جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Blockchain Driven Access Control Mechanisms, Models and Frameworks: A Systematic Literature Review

Aaqib Bashir Dar[1]*, Auqib Hamid Lone[2], Asif Iqbal Baba[3], Roohie Naaz[2], and Fan Wu[3]

[1] Independent Researcher, Jammu and Kashmir, 190015 India.

[2] Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, 190006 India.

[3] Department of Computer Science,Tuskegee University, Tuskegee, AL 36088, USA.

CrossMark

Received 15 Feb. 2022; Accepted 09 May. 2022; Available Online 22 June. 2022

Abstract

Access control or authorization is referred to as the confinement of specific actions of an entity, thereby allowing them to be performed as per certain rules. Blockchain-driven access control mechanisms gained considerable attention directly after applications beyond the premise of cryptocurrency were found. However, there are no systematic efforts to analyze existing empirical evidence. To this end, we aim to synthesize litera- ture to understand the state-of-the-art blockchain driven access control mechanisms with respect to underlying platforms, utilized blockchain properties, nature of the mod- els and associated testbeds and tools. We conducted the review in a systematic way. Meta analysis and thematic synthesis were performed on the findings from relevant primary studies, in order to answer the framed research questions in perspective. We identified 76 relevant primary studies that passed the quality assessment. The problems targeted by relevant studies were single point of failure, security, and privacy, etc. The meta-analysis of the primary studies suggests the use of different blockchain platforms along with several application domains where different blockchain proprieties were utilized.

In this paper, we present a systematic literature review of blockchain driven access control systems. In hindsight, we present a taxonomy of blockchain-driven access control systems to better understand the immense implications of this field spanning various application domains.

I. Introduction

Access Control [1], typically referred to as resource authorization or just authorization, is to confine the actions of a particular entity only to the services and the computing resources that it is authorized to use. This is achieved by enforcing predefined access control policies. Every access of an entity to a particular resource is governed by the underlying policies. The policies can be realized in the form of rules and attributes that associate with a set of entities and a set of resources. In order for the access control mechanisms to be sound and ensure integrity, this is achieved by securely establishing the identity of the entities. If enforcement of secure establishment of identities is absent, the attempts to enforce an access pol-

Keywords: Cybersecurity, Blockchain, Access Control, Decentralization, Smart Contracts.

Production and hosting by NAUSS

* Corresponding Author: Aaqib Bashir
Email: aaqibb13@gmail.com

doi: 10.26735/TYIF2196

icy are foiled and literally left useless. While there is a definite and dire need to enforce access control mechanisms in practice, it comes with issues that need thorough consideration before these mechanisms are put to implementation. To name a few, it is challenging to achieve access control in resource constrained devices [2], due to their heterogeneous nature and limited capabilities and resources. Other than that, the dynamic nature of devices makes it hard to implement access control policies. Other important aspects that are challenging are the dynamic topologies, distributive nature, and enforcement of policies dynamically. All of this comes down to whether a solution is viable (or scalable), taking into consideration various parameters like time-memory tradeoffs, behavior towards different types of traffic, resistance against various attacks and adaptability to dynamic changes to the network. However, these issues can be dealt with easily, if a different perspective is put into place. Blockchain technology has seen a tremendous rise, which grew exponentially after the inception of the cryptocurrency Bitcoin [3], which in essence is backed by blockchain technology itself. The whole idea that baffled researchers and academics was the blockchain itself, which was the core underlying principle of Nakamoto's idea [3]. However, over the years blockchain technology has bloomed, and there are applications that are beyond the realms of cryptocurrency. With the rise of different technological platforms like Ethereum [4], Hyperledger [5], Ripple [6], Multi-chain and many more, the field has moved to a different dimension of its own. However, right after the emergence of Ethereum the creation of smart contracts was supported [7] and followed by their execution. The turing completeness feature of smart contracts makes it viable for performing complex tasks thereby allowing enormous applications of its own. Smart contract-based solutions leverage inherent properties of blockchain like trust lessness, decentralization, and robustness, along with its own extensive features. The customizable and flexible nature of smart contracts makes enforcement of access control policies and mechanisms easy, attainable, and dynamic in nature, thereby allowing traceability, immutability and decentralization. The persistent issues with traditional access control mechanisms [8] are considered in this view, and it is evident from the existing literature that blockchain technology has clear dominance over them.

The remaining parts of this paper are structured as follows: Section II contains the related work in this area and a comparison of our work with earlier existing studies, Section III contains the methodology followed throughout the course of the paper, and Section IV encompasses the relevant key findings of the paper. In Section V, we constructed the themes for our research and provided a discussion based on those themes. Section VI contains a detailed taxonomy of blockchain-driven access control systems. In Section VII, we concluded the paper by providing appropriate insights.

II. Related Work

Several survey/review papers can be found in literature that target blockchain ap- plications. One of the earliest attempts in this direction is the work carried out by Yli-Huumo *et al.* in [9]. In their findings, they reveal that the majority of the papers focused on Bitcoin projects, specifically under a common theme of security and privacy. This study, in our opinion, provided a steppingstone for the corresponding research community to further explore in this direction. A comprehensive systematic review of blockchain applications was carried out by F. Casino *et al.* [10]. In particular, they provided classification of blockchain-based applications across diverse domains ranging from supply chains to IoT, and they also highlighted barriers in blockchain technology which limit mass use of blockchain technology. However, there are very few articles in the literature that have conducted a survey/review on blockchain application in access control and are thus closely related to our work. One such work was carried out by Sara Rouhani and Ralph Deters in [11]. The authors conducted a state-of-the-art survey on blockchain-based access control systems and challenges. In particular, they highlighted the problems encountered by the current access control systems and how blockchain can be used to overcome such problems. However, our work differs in that we considered different evaluation parameters and performed a more exhaustive study by considering major databases for relevant literature. Another work carried out by Imen Riabi *et al.* in [12] conducted a comprehensive survey on blockchain-based access control for IoT. However, their study was less exhaustive because they specifically targeted access control in IoT only.

In comparison to the existing works, our focus is blockchain-based access control systems in contrast to other similar works which either cover a part of our focused area or do not provide a wide variety of results in the same area. We analyze studies based on themes that align completely with our chosen area. Our major contributions are as follows:

- We studied a total of 76 studies in blockchain-based access control systems and provided key findings from them.
- We further classified the themes to contextualize the area of blockchain-based access control systems.
- We also categorized the studies based on application domains.
- We framed research questions and explained their relevance/significance.
- In addition, we also identified which issues were addressed by which studies.
- We provided a taxonomic view which showed whether the systems provided a reference implementation, the blockchain platform they utilized, the utilized blockchain properties, and the set of testbeds/tools used.
- Our categorization of blockchain based platforms on various fronts provided a comprehensive overview of this area.
- We furthermore concluded by providing generic insights into the field.

We chose certain parameters to draw a comparison with earlier studies that were relevant to this area. The comparison is presented in tabular form in Table I.

III. Research Methodology

For the collection of relevant literature pertaining to the topic, Kitchenham and Charters' [13] guidelines were followed thoroughly to answer the research questions effectively. The whole process followed the phases of planning, conducting, and reporting of the review iteratively to allow rigorous assessment of the state-of-the-art review.

A. Traversing the Kitchenham's path

Primary Study Selection:

Primary studies were identified through keyword searches in major scientific databases. The keywords were selected to foster the emergence of research results that would be more generic in nature and thus aid in providing answers to the research questions. The Boolean operator was restricted to AND. The search strings were: ("BLOCKCHAIN" AND "ACCESS CONTROL")

The search was conducted across the following platforms:

- IEEE Xplore Digital Library
- ScienceDirect
- ACM Digital Library
- SpringerLink
- Wiley
- Taylor and Francis
- MDPI

TABLE I
Comparison with Related Reviews/Surveys

Work	Primary Focus	Targeted Application areas by studies	Studies Analyzed
Yli Huumo	Bitcoin	Privacy and Security	41
F Casino	Blockchain based applications	Supply chain, Business, Healthcare, IoT, Privacy and Data management	260
Sara Rouhani	Blockchain driven access control mechanisms	IoT, EMR, Data Sharing, Plant Phenotyping, Digital Asset Management	40
Our Work	Blockchain driven access control mechanisms	IoT, Healthcare, Digital Currency, Industry 4.0, Knowledge Management Systems, Networks, File Sharing, Plant Phenotyping	76

The searches were run against title, keywords, abstract and full-text, depending on the platforms that we searched on. We conducted the searches on 23rd June, 2020, and all the studies published up to that date were processed. The results from these searches were then filtered through the inclusion/exclusion criteria, which is presented in the next section. This criteria helped in attaining the results, which were then put through Wohlin's snowballing process [14]. The forward and backward snowballing process was conducted iteratively until no intersection was found between any paper and inclusion criteria. We have presented a graphical representation of the relevant studies selected in Fig. 1.

Inclusion and Exclusion Criteria:

Studies that are included in this review must report empirical findings describing technical aspects of the technology in relevance to our topic, applications spanning several domains, and sufficient implementation details with thorough research results. Search engines like Google scholar were omitted to bar lower-grade papers in the search results, in order to maintain the integrity of the results being included. They must be peer-reviewed and written in English. The key inclusion and exclusion criteria are presented in Table II.

Selection of Results:

From the initial keyword searches along the major databases mentioned, a total of 1.517 results were identified. The number was reduced to 1.260 after only scanning through journal articles and conference proceedings. After the filtering process, the total number of articles was reduced to 82 based on the title relevance. While moving on to the next stage of filtering based on abstract relevance, the authors obtained 77 papers. And after moving ahead in a different stage that involved forward and backward snowballing, the number of papers was reduced to 76 in total. We have presented the year-wise distribution of relevant primary studies in Table III.

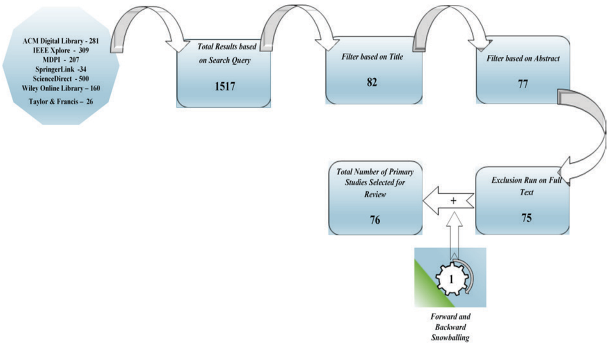
ACM Digital Library - 281
IEEE Xplore - 309
MDPI - 207
SpringerLink -34
ScienceDirect - 500
Wiley Online Library – 160
Taylor & Francis – 26
Total Results based on Search Query
1517
Filter based on Title
82
Filter based on Abstract
77
Exclusion Run on Full Text
75
+
Total Number of Primary Studies Selected for Review
76
1
Forward and Backward Snowballing

Fig. 1 Selection of Primary Studies.

TABLE II
Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Peer-reviewed research articles including articles in press	Studies that are not peer reviewed (Gray literature, newspapers, blog posts, etc.)
Papers presenting blockchain-driven access control	Studies written in languages other than English
Papers reporting substantial implementation details and research results	Studies presenting blockchain applications other than access control. Survey papers/review papers are also excluded.

TABLE III
The Year-Wise Distribution of Publications in Major Databases

Publication Year	Major Databases					Relevant Studies
	IEEE XPLORE	ACM DIGITAL LIBRARY	SCIENCEDIRECT	WILEY	MDPI	
2020	11	2	3	1	4	[15] to [35]
2019	20	3	3	2	2	[36] to [65]
2018	17	1	2	0	0	[66] to [85]
2017	3	0	0	1	0	[86] to [89]
2015	1	0	0	0	0	[90]
Total	52	6	8	4	6	

In order to present the distribution of relevant studies over the years, we have presented the graphical representation in Fig. 2.

B. Perils to Corroboration

One of the most important factors while conducting a review is to establish a common ground which seems to negate the chances of any pitfalls that might possibly affect the course of research, collection of results and sieve out any false negatives from the collected studies. To better emphasize, we consider shedding light on certain aspects that are key in making the path of systematically conducting the literature review easier, transparent and rigorous.

1) Bias towards Publication

The term publication bias refers to the problem of publishing more positive results in comparison to the negative results. It is to be noted that publication bias has immense implications in original literature. In accordance with choosing preferences, selecting some results over others actually leads to correct choices at times. Towards this end, we would like to add that some studies that present a significant amount of results might not be a valid choice although they do have relatively higher chances of getting published, statistically.

2) Importance of Search Terms

In order to conduct a review in a systematic way, it is always extremely important and a challenging task to find the relevant primary studies targeting a particular subject matter and specifically the topic under consideration. Keeping this problem in perspective, we prepared and presented a search strategy in our study. The title was identified after a thorough analysis and after it was found that no such prior study has been conducted around this particular title that focuses on the aspects that we have taken into consideration. The selection of the search string was done after a discussion with experts on the subject matter. A pilot study was conducted prior to the full-fledged study, which confirmed the applicability of the search string and its correctness with regard to the topic in hand. Other than searching the major electronic databases, forward and backward snowballing was carried out to include the studies that might have been excluded otherwise. This increased the confidence and authenticity of the relevant results, to a certain degree.

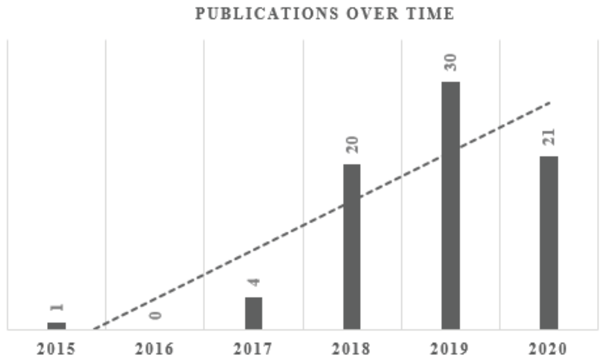

Fig. 2 Publications Over Time.

3) Selection Bias of the Selected Primary Studies

We filtered the selection of primary studies in stages. The filtering was carried out by two researchers separately to ensure that nothing of relevance was left out. During the first stage, studies were excluded based on title relevance followed by abstract relevance. During the pilot study, constructive disagreements were resolved and a solid foundation was laid to better understand and properly refine the inclusion/exclusion criteria. The selection procedure was iteratively repeated by the authors until both authors agreed to select relevant papers from a full set of papers. When both researchers were in doubt about the inclusion of a particular study, a third researcher was consulted. This was followed by the next phase where the studies were excluded based on full-text relevance. Due to the carefully constructed and well-established selection process, it is highly unlikely that any relevant studies were left out.

4) Extraction of Data and its Quality Assessment

The quality of each study was investigated by two researchers independently. The criteria for quality assessment were piloted and further modified according to the results from the pilot study. Constant feedback/input was provided by an expert in cases where the researchers could not reach a common point of agreement. These aforementioned actions mitigated the risk of missing any relevant study. The data extraction from the relevant studies was done by one researcher, which was then rechecked by the other researcher. After the pilot data extraction, the issues found during data extraction were discussed, and after carefully refining the criteria, the researchers were able to complete the data extraction process. The whole data extraction was carried out manually, thus improving the validity.

VI. Relevant Key Findings

Every single relevant study was read in full to extract sufficient qualitative and quantitative data to further summarize results in Table IV.

All the relevant studies had a theme in relation to how a particular problem was dealt with by blockchain technology. The focus of each paper is also recorded below in Table IV.

TABLE IV
Key Findings and Themes of Primary Studies

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[15]	Nachiket Tapas *et al.*	An authorization and delegation model for the IoT cloud based on blockchain technology.	Ethereum	Smart City
[16]	Guohua Gan *et al.*	A generalized data structure of access control token, explaining equivalence, split, merge & verification algorithms of access control token, thereby providing the system architecture for token-based access control.	Hyperledger Fabric	Digital currency, shopping vouchers, electronic tickets, electronic in- voices, And electronic cards.
[17]	Mohsin Ur Rehman *et al.*	A blockchain-based access control framework that allows manageability and auditability for DOSNs to define privacy policies.	Ethereum	Social Networks
[18] (BACS- IoD)	Basudeb Bera *et al.*	A blockchain-based access control scheme for IoD environment allowing secure communication between the Ground Server Station and drones.	Generic	Internet of Drones
[19]	Richa Gupta *et al.*	Blockchain-based framework utilizing fair access through dynamic access control to access any specific resource in the blockchain network.	Generic	—-
[20] (fabric-iot)	Han Liu *et al.*	A hyperledger fabric blockchain framework as an access control system in IoT based on attribute-based access control (ABAC).	Hyperledger Fabric	IoT
[21]	Jin Sun *et al.*	A ciphertext policy attribute-based encryption system that utilizes blockchain technology and IPFS storage environment for electronic medical records.	Generic	Electronic Medical Records
[22] (FADB)	Hui Li *et al.*	A blockchain and ciphertext-based attribute encryption (CP-ABE) leveraged fine-grained access control scheme for VANET data.	Ethereum	Cloud Servers
[23] (BDSS-FA)	Hong Xu *et al.*	A blockchain-based fine-grained access control (BSDS-FA) in the internet of things environment that allows secure data sharing.	Hyperledger fabric	IoT

TABLE IV
Key Findings and Themes of Primary Studies *(Cont inued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[24] (BloCyNfo-Share)	Shahriar Badsha *et al.*	A blockchain-supported fine-grained access control system that leverages proxy re-encryption and attribute-based encryption to allow privacy preserving cybersecurity information sharing by delegating the limited access to its cybersecurity information.	Ethereum	An Organization
[25]	Jehangir Arshad *et al.*	A private blockchain-based secure access control for monitoring different climatic parameters in agricultural fields.	Hyperleder Fabric	Smart Homes
[26] (BacCPSS)	Liang Tan *et al.*	A privacy-preserving blockchain-based access control scheme for big data in Cyber-Physical-Social System (CPSS).	EOS	Cloud Environment
[27] (AuthPrivacyC-Chaaiixni)	Caixia Yang *et al.*	A privacy protected blockchain-based access control framework in cloud towards solving the problem of security and privacy.	EOS	Cloud Environment
[28]	Ting Cai *et al.*	Blockchain-assisted secure authentication system and fine-grained access control for Social Linked Data (SOLID).	Hyperledger Fabric	Solid Ecosystem
[29]	Yan Zhang *et al.*	Blockchain-assisted attributed-based collaborative access control scheme for providing decentralized, flexible, and fine-grained authorization for IoT devices and providing resistance against possible attempts of unauthorized access on IoT device resources.	Hyperledger Fabric	IoT
[30]	Gabriel Nyame *et al.*	Blockchain smart contract driven role-based access control scheme for maintaining transparency and resource immutability in knowledge management systems.	Ethereum	Knowledge Management Systems
[31]	Tanzeela Sultana *et al.*	Smart contract-driven access policy enforcement to address the issues of trust and authentication for access control in IoT networks.	Ethereum	IoT
[32] (Cap-BAC)	Yuta Nakamura *et al.*	An Ethereum smart contract-driven capability-based access control scheme for IoT that is decentralized and trustworthy	Ethereum	IoT
[33]	Afnan Alniamy *et al.*	An attribute-based encryption scheme augmented with Hyperledger composer to provide fine-grained access control for secure data sharing	Hyperledger Composer	Cloud environment
[34] (BACC)	Nasrin Sohrabi *et al.*	Ethereum blockchain augmented with Shamir's secret scheme to provide privacy preserving access control to cloud data.	Ethereum	Cloud Environment
[35] (CBACS- EIoT)	Sourav Saha *et al.*	A blockchain-enabled access control scheme where mutual authentication between the entities take place in the internet of things environment	Generic	IoT

TABLE IV
Key Findings and Themes of Primary Studies *(Continued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[36]	Imen Riabi *et al.*	A smart contract leveraged blockchain-driven trustworthy and distributed access control solution for IoT.	Ethereum	Real Vehicular Environment
[37]	Sheng Ding *et al.*	A blockchain-driven attribute-based access control scheme for simplified access management in IoT systems.	Hyperledger Fabric	Internet of Things
[38]	MD Azharul Islam *et al.*	Leveraging permissioned blockchain smart contracts and distributed consensus for Attribute Based Access Control (ABAC) to enable a distributed access control for IoT	Hyperledger Fabric	Medical Emergency Service
[39] (CP-ABE)	Shangping Wang *et al.*	A ciphertext-policy attribute-based encryption (CP-ABE) and Ethereum blockchain-driven access control framework for secure cloud storage.	Ethereum	Cloud Environment Service
[40]	Peng Wang *et al.*	A blockchain technology-based distributive attribute-based access control framework (ADAC) for lightweight & open IoT devices.	Ethereum	IoT
[41]	Shadan Ghaffaripour *et al.*	A blockchain technology and Hierarchical Attribute-Based Encryption (HABE) leveraged access control mechanism for medical data management systems that allows multi-user data-sharing.	Hyperledger fabric	Medical Data Management Systems
[42]	Chao Wang *et al.*	A blockchain-based privacy preserving and data sharing scheme to effectively target the problem of single point of trust in the traditional data auditing service model.	Hyperledger fabric	Cloud Storage
[43]	Dwiyan Rezkia Putra *et al.*	Blockchain and smart contract-driven access control mechanism and architecture for IoT	Ethereum	IoT
[44] (SRBAC)	Fariza Sabrina *et al.*	A smart contract and blockchain-driven access control (SRBAC) model that is based on structural relationships for access rights delegation of resources to users while keeping in view the control of a user in an IoT scenario like smart city.	Generic	Smart City
[45]	Shuang Sun et al	A decentralized blockchain-based secure fine-grained access control for IoT system.	EOS	IoT
[46] (DAcc)	Issac Markus *et al.*	A novel decentralized ledger-based access control system utilizing cryptography for privacy and end user verifiability for compromised node detection in decentralized ledger.	Hyperledger Fabric	Enterprise Applications.
[47] (DCACI)	Sandeep Kiran Pinjala *et al.*	A decentralized capability-based access control framework using IOTA's Masked Authentication Messaging (MAM) for enabling privacy and integrity of the capability tokens.	IOTA	Smart City

TABLE IV
Key Findings and Themes of Primary Studies *(Cont inued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[48]	Leepakshi Bindra *et al.*	Blockchain smart contracts-driven methodology to delegate fine-grained permissions in decentralized fashion.	Ethereum	Smart Building
[49] (DACBBD)	Oussama Mounnan *et al.*	Blockchain-driven access control infrastructure for big data to publish the policies deployed in smart contracts.	Generic	Big Data
[50]	Sophie Drame` Maigne` *et al.*	A blockchain technology-based distributed attribute-based access control mechanism that dynamically manages multi-endorsed attributes and trust anchors	Generic	IoT
[51] (EACMS)	AHMED RAZA RAJPUT *et al.*	An emergency access control management system (EACMS) based on Hyperledger fabric and Hyperledger compose	Hyperledger Fabric	Healthcare Services
[52] (BDKMA)	Mingxin Ma *et al.*	Blockchain technology leveraged decentralized, fine-grained, auditable, highly scalable, and extensible hierarchical access control that allows privacy-preserving principles in IoT.	Generic	IoT
[53] (RBAC- HDE)	Raifa Akkaoui *et al.*	A blockchain-based immutable and decentralized role-based access control system to facilitate secure data exchange for healthcare	Ethereum	Healthcare
[54]	Mirei Yutaka *et al.*	An Ethereum smart contract-driven attribute-based access control (ABAC) framework for IoT systems.	Ethereum	IoT
[55] (BCON)	Gauhar Ali *et al.*	A blockchain-based fair, verifiable and decentralized access control for conflict-of-interest domains	Generic	Wireless Access control, cloud environment, IoT
[56] (BACI)	Gauhar Ali *et al.*	A novel decentralized architecture for event and query base permission delegation and access control in IoT application.	Generic	IoT
[57] (SBAC)	Qiuyun Lyu *et al.*	A secure blockchain-based access control framework that allows sharing, auditing and revocation in a secure way.	Ethereum	Information Centric Networks
[58]	Yuyang Zhou *et al.*	A blockchain-driven identity-based encryption, signcryption and signature scheme suitable for smart grids.	JPBC library	Smart Grids
[59]	Lei Xu *et al.*	A novel blockchain -assisted access control scheme leveraging decentralized feature of blockchain to control access-related operations and ring signature scheme to protect user privacy	Hyperledger Fabric	Enterprise Block- chain Appli- cations
[60]	Santiago Figueroa *et al.*	Blockchain-driven access control mechanism for addressing security and safety risks in healthcare applications.	Ethereum	RFID- based Health- care Applications

TABLE IV
Key Findings and Themes of Primary Studies *(Cont inued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[61]	Yongjun Ren *et al.*	Blockchain-based identity management augmented with access control mechanism to provide authentication, auditability, and confidentiality for resource- constrained edge devices.	Ethereum	Industrial IoT
[62]	Oliver Stengele *et al.*	Ethereum smart contract driven access control mechanism for protecting integrity of binaries.	Ethereum	Application Binaries
[63]	Mayra Samaniego *et al.*	Ethereum blockchain-driven access control for data management in the field of plant phenotyping.	Ethereum	Plant Phenotyping
[64]	YongJoo Lee *et al.*	Blockchain-driven role-based access control mechanism for anonymous user authentication.	Ethereum	Generic
[65]	Thein Than Thwan *et al.*	A blockchain-backed provably secure, privacy preserving and tamper resistant personal health record model that enables flexible and fine-grained access control	Hyperledger Fabric	Personal Health Record System
[66]	Ilya Sukhodol-skiy *et al.*	A Blockchain based access control scheme providing key generation, revocation or change, access policy assignment and access request.	Ethereum	Cloud Environment
[67]	Shangping Wang *et al.*	A decentralized fine-grained access control system based on Interplanetary File System (IPFS), Ethereum blockchain technology and ABE technology that allows data storage and sharing for decentralized storage systems.	Ethereum	Decentralized Storage Systems
[68]	Xiaobin Tan *et al.*	A Blockchain-combined access control mechanism where XOR-based encoding/decoding is utilized for faster realization of encryption and decryption in Information Centric Networking (ICN).	Generic	Information Centric Net- works
[69] (BLENDCAC)	Rong hua Xu *et al.*	A robust blockchain smart contract-driven identity-based capability token management scheme for registration, propagation and revocation of the access authorization.	Ethereum	IoT net- works
[70]	Uchi Ugobame Uchibeke *et al.*	A blockchain-based access control ecosystem providing effective access control authority to asset owners and protection against data breaches.	Hyperledger Fabric	Cloud Computing Environments
[71]	Damiano Di Francesco Maesa *et al.*	Blockchain smart contract leveraged new design approach for access control services.	Ethereum	Cloud Services
[72]	Harsha S. Gardiyawasam Pussewalage *et al.*	A Blockchai steered attribute-based access control scheme that offers controlled access delegation capabilities in a multi-domain e-health environment.	steered attribute	Health care System

TABLE IV
Key Findings and Themes of Primary Studies *(Continued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[73] (GAA-FQ)	Xiaoshuai Zhang *et al.*	A blockchain-oriented access authorisation scheme with granular access control, offering flexible data queries for secure EMR information management.	Generic	Electronic Medical Records
[74] (acl-IPFS)	Mathis Steichen *et al.*	An Ethereum smart contract-driven modified InterPlanetary Filesystem (IPFS) to provide access-controlled file sharing	Ethereum	KYC, IPFS and moving data off chain
[75] (CapChain)	Tam Le *et al.*	A blockchain-based privacy preserving access control framework that allows sharing and delegation of access rights of users in IoT devices.	Monero	IoT
[76]	DongYeop Hwang *et al.*	A blockchain-leveraged access control scheme that is dynamic in nature to solve the problems of the existing access control methods effectively for direct data communication among devices and to cope with the ever-changing environment of IoT.	Generic	IoT
[77] (BBACS)	Xiaoshuai Zhang *et al.*	A blockchain-based access control solution for exchanging Electronic Medical Records (EMRs) that encompasses an access model and an access scheme.	Generic	Electronic Medical Records
[78] (DAM- Chain)	Yan Zhu *et al.*	A new digital asset management platform based on distribution ABAC model and the blockchain technology which provides Transaction-based Access Control (TBAC).	Generic	Global Internet Economy
[79]	Sara Rouhani *et al.*	A Hyperledger Fabric and Hyperledger Composer-based access control application to control access to physical spaces.	Hyperledger Fabric	Access Permissions on Physical Spaces
[80] (RBAC-SC)	Jason Paul Cruz *et al.*	A smart contract-driven RBAC that makes use of Ethereum's smart contract technology to realize a trans-organizational utilization of roles	Ethereum	An Organization
[81]	Yuanyu Zhang et al	A smart contract-based framework consisting of multiple contracts for access control to achieve distributed and trustworthy access control for IoT systems.	Ethereum	IoT
[82] (TBAC)	Yan Zhu *et al.*	A blockchain and attribute-based access control (ABAC) backed new Transaction-based Access Control (TBAC) platform.	Generic	Large Scale Organization
[83] (Ancile)	Gaby G. Dagher *et al.*	A blockchain-based privacy preserving framework for secure, interoperable, and efficient access to medical records by several entities like patients, providers and third parties.	Ethereum	Electronic Health Records

TABLE IV
Key Findings and Themes of Primary Studies *(Continued)*

Relevant Primary Study	Authors	Key Finding	Blockchain Platform	Primary Application Domain
[84] (BSeIn)	Chao Lin *et al.*	A blockchain-based secure mutual authentication system to enforce fine-grained access control policies.	Bitcoin like	Industry 4.0 systems
[85]	Chethana Dukkipati *et al.*	A blockchain-based access control for critical IoT resources.	Custom	IoT
[86]	Damiano Di Francesco Maesa *et al.*	Leveraging blockchain technology to enforce, manage and create access control policies	Bitcoin	An Organization
[87] (ControlChain)	Otto Julio Ahlert Pinno *et al.*	A scalable, user-friendly, user transparent, fully decentralized and fault tolerant blockchain based architecture for IoT access authorizations.	Generic	IoT
[88]	Mayssa JEMEL *et al.*	Blockchain-verified decentralized access control mechanism for user legitimacy and added temporal dimension to file sharing using CP-ABE.	Generic	Cloud Storage
[89] (FairAccess)	Aafaf Ouaddah *et al.*	A blockchain-based access control framework that provides fully decentralized, pseudonymous and privacy preserving authorization management for IoT.	Customized Local Blockchain	IoT
[90] (TrustAccess)	Sheng Gao *et al.*	A blockchain-based privacy preserving trustworthy secure ciphertext-policy and attribute hiding access control scheme to achieve trustworthy access.	Generic	Distributed Local Storage

A further grouping of themes was done into a broader context to allow a sim- plified classification of relevant study themes. Studies focused on a variety of application domains. Studies that encompassed cloud services, cloud storage and cloud environment were grouped together. Under the Healthcare category, all the sub-domains that included applications like electronic health records, medical device management systems, electronic healthcare systems, medical emergency services and healthcare services were grouped into a single category. A major category was IoT, which included sub-domains like internet of drones, smart city, smart grids, industrial IoT, smart homes and smart buildings. Fig. 3 shows the percentages of the different themes of the 76 relevant studies which passed the quality assessment. The themes identified in the relevant studies highlight that (38.96%) of relevant studies focused on the IoT application domain. Healthcare and cloud are the second most popular themes, with a percentage of 15.58%. The other application domains that encompass the remaining relevant studies involved application domains like networks (3.90%), knowledge management systems (1.30%), organizational value (5.19%), storage (3.90%), enterprise applications (2.60%), application binaries (1.30%), plant phenotyping (1.30%), file sharing (1.30%), big data (1.30%), digital currency (1.30%), industry 4.0 systems (1.30%), solid ecosystem (1.30%), global internet economy (1.30%) and other generic applications (2.60%). We provided a taxonomical view of the application domains in Fig. 4.

V. Research Themes and Their Discussion

After the relevant literature was collected and relevant studies read in full, it was important to identify the research themes that were to be addressed in this study and discuss them in detail. We provide the research themes in Table V.

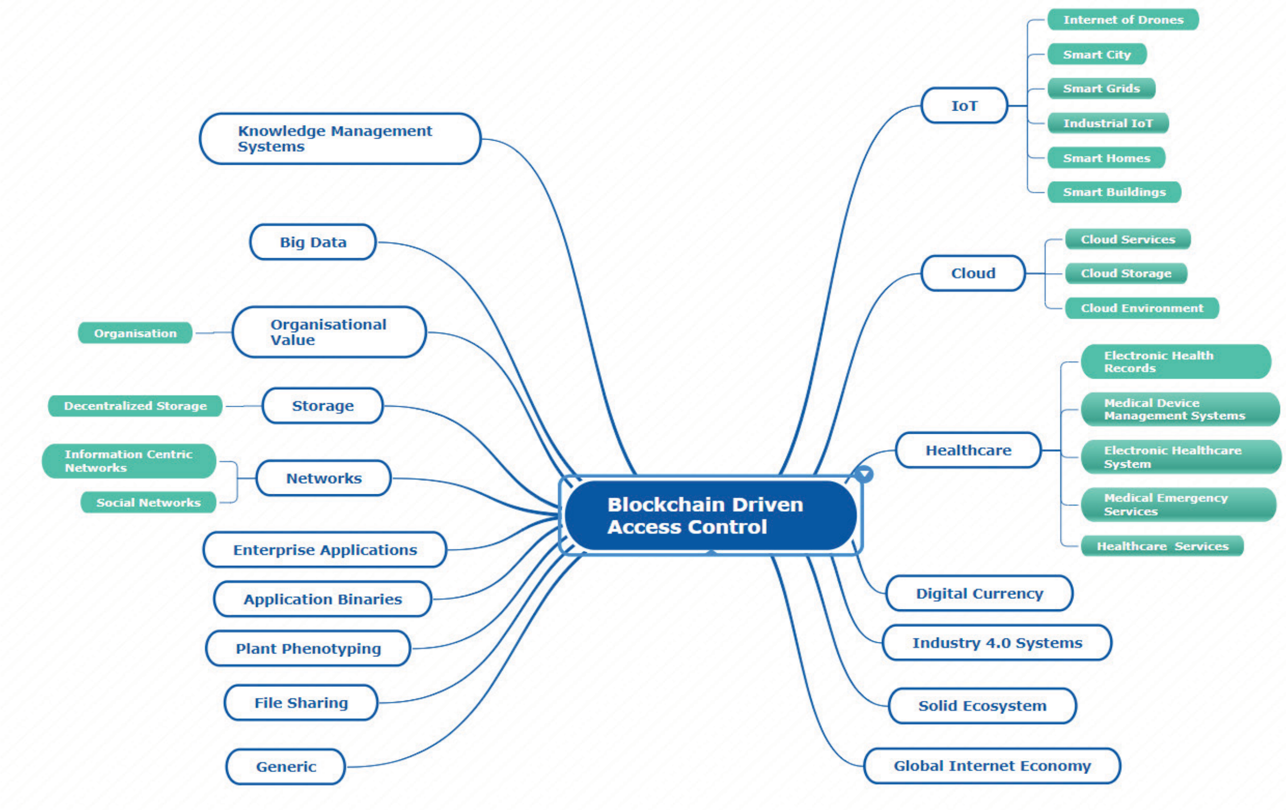

Fig. 3 Blockchain Access Control Application Domains.

TABLE V
Research Questions and Their Significance

Research Questions	Significance/Relevance
RQ1: How have blockchain-driven access control systems shown dominance over traditional access control systems?	The inherent properties of blockchain make it an ideal choice to be used in place of traditional access control systems. The underlying features of blockchain allow multiple degrees of freedom which were missing in traditional access control systems. Blockchain technology reinforces traditional access control systems. This will help in understanding how blockchain-based access control systems are gaining prominence over traditional access control systems.
RQ2: What were the shortcomings with traditional access control systems that were rectified by blockchain-driven access control systems?	There are several remaining issues in traditional access control systems which have been affecting the systems, despite efforts being made to overcome them. Some of the issues were addressed by blockchain-based access control systems. This will help in understanding the issues targeted and then resolved by blockchain technology and identify the issues that are still to be targeted in the research community.
RQ3: What are the various application domains covered by blockchain-driven access control systems?	The applicability of traditional access control systems is specific to a set of application domains. However, a broad spectrum of applications is covered by blockchain-based access control systems. This research question will look into all the application domains that are covered by blockchain access control systems.

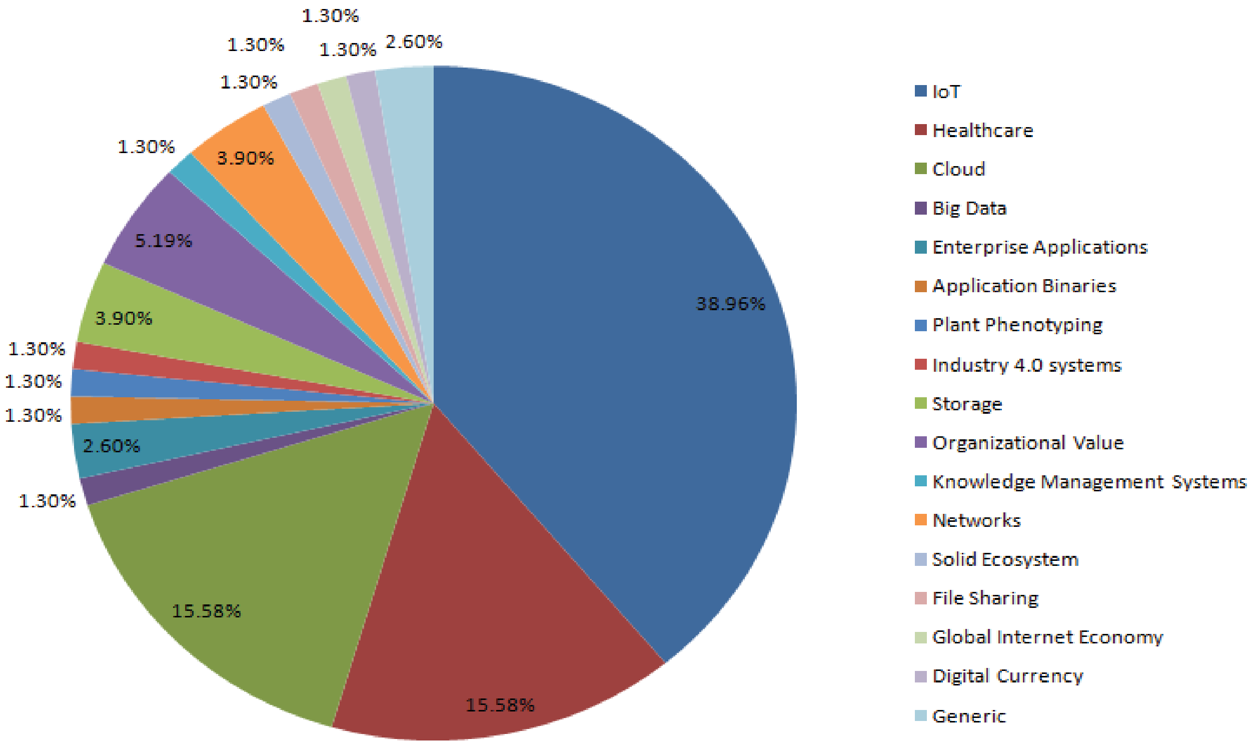

Fig. 4 Pie chart depicting percentage distribution of application domains.

The initial keyword searches suggest that there are an appreciably substantial amount of papers related to blockchain-driven access control systems, and the field is still booming and ever developing. The relevant studies cover a wide range of applications. An appreciable amount of related primary studies provide experimental evidence of their practicality, and a sizeable amount of studies approach concepts that are theoretical in nature. The relevant primary studies have displayed innovative ways to solve the persisting problems like single point of failure, security, and privacy, etc. And in relation to that, they have also provided experimental evidence to support their claims. The solutions either rely on intermingling of existing technologies with the blockchain technology or on a combination of various technologies to solve the underlying problems. In Table VI, we present persisting problems and different technologies used to solve them. Blockchain technology has shown dominance over the traditional techniques that were employed prior to the advent of blockchain technology. Among the proposed access control systems involving the use of blockchain technology, a substantial amount of proposals have utilized Ethereum as the underlying blockchain platform to conduct their experimentation, testing, prototyping and development, which shows promising results to be deployed in practice.

The reason for the wide adoption of Ethereum and hyperledger fabric as an underlying platform has various evident reasons. Ethereum comes with a flexible language solidity which in essence is very much similar to that of Javascript and Python and also allows customisable programming of smart contracts, which gives a programmer the freedom to devise solutions based on the need in perspective. It provides a useful and effective testbed for experimentation. Hyperledger fabric, on the other hand, allows features like permissioned membership of nodes, high degree of privacy, and enhanced and modular architecture providing support for additional plug-ins.

The consensus mechanisms are an important problem to be dealt with, since the wide adoption of IoT suggests use of devices that are lightweight in nature and thereby the underlying consensus mechanisms that are suitable for the resource constrained nature of IoT. However, the current consensus mechanisms like proof-of-work, which are adopted by Ethereum or Bitcoin, can prove to be pernicious to lightweight infrastructures.

The wide adoption of blockchain technology comes from its democratic nature and the inherent properties it offers like decentralization, robustness, strength, trustlessness and many more. The more entities or nodes participating in a blockchain suggests a better regulation mechanism, which in turn supports the better need for trust of individual nodes and thus improves reliability and blockchain security.

We categorized various key features of the studies to provide a comprehensive discussion based on those selected key features. We present the key problems targeted by relevant studies along with the corresponding solution they suggested for those problems in Table VI.

We start a comprehensive discussion to research questions, in light of the topic in focus. We have carefully examined the studies and extracted the relevant data for a strong and valuable discussion.

A. RQ1: How have blockchain-driven access control systems shown dominance over traditional access control systems?

Blockchain inherently offers various advantages over traditional systems. However, blockchain itself does not offer something different, for issues discussed in this review. They simply just provide a better way for existing efforts to be used in accordance to overcome the persisting issues. Blockchain utilizes encryption mechanisms, signature and lightweight algorithms to provide security, enable privacy and for authentication purposes as well. A substantial amount of studies utilize the existing technologies and further improve them by intermingling with blockchain technology. It is evident from the fact that most traditional systems relied on a single trusted authority, thus leaving the system vulnerable to many sorts of attacks and widening the window of opportunity for an attacker to focus on an individual target to commit DoS, DDoS, inject malicious content and many more. Incorporating mechanisms to ensure security in traditional mechanisms brought additional overheads. Likewise, privacy goes hand in hand with security and is an important feature in any modern-day system providing services on a large scale or in scenarios where access is specific to certain entities within an environment.

This is where the blockchain technology has a huge role to play and offers an upper- hand over the existing systems. We know for a fact that blockchain in a true sense is decentralized, thereby not requiring trust or authority of an individual member of a network or a group. Trust is eliminated in a sense that each participating node/member has a complete copy of all the past information available, and only after achieving consensus by a majority in a network will more data be added to the chain of existing information.

Based on the studies focused mostly on bolstering existing efforts with blockchain technology explicitly, we discuss in brief how blockchain was employed to improve the issues in existing access control systems.

Single Point of Failure – The single point of failure was addressed by some relevant studies by leveraging blockchain technology on top of existing technologies [67, 37, 21, 57, 32].

Security – The issue of security was targeted by many studies. The technologies with which the blockchain was intertwined were capability-based access control, at- tribute-based access control, emergence-based access control and others [27, 40, 47, 57, 82, 51, 33].

Privacy – Privacy is not inherently provided by the blockchain technology. So, some technologies were used in essence to help with privacy. This was guaranteed by leveraging blockchain with technologies like proxy re-encryption, hierarchical at- tribute-based encryption, capability-based access control and many more [21, 41, 24, 47, 22, 57, 33].

Authentication – The feature of authentication was focused on by a limited number of studies utilizing smart contracts and role-based access control mostly [61].

TABLE VI
ISSUES AND THEIR CORRESPONDING SOLUTIONS

Issues	How is the issue addressed	Relevant Studies
Single Point of Failure	Distributed Access Control, IPFS with Blockchain, Attribute based access control with blockchain, Smart Contracts with capability based access control, Decentralized blockchain based data integrity and privacy protection mechanism, Blockchain & attribute based access control, IPFS, Blockchain with heirarchical access control, Hidden policy CP-ABE, Blockchain based access control, Blockchain with Shamir's Secret Sharing Scheme	[15, 21, 22, 30] [31, 49, 55, 59] [65, 68, 69, 74] [32, 34]
Security	Encryption with AES, Signature and Signcryption algorithm, Blockchain with distributed based access control, Blockchain based decentralized access control management, Blockchain with capability based access control, Blockchain with capability based access control, Blockchain driven access control, Blockchain and CP-ABE, Blockchain with attribute based access control and cryptographic technology, Blockchain smart contracts, Blockchain and emergency based access control	[16, 23, 27, 32] [33, 42, 45, 47] [57, 63, 67, 71] [72, 74, 51, 58] [35, 60]
Privacy	Encryption with AES, Lightweight Symmetric Encryption algorithm, Encryption, IPFS with Blockchain, Signature and Signcryption algorithm, Key policy hierarchical attribute based encryption, Hierarchical attribute based encryption, Decentralized blockchain based privacy protection scheme, Blockchain based decentralized security system, Blockchain based fine grained access control, Attribute based Proxy re-encryption, Blockchain with capability based access control, Blockchain driven access control, Blockchain and CP-ABE, Blockchain and Heirarchical based access control, Hidden policy CP-ABE, Blockchain Smart contracts, Online Social Networks using blockchain, Blockchain with attribute based access control, Blockchain with Shamir's Secret Sharing Scheme	[16, 18, 20, 21] [23, 28, 29, 31] [32, 41, 42, 43] [45, 47, 57, 59] [65, 67, 70, 72] [74, 59, 89, 33] [34]
Key Escrow	Incentive and Penalty based consensus mechanism for consortium blockchain	[19]
Critical Access control	Blockchain Smart contracts based access control, Blockchain & Attribute based access control	[62, 66]
Management, Authorization & Delegation of Access rights	Blockchain Smart contracts, Blockchain Smart contracts and access control mechanisms, Blockchain and Attribute based access control, Blockchain based fine grained access control and attribute based Proxy Re-encryption, Blockchain smart contracts and role based access control	[34, 35, 36, 37] [73, 22, 41, 46] [61]
Key Abuse	IPFS with Blockchain& ABE, Blockchain with XOR coding	[21, 26]
Centralization of Access Control	Creation of access control policies & access control decision based on consensus mechanism, Decentralized & Distribution of access control, Blockchain and Smart contract inspired CBAC, Blockchain based access control	[24, 25, 30, 68]
Efficient implementation of Access Control	Blockchain based decentralized system, Blockchain and Role based access control	[38, 60, 61]
Authentication	Smart contract driven access control, Blockchain driven access control, Blockchain driven role based access control	[31, 61, 64]

B. RQ2: What were the shortcomings with traditional access control systems that were rectified by blockchain driven access control systems?

In our research, we tried to accumulate results on the basis of persisting issues with traditional access control systems and the way relevant studies targeted those issues. The categorization of results suggests the following:

Single point of failure – The majority of relevant studies targeted this issue, which is inherent in centralized systems since traditional access control systems are all centralized in nature. The relevant studies used various technologies to tackle this problem, such as distributed access control, interplanetary file system (IPFS), attribute-based access control with blockchain technology, smart contract enabled capability-based access control, Shamir's secret sharing scheme and many more.

Security – Security is another major feature that any access control system should possess. However, over time there have been advancements in attack vectors, attack tools and infrastructure. However, blockchain technology offers security as an intrinsic property with whatever technology it is intermingled with.

Although, various technologies like encryption mechanisms are used to achieve the highest levels of security in a system. The technologies that are mainly used by relevant studies are encryption mechanisms, signature algorithms, capability-based access control, blockchain-driven attribute-based access control, and smart contracts, emergence-based access control, etc.

Privacy– Privacy is not inherently a part of blockchain technology, which raises serious concerns over data breaches by analyzing the hashes of the transactions happening over the blockchain network. However, over the years there have been attempts to address this issue and research in this direction is leaving no stone un-turned to further strengthen this area. We found an appreciable number of relevant studies that focused on solving the issue of privacy up to a certain extent. However, further research is needed until a better and more viable solution is found.

This issue was addressed by leveraging lightweight symmetric encryption algorithms, signature algorithms, proxy re-encryption, smart contracts, blockchain-driven fine grained access control and many other technologies to address the issue of privacy while enabling access control in various application areas.

Management, Authorization and Delegation of Access rights

Another important aspect in access control systems is the delegation of access rights and their management and authorization. It is important to emphasize that access to a specific resource by authorized entities is of central importance in access control systems. Although this issue is usually supposed to be targeted by every access control system, there are relevant studies that have considered this issue as a point of focus.

The technologies that were mostly used to target this issue are smart contracts, blockchain-driven access control, proxy re-encryption and role-based access control.

Key Escrow – In our review, a relevant study used incentive and a penalty-based consensus mechanism to address the problem of key escrow.

Key Abuse – A few of the studies have targeted the issue of key abuse by taking advantage of interplanetary file system with attribute based encryption and blockchain technology with XOR coding.

Authentication – Authentication is achieved by some of the primary studies by leveraging smart contract-based access control and blockchain-driven role based access control.

C. RQ3: What are the various application domains covered by Blockchain-driven access control systems?

It is important to emphasize the fact that the review intends to focus on a broader context of applications of blockchain in modern access control systems. However, there are still some application domains that are yet to be addressed by blockchain driven access control systems.

With all this in mind, during the process of selection of primary studies, the researchers noted various studies targeting various issues in their own right. However, most of the studies took the opportunity to solve issues like single point of failure, security and privacy issues, etc. The prioritization of application domains suggests the proposals mostly target IoT. The clear reason for this is the augmentation of IoT in a variety of domains and its rapid increase in demand.

The relevant primary studies focus on certain application domains, and the application domains are believed to increase as time progresses.

IoT – The majority of the relevant primary studies are specific to the IoT domain, and the evident reasons have been discussed above. An authorization, delegation model and access control for IoT systems is based on blockchain technology targeting various sub-domains [15, 18, 23, 25, 31, 32, 35].

Cloud – The primary studies have shown various studies specifically targeting cloud. The subdomains of the studies are strictly under one blanket of cloud, thus the categorization of studies is based on their corresponding relevance [22, 26, 27, 33, 34, 39].

Healthcare – Healthcare encompasses studies that were relevant to the healthcare sector and includes various subdomains like electronic medical records, medical emergency services, medical data management systems and many more [21, 38, 41, 51, 53].

Organizational Value, Storage, Networks – Several studies have applications that are different from the usual and evident application domains. Some studies have shown applications that have organizational value [24, 80, 82, 86].

Several studies target the storage area as their primary application domain. In our research, we found some studies targeting this area [90, 67].

Networking in the modern age is an inherent part of everything that happens either digitally or non-digitally. However, networks play a vital role in our modern-day era of sophisticated and highly complex systems. We found some studies targeting involvement with network application domains as well [68, 17, 57].

Big Data, Application Binaries, Plant Phenotyping and Industry 4.0 Systems, Enterprise applications – The other application domains that the studies targeted have provided a direction to be followed to further the research in these application areas. The areas that were focused on were big data [49], application binaries [62], plant phenotyping [63], industry 4.0 systems [84], enterprise applications [46, 59], solid ecosystem [28], file sharing [74], digital currency [16], knowledge management systems [30], global internet economy [78] and some generic applications as well.

VI. Taxonomy of Blockchain-Driven Access Control Systems

With the idea of classifying access control systems on a broader level and context, we chose certain parameters based on their importance and relatability to our study in particular. We do understand the fact that the parameters can be added based on the relevance and after carefully examining the topic of study. For our topic, we chose the parameters that we found relevant to our study. We examined the blockchain platforms utilized by the access control systems along with the specific blockchain properties utilized by each system. A pie chart depicting the percentage of blockchain platforms used by access control systems is presented in Fig. 5.

We also presented the testbeds/tools used by each study, based on whether the particular study provided implementation or not. Based upon the type of solution presented by each access control system, we categorized the solutions in Table VIII and present the whole taxonomy in Table VII.

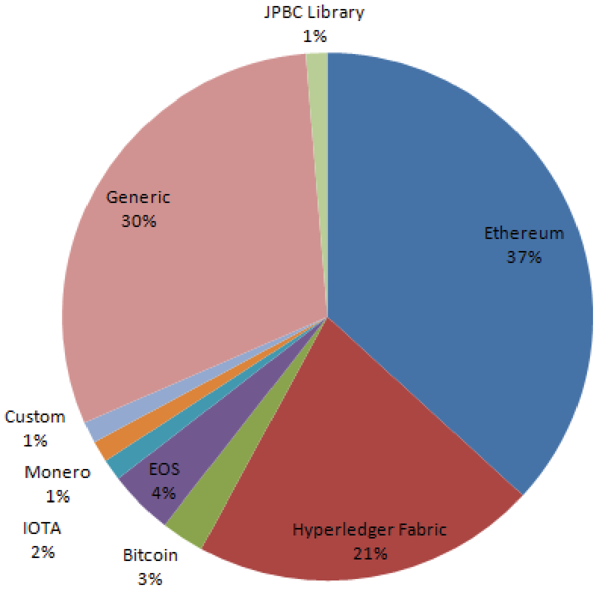

Fig. 5 Pie chart depicting percentage distribution of blockchain platforms.

TABLE VII
A Taxonomy of Blockchain-Driven Access Control Systems

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
Imen Riabi *et al.* [36]	Ethereum	Yes	Smart Contracts	Truffle, Go-Ethereum, Geth
AuthPrivacyChain [27]	EOS	Yes	Decentralization & Tamper-Resistance	Kylin & Jungle test
Ting Cai *et al.* [28]	Hyperledger Fabric	No	Secure Authentication	Kylin test chain
BacCPSS [26]	EOS	Yes	Decentralization	Kylin test chain
Yuyang Zhou *et al.* [58]	JPBC Library	Yes	Decentralization	Eclipse, Neon.1a Release (4.6.1)
Ilya Sukhodolskiy *et al.* [66]	Ethereum	Yes	Decentralization	Ethereum Virtual Machine
Shangping Wang *et al.* [67]	Ethereum	Yes	Decentralization & Distributiveness	Rinkeby
Sheng Ding *et al.* [37]	Hyperledger Fabric	Yes	Distributiveness	Ubuntu Linux 16.04LTS desktop, AVISPA tool
Jehangir Arshad *et al.* [25]	Custom	Yes	Immutability	Linux System
MD Azharul Islam *et al.* [38]	Hyperledger Fabric	Yes	Smart Contracts	MEMSICs TelosB Mote TPR2420CA devices
Shangping Wang *et al.* [39]	Ethereum	Yes	Decentralization	Ethereum Geth Client
Xiaobin Tan *et al.* [68]	Generic	No	Decentralization & Tamper-Resistance	-
ADAC [40]	Ethereum	Yes	Distributiveness & Trustworthiness	Ropsten test network
Shaddan Ghaffaripour *et al.* [41]	Hyperledger Fabric	No	Transparency, Tamper- resistance & Decentralization	-
BBACS [77]	Generic	Yes	Decentralization	MIRACL
BDSS-FA [23]	Hyperledger Fabric	Yes	Traceability	Zookeeper, Kafka
BLENDCAC [69]	Ethereum	Yes	Decentralization & Smart Contracts	Go-Ethereum
Chao Wang *et al.* [42]	Hyperledger Fabric	Yes	Decentralization & Smart Contracts	AWS EC2 cloud host
Uchi Ugobame Uchibeke *et al.* [70]	Hyperledger Fabric	Yes	Smart Contracts	Hyperledger Composer Client API
Dwiyan Rezkia Putra *et al.* [43]	Ethereum	Yes	Smart Contracts & Consensus Mechanisms	Geth, Remix
Damiano Di Francesco Maesa *et al.* [71]	Ethereum	Yes	Smart Contracts	International Educational blockchain academic testnet, Geth
Damiano Di Francesco Maesa *et al.* [86]	Bitcoin	Yes	Distributed Auditability	Bitcoin Network
Harsha S. Gardiyawasam *et al.* [72]	Generic	No	Delegatability & Tamper-Resistance	-
Shuang Sun *et al.* [45]	EOS	Yes	Decentralization	EOS Client
Jin Sun *et al.* [21]	Generic	Yes	Non-tamperable & Traceability	Ubuntu Server 15.4
Mathis Steichen *et al.* [74]	Ethereum	Yes	Immutability	Go ethereum's abigen, S/Kademlia

TABLE VII
A Taxonomy of Blockchain-Driven Access Control Systems *(Continued)*

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
BloCyNfo-Share *et al.* [24]	Ethereum	Yes	Transparency, Tamper-Resistance, Verifiability	Go Ethereum (Geth), cpabe
CapChain [75]	Monero	Yes	Decentralization, Trustlessness & Immutability	ARM Cortex-M0+ MCU, Raspberry Pi Zero W, MSU HPCC network
ControlChain [87]	Generic	No	Decentralization	-
DAcc [46]	Hyperledger Fabric	Yes	Decentralization & Verifiability	Hyperledger Fabric Cryptogen, Cryptoconfig tools
DCACI [47]	IOTA	Yes	Decentralization	Raspberry Pi, Ubuntu 18.04.1 LTS processor
Leepakshi Bindra *et al.* [48]	Generic	Yes	Smart Contracts	Query API, Simulated BACnet API
DACBBD [49]	Generic	No	Transparency & Traceability	-
Mayssa JEMEL *et al.* [88]	Generic	Yes	Decentralized & Verifiability	CP-ABE Toolkit, Multi-chain
DAM-Chain [78]	Generic	No	Verifiability & Traceability	-
Sophie Dram´e- Maign´e *et al.* [50]	Generic	No	Distributiveness, Resilience, & Auditability	-
DongYeop Hwang *et al.* [76]	Generic	No	Distributiveness	-
EACMS [51]	Hyperledger Fabric	Yes	Smart Contracts	Hyperledger Composer
Richa Gupta *et al.* [19]	Generic	No	Smart Contracts & Verifiability	-
Fabric-IoT [20]	Hyperledger Fabric	Yes	Decentralization, Tamper-Resistance & Traceability	Docker, Docker compose, Hyperledger fabric
FADB [22]	Ethereum	Yes	Smart Contracts	Ubuntu 16.04.4 LTS desktop, Ethereum ganache-cli
GAA-FQ [73]	Generic	Yes	Data Integrity	MIRACL, Raspberry Pi 2, Intel i5-4200H Processor
Sara Rouhani *et al.* [79]	Hyperledger Fabric	Yes	Tamper-Resistance	Hyperledger Caliper
BDKMA [52]	Fabric Generic	Yes	Decentralization, Auditability, Extensibility	OMNeT++ 5.4.1, ECIES, Intel Core i5 CPU
RBAC-HDE [53]	Ethereum	Yes	Immutability & Decentralization	Ethereum Remix IDE
RBAC-SC [80]	Ethereum	Yes	Decentralization & Smart Contracts	Ropsten Testnet
Yuanyu Zhang *et al.* [81]	Ethereum	Yes	Distributiveness & Trustworthiness	Macbook Pro, Raspberry Pi 3, Dell Inspiron 3650, Geth Clients
SRBAC [44]	Generic	No	Delegatability & Smart Contracts	-
TBAC [RS68]	Generic	No	Decentralization, Authenticity & Traceability	-

TABLE VII
A Taxonomy of Blockchain-Driven Access Control Systems *(Continued)*

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
GUOHUA GAN *et al.* [16]	Hyperledger Fabric	No	Fault Tolerance & Trustworthiness	Customized test tools
TrustAccess [90]	Generic	Yes	Decentralization & Transparency	Intel (R) Core (TM) i5-8250U CPU
Mirei Yutaka *et al.* [54]	Ethereum	Yes	Smart Contracts, Tamper- ResisЄ tance & Distributiveness	Intel Xeon CPU E5-1620, Geth, Remix IDE
Oliver Stengele *et al.* [62]	Ethereum	Yes	Tamper-Resistance & Verifiability	Remix IDE, Ganache
BACC [34]	Ethereum	No	Smart Contracts & Decentralization	-
Mayra Samaniego *et al.* [63]	Ethereum	Yes	Decentralization & Smart Contracts	Intel(R) Core(TM) i7-6700 CPU
Afnan Alniamy *et al.* [33]	Hyperledger Fabric	Yes	Confidentiality & Integrity	Hyperledger Composer
YongJoo Lee *et al.* [64]	Ethereum	Yes	Trustlessness	Geth, Intel Core i7-4790 CPU
Chethana Dukkipati *et al.* [85]	Generic	Yes	Decentralization, Transparency	-
CapBAC [32]	Ethereum	Yes	Decentralization, Smart Contracts & Verifiability	MacBook Pro, MacBook Air, Two Raspberry Pi's
Gabriel Nyame *et al.* [30]	Ethereum	Yes	Transparency & Immutability	Ropsten, Remix IDE, MetaMask, Intel Core i7 6700HQ CPU
Santiago Figueroa *et al.* [60]	Ethereum	Yes	Decentralization & Smart Contracts	ETH Network Stats, Etherscan Ropsten, Truffle, Infura Dashboard
Tanzeela Sultana *et al.* [31]	Ethereum	Yes	Distributiveness & Smart Contracts	Intel Core i5 CPU
Yan Zhang *et al.* [29]	Hyperledger Fabric	Yes	Authenticity & Reliability	Intel core i7-4510U, Intel Core i5-7200U, three Raspberry Pi 3B+, Hyperledger Caliper
Yongjun Ren *et al.* [61]	Ethereum	Yes	Decentralization & Tamper-Resistance	Intel Core i7, Raspberry Pi 3
Ancile [83]	Ethereum	No	Decentralization & Smart Contracts	-
BACS-IOD [18]	Generic	No	Tamper-Resistance	SPAN for AVISPA, Intel Core i5-4460S, Samsung Galaxy S5
BCON [55]	Generic	No	Decentralized, Fairness, Verifiability & Tamper- Resistance	Spin Model Checker
BSeIn [84]	Generic	Yes	Decentralization, Verifiability & Immutability	JUICE, Intel Core i7-6700 CPU
BACI [56]	Generic	No	Trusted, Verifiability, Decentralized	SPIN model checker
Mohsin Ur Rahman *et al.* [17]	Ethereum	Yes	Decentralization	Rinkeby Ethereum testnet
Nachiket tapas *et al.* [15]	Ethereum	Yes	Immutability, Verifiability & Decentralization	Ganache, Rinkeby

TABLE VII
A Taxonomy of Blockchain-Driven Access Control Systems *(Continued)*

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
SBAC [57]	Ethereum	Yes	Transparency, Smart Contracts & Distributiveness	Intel(R) Core(TM) i5-7200U CPU
Lei Xu *et al.* [59]	Hyperledger Fabric	Yes	Decentralization	Cryptogen and Crypto-config tools
CBACS-EIOT [35]	Generic	Yes	Immutability, Transparency & De-centralization	AVISPA tool, Intel Core i5- 4460S, Samsung Galaxy S5
FairAccess [89]	Bitcoin	Yes	Distributiveness, Transparency & Smart Contracts	Camera module & Raspberry Pi
Thein Than Thwin *et al.* [65]	Hyperledger Fabric	Yes	Tamper-Resistance	Intel Core i7-4510U CPU, Eclipse IDE

TABLE VIII
Underlying Nature of the Proposed Access Control Model

Access Control Solution	Theoretic	Simulation	Prototype
Imen Riabi *et al.* [36]			✓
AuthPrivacyChain [27]			✓
Ting Cai *et al.* [28]		✓	
BacCPSS [26]			✓
Yuyang Zhou *et al.* [58]		✓	
Ilya Sukhodolskiy *et al.* [66]			✓
Shangping Wang *et al.* (2018) [67]		✓	✓
Sheng Ding *et al.* [37]		✓	✓
Jehangir Arshad *et al.* [25]			✓
MD Azharul Islam *et al.* [38]			✓
Shangping Wang *et al.* (2019) [39]		✓	✓
Xiaobin Tan *et al.* [68]	✓		
Peng Wang *et al.* [40]		✓	
Shaddan Ghaffaripour *et al.* [41]	✓		
BBACS [77]		✓	
BDSS-FA [23]		✓	
BLENDCAC [69]		✓	✓
Chao Wang *et al.* [42]			✓
Uchi Ugobame Uchibeke *et al.* [70]			✓
Dwiyan Rezkia Putra *et al.* [43]			✓
Damiano Di Francesco Maesa *et al.* [71]		✓	
Damiano Di Francesco Maesa *et al.* [86]		✓	

TABLE VIII
Underlying Nature of the Proposed Access Control Model *(Cont inued)*

Access Control Solution	**Theoretic**	**Simulation**	**Prototype**
Harsha S. Gardiyawasam Pussewalage *et al.* [72]	✓		
Shuang Sun *et al.* [45]			✓
Jin Sun *et al.* [21]		✓	
Mathis Steichen *et al.* [74]		✓	
BloCyNfo-Share [24]		✓	
CapChain [75]		✓	✓
ControlChain [87]		✓	
DAcc [46]			✓
DCACI [47]			✓
Leepakshi Bindra *et al.* [48]	✓		
DACBBD [49]	✓		
Mayssa JEMEL *et al.* [88]		✓	
DAM-Chain [78]	✓		
Sophie Drame`-Maigne` *et al.* [50]	✓		
DongYeop Hwang *et al.* [76]	✓		
EACMS [51]			✓
Richa Gupta *et al.* [19]	✓		
fabric-iot [20]		✓	✓
FADB [22]		✓	
GAA-FQ [73]		✓	
Sara Rouhani *et al.* [79]		✓	
BDKMA [52]		✓	
RBAC-HDE [53]		✓	
RBAC-SC [80]			✓
Yuanyu Zhang *et al.* [81]		✓	✓
SRBAC [44]	✓		
TBAC [82]	✓		
GUOHUA GAN *et al.* [16]		✓	
TrustAccess [90]		✓	
Mirei Yutaka *et al.* [54]		✓	
Oliver Stengele *et al.* [62]		✓	
BACC [34]	✓		
Mayra Samaniego *et al.* [63]			✓
Afnan Alniamy *et al.* [33]		✓	

TABLE VIII
Underlying Nature of the Proposed Access Control Model *(Continued)*

Access Control Solution	Theoretic	Simulation	Prototype
YongJoo Lee *et al.* [64]		✓	
Chethana Dukkipati *et al.* [85]	✓		
CapBAC [32]		✓	✓
Gabriel Nyame *et al.* [30]			✓
Santiago Figueroa *et al.* [60]		✓	
Tanzeela Sultana *et al.* [31]		✓	
Yan Zhang *et al.* [29]			✓
Yongjun Ren *et al.* [61]			✓
Ancile [83]	✓		
BACS-IOD [18]		✓	✓
BCON [55]		✓	
BSeIn [84]		✓	
BACI [56]	✓		
Mohsin Ur Rahman *et al.* [17]			✓
Nachiket Tapas *et al.* [15]		✓	
SBAC [57]			✓
Lei Xu *et al.* [59]			✓
CBACS-EIOT [35]		✓	
FairAccess [89]			✓
Thein Than Thwan *et al.* [65]	✓		

VII. Conclusion

Access control has proven time and again to be an equally important security feature, like any other in any security system. Although there have been certain flaws with the traditional access control systems, efforts are in place to overcome the issues one after the other. However, after the inception of blockchain, access control systems have started to prepare a different roadmap of upcoming challenges to overcome, particularly after the proliferation of IoT devices around us. This is due to the inherently strong nature of blockchain technology. In this paper, we presented a detailed review of blockchain-driven access control systems. In essence, we presented the key findings from the relevant studies and discussed the research problems in perspective and shed light on them in relevance to the relevant studies. We also presented a taxonomy of blockchain-driven access control systems, to better understand the role of these systems in various application domains. Our findings reveal that Ethereum and Hyper-ledger Fabric were the two most commonly preferred blockchain platforms for developing innovative access control methods. We also observed that most of the access control solutions proposed by the relevant studies aim at addressing the key security requirements of IoT based applications. One of the open research directions in this area is IoT devices, due to the limitation of resources, which has been an obstacle in identifying a general and reliable access control mechanism while keeping account of the required computations, the storage and resources of the devices. Another such direction is the development of these access control solutions/protocols and their feasibility assessment for interoperability. A few other directions include dealing with problems like the single point of failure, heterogeneous nature of devices and many more. As part of future work, we aim to build a lightweight, scalable and reliable access control framework for resource constraint devices. In particular, we aim to a build secure and lightweight consensus mechanism for post-quantum blockchains which will act as building block for developing quantum resistant access control mechanisms.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] R. S. Sandhu and P. Samarati, “Access control: principle and practice,” *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40-48, Sept. 1994, doi: 10.1109/35.312842.

[2] K. Ashton, “That ‘Internet of Things’ Thing,” June 22, 2009. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Bus. Rev.*, Oct. 31, 2008. [Online]. Available: https://www.debr.io/article/21260-bitcoin-a-peer-to-peer-electronic-cash-system

[4] V. Buterin, “Ethereum White Paper,” 2013. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[5] E. Androulaki *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *EuroSys’18: Proc. Thirteen. EuroSys Conf.*, Porto, Portugal, Apr. 23-26, 2018, pp. 1-15, doi: 10.1145/3190508.3190538.

[6] D. Schwartz, N. Youngs, and A. Britto, “The Ripple Protocol Consensus Algorithm,” unpublished.

[7] N. Szabo, “Formalizing and Securing Relationships on Public Networks,” *First Monday*, vol. 2, no. 9, Sept. 1997, doi: 10.5210/fm.v2i9.548

[8] P. Samarati and S. Vimercati, “Access Control: Policies, Models, and Mechanisms,” in *FOSAD 2000*, in Foundation of Security Analysis and Design, R. Focardi and R. Gorrieri, Eds., in Lecture Notes in Computer Science, vol. 2171, Oct. 2001, doi: 10.1007/3-540-45608-2_3.

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology?—A Systematic Review,” *PLoS One*, vol. 11, no. 10, 2016, doi: 10.1371/journal.pone.0163477.

[10] F. Casino, T. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics Inform.*, vol. 36, pp. 55-81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[11] S. Rouhani and R. Deters, “Blockchain based access control systems: State of the art and challenges,” in *WI ’19: IEEE/WIC/ACM Int. Conf. Web. Intell.*, Greece, Oct. 14-17, 2019, pp. 423-428, doi: 10.1145/3350546.3352561.

[12] I. Riabi, H. K. B. Ayed, and L. A. Saidane, “A survey on Blockchain based access control for Internet of Things,” in *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. (IWCMC)*, 2019, pp. 502-507, doi: 10.1109/IWCMC.2019.8766453.

[13] B. A. Kitchenham and S. Charters, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” Sch. Comput. Sci. Math., Keele Univ., UK, Dept. Comput. Sci., Univ. Durham, UK, Rep. EBSE-2007-01, 2007.

[14] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *EASE ’14: Proc. 18th Int. Conf. Eval. Assess. Softw. Eng.*, UK, May 13-14, 2014, pp. 1-10, doi: 10.1145/2601248.2601268.

[15] N. Tapas, F. Longo, G. Merlino, and A. Puliafito, “Experimenting with smart contracts for access control and delegation in IoT,” *Future Gener. Comput. Syst.*, vol. 111, pp. 324-338, Oct. 2020, doi: 10.1016/j.future.2020.04.020.

[16] G. Gan, E. Chen, Z. Zhou, and Y. Zhu, “Token-Based Access Control,” *IEEE Access*, vol. 8, pp. 54189-54199, 2020, doi: 10.1109/ACCESS.2020.2979746.

[17] Mohsin Ur Rahman, B. Guidi, and F. Baiardi, “Blockchain-based access control management for Decentralized Online Social Networks,” *J. Parallel Distrib. Comput.,* vol. 144, pp. 41-54, Oct. 2020, doi: 10.1016/j.jpdc.2020.05.011.

[18] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,” *Comput. Commun.*, vol. 153, pp. 229-249, Mar. 2020, doi: 10.1016/j.comcom.2020.02.011.

[19] R. Gupta, V. K. Shukla, S. S. Rao, S. Anwar, P. Sharma, and R. Bathla, “Enhancing Privacy through “Smart Contract” using Blockchain-based Dynamic Access Control,” in *2020 Int. Conf. Comput. Autom. Knowl. Manag. (ICCAKM)*, UAE, 2020, pp. 338-343, doi: 10.1109/ICCAKM46823.2020.9051521.

[20] H. Liu, D. Han, and D. Li, “Fabric-iot: A Blockchain-Based Access Control System in IoT,” *IEEE Access*, vol. 8, pp. 18207-18218, 2020, doi: 10.1109/ACCESS.2020.2968492.

[21] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS,” *IEEE Access*, vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[22] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, “FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain,” *IEEE Access*, vol. 8, pp. 85190-85203, 2020, doi: 10.1109/ACCESS.2020.2992203.

[23] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, “BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control,” *IEEE Access*, vol. 8, pp. 87552-87561, 2020, doi: 10.1109/ACCESS.2020.2992649.

[24] S. Badsha, I. Vakilinia, and S. Sengupta, “BloCyNfo-Share: Blockchain based Cybersecurity Information Sharing with Fine Grained Access Control,” in *2020 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, USA, 2020, pp. 0317-0323, doi: 10.1109/CCWC47524.2020.9031164.

[25] J. Arshad *et al.*, “A Novel Remote User Authentication Scheme by using Private Blockchain-Based Secure Access Control for Agriculture Monitoring,” in *2020 Int. Conf. Eng. Emerg. Technol. (ICEET)*, Pakistan, 2020, pp. 1-9, doi: 10.1109/ICEET48479.2020.9048218.

[26] L. Tan, N. Shi, C. Yang, and K. Yu, “A Blockchain-Based Access Control Framework for Cyber-Physical-Social System Big Data,” *IEEE Access*, vol. 8, pp. 77215-77226, 2020, doi: 10.1109/ACCESS.2020.2988951.

[27] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, “AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud,” *IEEE Access*, vol. 8, pp. 70604-70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[28] T. Cai, Z. Yang, W. Chen, Z. Zheng, and Y. Yu, “A Blockchain-Assisted Trust Access Authentication System for Solid,” *IEEE Access*, vol. 8, pp. 71605-71616, 2020, doi: 10.1109/ACCESS.2020.2987608.

[29] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, “An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices,” *Electron.*, vol. 9, no. 2, 2020, Art. no. 285, doi: 10.3390/electronics9020285.

[30] G. Nyame, Z. Qin, K. O. Agyekum, and E. B. Sifah, “An ECDSA Approach to Access Control in Knowledge Management Systems Using Blockchain,” *Inf.*, vol. 11, no. 2, 2020, Art. no. 111, doi: 10.3390/info11020111.

[31] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, “Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices,” *Appl. Sci.*, vol. 10, no. 2, 2020, Art. no. 488, doi: 10.3390/app10020488.

[32] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara, “Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things,” *Sens.*, vol. 20, no. 6, 2020, Art. no. 1793, doi: 10.3390/s20061793.

[33] A. Alniamy, and B. D. Taylor, “Attribute-based Access Control of Data Sharing Based on Hyperledger Blockchain,” in *ICBCT '20: Proc. 2020 2nd Int. Conf. Blockchain Technol.*, USA, Mar. 12-14, 2020, pp. 135-139, doi: 10.1145/3390566.3391688.

[34] N. Sohrabi, X. Yi, Z. Tari, and I. Khalil, “BACC: Blockchain-Based Access Control For Cloud Data,” in *ACSW '20: Proc. Australasian Comput. Sci. Week Multiconf.*, Australia, Feb. 4-6, 2020, pp. 1-10, doi: 10.1145/3373017.3373027.

[35] S. Saha, D. Chattaraj, B. Bera, and A. K. Das, “Consortium blockchain-enabled access control mechanism in edge computing based generic Internet of Things environment,” *Trans. Emerging Tel. Tech.*, vol. 32, no. 6, 2021, Art. no. e3995, doi: 10.1002/ett.3995.

[36] I. Riabi, Y. Dhif, H. K. Ben Ayed, and K. Zaatouri, "A Blockchain based access control for IoT," in *2019 15th Int. Wireless Commun. Mob. Comput. Conf. (IWCMC)*, Morocco, 2019, pp. 2086-2091, doi: 10.1109/IWCMC.2019.8766506.

[37] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431-38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[38] M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," in *2019 IEEE Int. Conf. Blockchain (Blockchain)*, USA, 2019, pp. 469-476, doi: 10.1109/Blockchain.2019.00071.

[39] S. Wang, X. Wang, and Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain," *IEEE Access*, vol. 7, pp. 112713-112725, 2019, doi: 10.1109/ACCESS.2019.2929205.

[40] P. Wang, Y. Yue, W. Sun, and J. Liu, "An Attribute-Based Distributed Access Control for Blockchain-enabled IoT," in *2019 Int. Conf. Wireless Mob. Comput. Netw. Commun. (WiMob)*, Spain, 2019, pp. 1-6, doi: 10.1109/WiMOB.2019.8923232.

[41] S. Ghaffaripour and A. Miri, "Application of Blockchain to Patient-Centric Access Control in Medical Data Management Systems," in *2019 IEEE 10th Annu. Inf. Technol. Electron. Mob. Commun. Conf. (IEMCON)*, Canada, 2019, pp. 0190-0196, doi: 10.1109/IEMCON.2019.8936186.

[42] C. Wang, S. Chen, Z. Feng, Y. Jiang, and X. Xue, "Block Chain-Based Data Audit and Access Control Mechanism in Service Collaboration," in *2019 IEEE Int. Conf. Web Serv. (ICWS)*, Italy, 2019, pp. 214-218, doi: 10.1109/ICWS.2019.00044.

[43] D. R. Putra, B. Anggorojati, and A. P. Pratama Hartono, "Blockchain and smart-contract for scalable access control in Internet of Things," in *2019 Int. Conf. ICT Smart Soc. (ICISS)*, Indonesia, 2019, pp. 1-5, doi: 10.1109/ICISS48059.2019.8969807.

[44] F. Sabrina, "Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case," in *2019 IEEE 44th Conf. Local Comput. Netw. (LCN)*, Germany, 2019, pp. 137-140, doi: 10.1109/LCN44214.2019.8990757.

[45] S. Sun, S. Chen, R. Du, W. Li, and D. Qi, "Blockchain Based Fine-Grained and Scalable Access Control for IoT Security and Privacy," in *2019 IEEE Fourth Int. Conf. Data Sci. Cyberspace (DSC)*, China, 2019, pp. 598-603, doi: 10.1109/DSC.2019.00097.

[46] I. Markus, L. Xu, I. Subhod, and N. Nayab, "DAcc: Decentralized Ledger based Access Control for Enterprise Applications," in *2019 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Korea, 2019, pp. 345-351, doi: 10.1109/BLOC.2019.8751479.

[47] S. K. Pinjala and K. M. Sivalingam, "DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things," in *2019 IEEE 5th World Forum Internet Things (WF-IoT)*, Ireland, 2019, pp. 13-18, doi: 10.1109/WF-IoT.2019.8767356.

[48] L. Bindra, C. Lin, E. Stroulia, and O. Ardakanian, "Decentralized Access Control for Smart Buildings Using Metadata and Smart Contracts," in *2019 IEEE/ACM 5th Int. Workshop Softw. Eng. Smart Cyber-Physical Syst. (SEsCPS)*, Canada, 2019, pp. 32-38, doi: 10.1109/SEsCPS.2019.00013.

[49] O. Mounnan, A. A. E. Kalam and L. El Haourani, "Decentralized Access Control Infrastructure using Blockchain for Big Data," in *2019 IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, UAE, 2019, pp. 1-8, doi: 10.1109/AICCSA47632.2019.9035221.

[50] 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 Int. Wireless Commun. Mob. Comput. Conf. (IWCMC)*, Morocco, 2019, pp. 1582-1587, doi: 10.1109/IWCMC.2019.8766478.

[51] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain," *IEEE Access*, vol. 7, pp. 84304-84317, 2019, doi: 10.1109/ACCESS.2019.2917976.

[52] M. Ma, G. Shi, and F. Li, "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario," *IEEE Access*, vol. 7, pp. 34045-34059, 2019, doi: 10.1109/ACCESS.2019.2904042.

[53] R. Akkaoui, X. Hei, C. Guo, and W. Cheng, "RBAC-HDE: On the Design of a Role-based Access Control with Smart Contract for Healthcare Data Exchange," in *2019 IEEE Int. Conf. Consumer Electron. - Taiwan*

(ICCE-TW), Taiwan, 2019, pp. 1-2, doi: 10.1109/ICCE-TW46550.2019.8991965.

[54] M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, "Using Ethereum Blockchain for Distributed Attribute-Based Access Control in the Internet of Things," in *2019 IEEE Glob. Commun. Conf. (GLOBECOM)*, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014155.

[55] G. Ali, N. Ahmed, Y. Cao, Q. Ali, F. Azim, and H. Cruickshank, "BCON: Blockchain based access CONtrol across multiple conflict of interest domains," *J. Netw. Comput. Appl.*, vol. 147, p. 102440, Dec. 2019, doi: 10.1016/j.jnca.2019.102440.

[56] G. Ali, N. Ahmed, Y. Cao, M. Asif, H. Cruichshank, and Q. Ali, "Blockchain based permission delegation and access control in Internet of Things (BACI)," *Comput. Secur.*, vol. 86, pp. 318-334, Sept. 2019, doi: 10.1016/j.cose.2019.06.010.

[57] Q. Lyu, Y. Qi, X, Zhang, H. Liu, Q. Wang, and N. Zheng, "SBAC: A secure blockchain-based access control framework for information-centric networking," *J. Netw. Comput. Appl.*, vol. 149, p. 102444, Jan. 2020, doi: 10.1016/j.jnca.2019.102444.

[58] Y. Zhou, Y. Guan, Z. Zhang and F. Li, "A Blockchain-Based Access Control Scheme for Smart Grids," in *2019 Int. Conf. Netw. Netw. Appl. (NaNA)*, Korea, 2019, pp. 368-373, doi: 10.1109/NaNA.2019.00070.

[59] L. Xu, I. Markus, Subhod I, and N. Nayab, "Blockchain-based access control for enterprise blockchain applications," *Int. J. Netw. Manag.*, vol. 30, no. 5, Dec. 23, 2019, Art. no. e2089, doi: 10.1002/nem.2089.

[60] S. Figueroa, J. Añorga, and S. Arrizabalaga, "An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments," *Comput.*, vol. 8, no. 3, 2019, Art. no. 57, doi: 10.3390/computers8030057.

[61] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, 2019, Art. no. 2058, doi: 10.3390/app9102058.

[62] O. Stengele, A. Baumeister, P. Birnstill, and H. Hartenstein, "Access Control for Binary Integrity Protection using Ethereum," in *SACMAT '19: Proc, 24th ACM Symp. Access Control Model. Technol.*, Canada, 2019, pp. 3-12, doi: 10.1145/3322431.3325108.

[63] M. Samaniego, C. Espana, and R. Deters, "Access Control Management for Plant Phenotyping Using Integrated Blockchain," in *BSCI '19: Proc. 2019 ACM Int. Symp. Blockchain Secure Critical Infrastruct.*, New Zealand, July 2019, pp. 39-46, doi: 10.1145/3327960.3332380.

[64] Y. Lee and K. M. Lee, "Blockchain-based RBAC for user authentication with anonymity," in *RACS '19: Proc. Conf. Res. Adapt. Convergent Syst.*, Sept. 2019, pp. 289-294, doi: 10.1145/3338840.3355673.

[65] T. Thwin and S. Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems," *Secur. Commun. Netw.*, vol. 2019, Jun 25, 2019, Art. ID 8315614, doi: 10.1155/2019/8315614.

[66] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in *2018 IEEE Conf. Russian Young Res. Elect. Electron. Eng. (EIConRus)*, Russia, 2018, pp. 1575-1578, doi: 10.1109/EIConRus.2018.8317400.

[67] S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," *IEEE Access*, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[68] X. Tan, C. Huang, and L. Ji, "Access Control Scheme Based on Combination of Blockchain and XOR-Coding for ICN," in *2018 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/2018 4th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, China, 2018, pp. 160-165, doi: 10.1109/CSCloud/EdgeCom.2018.00036.

[69] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs," in *2018 IEEE Int. Conf. Internet of Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1027-1034, doi: 10.1109/Cybermatics_2018.2018.00191.

[70] U. Ugobame Uchibeke, K. A. Schneider, S. Hosseinzadeh Kassani, and R. Deters, "Blockchain Access Control Ecosystem for Big Data Security," in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1373-1378, doi: 10.1109/Cybermatics_2018.2018.00236.

[71] D. Di Francesco Maesa, P. Mori, and L. Ricci, “Blockchain Based Access Control Services,” in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1379-1386, doi: 10.1109/Cybermatics_2018.2018.00237.

[72] H. S. Gardiyawasam Pussewalage, and V. A. Oleshchuk, “Blockchain Based Delegatable Access Control Scheme for a Collaborative E-Health Environment,” in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1204-1211, doi: 10.1109/Cybermatics_2018.2018.00214.

[73] X. Zhang and S. Poslad, “Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR),” in *2018 IEEE Int. Conf. Commun. (ICC)*, USA, 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422883.

[74] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, “Blockchain-Based, Decentralized Access Control for IPFS,” in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1499-1506, doi: 10.1109/Cybermatics_2018.2018.00253.

[75] T. Le and M. W. Mutka, “CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments,” in *2018 IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Italy, 2018, pp. 57-64, doi: 10.1109/SMARTCOMP.2018.00074.

[76] D. Hwang, J. Choi, and K. Kim, “Dynamic Access Control Scheme for IoT Devices using Blockchain,” in *2018 Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, Korea, 2018, pp. 713-715, doi: 10.1109/ICTC.2018.8539659.

[77] X. Zhang, S. Poslad and Z. Ma, “Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth,” in *2018 IEEE Glob. Commun. Conf. (GLOBECOM)*, UAE, 2018, pp. 1-7, doi: 10.1109/GLOCOM.2018.8647433.

[78] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu and W. C. -C. Chu, “Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control,” in *2018 IEEE Int. Conf. Services Comput. (SCC)*, UAE, 2018, pp. 193-200, doi: 10.1109/SCC.2018.00032.

[79] S. Rouhani, V. Pourheidari, and R. Deters, “Physical Access Control Management System Based on Permissioned Blockchain,” in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Canada, 2018, pp. 1078-1083, doi: 10.1109/Cybermatics_2018.2018.00198.

[80] J. P. Cruz, Y. Kaji, and N. Yanai, “RBAC-SC: Role-Based Access Control Using Smart Contract,” *IEEE Access*, vol. 6, pp. 12240-12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[81] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594-1605, April 2019, doi: 10.1109/JIOT.2018.2847705.

[82] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, and W. C. -C. Chu, “TBAC: Transaction-Based Access Control on Blockchain for Resource Sharing with Cryptographically Decentralized Authorization,” in *2018 IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Japan, 2018, pp. 535-544, doi: 10.1109/COMPSAC.2018.00083.

[83] 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,” *Sustain. Cities Soc.*, vol. 39, pp. 283-297, May 2018, doi: 10.1016/j.scs.2018.02.014.

[84] 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,” *J. Netw. Comput. Appl.*, vol. 116, pp. 42-52, Aug. 15, 2018, doi: 10.1016/j.jnca.2018.05.005.

[85] C. Dukkipati, Y. Zhang, and L. C. Cheng, “Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things,” in *ABAC ’18: Proc. 3rd ACM Workshop Attribute-Based Access Control*, USA, Mar. 2018, pp. 61-69, doi: 10.1145/3180457.3180458.

[86] D. Maesa, P. Mori, and L. Ricci, “Blockchain Based Access Control,” in *17th IFIP Int. Conf. Distrib. Appl. Interoperable Syst. (DAIS)*, Switzerland , Jun 2017, pp.206-220, doi: 10.1007/978-3-319-59665-5_15.

[87] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, “ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT,” in *GLOBECOM 2017 - 2017 IEEE Glob. Commun. Conf.*, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8254521.

[88] M. Jemel and A. Serhrouchni, "Decentralized Access Control Mechanism with Temporal Dimension Based on Blockchain," in *2017 IEEE 14th Int. Conf. e-Bus. Eng. (ICEBE)*, China, 2017, pp. 177-182, doi: 10.1109/ICEBE.2017.35.

[89] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943-5964, Feb. 19, 2017, doi: 10.1002/sec.1748.

[90] S. Gao, G. Piao, J. Zhu, X. Ma and J. Ma, "TrustAccess: A Trustworthy Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5784-5798, June 2020, doi: 10.1109/TVT.2020.2967099.