Authentication and access control based on distributed ledger technology

Fariba Ghaffari, Emamnuel Bertin, Julien Hatin, Noel Crespi

Authentication and Access Control based on Distributed Ledger Technology: A survey

Fariba Ghaffari, Emamnuel Bertin, Julien Hatin
Orange Labs, France
{fariba.ghaffari, emmanuel.bertin,
julien.hatin}@orange.com

Noel Crespi
Institut Telecom, Telecom SudParis,
CNRS 5157, France
noel.crespi@it-sudparis.eu

***Abstract*— As the first step in preserving system security, Authentication and Access Control (AAC) plays a vital role in all businesses. Recently, emerging the blockchain and smart contract technology has attracted significant scientific interest in research areas like authentication and access control processes. In the context of authentication and access control, 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. To categorize and find the most important open problems in this research area, having a comprehensive review is crucial. To the best of our knowledge, for the first time in this survey, we aim to describe the current state of the art in deploying blockchain and smart contracts specifically in authentication and access control. Following an introduction to AAC and blockchain technology, we present a brief background of distributed ledger technology, access control and authentication. To offer a clearer understanding of the state of the art, we propose taxonomy to categorize the existing methods based on their type, application environment and their justification for exploiting blockchain. For the conclusion of the paper, we examined the advantages and disadvantages of the proposed method in different contexts like security, resource consumption and privacy. Also we discussed about the future work.**

Keywords—Authentication, access control, blockchain, smart contract, taxonomy

I. INTRODUCTION

As information systems have dramatically increased the number of their users, authentication and access control (AAC) has become a critical factor in resource and information protection. Authentication and access control are different in meaning; authentication is the act of verifying that the subject performing an operation is who they say they are [1]. On the other hand, as a simple definition of access control, it 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.*) [1]. In other words, access control is a security technique that regulates who or what can do an action (*e.g.* use, read, write, execute or view) on specific resources in a computing environment [2].

Recently, the introduction of blockchain [3] and smart contracts [4][5] as extensions of distributed ledger technology (DLT) are changing different aspects of business models, management, and even authentication and access control processes in telecommunication, healthcare, IoT and smart cities, *etc*. The first version of the blockchain technology is known as blockchain v1.0 and includes the cryptocurrencies and distributed ledger, while in blockchain v2.0, smart contracts are added to this technology via the introduction and emerging of Ethereum [25].

Immutability (*i.e.* any confirmed transaction cannot be altered), decentralized (*i.e.* no central authority to control the network), traceability (*i.e.* all transactions can be seen and track by nodes) and non-repudiation (*i.e.* no one can deny his action) are the most attractive blockchain features for using this technology in authentication and access control. 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 action and access.

To the best of our knowledge, despite different comprehensive researches about blockchain technology and its application, there is lack of specific review about the application of this technology in authentication and access control. In this paper we examine existing blockchain-based authentication and access control methods in different application environments, including healthcare, cloud computing, resource sharing, telecommunications, and the Internet of Things (IoT). We propose taxonomy for categorizing the existing methods and comparing them in terms of their advantages and disadvantages regarding security capabilities, time consumption, cost effectiveness, performance, *etc*.

The rest of this paper is organized as follow: Section II briefly reviews the AAC, blockchain and smart contracts. The proposed taxonomy is depicted in section III. Section IV describes the current state of the art in authentication, and then Section V examines the current access control methods in two main categories namely, using the blockchain as a distributed database and using that for access management process. Finally, Section VI 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.

II. BACKGROUND

The main focus of this paper is to categorize different authentication and access control mechanisms that use blockchain and smart contract. In this section we describe the main background for this work: access control mechanisms, authentication methods and a brief description of distributed ledger technology (including blockchain and smart contracts).

A. Access control

As mentioned above, access control is a security technique that regulates who or what can perform an action on resources. While there are several different access control mechanisms, the most well-known methods are listed below:

1) Discretionary access control (DAC): this method considers owner-based administration of the objects. In

978-1-7281-7091-6/20/$31.00 ©2020 IEEE

other words the owner of the object will define the access rules and policies over that. DAC can be implemented via Access Control List (ACL) or access control matrix (*i.e.* In this case it will be named by capability-based access control) [6][7].

2) Mandatory access control (MAC): This model is based on the classification of the objects and subjects. It means, the subjects whose level is upper than the object can have access on it. The access decision in this method will made by an central authority and not by the owner. MAC can be useful in environments that require very restricted access control policies [6][7][2].

3) Role-based access control (RBAC): This method manage the access of subjects based on their role within the system and on rules defining what kind of accesses are 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 [6].

4) Attribute-based access control (ABAC): This method is a logical access control model that 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 or combination of these attributes. ABAC is useful for fine-grained access control [51]. In ABAC method subject attributes are related to identifiers that specify the subject who is demanding access to an information asset like user roles, group memberships, certifications, management level, user ID *etc*. Object attributes distinguish the resources that the subject want to access to them, for example, file, folder, application *etc*. The action that will be performed by the subject on object defines by action attributes. These actions are but not limited to read, write, execute and view. Environment attributes describe the environment identifying the context in which access is requested, for example time and location from where access is requested, type of communication channel *etc* [1].

B. 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. There are four main authentication methods [8]:

1) Knowledge-based authentication: Relies on knowledge about the users, such as their IDs and passwords;

2) Possession-based authentication: Based on a user's possessions, including their credentials, RFID, or other identifiers that only the principal user could have;

3) Inherence-based authentication or Biometric-based authentication: Uses biometric features, such as fingerprints, iris data, *etc.* [9].; and

4) Multi-factor authentication: This method combines two or more of the previous methods.

Traditional authentication methods and systems use a central authority for assessing the request; this central authority could be the main single point of failure for a system [10].

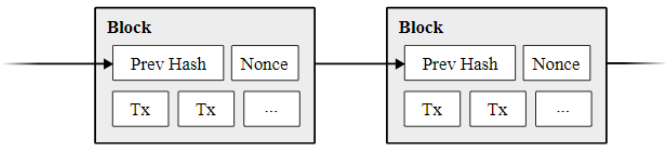

Fig. 1. The architecture of blockchain

C. Blockchain and smart contract

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 [11] [3]. 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 [12][13]. These features make blockchain attractive as a decentralized consensus mechanism, since there is no central authority for controlling the ledger. From an architectural perspective, blockchain is a linked-list data structure that uses a hash of each previous blocks to create a link. 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.

Introduced by Szabo in 1998 [4], 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 distributed ledger technology. The main purpose of smart contracts is to satisfy common contractual conditions, minimize exceptions both malicious and 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 [14]. This platform has a Turing complete virtual machine which can run distributed applications and allow the execution of smart contracts [5].

III. Proposed Taxonomy

Based on our study, the existing researches on blockchain based authentication and access control mechanisms can be categorized as shown in Fig. 2. As mentioned earlier, authentication methods can be categorized based on their type and application environment into Knowledge-based, Possession-based, Biometric-based and multi factor authentication types that can be used in different contexts, including 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 environments. Note that, blockchain is mostly used as a distributed, immutable and secure storage for credentials and user identity in authentication procedure.

Access control methods, meanwhile, can be classified in three different categories based on the access control mechanism, the application, and how it uses the blockchain network. Access control mechanisms can be divided into three main categories: ABAC, RBAC, and ACL-based methods such as DAC (see Fig. 2). 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

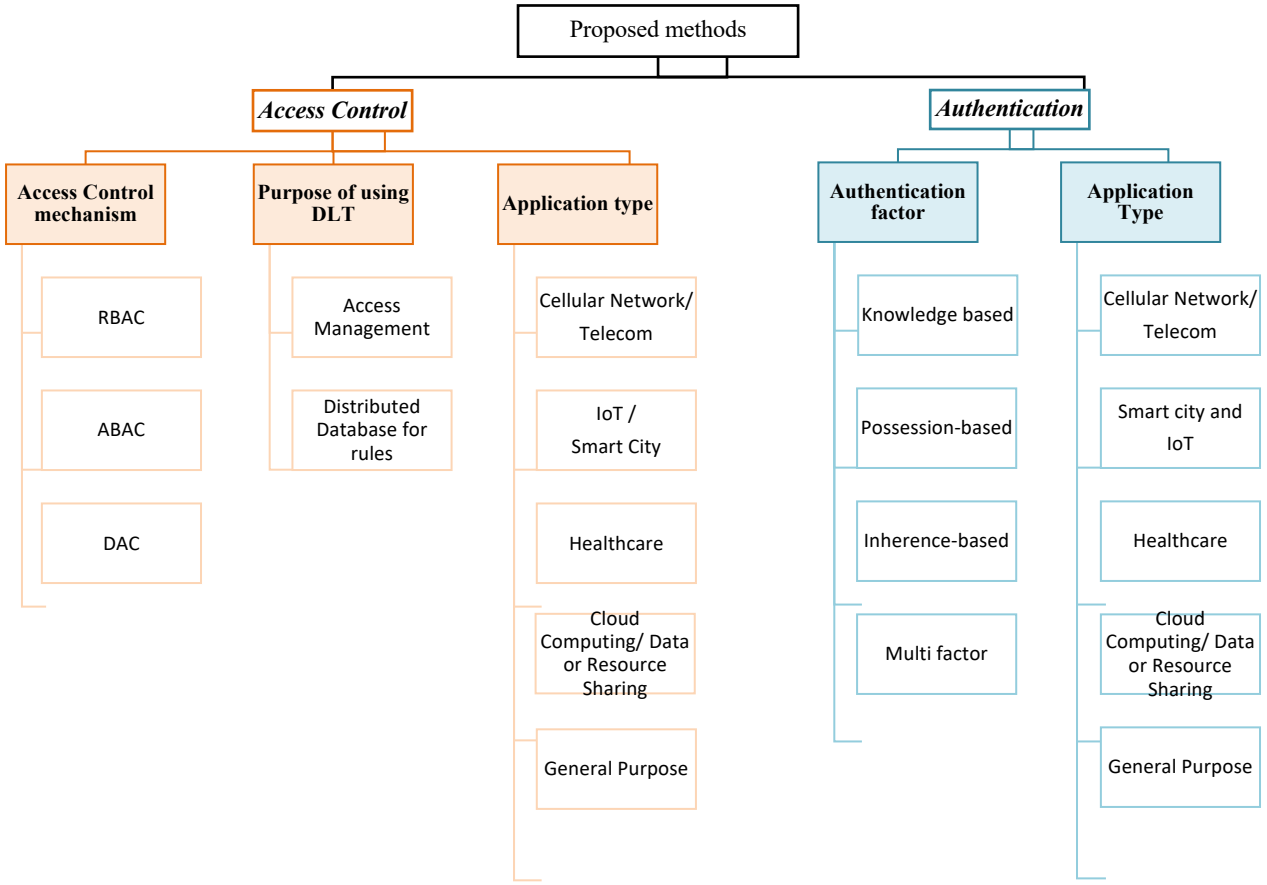

Fig. 2. Taxonomy of existing AAC mechanisms based on blockchain

access management process. Similar to the authentication methods, these solutions can be general purpose methods, or they can be used in specific contexts (*i.e.*, cellular network and telecommunication, IoT devices and smart cities, healthcare and medical data records, cloud computing and resource sharing).

IV. Authentication Methods

In this section we will explain and discuss existing authentication methods that use blockchain or smart contracts. Table I depicts the four categories of these methods based on the taxonomy.

L. Zhang *et al.* [15] 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.

TABLE I. Authentication Methods Based on Blockchain

Auth. / *App.*	*Knowledge*	*possession*	*Inherence*	*Multi factor*
Telecom/ Cellular network	[23]	[24] [26]	-	-
IoT/ Smart city	-	[26] [21] [22][19]	[18]	[20]
Healthcare	-	[16]	-	-
Cloud/ Resource sharing	-	[16]	-	[17]
General	-	[15]	-	-

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.* [16] 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 use blockchain as a distributed database for storing credentials on it. Another authentication method proposed for cloud environment is introduced by Kim *et al.* [17] 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.* [18] 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 is proposed by Widick *et al.* [19] 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.* [20] 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 seconds 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 [21]. This system is a mutual authentication method that consists of four tangible layers which combine vertically inter-organizational 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 [22] proposed an AAC system for IoT. On the authentication part it creates token for user's based on their credentials. This method explained more in next part of the paper. FairAccess just support token-based authorization, 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.* [23]. 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 Colored Coins inspired the development of this scheme. Another authentication method in telecommunication environment is proposed by Sandra *et al.* [24] 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 [25]. 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 allow user to connect to the internet. Moreover, BIDaaS [26] 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.

TABLE II. ACCESS CONTROL METHODS BASED ON BLOCKCHAIN

Purpose	***A.C.*** / ***App.***	***ABAC***	***RBAC***	***DAC***
Distributed DB	Telecom/ Cellular network	[32]	[32]	[32]
	IoT/ Smart city	[35] [34]	[34]	[34] [33]
	Healthcare	-	-	-
	Cloud/ Resource sharing	[36] [37]	-	-
	General	[27] [29] [38]	[30] [31]	-
Access management	Telecom/ Cellular network	-	-	-
	IoT/ Smart city	[40] [42] [44] [45]	[22]	[43]
	Healthcare		[47] [46]	-
	Cloud/ Resource sharing	[50]	-	-
	General	[48]	[49]	-

I. ACCESS CONTROL

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 some others use blockchain transactions for granting/ denying user access. In summary Table II shows the category of the methods based on the taxonomy.

A. using blockchain as database for rules

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

Masea *et al.* [27], proposed a general purpose access control for storing and publishing policies of attribute based access control 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 [28] [29]. Other general purpose AC is addressed by Ihle *et al.* [30] for role based access control 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 *role-based access* control mechanism usable in all environments [31]. 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.* [32] proposed an access control system for cognitive cellular networks 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), Cognitive Cellular Network (CCN) and Identity and Credibility Service (ICS). ICS uses blockchain and smart contract as an access control and identity management mechanism. At first user registers his personally identifiable information (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 [33]. 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.* [34] 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 get broadcasted to all nodes of the system. Dramé-Maigné *et al.* [35] 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.* [36] proposed a method for fine-grained ABAC that can be applied in cloud oriented data access control environments. Central Authority (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 performs 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.* [37] 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 save it to the blockchain and then deploys a smart contract, then user send the registration request to owner; and owner manages the secret key for the user and save 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.* [38] proposed a general purpose decentralized attribute based access control mechanism using Tangle (*i.e.* a new decentralized and tamper-proof distributed ledger) [39]. In this method owner define and manage AC over his objects and defines the security policies and the level of authorization granularity of the resources, and store 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.

B. 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.* [40] 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, manage the access control and misbehavior judging methods. Finally, 3) The JC implements a misbehavior judging method, which judges the misbehavior of the subject and determines the corresponding penalty, based on misbehavior report from an ACC. Nonetheless, the environment attributes those are used in the attribute based access control is limited to time attributes. Other AAC mechanism that implements RBAC and OrBAC solution for IoT environment is FairAccess [22]. Note that OrBAC is a model that can handle simultaneously several security policies associated with different organizations [41]. 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 support token-based authorization, 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.* [42] 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 store contextual information from entities to manage the access based on environmental situation. 3) Accountability Blockchain registers a history of permissions or denies of access to object. Finally, 4) the Rules Blockchain keeps the authorization rules defined by owners. When a user send 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.* [43] 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.* [44] 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 that act as the consortium nodes in consortium blockchain and the key generation center. When a user wants to access to another user's data, at first they generate a connection based on 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 at 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 [45] 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 [46] 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) Register Contract maps participant identification strings to their Ethereum address identity; 2) Patient-Provider Relationship Contract for the nodes who 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 is 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 [47] is proposed that utilizes smart contracts for role based access control, 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.* [48] is a general purpose ABAC method. This method consists of Policy Enforcement Point, Policy Administration Point, Attribute Managers, Policy Information Points, 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) [49]. 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, disabling the user or by changing his role.

TBAC [50] 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.

II. Discussion

More and more aspects of businesses are being modified as a result of the emerging distributed ledger technology and its associated blockchain and smart contracts systems. Authentication and access control is one of these areas. Proposing a comprehensive review about using blockchain in AAC can be helpful for researchers to find the most important open issues and advantages/disadvantages of this technology. To the best of our knowledge, despite researches about blockchain application, there is no specific survey about application of smart contract and blockchain in authentication and access control.

To address this issue, in this paper we examined different AAC methods based on blockchain. Taxonomy of existing

AAC methods is proposed. Authentication methods can be categorized based on their type (*i.e.* knowledge-based, possession-based, inherence-based and Multi factor) and application (*e.g.* IoT, smart cities, cellular network and telecommunication, Cloud, *etc*.). On the other hand, access control methods can be classified in three different categories based on AC mechanism (*e.g.* ABAC, RBAC, *etc*.), application (*e.g.* IoT, smart cities, cellular network and telecommunication, Cloud, *etc*.) 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 and their future desire as follow.

Generally speaking using blockchain and smart contract in authentication methods can increase the integrity of the data, more specifically impossibility of data falsification regarding user credentials is guaranteed. In the case of fully distributed implementation of authentication method, 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 researches use blockchain as a database for storing the credentials and in the case of authentication, they retrieve these credentials. This method will inherit the main problems of the conventional methods, like having a central authority will be single point of failure or it will decrease 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 real world. Because in real world there is no guarantee that a server is 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.

In the case of using the blockchain and smart contract for access control, increasing the integrity and availability of the data and service are the most significant benefits in general view. Also in the case of using smart contract, the public availability of the code and data and the fact that the code is always a right paradigm are some of the most precious features. Specifically when the method use 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 is impossible for these methods. Also it can decrease the service cost by removing the third party, make the rules and policies immutable and access traceability is more feasible. 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 consensus model has been used to decrease the resource consumption, but it has some bad effects on blockchain security regarding to immutability. On the other hand, proposing auditable access control method can violate user privacy. Similar to authentication methods, some researches have used blockchain as a database for storing the rules and policies and not for access management process, in these cases the main problems of the conventional methods like single point of failure will be inherited. Another significant problem in the proposed methods is scalability (*e.g*. in terms of block and memory size). As a result the performance of system can be negatively influenced by an oversized chain. For example, this increases the synchronization time of new users [25].

In conclusion, protecting user privacy in line with access control auditability, decreasing the resource consumption, removing the central authority by proposing the fully distributed access control mechanism and solving the scalability problem specifically for IoT environment are more significant research interests regarding to access control mechanisms.

REFERENCES

[1] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, and K. Scarfone. "Guide to attribute based access control (abac) definition and considerations," *NIST special publication, 800(162)*, 2013.

[2] D.C. Vimercati, S. Foresti and P. Samarati. "Authorization and Access Control," *Springer Berlin Heidelberg.* 2007. [Online] Available: https://doi.org/10.1007/978-3-540-69861-6_4

[3] S. Nakamoto, "A peer-to-peer electronic cash system," 2008, Accessed on: Feb. 28, 2020, [Online] Available: https://bitcoin. org/bitcoin. Pdf.

[4] N. Szabo, "Secure property titles with owner authority," 1998, Accessed on: Feb. 28, 2020, [Online] Available: https://nakamotoinstitute.org/ secure-property-titles.

[5] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum project yellow paper, pp. 1–32, 2014

[6] E. Bertin, D. Hussein, C. Sengul, and V. Frey. "Access control in the Internet of Things: a survey of existing approaches and open research questions", *Annals of Telecommunications*, vol. 74, no. 7-8, p.p. 375-388, 2019.

[7] S. Osborn, R. Sandhu, and Q. Munawer. "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 2, p.p. 85-106, 2000.

[8] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *In 2012 IEEE Symposium on Security and Privacy*, p.p. 553-567, 2012.

[9] A. K. Jain, A. Ross, and S. Prabhakar. "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, p. p. 4-20, 2004.

[10] F. H. Pohrmen, R. K. Das, and G. Saha. "Blockchain‐based security aspects in heterogeneous Internet‐of‐Things networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, p.p, e3741, 2019.

[11] X. Liu, B. Farahani and F. Firouzi. "Distributed Ledger Technology," *Intelligent Internet of Things-Springer*, pp. 393–431, 2020.

[12] I. Bashir. "Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained," *Packt Publishing Ltd*, 2018.

[13] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke. "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, p.p. 2188-2204, 2018.

[14] V. Buterin. "Ethereum white paper." *GitHub repository 1,* 2013.

[15] L. Zhang, L. Hong, S. Limin, S. Zhiqiang, and H. Yunhua. "Poster: Towards Fully Distributed User Authentication with Blockchain," *IEEE Symposium on Privacy-Aware Computing (PAC)*. 2017

[16] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain. "Authentication Protocol for Cloud Databases Using Blockchain Mechanism," *Sensors*, vol. 19, no. 20, 2019.

[17] H. W. Kim, and Y. S. Jeong. "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain," *Human-centric Computing and Information Sciences*,vol. 8, 2018.

[18] J. H. Huh, and K Seo. "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," *The Journal of Supercomputing*, vol. 75, no.6, p.p. 3123-3139, 2019.

[19] L. Widick, I. Ranasinghe, R. Dantu, and S. Jonnada. "Blockchain Based Authentication and Authorization Framework for Remote Collaboration Systems," *IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"*, 2019.

[20] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, p.p. 126-142, 2018.

[21] C. Lin, D. He, X. Huang, K. K. R. Choo, and A. V. Vasilakos. "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0." *Journal of Network and Computer Applications*, p.p. 42-52, 2018.

[22] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain‐based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943-5964, 2016.

[23] Y. Niu, L. Wei, C. Zhang, J. Liu, and Y. Fang. "An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain," *In 2017 IEEE/CIC International Conference on Communications in China (ICCC)*, 2017.

[24] T. Sanda, and H. Inaba. "Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0," *In 2016 IEEE 5th Global Conference on Consumer Electronics*, 2016.

[25] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. Albahri, M. A. Alsalem, and K. I. Mohammed. "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Computer Standards & Interfaces*, p.p. 41-60, 2019.

[26] J. H. Lee. "BIDaaS: Blockchain based ID as a service," *IEEE Access*, p.p. 2274-2278, 2017.

[27] D. Maesa, M. Paolo, and R. Laura. "Blockchain based access control," *IFIP International Conference on Distributed Applications and Interoperable Systems. Springer*, 2017

[28] S. Rouhani, and R. Deters. "Blockchain based access control systems: State of the art and challenges," *In IEEE/WIC/ACM International Conference on Web Intelligence*, pp. 423-428, 2019.

[29] D. Maesa, P. Mori, and L. Ricci. "Blockchain based access control services," *In 2018 IEEE International Conference on Internet of Things (iThings)*. pp. 1379-1386, 2018.

[30] C. Ihle, and O. Sanchez. "Smart contract-based role management on the blockchain," *In International Conference on Business Information Systems*, pp. 335-343, 2018.

[31] J. P. Cruz, Y. Kaji, and N. Yanai. "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, p.p. 12240-12251, 2018.

[32] S. Raju, B. Sai, G. Suraj, Y. Qiben, and S. D. Jitender, "Identity management using blockchain for cognitive cellular networks," *In 2017 IEEE International Conference on Communications(ICC)*, pp. 1-6, 2017.

[33] R. Xu, Y. Chen, E. Blasch, and G. Chen. "Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT," *Computers*, 2018.

[34] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, and Q. E. Ali. "Blockchain based permission delegation and access control in Internet of Things (BACI)," *Computers & Security*, p.p. 318-334, 2019.

[35] S. Dramé-Maigné, M. Laurent, and L . Castillo. « Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts," *In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1582-1587, 2019.

[36] X. Qin, H. Yongfeng, Y. Zhen, and L. Xing, "An access control scheme with fine-grained time constrained attributes based on smart contract and trapdoor," *26th International Conference on Telecommunications (ICT)*, pp. 249-253, 2019.

[37] S. Wang, Y. Zhang. "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, p.p. 38437-38450, 2018.

[38] S. Shafeeq, M. Alam, and A. Khan. "Privacy aware decentralized access control system," *Future Generation Computer Systems*, p.p. 420-433, 2019.

[39] S. Popov. "The tangle in: IOTA," 2016. [Online]. Available: https://iota.org/ IOTAWhitepaper.pdf

[40] Y. Zhang, K. Shoji, S. Yulong, J. Xiaohong, and W. Jianxiong, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594-1605, 2018

[41] A. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, and G. Trouessin. "Organization based access control," *In Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*. pp. 120-131, 2003.

[42] O. *Pinno*, A. Gregio, and L. De Bona. "Controlchain: Blockchain as a central enabler for access control authorizations in the IoT," *In GLOBECOM 2017 IEEE Global Communications Conference*, 2017.

[43] N. Rifi, E. Rachkidi, N. Agoulmine, and N. Taher. "Towards using blockchain technology for IoT data access protection," *In 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB)*. 2017

[44] S. Ding, J. Cao, C. Li, K. Fan, and H. Li. "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, p.p. 38431-38441, 2019.

[45] H. Liu, D. Han, and D. Li. "Fabric-iot: A Blockchain-Based Access Control System in IoT," *IEEE Access*, p.p. 18207-18218, 2020.

[46] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. "Medrec: Using blockchain for medical data access and permission management," *In 2016 2nd International Conference on Open and Big Data (OBD),* pp. 25-30, 2016.

[47] G.G. Dagher, J. Mohler, M. Milojkovic, and P.B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283-297, 2018

[48] D. Maesa, P. Mori, and L. Ricci. "A blockchain based approach for the definition of auditable Access Control systems," *Computers & Security*, p.p. 93-119, 2019.

[49] Y. Ding, J. Jin, J. Zhang, Z. Wu, and K. Hu, K. "SC-RBAC: A Smart Contract based RBAC Model for DApps," *In International Conference on Human Centered Computing*, p.p. 75-85, 2019.

[50] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, and W. Chu. "TBAC: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization," *In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. p.p. 535-544, 2018.

[51] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data," *In Proceedings of the 13th ACM conference on Computer and communications security*. pp. 89-98, 2006.