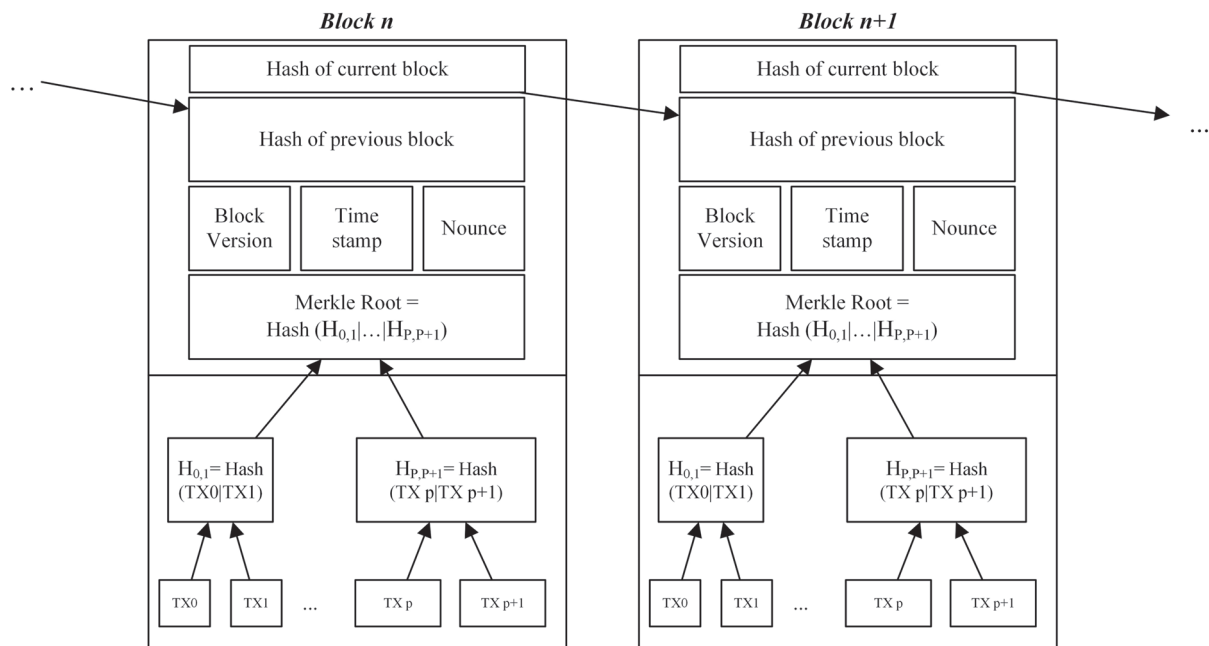


FIGURE 2 The structure of block in Blockchain

accidental and minimize the need for trusted intermediaries. Today, there are different Blockchains supporting the smart contract paradigm. Ethereum was the first that introduced Blockchain smart contract in 2014.<sup>36</sup> This platform has a Turing complete virtual machine which can run distributed applications and allow the execution of smart contracts.<sup>13</sup>

Depending on user's access to the Blockchain, this technology is categorized into three different types: (1) *public or permission-less Blockchain* that is accessible to the public and anyone can participate in consensus and reading/writing transactions. Public Blockchains provide the anonymity feature but lacks the privacy. (2) *Consortium Blockchain* mostly is used by some predefined organizations or users as legitimate nodes. This type of Blockchains is only accessible for preselected nodes. (3) *Private (permissioned) Blockchains* are developed to serve organization's specific needs, and similar to consortium Blockchains, they are only accessible by the users who are verified. In this model, the anonymity of the users can be violated.

As the data are the most valuable asset today, using the Blockchain in data-driven architecture can bring features of decentralization, anonymity, audibility and persistency.<sup>37</sup> Also, some of the other important features of Blockchain are as below<sup>38,39</sup>:

- *Immutability*: thanks to this feature, any confirmed transaction or data cannot be altered.
- *Decentralized*: there is no CA in Blockchain, and all nodes have a copy of the ledger. It can remove single point of failure and also improve the reliability of system. Since there is no need to third party, the processes can be done more efficiently and in low cost.
- *Non-repudiation*: because of using nodes signatures on the transactions, no one can deny their actions.
- *Permanence*: all data in the Blockchain can be available at any time, and nothing may be removed from the network.

### 3 | NEED OF BLOCKCHAIN AND TAXONOMY OF DLT-BASED IAM

The Blockchain technology provides some interesting properties that coincide with the desirable principles of secure IAM systems; in the following, we will discuss about Blockchain's essential features for the three vital parts of IAM systems (i.e., IdM and secure AAC).

- IdM: by leveraging the Blockchain, 10 principles of SSI,<sup>19</sup> can be achieved to overcome digital identity issues. For instance, the consensus mechanism fulfils the needs of trustworthiness for verified published attributes. As

Blockchain is temper-resistant ledger, the persistent of claims can be attained and forge proof storage of identities can be achieved. The data stored in the Blockchain is available to authorized users and owner of PII can realize full control over their data and dedicates how and what data is shared with other users. The Blockchain-based structure that provides chain per identity (e.g., *trust chain*<sup>40</sup> or *the tangle*<sup>41</sup>) has been proposed to enable the full control. Such chain structure can also establish the existence principle for user to give the right to be forgotten. The claim blocks withhold the personal information, and authentication of claims ensures the protection and data minimization. The advances in the Blockchain technology allow users to implement and deploy the robust and autonomous smart contracts which could be leverage to create the data sharing controller with fine-grained access control. Additionally, the Blockchain technology seems promising to provide benefits of sustainability, distributed control and transparency. The interoperability and portability issues in IdM have not been addressed widely in terms of Blockchain usage, and it remains open issue for flexible digital identity and online services. We believe that the intervention with other technologies can more likely generate the optimal solution.

- AAC: the most well-known advantages of Blockchain (i.e., immutability, decentralized nature, no need for a third party, reaching consensus, non-repudiation and permanence) can transform this technology to an outstanding candidate for evolution in AAC solutions. Integration of AAC mechanisms with Blockchain technology can significantly improve reliability, availability, security, scalability and transparency of the system. Majority of existing AAC solutions are centralized and suffer from single point of failure and low scalability; Using Blockchain, single point of failure can be removed from the system, and also other inherited security gaps such as vulnerabilities to DDoS and reply attacks or having a single point of failure in the Kerberos authentication method<sup>42</sup> can be addressed using this technology. Non-repudiation can prevent the malicious users from denying their action in the system. Also, consensus can improve the data integrity in the system.

Based on our study, the existing researches on Blockchain-based IAM solutions mostly implement different components of IAM systems (i.e., IdM, access control and monitoring) separately. These systems can be categorized based on their components and application environment as shown in Figure 3.

As mentioned earlier, IdM component of IAM comprises registration, authentication and data management. Authentication methods can be categorized based on their type into knowledge-based, possession-based, biometric-based and multifactor authentication. Note that Blockchain is mostly used as a distributed, immutable and secure storage for credentials and user identity in authentication procedure.

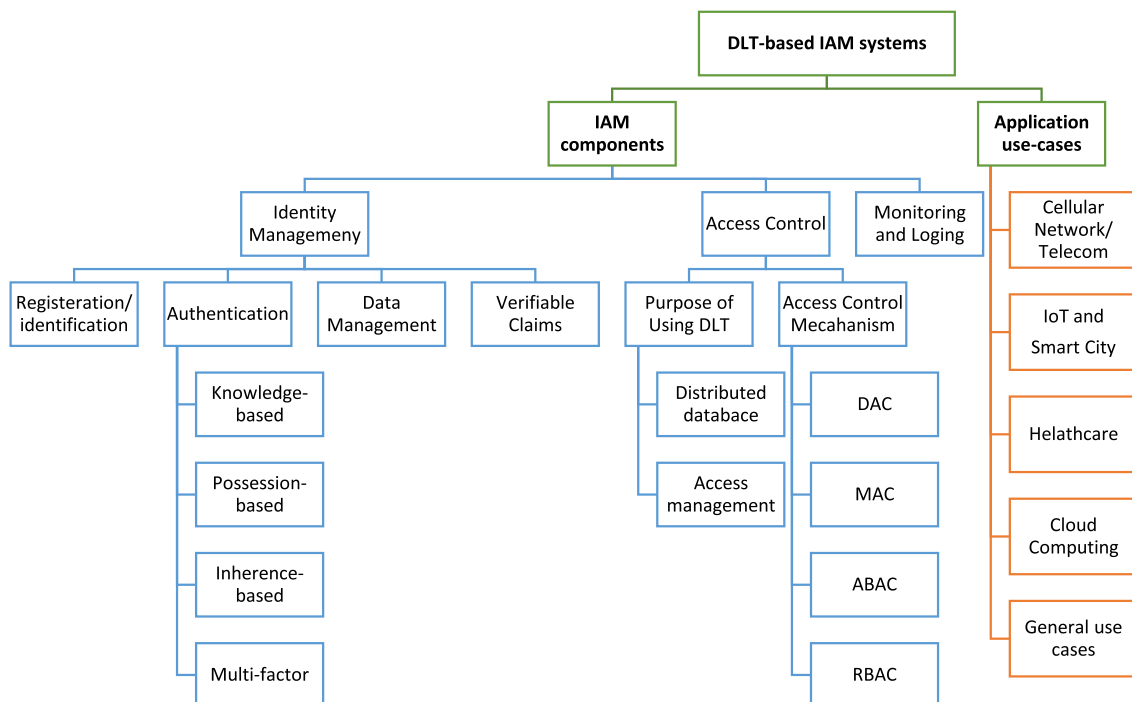


FIGURE 3 Taxonomy of existing distributed ledger technology (DLT)-based identity and access management (IAM) solutions



Access control methods, meanwhile, can be classified in two different categories based on the access control mechanism and how it uses the Blockchain network. Access control mechanisms can be divided into four main categories: MAC-, ABAC-, RBAC- and Access Control List (ACL)-based methods such as DAC (see Figure 3). These methods have two main motivations for using Blockchain technology. While some of them use Blockchain as a safe, immutable and distributed database for the access rules and policies, others use the Blockchain and smart contracts for handling whole access management process.

Existing IdM or access control methods also can be categorized based on their application in different specific contexts such as cellular network and telecommunication, IoT devices and smart cities, healthcare and medical data records, cloud computing and resource sharing. Regardless of the application, some methods are general purpose methods that can be used in all use cases.

## 4 | BLOCKCHAIN-BASED IAM SOLUTIONS

As mentioned before, in IAM solutions, there are three main parts as IdM and access control and monitoring. In this section, we will provide a review on existing Blockchain-based IdM (i.e., registration/identification/data management/verifiable claims (IdM) and authentication), as well as access control and monitoring solutions.

### 4.1 | Self-sovereign IdM solutions

In this subsection, the existing methods for IdM are discussed. As mentioned before, IdM part of IAM includes registration/identification, authentication and data management. Since recent methods mostly provide SSI as well as data management, in this subsection, we will talk about these two components in one subsection. In case of authentication, there are different solutions which deserve to mention separately. Table 1 summarizes existing Blockchain-based IdM solutions.

TABLE 1 Blockchain-based identity management solutions

Auth. App.	Registration/ identification	Authentication				Data management	Verifiable claims
		Knowledge	Possession	Inherence	Multifactor		
Telecom/ cellular network		Niu et al. <sup>43</sup>	Sanda et al. <sup>44</sup> Lee et al. <sup>45</sup>	-	-		
IoT/smart city		Nuss et al. <sup>7</sup>	Lee et al. <sup>45</sup> Lin et al. <sup>46</sup> Ouaddah et al. <sup>47</sup> Widick et al. <sup>48</sup> Ourad et al. <sup>49</sup>	Huh et al. <sup>50</sup>	Hammi et al. <sup>51</sup>		
Healthcare		-	Deep et al. <sup>52</sup>	-	Mohsin et al. <sup>53</sup>		
Cloud/resource sharing		-	Deep et al. <sup>52</sup>	-	Kim et al. <sup>54</sup>		
General	Lundkvist et al. <sup>55</sup> Jolocom <sup>56</sup> Tobin et al. <sup>57</sup> SelfKey <sup>58</sup> Microsoft <sup>59</sup> Nuss et al. <sup>7</sup>	-	Zhang et al. <sup>60</sup> Ali et al. <sup>61</sup> ShoCard <sup>62</sup> Xiong et al. <sup>63</sup>	-	-	Lundkvist et al. <sup>55</sup> Jolocom <sup>56</sup> Tobin et al. <sup>57</sup> ShoCard <sup>62</sup> Ali et al. <sup>61</sup> Microsoft <sup>59</sup> Nuss et al. <sup>7</sup>	Lundkvist et al. <sup>55</sup> Jolocom <sup>56</sup> Tobin et al. <sup>57</sup> ShoCard <sup>62</sup>

#### 4.1.1 | Registration/identification and data management mechanisms

Many solutions have been proposed and developed from the perspective of digital IdM and personal data security and privacy. We limit our discussion to the systems and architectures that proposed IdM and data privacy using Blockchains. There is no definitive evaluation scale available for the evaluation of proposed solutions, and many of them have been evaluated and compared with other solutions based on the law of identity or SSI taxonomy. We aim to highlight the design and implementation of existing Blockchain-based solutions in the light of self-sovereign architecture.

The uPort<sup>55</sup> provides the framework for users to gather attributes from an eco-system of trust providers but does not provide identity proofing. For revocation in case of key lost, Quorum of Blockchain is used. It provides data ownership and selective disclosure; however, the privacy of user information in JSON data structure on message server can be compromised. This framework provides registration/identification, verifiable claims and data management in IdM. Jolocom<sup>56</sup> is another self-sovereign IdM which is also developed on top of Ethereum and provides similar functionalities of uPort. The difference between uPort and jolocom is the how the data are structured and represented in both systems. This system also provides all functionalities of IdM.

The Sovrin Foundation is a non-profit organization established to lead the global SSI network. They have developed the Sovrin IdM<sup>57</sup> to overcome the identity crisis through fulfilling the SSI principles. It uses the attribute-based credentials which allow users to only reveal credentials that they choose with relying parties. In this solution, WebOfTrust (WOT) helps protect user against deception. For recovery mechanism, it relays on attribute-based shredding. It does not provide verification of relying parties, so user needs to relay on WOT. User has full control over their identity, but personal data protection is less secure as it lacks claim verification support. The adoption and integration and Sovrin standard seem constructive in novel SSI systems. Sovrin provides registration/identification, verifiable claims and data management. Ferdous et al.<sup>64</sup> analysed the evaluation of uPort, jolocom and Sovrin under the comprehensive taxonomy of SSI. It has been shown that none of the existing systems fulfil the requirements of flexibility needs of digital identity for the heterogeneous online service.

The shoCard<sup>62</sup> provides identity verification, and as backup, it uses stored encrypted version of attribute certificate on server. A central server is used as intermediate between user and relying parties. As one of the existing disadvantages in this technology can be data minimization which is not supported well. In shoCard, Bitcoin network records a commitment to personal data that were verified during identity proofing and stores the hashes of certifications which are built upon the user's seal created by relying parties. This system provides verifiable claims, authentication and data management components of IdM solutions.

Selfkey<sup>58</sup> is another system to provide identification/registration and data management. Using Selfkey, users can verify the identity and access multiple services. The Selfkey digital wallet is used to digital identification (i.e., public/private key), and users can access their digital identification attributes and other locally stored documents through mentioned wallet. The public key is shared across the network and used to receive attestation for documents from other parties. Blockstack<sup>61</sup> is another IdM system which attempts to redesign the naming system in order to provide elucidation of identity. It has PKI authentication features using state machines and storage aspect in Blockchain to preserve privacy and resource identification. This system provides identification/registration, authentication and data management. *Identity overlay network (ION)*<sup>59,65</sup> is a new concept of IdM on the network proposed by Microsoft Corporation. It is a public decentralized identifier (DID) network that implements Sidetree protocol<sup>65</sup> via Bitcoin (to support DIDs and Decentralized Public Key Infrastructure [DPKI]) in large scale. All transactions in ION are encoded with a hash that its nodes use to fetch, store and replicate the hash-associated DID operations via InterPlanetary File System (IPFS).<sup>66</sup>

#### 4.1.2 | Blockchain-based authentication mechanisms

Among solutions which are discussed in previous subsection, Blockstack<sup>61</sup> and shoCard<sup>62</sup> support Blockchain-based authentication. Beside them, in this part, we will provide other authentication solutions which are implemented via Blockchain or smart contracts technology. Table 1 depicts the four categories of these methods based on the taxonomy.

Zhang et al.<sup>60</sup> proposed a general purpose framework that stores user's identity in the Blockchain and exploits a smart contract for managing different permissions based on user's related data for different websites. This method consists of four main actors (i.e., users, websites, Blockchain and an off-chain storage). A user stores his identity in the Blockchain and his encrypted personal data in the off-chain storage. In order to prepare different websites with



different and related data of user, a smart contract will be attached to the user's identity in the Blockchain. When a user sends the login request to a website, the service provider verifies the identity of the user and retrieves the user's personal data from the off-chain storage based on the rules in the smart contract.

Deep et al.<sup>52</sup> proposed an authentication algorithm for cloud centric databases used in cloud and healthcare environment. This method covers both insider and outsider user. It initially checks user credentials and valid Blockchain node parameters. If the user's credentials information does not exist in the cloud database, then the user is asked for retrying or for new user account creation. The proposed method uses Blockchain as a distributed database for storing credentials on it. A multifactor authentication solution for healthcare use cases is proposed by Mohsin et al.<sup>53</sup> in which access point will authenticate a node database for patients. RFID and finger vein (FV) are two factors to authenticate the use. First, the user's FV and RFID data are extracted; then a hybrid, random binary pattern (i.e., Advanced Encryption Standard (AES) cryptography and MD5 hash) is derived from these data and stored on Blockchain. The encrypted pattern for each user is stored in an image with a steganography algorithm. When a user sends an authentication request to the access point, the FV and RFID parameters are extracted by reversing the AES method, and if these data match, the authentication is successful. Another authentication method proposed for cloud environment is introduced by Kim et al.<sup>54</sup> called SAMS. This method uses a master node as coordinator that manages the security of whole system. For user authentication at first, the master node creates its own block and stores it on the Blockchain. When a new client node wants to connect, he creates another block and sends his information and the created block to master node. Master node creates a block with the received information from client and checks the identity of the block. If they are identical, the client block will be connected. In this method, Blockchain is used as an immutable database for credentials.

Huh et al.<sup>50</sup> proposed an automatic door locking system based on fingerprint authentication and verification method for mobile phones using Blockchain. A user authenticates him through mobile devices via fingerprint recognition. The hash amount of user's finger print will be saved to the Blockchain to be secure against forging, tampering or leaking. In this method, the mobile phone should execute PoW consensus mechanism, and it would be very resource consuming for these devices. Another Blockchain-based authentication and authorization solution are proposed by Widick et al.<sup>48</sup> to control the user access to the resources of an IoT device. This method consists of two smart contracts. One of them is for handling digital certificates and operations, while the other handles access control. Both of these contracts are managing by agent node. This system uses the Ethereum Blockchain to provide a tamper-evident, auditable log of all steps and decentralize some processes (e.g., evidence review). Hammi et al.<sup>51</sup> proposed a decentralized Blockchain-based authentication system called bubbles of trust, based on user's ID and token for IoT environment. Data integrity and availability are main concerns of this paper. This approach relies on security advantages provided by Ethereum and serves to create secure virtual zones (bubbles) where things can identify and trust each other. Bubbles of trust take about 14 s to validate a transaction, and it is a long period for real-time applications and also it uses public Blockchain that requires fees to be paid for each transaction.

Industry 4.0 is other interesting application that is addressed by BSeIn.<sup>46</sup> This system is a mutual authentication method that consists of four tangible layers which combine vertically interorganizational value networks, manufacturing factories and engineering value chain. This conceptual framework allows the efficient implementation of a flexible and reconfigurable smart factory. For mutual authentication, this method used one-time public/private key pair for each request. This pair can be used for message encryption and calculating message authentication code. FairAccess<sup>47</sup> proposed an AAC system for IoT. On the authentication part, it creates token for users based on their credentials. This method explained more in next part of the paper. FairAccess just supports token-based authorization and does not have mechanism for renewing the expired token, and it takes more time (i.e., at least two blocks should be mined) to a token to be available and usable.

An authentication method for Wi-Fi hotspot access has been proposed by Niu et al.<sup>43</sup> This method consists of the service provider, hotspot APs, users and the Blockchain. All users credential are saved in the Blockchain and when the user requested to connect to the network, service provider and Wi-Fi hotspot will connect to the Blockchain to get the valid credentials and provide the connection. This method can provide accountability and anonymity in a simultaneous manner. CoinsShuffle protocol and Coloured Coins inspired the development of this scheme. Another authentication method in telecommunication environment is proposed by Sandra et al.<sup>44</sup> using Bitcoin 2.0. In this method, user installs 'Auth-Wallet' that allows him to get authorized by exchanging the 'Auth-Coins' instead of user information. This method aims to enhance user privacy.<sup>67</sup> Registration and authentication are two main protocols to implement the desired solution of authentication. Registration protocol is executed at user's first access to send user information to the server of Auth-Wallet. Authentication protocol is used for the process of connecting to the internet. User connects to access point using its unique ID. Access point generates a transaction which sends Auth-Coin to user. User verifies

the message and signs it. If the verification protocol of access point returns success, the token will be broadcasted to the Blockchain, and then access point allows user to connect to the internet. Moreover, BIDaaS<sup>45</sup> is proposed as authentication management system for telecommunication and IoT environment. This system generated a Blockchain-based ID for users, and then this ID will be registered on the Blockchain. This system is just used as a distributed database for user registration. Mutual authentication is the most notable security mechanism in this paper.

Xiong et al.<sup>63</sup> proposed an authentication method aims to provide privacy multiserver environments. This system supports mutual authentication of users and servers. Any potential threats can be detected in the model and reflected on the Blockchain, so that they can be prevented from damaging the system.<sup>68</sup> At first, a user will be registered in the system by sending his data to the nearest server. Then, the server sends some data to the user to add it on the smart card which will be used in next connections. After having user data in smart cards and Blockchain, user's verification is done by consensus among Blockchain nodes.

Ourad et al.<sup>49</sup> proposed authentication solution; authentication is done by the Ethereum address of the IoT device. In the case of successful validation, smart contract broadcasts an access token and the sender's Ethereum address. The user and the IoT device receive these access tokens. The user combines and signs the 'token', 'user IP', 'access duration' and the 'public key' and sends it to the IoT device to verify the content. Having correct data, the device grants access to the user from the sender's IP for the duration specified.

## 4.2 | Blockchain-based access control solutions

This section is devoted to existing access control methods based on Blockchain. Some of recent studies use Blockchain as a distributed database for rules or policies, and the access control is done by fetching these rules from database. On the other hand, others use Blockchain transactions for granting/denying user access. In summary, Table 2 shows the category of the existing access control methods relied on Blockchain, based on the taxonomy.

### 4.2.1 | Using Blockchain as a distributed database for rules

Using Blockchain as a database for policies and rules can be seen in different recent researches.

TABLE 2 Access control methods based on Blockchain

Purpose	A.C. model				
	Application	ABAC	RBAC	DAC	
Distributed DB	Telecom/cellular network	Raju et al. <sup>69</sup>	Raju et al. <sup>69</sup>	Raju et al. <sup>69</sup>	
	IoT/Smart city	Dramé-Maigné et al. <sup>70</sup>	Ali et al. <sup>71</sup>	Ali et al. <sup>71</sup>	
		Ali et al. <sup>71</sup>		Xu et al. <sup>72</sup>	
	Healthcare	Zhang et al. <sup>73</sup>	Zhang et al. <sup>73</sup>	Zhang et al. <sup>73</sup>	
	Cloud/resource sharing	Qin et al. <sup>74</sup>	—	—	
		Wang et al. <sup>75</sup>			
General	Maesa et al. <sup>76</sup>		Ihle et al. <sup>79</sup>	—	
	Maesa et al. <sup>77</sup>		Cruz et al. <sup>80</sup>		
	Shafeeq et al. <sup>78</sup>				
Access management	Telecom/cellular network	—	—	—	
	IoT/smart city	Zhang et al. <sup>81</sup>		Ouaddah et al. <sup>47</sup>	Rifi et al. <sup>85</sup>
		Pinno et al. <sup>82</sup>			
		Ding et al. <sup>83</sup>			
		Liu et al. <sup>84</sup>			
		Nuss et al. <sup>7</sup>			
Healthcare		Dagher et al. <sup>86</sup> Azaria et al. <sup>87</sup>	—		
Cloud/resource sharing	Zhu et al. <sup>88</sup>	-	-		
General	Maesa et al. <sup>89</sup>		Ding et al. <sup>90</sup>	-	

Masea et al.<sup>77</sup> proposed a general purpose access control for storing and publishing policies of ABAC and to allow distributed transfer of access rights among users on Bitcoin network. In this paper, the policies and rules are defined by the resource owner and then are stored in the Blockchain using policy creation transaction. Altering, transferring and revoking of these rules are just allowed by the owner. Also, in this paper, the author proposed a novel idea to avoid extra resource consumption because of growing size of distributed ledger and rules. They propose to store only a link to an external source containing the policy, coupled with a cryptographic hash of the policy itself in the Blockchain. In their next study, they used smart contracts to enforce access control policies instead of simple transactions.<sup>76,91</sup> Other general purpose AC is addressed by Ihle et al.<sup>79</sup> for RBAC model. This method saves all the subject roles and other data in key-value data model on the smart contracts. Moreover, RBAC-SC is another RBAC mechanism usable in all environments.<sup>80</sup> This method consists of two main parts, including a smart contract and a challenge–response protocol. The smart contract is used for the creation, changing and revoking of the user role assignments, and the challenge–response protocol is for authentication of the ownership of roles and the verification of the user role assignment.

Raju et al.<sup>69</sup> proposed an access control system for cognitive cellular networks (CCNs) focusing on user privacy. This paper considers the anonymity as important attribute and improves the privacy of the users who want to connect to the cellular networks. The proposed method can be applied for all access control mechanisms and has three main actors cognitive cellular user (CCU), CCN and identity and credibility service (ICS). ICS uses Blockchain and smart contract as an access control and IdM mechanism. At first, user registers his PII in ICS, and ICS provides the CCU with pseudonymous unique Blockchain ID (UID) as the result. When user requests for network access from CCN, it sends this request to ICS to be sure that user is a known one. If at the first step, user identity assertion is successful; the ICS sends a positive reply to the CCN. In this step, it also sends some rules about privacy preservation of the user and service-level agreement rules to the CCN. After accepting this contract by the CCN, user will have access to the network and will be able to pay for it.

BlendCAC is a capability-based access control mechanism (i.e., DAC that is implemented by access control matrix) based on smart contract for the IoT environment.<sup>72</sup> In this method, the access control process (i.e., registration, delegation and revocation of access rights) will be done using capability tokens. Smart contracts are used for storing the access control matrix. Each node interacts with the smart contract through the provided contract address and the remote procedure call (RPC) interface to check the validity of the tokens or access permission. Another method that is suitable for all access control mechanisms in IoT is proposed by Ali et al.<sup>71</sup> with focus on right delegation. In this method, the device (owner) in the process of registration in the Blockchain will sign a contract. The smart contract stores devices platform hashes and delegation policies. This data will be added on the Blockchain using PoW consensus mechanism. In the case of requesting for permission delegation, the owner of the object can send a request to the Blockchain, and the smart contract after validating the request sends the confirmation message to the Blockchain and this update gets broadcasted to all nodes of the system. Dramé-Maigné et al.<sup>70</sup> designed an ABAC solution in IoT and smart cities. This system consists of IoT devices, administrators, Blockchain nodes, gateways, attribute issuing entities and user. In the proposed method, administrators establish the trust relationships for their devices. In parallel, the user deploys an attribute contract. Using smart contract, one or several attribute issuing entities endorse the appropriate attributes for user access. When a user sends the request to the Blockchain, the device connects to its gateway to retrieve attributes, and finally, the device evaluates the request against the policies and makes its decision.

Qin et al.<sup>74</sup> proposed a method for fine-grained ABAC that can be applied in cloud oriented data access control environments. CA, data owner, data user, cloud service provider (CSP) and a Blockchain network are the four main actors of this system. In this method, a CA is responsible for managing the security of the whole system. The operations of the proposed method can be divided into two phases, namely, attribute management and access control. In the first phase, the CA issues an attribute key to the user, sets the validity period of the attributes in the smart contract, and issues a key to the CSP. Then, in the access control phase, the data owner first uploads the ciphered text to the CSP, the CSP invokes the contract to obtain the user's valid attribute set, and if the user who requested for the data is valid for accessing them, he can perform final decryption to access the desired information. The main problem of this method is using CA as a central point for security that can be single point of failure for whole system. Another method for data sharing is addressed by Wang et al.<sup>75</sup> for fine-grained AC using attribute encryption mechanism. It consists of two main actors (owner and user). At first, owner encrypts the system master key and saves it to the Blockchain and then deploys a smart contract, and then user sends the registration request to owner; and owner manages the secret key for the user and saves it in the Blockchain and sends transaction ID and smart contract address to the user through a secure channel. These data will be used for next connections.

Shafeegh et al.<sup>78</sup> proposed a general purpose decentralized attribute based access control mechanism using tangle (i.e., a new decentralized and tamper–proof-distributed ledger).<sup>41</sup> In this method, owner defines and manages AC over

his objects and defines the security policies and the level of authorization granularity of the resources and stores it in the Blockchain which guarantees distributed auditability and prevents the user from fraudulently denying the granted access rights. In the case of access request the owner sends the authorization token to the requester only if the requester meets the conditions defined in the access control policy.

Zhang et al.<sup>73</sup> proposed a Block-Based Access Control Scheme for healthcare named by BBACS which is a general solution to support all access control methods. BBACS stores all the electronic medical records (EMRs) of users in Blockchain, and also, it verifies the access permissions and authorizes the block(s) access in EMR server. In this mechanism, the Blockchain is only used as a distributed storage for data records, and the EMR server is a central point for managing the user's access. User sends a parameter named by *Sid* including all the indexes of the queried blocks accompanied by an Elliptic curve point ( $P$ ) to the EMR server. Server fetches the token from the Blockchain and calculates  $P'$ . If  $P$  and  $P'$  were same, the server sends data to the user.

#### 4.2.2 | Using Blockchain for access management

Besides using Blockchain and smart contracts as distributed database, some researchers use different smart contracts for controlling user access.

Zhang et al.<sup>81</sup> proposed a smart contract-based framework using three types of smart contract to achieve distributed and trustworthy attribute based access control in IoT environment, namely, multiple access control contracts (ACCs), one judge contract (JC) and one register contract (RC). Note that RC is a distributed database for registering the policies in the system. In this method, the three main smart contracts act as following. (1) AAC is defined for each pair of (subject, object) and consists of four main attributes, namely, resource (i.e., object), action, permission (i.e., allow, deny, etc.) and time of last request (i.e., time of the last access request from the subject). (2) The RC that stores the policies manages the access control and misbehaviour judging methods. Finally, (3) The JC implements a misbehaviour judging method, which judges the misbehaviour of the subject and determines the corresponding penalty, based on misbehaviour report from an ACC. Nonetheless, the environment attributes those are used in the ABAC is limited to time attributes. Other AAC mechanisms that implement RBAC and OrBAC solution for IoT environment are FairAccess.<sup>50</sup> Note that OrBAC is a model that can handle simultaneously several security policies associated with different organizations.<sup>92</sup> This method consists of two levels for central and distributed access control. In centralized part, access policies over operations between cooperative organizations will be managed. The distributed part is implemented by Bitcoin Blockchain and is based on access tokens. The process of granting permission is done by a cryptographic problem that should be solved by sender and receiver of the token. FairAccess just supports token-based authorization and does not have mechanism for renewing the expired token, and it takes more time to a token to be available and usable.

Pinno et al.<sup>82</sup> proposed ControlChain as architecture to provide ABAC in IoT environment. Controlchain uses four types of Blockchain to store data and also managing the access of the users. (1) Relationships Blockchain is responsible for the storing the public credentials and relationships of all entities. (2) The context Blockchain stores contextual information from entities to manage the access based on environmental situation. (3) Accountability Blockchain registers a history of permissions or denials of access to object. Finally, (4) the rules Blockchain keeps the authorization rules defined by owners. When a user sends an access request to the ControlChain, the decision engine will gather data from relationship, context and rule Blockchain, and then the result will be registered to accountability Blockchain. Rifi et al.<sup>85</sup> proposed an access control mechanism suitable for ACL-based access control methods in IoT and specifically smart cities environment. This method uses smart contracts, which provide security and privacy in the IoT system using a publisher-subscriber mechanism. These access control methods and protocols in IoT systems are used for data collection and data processing, and it is applicable in the ACL-based access control mechanisms like DAC.

Moreover, Ding et al.<sup>83</sup> proposed an ABAC for IoT environment. In this method, there are two main actors as attribute authorities and IoT devices. Attribute authorities in the system act as the consortium nodes in consortium Blockchain and the key generation centre. When a user wants to access to another user's data, at first, they generate a connection based on Authentication and Key Agreement (AKA)-based authentication method and a session key for symmetric encryption algorithm. Then, the owner sends policies to indicate who can communicate with him. The requestor chooses a satisfied subset of the policies regarding his needs. Then, the owner checks requestor's identity in the Blockchain and then checks whether the submitted set of attributes satisfy the access policy he specified. Finally, if the connection requestor satisfies the access policy that the owner specified, he will be able access the desired data. Finally, Fabric-IoT<sup>84</sup> is another research regarding ABAC in IoT environment. The system contains three kinds of smart

contracts, which are device contract to provide a method to store the URL of resource data produced by devices and a method to query it, policy contract to manage and store ABAC policies for admin users, and access contract as the sore contract to implement an access control method for normal users.

MedRec<sup>87</sup> is a RBAC for recording and accessing data in healthcare environment. This method is implemented in a private Blockchain and consists of three different smart contracts. (1) RC maps participant identification strings to their Ethereum address identity; (2) patient-provider relationship contract for the nodes manages medical records for the other; and (3) summary contract holds a list of references to patient-provider relationship contracts, representing all the participant's previous and current engagements with other nodes in the system. In this system, the rules and policies are implemented in the context of patient-provider relationship contracts and when a user wants to access his data, selects data to share and updates the corresponding PPR with the third-party address and query string. To overcome the existing problems of MedRec system, Ancile<sup>86</sup> is proposed that utilizes smart contracts for RBAC, data security, privacy and obfuscation in healthcare environment. Patients, providers and third parties are three main actors of Ancile. This method is based on three main roles as owner, view and blind. This system uses six unique types of smart contracts named by consensus (for registration of users and their addresses), classification (for classifying patients, providers or third parties), service history (maintaining the relationship histories of nodes), ownership (tracking the records that providers store for patients), permissions (built by the Ownership contract when a new record is added to the system) and re-encryption (proxy re-encryption). Adding a node, registering a patient, changing access permissions, adding a record, retrieving a record and transferring a record can be done by the proposed smart contracts in this paper.

Masea et al.<sup>89</sup> is a general purpose ABAC method. This method consists of policy enforcement point, policy administration point, attribute managers, policy information points and policy decision point as the evaluation engine that takes a policy, an access request in order to access decision. SC-RBAC is another general purpose RBAC method that can be used in all types of distributed applications (DApps).<sup>90</sup> This method consists of three different smart contracts. Permission contract is responsible for handling the user and role permissions by creating, changing and disabling the specific permissions. Role contract is usable for creating roles, changing the role or permissions of a role and disabling a role. Finally, user contract is responsible for managing the user access by creating, enrolling and disabling the user or by changing his role.

TBAC<sup>88</sup> is an ABAC solution for resource sharing in cloud environment. In this platform, four types of transactions are used for access control procedure as follow: (1) Subject registration used to record the information of one or more subjects. (2) Object escrowing used to record various information of protected objects. (3) Access request that contains all necessary information of access request and this information will be used by the subsequent decision making for the access request. Finally, (4) access grant is the final form of access after all empty signatures are fulfilled, and then it will be stored into Blockchain as an access log once all of signatures are validated by the block generator.

### 4.3 | Blockchain-based monitoring solutions

Because of Blockchain's distributed nature, there is no central database in this technology. This interesting feature encourages the researchers and communities to propose a monitoring and log management solution on top of Blockchain. Having IdM/access logs on Blockchain can prevent the possibility of data loss or integrity violation.

Yang et al.<sup>93</sup> proposed an authentication method in which Blockchain is used as authentication log storage. In this solution, user's access to fifth generation (5G) network will be done via their public key in the network. If user's validation is successful, the device can access the network, and the log data will be stored in the Blockchain. DRAMS<sup>94</sup> is another platform that uses Blockchain for log management in access control process. DRAMS relies on smart contract to store logs and implements a policy analyser that evaluates whether an access decision is correct according to the semantics of the available policies. Azaria et al.<sup>87</sup> proposed a backup and monitoring functionality based on Blockchain technology. Similar to other solutions, using this system, a complete log of the issued transactions and accesses will remain in the Blockchain. Users can access to the logs only via downloading the latest version of the Blockchain ledger.

### 4.4 | Comprehensive IAM solution

Besides proposing different components of IAM solutions separately, based on Blockchain, some researchers have integrated these parts as a comprehensive IAM solution.



Nuss et al.<sup>7</sup> proposed an IAM solution based on Blockchain for IoT in the enterprise and for its employees. In this paper, authors pointed the challenges of IAM methods in IoT environments, and then they proposed their method as follows. The IdM process was initiated by entering the identity information of a new employee or device into the system. The encrypted version of these data will be stored in a central identity store. Also, a key pair is created and encapsulated to a transaction together with combined with the hash of the identity. This transaction is added to the network, after consensus. For access control, the authors implemented ABAC solution in which an administrator who creates new access control policies and issues them as transactions to the Blockchain. In the access management step, access decision logic is implemented directly on the Blockchain using smart contracts. For log management and monitoring, the proposed method stores all logs into the Blockchain, and all nodes appended to the Blockchain can be monitored as the Blockchain itself can be regarded as a log storage. The main concern of this method is the user's privacy.

## 5 | DISCUSSION AND FUTURE DIRECTIONS

More and more aspects of businesses are being modified as a result of the emerging DLT and its associated Blockchain and smart contracts systems. Blockchain technology can disrupt the traditional approach of IdM and access control (IAM) solutions. Proposing a comprehensive review about using Blockchain in IAM can be helpful for researchers to find the most important open issues and advantages/disadvantages of this technology.

To address the challenges and to provide a future direction, in this paper, we discussed different components of IAM methods and also mentioned that existing methods mostly are implemented different components separately. To have a clearer understanding of the state of the arts, we proposed a taxonomy in which the solutions are categorized based on the IAM components and the applied use cases. IAM solutions are categorized based on IdM, access control, and monitoring solutions. In IdM user's registration/identification, authentication, verifiable claims, and data management are classified. Also, authentication methods can be categorized based on their type (i.e., knowledge-based, possession-based, inherence-based, and multifactor). For the next part, access control methods can be classified into two different categories based on AC mechanism (e.g., ABAC, RBAC) and the way that method is using the Blockchain network (i.e., access management, distributed database). As a brief conclusion, we can highlight the general advantages and disadvantages of the proposed method (IdM and AC) and their future desire as follows. Note that, because of the lack of enough resources in monitoring and comprehensive IAM solutions, we were not able to provide precise analysis about these two topics.

### 5.1 | Challenges and future direction in IdM solutions

In IdM, we have discussed SSI architecture and various Blockchain-based identity solutions that claim to fulfill self-sovereignty. The ongoing research in this domain includes the implementation of proof of concept for proposed solutions based on the principle of SSI that now act as evaluation criteria. However, the need for open standards, network scalability and flexible identity, adoption of novel solutions, and user empowering identity objectives such as giving full control has been highlighted. These concerns are much needed to be addressed in future novel solutions or as enhancement in existing solutions. Below, we have explained these challenges and trade-offs in building a feasible and effective IdM.

- **Removal of intermediaries:** each Blockchain-based IdM offers a decentralized solution to alleviate the control of centralized authorities. However, most of these solutions rely upon a central server or intermediaries for data storage and key revocation. More so, the complete removal of CA can compromise several functions of IdM such as backup of cryptographic keys, identity recovery, lookup services, etc. It has been shown in the practice that user consent often leads to disclosure of maximum information as they are habitual to the different warnings.
- **The scalability and flexibility:** scalability and optimization aspects for distributed IdM are essential to uptake adoption to avoid considerable delay in specific use cases such as identity verification for digital visa systems or payment verification. On the other hand, to ensure interoperability in real-world applications, backward compatibility is much needed. The integration of Blockchain-based IdM with existing solutions can initiate rapid acceptance in the market as compare to novel solutions. The research and technical workaround portability of the digital identity must be taken into consideration. It must ensure the smooth transfer with minimum identity data of identity to other platforms when existing platforms disappear due to some reasons.



- Trust and privacy: the trust and reputation between attestation verifiers and relying parties are essential to certify identity attributes in WOT where any node can certify others and it becomes difficult to quantify the trust anchors in the network. On the other hand, the user-controlled identity demands a transparent flow of data; IdM infrastructure should be designed to support pseudonymity while maintaining required degrees of confidentiality, integrity, authenticity, nonrepudiation, and robustness. In authorized access to certain services as an anonymous user, identity holder needs to show authorizations to the service which are issued by a third party while they remain unlinkable to pseudonyms. The verification of third parties and mechanism to build a trust relationship between the service provider and third parties needs a secure communication channel.
- User experience: the user experience and human integration are other challenges that need to be addressed by DLT-based IdM. The research in usability and user experience of IdM is still in the incipient stage and seems to lack the vision of long-term span. The wide adoption of federated IdM by users suggests that novel solutions for IdM built upon the same user interaction are unlikely to uptake. The authentication and identity proofing methods merely rely on unique identification through Blockchain identifiers, and poor management of private keys by users limits the scope of IdM for non-technical users. The design of IdM must be based on open standards and established protocols to ensure maximum transparency and adoption.

Regarding authentication, generally speaking, using Blockchain and smart contracts in authentication methods can increase the integrity of the data; more specifically, the impossibility of data falsification regarding user credentials is guaranteed. In the case of fully distributed implementation of authentication methods, Blockchain can improve the availability of the system. On the other hand, the proposed methods mostly are suffering from high computational time, transaction fee, and resource usage (i.e., mostly for resource-limited devices in IoT environment). Some researchers use Blockchain as a database for storing the credentials, and in the case of authentication, they retrieve these credentials. This method inherits the main problems of the conventional methods (e.g., having a central authority and single point of failure, and decreasing the availability of the system in the case of congestion). This type of methods can be useful only because of immutability of credentials. Also, there are some other problems that are not related to Blockchain and smart contract like mutual authentication (i.e., two parties of the connection authenticating each other at the same time). This problem is mentioned as future work for several papers and can be their next research focus. Besides, in several cases, the author's assumption about having the trusted server for authentication could be an obstacle to implement the method in the real world, because in the real world, there is no guarantee that a server is a fully trusted party (i.e., it can be a forged server of a man in the middle attack) since the mutual authentication concept is developed. User privacy remains an unsolved challenge for several methods. Overall, adding mutual authentication, providing user privacy, and increasing the performance of these methods by lowering the time and cost consumption are the most popular problems for future work.

## 5.2 | Challenges and future direction in access control solutions

In the general view, using the Blockchain and smart contract for access control results in increasing the integrity and availability of the data and service. Also, using a smart contract, the public availability of the code and data, and the fact that the code is always the right paradigm are some of the most highlighted features. When the method uses the Blockchain for access management, the availability of the system by removing the single point of failure is guaranteed. It means some attacks like DDoS are impossible for these methods. Also, it can decrease the service cost (by removing the third party), make the rules and policies immutable, and provide access traceability. On the negative side, similar to authentication methods, these methods can be problematic for resource constraint devices like IoT. In some cases, the adjusted version of the consensus model has been used to decrease resource consumption. This approach can threaten the immutability of Blockchain. On the other hand, proposing an auditable access control method can violate user privacy. Similar to authentication methods, some researchers have used Blockchain as a database for storing the rules and policies and not for the access management process; in these cases, the main problems of the conventional methods like a single point of failure will be inherited. Another significant problem in the proposed methods is scalability in terms of block and memory size. As a result, the performance of the system can be negatively influenced by an oversized chain. For example, this increases the synchronization time of new users. In conclusion, protecting user privacy in line with access control auditability, decreasing resource consumption, removing the CA by proposing the fully distributed access control mechanism, and solving the scalability

problem specifically for the IoT environment are more significant research interests regarding access control mechanisms.

## DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

## ORCID

Fariba Ghaffari  <https://orcid.org/0000-0003-2785-9950>

## REFERENCES

1. Kling J, Thompson B, Green W. IAM System Implementing Iam Data Model. *US Patent 9*. 2016:529-989.
2. Goel V. Facebook tinkers with users' emotions in news feed experiment, stirring outcry. *The New York Times*. 2014:29. <https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html>
3. Abraham A. Self-sovereign identity. *Styria EGIZ GV AT*. 2017. <https://technology.a-sit.at/en/whitepaper-self-sovereign-identity>
4. Hardt D. (2021) RFC6749—The OAuth 2.0 Authorization Framework. <https://tools.ietf.org/html/rfc6749>. Accessed February 18, 2021.
5. Hu VC, Ferraiolo D, Kuhn R, et al. Guide to attribute based access control (abac) definition and considerations. *NIST Special Publ*. 2013; 800(162):4-16.
6. Vimercati DC, Foresti DC, Samarati SP. Authorization and access control. In: *Security, Privacy, and Trust in Modern Data Management*. Berlin: Springer Berlin Heidelberg; 2007:39-53 [https://doi.org/10.1007/978-3-540-69861-6\\_4](https://doi.org/10.1007/978-3-540-69861-6_4)
7. Nuss M, Puchta A, Kunz M. Towards Blockchain-based identity and access management for Internet of Things in enterprises. *Intern Conf Trust and Priv Digital Bus*. 2018:167-181. Accessed February 18, 2021.
8. Zhu X, Badr Y, Pacheco J, Hariri S. Autonomic identity framework for the Internet of Things. *Intern Conf Cloud and Auto Comp (ICCAAC)*. 2017:69-79. Accessed February 18, 2021.
9. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the Internet of Things (IoT). *Recent Trends in Net Sec App*. 2010:420-429. Accessed February 18, 2021.
10. Osmanoglu E. *Identity and Access Management: Business Performance Through Connected Intelligence*. Newnes; 2013.
11. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Decentralized Busi Rev*. 2008:1-9. <https://bitcoin.org/bitcoin.pdf> Accessed January 30, 2021.
12. Szabo N. Secure property titles with owner authority. Nakamotoinstitute. <https://nakamotoinstitute.org/secure-property-titles>. Published 1998. Accessed February 18, 2021.
13. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Github. <https://ethereum.github.io/yellowpaper/paper.pdf>. Published: 2014. Accessed February 18, 2021.
14. Ghaffari F, Bertin E, Hatin J, Crespi N. Authentication and access control based on distributed ledger technology: a survey. *2nd Con Blockchain Res App Inno Net Ser (BRAINS)*. Paris, France; 2020:79-86. September 27, 2020.
15. Gilani K, Bertin E, Hatin J, Crespi N. A survey on Blockchain-based identity management and decentralized privacy for personal data. *2nd Con Blockchain Res App Inno Net Ser (BRAINS)*. Paris, France; 2020:97-101. September 27, 2020.
16. Jøsang A, Pope S. User centric identity management. *AusCERT Conference*. 2005:1-13. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=rep1&type=pdf> Accessed February 18, 2021
17. el Maliki T, Seigneur JM. User-centric mobile identity management services. *SECURWARE Intern Conf*. 2007:33-76.
18. Chadwick DW. Federated identity management. In: *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*. Berlin: Heidelberg: Springer Berlin Heidelberg; 2009:96-120.
19. Allen C. The Path to Self-Sovereign Identity. *Lifewithalacrity*. 2016. <https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html#dfref-1212> Published Accessed February 18, 2021
20. Clauß S, Kesdogan D, Kölsch T. Privacy enhancing identity management: protection against re-identification and profiling. *Proceedings of the 2005 workshop on Digital identity management*. Seoul, Korea; 2005:84-93. November 15, 2005.
21. Pfitzmann A, Hansen M. Anonymity, unlinkability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology. [https://www.researchgate.net/publication/228622491\\_Anonymity\\_Unlinkability\\_Undetectability\\_Unobservability\\_Pseudonymity\\_and\\_Identity\\_Management-A\\_Consolidated\\_Proposal\\_for\\_Terminology](https://www.researchgate.net/publication/228622491_Anonymity_Unlinkability_Undetectability_Unobservability_Pseudonymity_and_Identity_Management-A_Consolidated_Proposal_for_Terminology). Published: January 2007. Accessed February 18, 2021.
22. Voigt P, von Dem Bussche A. *The EU General Data Protection Regulation (GDPR) A Practical Guide*. 1sted. Springer International Publishing; 2017.
23. Pohrmen FH, Das RK, Saha G. Blockchain-based security aspects in heterogeneous Internet-of-Things networks: A survey. *Trans Emerg Telecommun Technol*. 2019;30(10):1-26.
24. Bonneau J, Herley C, Van Oorschot PC, Stajano F. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. *IEEE Symposium on Security and Privacy*. San Francisco, CA; 2012:553-567. May 20, 2012.
25. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Transac Circu Sys Video Tech*. 2004;14(1):4-20.
26. Bertin E, Hussein D, Sengul C, Frey V. Access control in the Internet of Things: a survey of existing approaches and open research questions. *Annals of Telecommu*. 2019;74(7):375-388.

27. Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Trans Inform Sys Sec (TISSEC)*. 2000;3(2):85-106.
28. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security*. Alexandria Virginia USA; 2006:89-98.
29. Liu X, Farahani B, Firouzi F. Distributed ledger technology. *Intell Inte Things*. 2020;393-431.
30. Bashir I. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd.; 2018.
31. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H. Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet Things J*. 2018;6(2):2188-2204.
32. Dwork C, Naor M. Pricing via processing or combatting junk mail. *Annual Intern Crypt Conf*. 1992:139-147.
33. Jakobsson M, Juels A. Proofs of work and bread pudding protocols. *Secure Inform Net*. 1999:258-272.
34. King S, Nadal S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake. self-published paper. <https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf> Published 2012. Accessed February 18, 2021.
35. Castro M, Liskov B. Practical byzantine fault tolerance. *OSDI*. 1999:173-186.
36. Ethereum Team. Ethereum white paper. ethereum. <https://ethereum.org/en/whitepaper>. 2013. Updated 2021. Accessed February 18, 2021.
37. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of Blockchain technology: architecture, consensus, and future trends. *IEEE international congress on big data (BigData congress)*. Boston, USA; 2017:557-564. June 2017.
38. Salman T, Zolanvari M, Erbad A, Jain R, Samaka M. Security services using Blockchains: a state of the art survey. *IEEE Commu Surv & Tutor*. 2018;21(1):858-880.
39. Lim SY, Fotsing PT, Almasri A, et al. Blockchain technology the identity management and authentication service disruptor: a survey. *Intern J Adv Sci, Engin Inform Tech (IJASEIT)*. 2018;8(4-2):1735-1745.
40. Otte P, de Vos M, Pouwelse J. TrustChain: a Sybil-resistant scalable Blockchain. *Future Gene Comp Sys*. 2020;107:770-780.
41. Popov S, The tangle. assets. [https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle\\_White\\_Paper\\_v1.4.2.pdf](https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf). Published 2016. Accessed February 18, 2021.
42. Ohl J, Neuman C. The Kerberos network authentication service (V5). *RFC 1510*. 1993:1-112. [https://www.hjp.at/\(st\\_a\)/doc/rfc/rfc1510.html](https://www.hjp.at/(st_a)/doc/rfc/rfc1510.html)
43. Niu Y, Wei L, Zhang C, Liu J, Fang Y. An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin Blockchain. *IEEE/CIC International Conference on Communications in China (ICCC)*. Qingdao, China; 2017:1-6. October 22, 2017.
44. Sanda T, Inaba H. Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0. *IEEE 5th Global Conference on Consumer Electronics*. Tokyo, Japan; 2016:1-5. October 11, 2016.
45. Lee JH. BIDaaS: Blockchain based ID as a service. *IEEE Access*. 2017;6:2274-2278.
46. Lin C, He D, Huang X, Choo KKR, Vasilakos AV. BSEIn: a Blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *J Net Comp App*. 2018;116:42-52.
47. Ouaddah A, Abou Elkalam A, Ait OA. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Commu Netw*. 2016;9(18):5943-5964.
48. Widick L, Ranasinghe I, Dantu R, Jonnada S. Blockchain based authentication and authorization framework for remote collaboration systems. *IEEE 20th International Symposium on WoWMoM*. Washington DC, United States; 2019:1-7. June 10, 2019.
49. Ourad AZ, Belgacem B, Salah K. Using Blockchain for IOT access control and authentication management. *Intern Conf Intern Things*. 2018:150-164.
50. Huh JH, Seo K. Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *The J Supercomp*. 2019;75(6):3123-3139.
51. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of trust: a decentralized Blockchain-based authentication system for IoT. *Comput Secur*. 2018:126-142.
52. Deep G, Mohana R, Nayyar A, Sanjeevikumar P, Hossain E. Authentication protocol for cloud databases using Blockchain mechanism. *Sensors*. 2019;19(20):1-13.
53. Mohsin AH, Zaidan AA, Zaidan BB, et al. Based Blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication. *Comp Stand & Inter*. 2019;66:1-25, 103343.
54. Kim HW, Jeong YS. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with Blockchain. *HCIS*. 2018;8(1):1-13.
55. Lundkvist C, Heck R, Torstensson J, Mitton Z, Sena M. *uPort: a platform for self-sovereign identity*; 2017.
56. Jolocom Team. A decentralized, open source solution for digital identity and access management. Jolocom. <https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf>. Published 2019. Accessed January 30 2021.
57. Tobin A, Reed D. The inevitable rise of self-sovereign identity. *The Sovrin Found*. 2016:1-24. <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>
58. SelfKey Team. Selfkey. The SelfKey Foundation, <https://selfkey.org/wp-content/uploads/2019/03/selfkey-whitepaper-en.pdf>. Published 2017. Accessed February 18, 2021.
59. Microsoft Corp. Identity overlay network. github. <https://github.com/decentralized-identity/ion>. Published 2019. Accessed 31 Jan 2021.
60. Zhang L, Li H, Sun L, Shi Z, He Y. Poster: towards fully distributed user authentication with Blockchain. *IEEE Symposium on Privacy-Aware Computing (PAC)*. Washington, DC, USA; 2017:202-203. August 1, 2017.

61. Ali M, Nelson J, Shea R, Freedman MJ. Blockstack: design and implementation of a global naming system with Blockchains. 2016.
62. ShoCard. Travel identity of the future – White Paper. SITA. Blockchainlab. <https://Blockchainlab.com/pdf/2016-05-00-idm-ShoCard-travel-identity-of-the-future.pdf>. Published 2016. Accessed January 30 2021.
63. Xiong L, Li F, Zeng S, Peng T, Liu Z. A Blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures. *IEEE Access*. 2019;7:125840-125853.
64. Ferdous MS, Chowdhury F, Alassafi MO. In search of self-sovereign identity leveraging Blockchain technology. *IEEE Access*. 2019;7:103059-103079.
65. Simons A. Toward scalable decentralized identifier systems. Microsoft Corp. <https://techcommunity.microsoft.com/t5/azure-active-directory-identity/toward-scalable-decentralized-identifier-systems/ba-p/560168>. Published 2019. Accessed 31 Jan 2021.
66. Benet J. IPFS—content addressed, versioned, P2P file system. Arxiv. <https://arxiv.org/abs/1407.3561>. Published 2014. Accessed 31 Jan 2021.
67. Mohsin AH, Zaidan AA, Zaidan BB, et al. Blockchain authentication of network applications: taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Comp Stand & Inter*. 2019;64:41-60.
68. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: a state of the art survey. *J Net Comp App*. 2020;166:1-38, 102693.
69. Raju S, Boddepalli S, Gampa S, Yan Q, Deogun JS. Identity management using Blockchain for cognitive cellular networks. *IEEE Intern Conf Comm (ICC)*. 2017:1-6.
70. Dramé-Maigné S, Laurent M, Castillo L. Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts. *15th Intern Wireless Commu & Mobile Comp Conf (IWCMC)*. 2019:1582-1587.
71. Ali G, Ahmad N, Cao Y, Asif M, Cruickshank H, Ali QE. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput Secur*. 2019;86:318-334.
72. Xu R, Chen Y, Blasch E, Chen G. Blendcac: a smart contract enabled decentralized capability-based access control mechanism for the iot. *Comput Secur*. 2018;7(3):1-27.
73. Zhang X, Posladand S, Ma Z. Block-based access control for Blockchain-based electronic medical records (EMRs) query in eHealth. *IEEE Global Commu Conf (GLOBECOM)*. 2018:1-7.
74. Qin X, Huang Y, Yang Z, Li X. An access control scheme with fine-grained time constrained attributes based on smart contract and trap-door. *26th Intern Conf Telecommu (ICT)*. 2019:249-253.
75. Wang S, Zhang Y, Zhang Y. A Blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*. 2018;6:38437-38450.
76. Maesa DDF, Mori P, Ricci L. Blockchain based access control services. *iThin GreenCom and CPSCom SmartData*. 2018:1379-1386.
77. Maesa DDF, Mori P, Ricci L. Blockchain based access control. *IFIP Intern Conf Distributed App Intero Syst*. 2017:206-220.
78. Shafeeq S, Alam M, Khan A. Privacy aware decentralized access control system. *Future Gene Comp Sys*. 2019;101:420-433.
79. Ihle C, Sanchez O. Smart contract-based role management on the Blockchain. *Intern Conf Busi Inform Sys*. 2018:335-343.
80. Cruz JP, Kaji Y, Yanai N. RBAC-SC: role-based access control using smart contract. *IEEE Access*. 2018;6:12240-12251.
81. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the Internet of Things. *IEEE Internet Things J*. 2018;6(2):1594-1605.
82. Pinno OJA, Gregio ARA, De Bona LC. Controlchain: Blockchain as a central enabler for access control authorizations in the IoT. *GLOBECOM 2017-2017 IEEE Global Commu Conf*. 2017:1-6.
83. Ding S, Cao J, Li C, Fan K, Li H. A novel attribute-based access control scheme using Blockchain for IoT. *IEEE Access*. 2019;7:38431-38441.
84. Liu H, Han D, Li D. Fabric-IoT: a Blockchain-based access control system in IoT. *IEEE Access*. 2020;8:18207-18218.
85. Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using Blockchain technology for IoT data access protection. *IEEE 17th Intern Conf Ubiqu Wire Broad (ICUWB)*. 2017:1-5.
86. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using Blockchain technology. *Sustain Cities Soc*. 2018;39:283-297.
87. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: using Blockchain for medical data access and permission management. *2nd Intern Conf Open and Big Data (OBD)*. 2016:25-30.
88. Zhu Y, Qin Y, Gan G, Shuai Y, Chu WCC. TBAC: transaction-based access control on Blockchain for resource sharing with cryptographically decentralized authorization. *IEEE 42nd Annual Comp Soft App Conf (COMPSAC)*. 2018:535-544.
89. Maesa DDF, Mori P, Ricci L. A Blockchain based approach for the definition of auditable access control systems. *Comput Secur*. 2019;84:93-119.
90. Ding Y, Jin J, Zhang J, Wu Z, Hu K. SC-RBAC: a smart contract based RBAC Model for DApps. *Intern Conf Human Centered Comp*. 2019:75-85.
91. Rouhani S, Deters R. Blockchain based access control systems: state of the art and challenges. *IEEE/WIC/ACM International Conf Web Intelli*. 2019:423-428.
92. Kalam AAE, Baida RE, Balbiani P, et al. Organization based access control. *Proc POLICY 2003 IEEE 4th Intern Works Poli Distrib Sys Net*. 2003:120-131.
93. Yang H, Zheng H, Zhang J, Wu Y, Lee Y, Ji Y. Blockchain-based trusted authentication in cloud radio over fiber network for 5G. *16th Intern Conf Optical Commu Net (ICOON)*. 2017:1-3.
94. Ferdous MS, Margheri A, Paci F, Yang M, Sassone V. Decentralised runtime monitoring for access control systems in cloud federations. *IEEE 37th Intern Conf Distr Comp Sys (ICDCS)*. 2017:2632-2633.



## AUTHOR BIOGRAPHIES



**Fariba Ghaffari** is pursuing her PhD with Institut Polytechnique de Paris (Telecom Sud-Paris). She has been involving in the field of authentication and access control mechanisms based on Blockchain and smart contracts at Orange Labs, France, since 2019. She received her master Degree of Science in the field of Information Security.



**Komal Gilani** is pursuing her PhD with Institut Polytechnique de Paris (Telecom SudParis). She has been involving in the field of identity and access management based on Blockchain and smart contracts at Orange Labs, France, since 2019. She received her Master Degree of Engineering in the field of Software and Information Security in 2019 from Sejong University, South Korea where she worked on theoretical and experimental research in the field of Semantic Web and Internet of Things.



**Emmanuel Bertin** is chairing an expert community dedicated to Transaction and Communication Services with Orange Labs and is an adjunct professor at the Institut Mines-Telecom, France. His activities are focused on 5G and 6G, NFV, Blockchain and service engineering, with more than 100 published researched articles. He received a Diplome d'ingénieur from IMT Atlantique, a PhD in computer science from the University of Paris VI and Habilitation from Sorbonne University. He is a senior member of the IEEE.



**Noel Crespi** holds Masters Degrees from the Universities of Orsay and Canterbury, a “Diplome d'ingénieur” from Telecom ParisTech and a PhD and Habilitation from Paris VI University. He joined Institute Mines-Telecom in 2002 and is currently Professor and MSc Programme Director, leading the Service Architecture Laboratory. He coordinates the standardization activities for Institute Telecom at ETSI, 3GPP, and ITU-T. He is also an adjunct professor at KAIST (South Korea), an affiliate professor at Concordia University (Canada), and guest researcher at the University of Goettingen (Germany). He is the scientific director the French-Korean laboratory ILLUMINE. His current research interests are in Data Analytics, Internet of Things and Softwarisation. He is the author/co-author of 400 articles and contributions in standardization. He is a senior member of the IEEE.

**How to cite this article:** Ghaffari F, Gilani K, Bertin E, Crespi N. Identity and access management using distributed ledger technology: A survey. *Int J Network Mgmt*. 2021;e2180. <https://doi.org/10.1002/nem.2180>