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

Aaqib Bashir Dar[a,*], Auqib Hamid Lone[b], Asif Iqbal Baba[c], Roohie Naaz[b], Fan Wu[c]

[a] *Independent Researcher, Jammu and Kashmir, India, 190015*
[b] *Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, India,190006*
[c] *Department of Computer Science,Tuskegee University, Tuskegee, AL 36088*

Abstract

Access Control or authorization is referred to as the confinement of specific actions of an entity to perform an action. Blockchain driven access control mechanisms have gained considerable attention since applications for blockchain were found beyond the premises of cryptocurrencies. However, there are no systematic efforts to analyze existing empirical evidence. To this end, we aim to synthesize literature to understand the state-of-the-art in blockchain driven access control mechanisms with respect to underlying platforms, utilized blockchain properties, nature of the models and associated testbeds & tools. We conducted the review in a systematic way. Meta Analysis and thematic synthesis was performed on the findings and results from the relevant primary studies in order to answer the research questions in perspective. We identified 76 relevant primary studies passing the quality assessment. A number of problems like single point of failure, security, privacy etc were targeted by the relevant primary studies. The meta analysis suggests the use of different blockchain platforms, several application domains and different utilized blockchain properties. In this paper, we present a systematic literature review of blockchain driven access con-

*Aaqib Bashir Dar
Email addresses: aaqibb13@gmail.com (Aaqib Bashir Dar), ahl@nitsri.net (Auqib Hamid Lone), ababa@tuskegee.edu (Asif Iqbal Baba), naaz310@nitsri.net (Roohie Naaz), fwu@tuskegee.edu (Fan Wu)

trol systems. In hindsight, we present a taxonomy of blockchain driven access control systems to better under the immense implications this field has over various application domains.

Keywords: Blockchain, Access Control, Decentralization, Smart Contracts

1. Introduction

Access Control, typically referred to as resource authorization or just authorization, is the confinement of the actions of a particular entity or an individual only to the computing resources and services that it is authorized to use. This is achieved by enforcing predefined access control policies. The underlying policies govern every access of an entity to a particular resource. The policies can be realized in the guise of attributes and the corresponding rules associated with a set of entities and a set of resources. For the access control mechanisms to be sound and ensure integrity, this is achieved by securely establishing the identity of the entities. If this secure enforcement of the establishment of identities is absent, enforcing an access policy is foiled and left useless. While there is an absolute 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. Some of the challenges are; it is challenging to achieve access control in resource constrained devices due to their heterogeneous nature and limited computation capabilities. Also, 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 policy enforcement dynamically. While all of this comes down to whether a solution is viable (or scalable), taking into consideration parameters like time-memory tradeoffs, behavior to different types of traffic, resistance against various attacks, and adaptability to dynamic changes to the network are paramount. However, these issues can be dealt with much ease if a different perspective is put into place.

Blockchain technology has seen a tremendous rise, which grew exponentially after the inception of cryptocurrency Bitcoin[1], which in essence, is backed by Blockchain technology itself. The whole idea that baffled researchers and academics was that of the blockchain itself, which was the core underlying principle of Nakamoto's idea [1]. However, over the years, blockchain technology is booming, and some applications are beyond the realms of cryptocurrency.

With the rise of different technological platforms like Ethereum[2], Hyperledger[3], Ripple[4], and many more. The field has moved to a different dimension of its own. However, right after the emergence of Ethereum, that supported the creation of smart contracts 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 trustlessness, decentralization, robustness, and its own extensive features.

The customisable 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 are considered in this view, and it is evident from the existing literature that blockchain technology indeed have dominance over it.

1.1. Related Work

In literature, there are quite a few survey/review papers on Blockchain applications. One of the earliest attempts in this direction is the work carried out by Huumo et al. in [5]. In their findings, they reveal the majority of the papers focused on Bitcoin projects, specifically under a common theme of security and privacy. In our opinion, this study provided a stepping stone for the corresponding research community to explore in this direction further. A comprehensive systematic review of Blockchain applications was carried by Casino et al. [6]. In particular, they provided a classification of Blockchain-based applications across diverse domains ranging from supply chains to IoT, and they also highlighted barriers in Blockchain technology, which limit the mass use of Blockchain technology. However, very few articles in the literature have conducted a survey/review on Blockchain application in access control and thus closely related to our work. One such work is carried out by Sara Rouhani and Ralph Deters in [7]. Authors have conducted a state of the art survey on blockchain-based access control systems and challenges. In particular, they have 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 a way 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 [8] has conducted a comprehensive survey on blockchain-based access control for IoT. However, their study is less exhaustive because they specifically targeted access control in IoT only.

Rest of the paper is structured as follows: Section 2 contains the methodology followed throughout the paper, Section 3 encompasses the relevant key findings of the paper. In Section 4, we constructed the themes for our research and provided a discussion based on those themes. Section 5 contains a detailed taxonomy of blockchain-driven access control systems. In Section 6, we concluded the paper by providing relevant insights.

2. Research Methodology

For the collection of relevant literature about the topic, Kitchenham and Charters [9] guidelines were followed to target the research themes effectively. The whole process went through the phases of planning, conducting, and reporting the review iteratively to allow rigorous assessment of the state-of-the-art in this area in a systematic manner.

- **Primary Study Selection:**

  Primary studies were emphasized through keyword search put through major scientific databases. The keywords were selected to foster the emergence of research results that would be more generic in nature and allow us to answer the research questions. The Boolean operator was restricted to AND. The search strings were: "BLOCKCHAIN" AND "ACCESS CON-

TROL"

The search was conducted across the following platforms:

IEEE Xplore, ScienceDirect, ACM Digital Library, SpringerLink, Wiley, Taylor & Francis, MDPI.

The searches were run against title, keywords, abstract, and full-text, depending on the platforms we searched on. We conducted the searches in June 2020, and all the studies published up to this were processed. The results from these searches were then filtered through the inclusion/exclusion criteria, which is presented in the next section. These criteria helped in attaining the results, which were then put through Wohlin's snowballing process [10]. The forward and backward snowballing process was conducted iteratively until no intersection was found between any paper and inclusion criteria.

- **Inclusion and Exclusion Criteria:**

  Studies included in this review must report empirical findings describing technical aspects of the technology in relevance to our topic, applications spanning through several domains, and sufficient implementation details with detailed 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 is included. They must be peer-reviewed and written in English. The key inclusion and exclusion criteria are presented in Table 1.

- **Selection of Results:**

  From the initial keyword searches along the major databases mentioned, a total of 1517 results were identified. The number was reduced to 1260 after only scanning through journal articles and conference proceedings. After the filtering process, the total articles were reduced to 82 in number based on the title relevance. While moving on to the next stage of filtering based on abstract relevance, the authors obtained 77 papers. After moving ahead in a different stage that involved forward and backward snowballing,

Table 1: 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

the number of papers was reduced to 76 in total. We have presented the year-wise distribution of relevant primary studies in Table 2.

Table 2: Distribution of Relevant Studies (yearly)

Publication Year	Major Databases					Relevant Studies
	IEEE XPLORE	SCIENCE DIRECT	ACM DIGITAL LIBRARY	WILEY	MDPI	
2020	11	2	3	1	4	[RS01] to [RS21]
2019	20	3	3	2	2	[RS22] to [RS51]
2018	17	1	2	0	0	[RS52] to [RS71]
2017	3	0	0	1	0	[RS72] to [RS75]
2015	1	0	0	0	0	[RS76]
Total	52	6	8	4	6	76

A graphical representation of yearly distribution of relevant studies is presented in Figure 1.

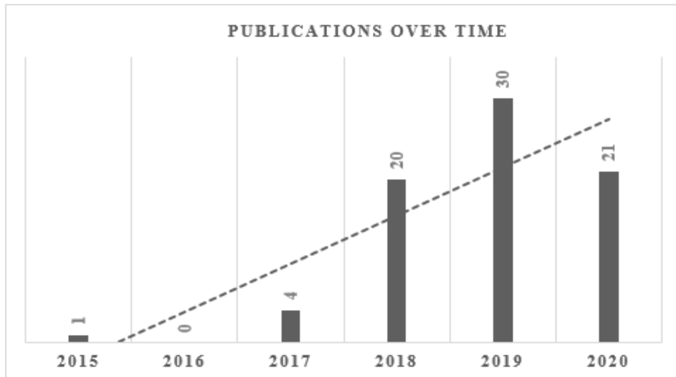

Figure 1: Publications Over Time

2.1. Perils to Corroboration

2.1.1. Bias towards Publication

The term publication bias refers to the problem of publishing more positive results in comparison to negative results. It is to be noted that publication bias has immense implications in the original literature. By choosing preferences, selecting some results over others 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 good choice. However, they do have relatively higher chances of getting published statistically.

2.1.2. Importance of Search Terms

In order to conduct a review systematically, it is always imperative and a challenging task to find the relevant primary studies targeting a particular subject matter, specifically the topic in 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 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 search string selection was made after the authors carried out a discussion with the experts on the subject matter. A pilot study was conducted before the full-fledged study, which confirmed the

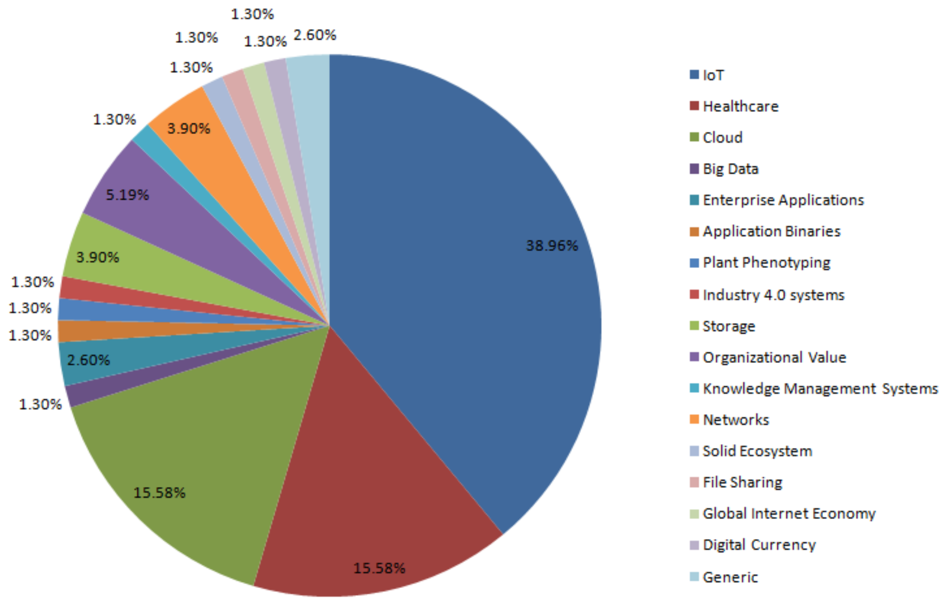

Figure 2: Blockchain Access Control Application Domains

applicability of the search string and its correctness concerning the topic at hand. Besides 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.

2.1.3. 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 is left out. We excluded the studies based on the title relevance, followed by abstract relevance during the first stage. During the pilot study, constructive disagreements were resolved, and a solid foundation was laid to understand better and properly refine the inclusion/exclusion criteria. The authors repeated the selection procedure until the authors agreed to a substantial degree for selecting relevant studies from a full set of research papers. In instances where multiple authors were in doubt about a research paper's inclusion, a third researcher was consulted to solve the conflict. This was followed by the next phase, where the studies were included based on their full-text relevance to the topic. Due to the carefully constructed and well-established selection criteria, it is quite highly unlikely that any relevant studies must have been left out.

2.1.4. Data Extraction and Evaluation Quality

The quality of each relevant primary study was investigated by two researchers independently. The criteria for quality assessment were piloted and further modified based on the results of the pilot study. Constant feedback was asked from an expert on the subject matter when researchers could not reach a consensus. Therefore, these measures mentioned above mitigated the risk of missing any relevant primary study to a large extent. The data extracted from the relevant studies were 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 finally able to complete the process of data extraction. The whole data extraction was carried out manually, thus improving the validity.

3. Relevant Key Findings

Every single relevant study was read in full to extract sufficient qualitative and quantitative data. The results are presented in Table 3. All the relevant studies had a theme about how a particular problem was dealt with by blockchain technology. The focus of each paper is also recorded in Table 3.

A further grouping of themes was done into a broader context to simplify the classification of relevant study themes. Studies were focusing on a variety of application domains. Studies that encompassed cloud services, cloud storage, and cloud environments 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 is found to be IoT, which included sub-domains like the Internet of Drones, Smart City, Smart Grids, Industrial IoT, Smart Homes, and Smart Buildings. Figure 2, shows the percentages of different application areas 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 rest of the relevant studies involved application domains like Networks (3.90%), Knowledge Management Systems (1.30%), Organisational 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 Figure 3.

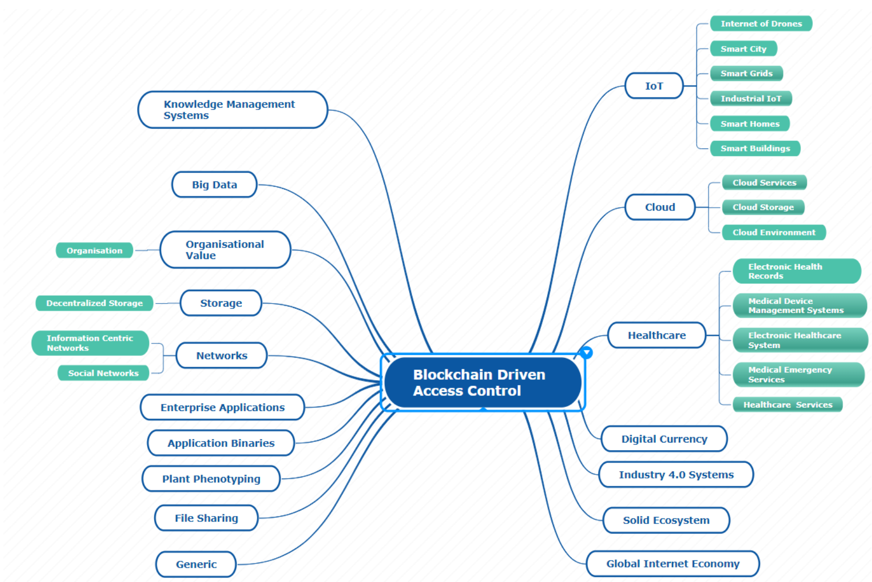

Figure 3: Blockchain access control application domain classification

Table 3: Key Findings and Themes of Primary Studies

Relevant Study	Key Finding	Blockchain Platform	Primary Application Domain
[RS01]	An authorization and delegation model for the IoT Cloud based on blockchain technology.	Ethereum	Smart City
[RS02]	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 invoices, and electronic cards.
[RS03]	A blockchain based access control framework that allows manageability and auditability for DOSNs to define privacy policies	Ethereum	Social Networks
[RS04]	A blockchain-based access control scheme for IoD environment allowing secure communication between the Ground Server Station and drones.	Generic	Internet of Drones
[RS05]	Blockchain based framework utilizing Fairaccess through Dynamic Access control to access any specific resource in the blockchain network.	Generic	—-
[RS06]	A Hyperledger Fabric blockchain framework as an access control system in IoT based on attribute based access control (ABAC)	Hyperledger Fabric	IoT
[RS07]	A ciphertext policy attribute-based encryption system that utilizes blockchain technology and IPFS storage environment for electronic medical records.	Generic	Electronic Medical Records
[RS08]	A blockchain and ciphertext-based attribute encryption (CP-ABE) leveraged fine-grained access control scheme for VANET data.	Ethereum	Cloud Servers
[RS09]	A blockchain based fine-grained access control(BSDS-FA) in the Internet of things environment that allows secure data sharing	Hyperledger fabric	IoT
[RS10]	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
[RS11]	A Private Blockchain based secure access control for monitoring different climatic parameters in agricultural fields	Hyperleder Fabric	Smart Homes
[RS12]	A privacy-Preserving Blockchain based access control scheme for big data in Cyber-Physical-Social System (CPSS)	EOS	Cloud Environment
[RS13]	A Privacy protected blockchain based access control framework in Cloud towards solving the problem of security and Privacy	EOS	Cloud Environment
[RS14]	Blockchain assisted secure authentication system and fine-grained access control for Social Linked Data (SOLID)	Hyperledger Fabric	Solid Ecosystem

Continued on next page

Table 3 – *Continued from previous page*

Relevant Study	**Key Finding**	**Blockchain Platform**	**Primary Application Domain**
[RS15]	Blockchain assisted attribute based collaborative access control scheme for providing decentralized, flexible, and fine-grained authorization for IoT devices and also provides resistance against possible attempts of unauthorised access on IoT device resources	Hyperledger Fabric	IoT
[RS16]	Blockchain smart contract driven role-based access control scheme for maintaining transparency and resource immutability in knowledge management systems	Ethereum	Knowledge Management Systems
[RS17]	Smart contract driven access policy enforcement to address the issues of trust and authentication for access control in IoT networks	Ethereum	IoT
[RS18]	An Ethereum smart contract driven capability-based access control scheme for IoT that is decentralized and trustworthy	Ethereum	IoT
[RS19]	An attribute-based encryption scheme augmented with Hyperledger Composer to provide fine grained access control for secure data sharing	Hyperledger Composer	Cloud Environment
[RS20]	Ethereum Blockchain augmented with Shamir's secret scheme to provide provide privacy preserving access control to cloud data	Ethereum	Cloud Environment
[RS21]	A blockchain-enabled access control scheme where mutual authentication between the entities take place in the Internet of Things environment	Generic	IoT
[RS22]	A smart contract leveraged blockchain driven trustworthy and distributed access control solution for IoT	Ethereum	Real Vehicular Environment
[RS23]	A Blockchain driven attribute based access control scheme for simplified access management in IoT Systems	Hyperleder Fabric	Internet of Things
[RS24]	Leveraging permissioned blockchain smart contracts and distributed consensus for Attribute Based Access Control(ABAC) to enable a distributed access control for IoT	Hyperleder Fabric	Medical Emergency Service
[RS25]	A ciphertext-policy attribute-based encryption (CP-ABE) and ethereum blockchain driven access control framework for secure cloud storage	Ethereum	Cloud Environment Service
[RS26]	A blockchain technology based distributive attribute-based access control framework (ADAC) for lightweight & open IoT devices	Ethereum	IoT
[RS27]	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
[RS28]	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

Continued on next page

Table 3 – *Continued from previous page*

Relevant Study	**Key Finding**	**Blockchain Platform**	**Primary Application Domain**
[RS29]	Blockchain and Smart contract driven access control mechanism and architecture for IoT	Ethereum	IoT
[RS30]	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 user in an IoT scenario like smart city	Generic	Smart City
[RS31]	A decentralized blockchain based secure fine-grained access control for IoT system.	EOS	IoT
[RS32]	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.
[RS33]	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
[RS34]	Blockchain smart contracts driven methodology to delegate fine-grained permissions in decentralized fashion.	Ethereum	Smart Building
[RS35]	Blockchain driven access control infrastructure for Big Data to publish the policies, deployed in smart contracts.	Generic	Big Data
[RS36]	A blockchain technology based distributed attribute-based access control mechanism that dynamically manages multi-endorsed attributes and trust anchors.	Generic	IoT
[RS37]	An emergency access control management system (EACMS) based on hyperledger fabric and hyperledger composer.	Hyperledger Fabric	Healthcare Services
[RS38]	Blockchain technology leveraged decentralized, fine-grained, auditable, highly scalable, and extensible hierarchical access control that allows privacy-preserving principles in IoT.	Generic	IoT
[RS39]	A blockchain based immutable and decentralized role-based access control system to facilitate secure data exchange for healthcare.	Ethereum	Healthcare
[RS40]	An Ethereum smart contract driven attribute-based access control (ABAC) framework for IoT systems	Ethereum	IoT
[RS41]	A Blockchain based fair, verifiable and decentralized access control for conflict of interest domains.	Generic	Wireless Access control, Cloud environment, IoT
[RS42]	A novel decentralized architecture for event and query base permission delegation and access control in IoT application	Generic	IoT
[RS43]	A secure blockchain-based access control framework that allows sharing, auditing and revocation in a secure way.	Ethereum	Information Centric Networks

Continued on next page

Table 3 – *Continued from previous page*

Relevant Study	**Key Finding**	**Blockchain Platform**	**Primary Application Domain**
[RS44]	A Blockchain driven identity-based encryption, signcryption and signature scheme suitable for smart Grids	JPBC library	Smart Grids
[RS45]	A novel Blokchain assisted access control scheme leveraging decentralised feature of Blockchain to control access-related operations and ring signature scheme to protect user privacy	Hyperledger Fabric	Enterprise Blockchain Applications
[RS46]	Blockchain driven access control mechanism for addressing security and safety risks in healthcare applications	Ethereum	RFID-based Healthcare Applications
[RS47]	Blockchain-based identity management augmented with access control mechanism to provide authentication, auditability, and confidentiality for resource-constrained edge devices	Ethereum	Industrial IoT
[RS48]	Ethereum smart contract driven access control mechanism for protecting integrity of binaries	Ethereum	Application Binaries
[RS49]	Ethereum Blockchain driven access control for data management in the field of plant phenotyping	Ethereum	Plant Phenotyping
[RS46]	Blockchain driven access control mechanism for addressing security and safety risks in healthcare applications	Ethereum	RFID-based Healthcare Applications
[RS47]	Blockchain-based identity management augmented with access control mechanism to provide authentication, auditability, and confidentiality for resource-constrained edge devices	Ethereum	Industrial IoT
[RS48]	Ethereum smart contract driven access control mechanism for protecting integrity of binaries	Ethereum	Application Binaries
[RS49]	Ethereum Blockchain driven access control for data management in the field of plant phenotyping	Ethereum	Plant Phenotyping
[RS50]	Blockchain driven role-based access control mechanism for anonymous user authentication	Ethereum	Generic
[RS51]	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
[RS52]	A Blockchain based access control scheme providing key generation, revocation or change, access policy assignment and access request	Ethereum	Cloud Environment
[RS53]	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

Continued on next page

Table 3 – *Continued from previous page*

Relevant Study	**Key Finding**	**Blockchain Platform**	**Primary Application Domain**
[RS54]	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 Networks
[RS55]	A robust blockchain smart contract driven identity-based capability token management scheme for registration, propagation and revocation of the access authorization	Ethereum	IoT networks
[RS56]	A blockchain based access control ecosystem providing effective access control authority to asset owners and protection against data breaches	Hyperledger Fabric	Cloud Computing Environments
[RS57]	Blockchain smart contract leveraged new design approach for access control services	Ethereum	Cloud Services
[RS58]	A Blockchain steered attribute based access control scheme that offers controlled access delegation capabilities in a multi-domain e-health environment.	Generic	Electronic Healthcare System
[RS59]	A Blockchain-oriented access authorisation scheme with granular access control, offering flexible data queries for secure EMR information management.	Generic	Electronic Medical Records
[RS60]	An Ethereum smart contracts driven modified InterPlanetary Filesystem (IPFS) to provide access controlled file sharing.	Ethereum	KYC, IPFS and moving data off-chain
[RS61]	A Blockchain based privacy preserving access control framework that allows sharing and delegation of access rights of users in IoT devices	Monero	IoT
[RS62]	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
[RS63]	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
[RS64]	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
[RS65]	A Hyperledger Fabric and Hyperledger Composer based access control application to control access to physical spaces.	Hyperledger Fabric	Access Permissions on Physical Spaces
[RS66]	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
[RS67]	A smart contract-based framework consisting of multiple contracts for access control to achieve distributed and trustworthy access control for IoT systems	Ethereum	IoT

Continued on next page

Table 3 – *Continued from previous page*

Relevant Study	Key Finding	Blockchain Platform	Primary Application Domain
[RS69]	A blockchain-based privacy preserving framework for secure, interoperable, and efficient access to medical records by severl entities like patients, providers and third parties.	Ethereum	Electronic Health Records
[RS70]	A blockchain-based secure mutual authentication system to enforce fine-grained access control policies	Bitcoin like	Industry 4.0 systems
[RS71]	A Blockchain-based access control for critical IoT resources	Custom	IoT
[RS72]	Leveraging blockchain technology to enforce, manage and create access control policies	Bitcoin	An Organization
[RS73]	A scalable, user-friendly, user transparent, fully decentralized and fault tolerant blockchain based architecture for IoT access authorizations.	Generic	IoT
[RS74]	Blockchain verified decentralized accesscontrol mechanism for user legitimacy and added temporal dimension to file sharing using CP-ABE.	Generic	Cloud Storage
[RS75]	A Blockchain-based access control framework that provides fully decentralized, pseudonymous and privacy preserving authorization management for IoT.	Customized Local Blockchain	IoT
[RS76]	A blockchain based privacy preserving trustworthy secure ciphertext-policy and attribute hiding access control scheme, to achieve trustworthy access	Generic	Distributed Local Storage

4. Research themes and their discussion

After the relevant literature was collected and relevant studies read in full, it was essential to identify the research themes that are to be addressed in this study and thereby providing an elaborate discussion to those identified themes. We provide the research themes in Table 4.

The initial keyword searches suggest that there are an appreciably substantial amount of papers related to Blockchain driven access control systems. Although the field is still booming and ever-developing, the relevant studies cover a wide range of applications. An appreciable amount of related primary studies have experimental evidence of their practicality, and a sizeable amount of studies are concepts of theoretical nature. The relevant primary studies have

Table 4: Research questions and their significance

Research Questions	Significance/Relevance
RQ1: How has blockchain driven access control systems shown dominance over traditional access control systems?	The inherent properties of blockchain makes it an ideal choice to be used in place of traditional access control systems. The underlying features of blockchain allows 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 prominance 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 with-standing issues in traditional acccess 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 applications domains covered by blockchain driven access control systems?	The applicability of traditional access control systems are specific to a set of application domains. However, a broad spectrum of applications are 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.

displayed innovative ways to solve the persisting problems like a single point of failure, security, privacy, etc. They have also provided experimental evidence to support their claims. The solutions either rely on intermingling existing technologies with Blockchain technology or various technologies to solve the underlying problems. In Table 5, we depicted persisting problems and different technologies used to solve them. Blockchain technology has shown dominance over the traditional techniques that were being 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 is very similar to that of Javascript and Python. It allows customizable programming of smart contracts, giving a programmer a free hand 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, a high degree of privacy, 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 the 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 suggest a better regulation mechanism, which in turn supports the better need for the trust of individual nodes, thus an improvement in 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 and the corresponding solution they suggested for those problems in Table 5.

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 an intense and valuable discussion.

4.1. 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 the issues discussed in this review. They simply provide a better way for existing efforts to be used to overcome the persisting issues. Blockchain utilizes encryption mechanisms, signature, and lightweight algorithms to provide security and enable privacy for authentication purposes. A substantial amount of studies utilizes the existing technologies and further improves it by intermingling with Blockchain

Table 5: 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	[RS01, RS07, RS08, RS16] [RS17, RS35, RS41, RS45] [RS51, RS54, RS55, RS60] [RS18, RS20]
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	[RS02, RS09, RS13, RS18] [RS19, RS28, RS31, RS33] [RS43, RS49, RS53, RS57] [RS58, RS60, RS37, RS44] [RS21, RS46]
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	[RS02, RS04, RS06, RS07] [RS09, RS14, RS15, RS17] [RS18, RS27, RS28, RS29] [RS31, RS33, RS43, RS45] [RS51, RS53, RS56, RS58] [RS60, RS45, RS75, RS19] [RS20]
Key Escrow	Incentive and Penalty based consensus mechanism for consortium blockchain	[RS05]
Critical Access control	Blockchain Smart contracts based access control, Blockchain & Attribute based access control	[RS48, RS52]
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	[RS20, RS21, RS22, RS23] [RS59, RS08, RS27, RS32] [RS47]
Key Abuse	IPFS with Blockchain& ABE, Blockchain with XOR coding	[RS07, RS12]
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	[RS10, RS11, RS16, RS54]
Efficient implementation of Access Control	Blockchain based decentralized system, Blockchain and Role based access control	[RS24, RS46, RS47]
Authentication	Smart contract driven access control, Blockchain driven access control, Blockchain driven role based access control	[RS17, RS47, RS50]

technology. It is evident from the fact that most traditional systems relied on a single trusted authority, thus leaving the system vulnerable to many attacks. These attacks widen 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. It is an important feature in any modern-day system providing services at 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. In a true sense, we know that Blockchain is decentralized, thereby not requiring the trust or authority of an individual member of a network or a group. Trust is eliminated by allowing each participating node/member has a complete copy of all the past information available. After achieving consensus by most nodes in a network, more data will be added to the chain of existing information.

Based on the studies focused mostly on bolstering existing efforts with Blockchain technology explicitly, we briefly discuss 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. [RS53, RS23, RS07, RS43, RS18].

Security– Many studies targeted the issue of security. The technologies with which the Blockchain was intertwined were capability-based access control, attribute-based access control, emergence based access control, and others [RS13, RS26, RS33, RS43, RS68, RS37, RS19].

Privacy– Privacy is not inherently provided by 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 attribute-based encryption, capability-based access control, and many more [RS07, RS27, RS10, RS33, RS08, RS43, RS19].

Authentication– The feature of authentication was focused on by a limited number of studies utilizing smart contracts and role-based access control mostly [RS47].

4.2. RQ2: What were the shortcomings of traditional access control systems rectified by Blockchain-driven access control systems?

Our research tried to accumulate results based on 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– 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 like 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, as time progresses, 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, 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, smart contracts, emergence based access control, etc.

Privacy– Since it is known that privacy is not inherently a part of Blockchain technology, serious concerns are raised over data breaches by analyzing the hashes of the transactions happening over the Blockchain network. However, there have been attempts to address this issue over the years, and research in this direction is leaving no stone unturned to strengthen this area further. We found an appreciable number of relevant studies that focused on solving privacy up to a certain extent. It is obvious that the notion of research does not allow us to settle for something and rather further in a research direction until a better and 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 privacy, enabling access control in various application areas.

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

The technologies 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 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 the 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.

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

It is important to emphasize that the review intends to focus on a broader context of Blockchain applications 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 an opportunity to solve issues like a single point of failure, security, and privacy issues, etc. The prioritization of application domains suggests the proposals mostly targeting IoT, thus clearly in abundance. 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– Majority of the relevant primary studies are specific to the IoT domain, and the evident reasons are discussed above already. An authorization, delegation model and access control for IoT systems based on blockchain technology targeting various subdomains [RS01, RS04, RS09, RS11, RS17, RS18, RS21].

Cloud– The primary studies have shown various studies targeting cloud specifically. The subdomains of the studies are strictly under one blanket of cloud, thus the categorization of studies based on their corresponding relevance [RS08, RS12, RS13, RS19, RS20, RS25].

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 [RS07, RS24, RS27, RS37, RS39].

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 [RS10, RS66, RS68, RS72].

Several studies target the storage area as their primary application domain. In our research, we found some studies targeting this area [RS76, RS53].

Networking in the modern day is inherently a 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 being involved with the network application domain as well [RS54, RS03, RS43].

Big Data, Application Binaries, Plant Phenotyping & 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 [RS35], Application Binaries [RS48], Plant Phenotyping [RS49], Industry 4.0 Systems [RS70], Enterprise applications [RS32, RS45], Solid Ecosystem [RS14], File Sharing [RS60], Digital Currency [RS02], Knowledge Management Systems [RS16], Global Internet Economy [RS64] and some generic applications as well.

5. 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 undertook 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 in presented in Figure 4. Other than that we also presented testbeds/tools used by each study based on whether the particular study has provided implementation or not. We present the whole taxonomy in Table 6. Based upon the type of solution presented by each access control system, we categorized the solutions in Table 7.

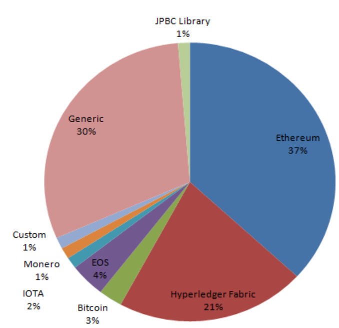

Figure 4: Blockchain Platforms employed by the relevant studies

Table 6: A Taxonomy of Blockchain driven Access Control Systems

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
Imen Riabi et al [RS22]	Ethereum	Yes	Smart Contracts	Truffle, Go-Ethereum, Geth
AuthPrivacyChain [RS13]	EOS	Yes	Decentralization & Tamper-Resistance	Kylin & Jungle test chain
Ting Cai et al [RS14]	Hyperledger Fabric	No	Secure Authentication	Kylin test chain
BacCPSS [RS12]	EOS	Yes	Decentralization	Kylin test chain
Yuyang Zhou et al [RS44]	JPBC Library	Yes	Decentralization	Eclipse, Neon.1a Release (4.6.1)
Ilya Sukhodolskiy et al [RS52]	Ethereum	Yes	Decentralization	Ethereum Virtual Machine
Shangping Wang et al [RS53]	Ethereum	Yes	Decentralization & Distributiveness	Rinkeby
Sheng Ding et al [RS23]	Hyperledger Fabric	Yes	Distributiveness	Ubuntu Linux 16.04LTS desktop, AVISPA tool
Jehangir Arshad et al [RS11]	Custom	Yes	Immutability	Linux System
MD Azharul Islam et al [RS24]	Hyperledger Fabric	Yes	Smart Contracts	MEMSICs TelosB Mote TPR2420CA devices
Shangping Wang et al [RS25]	Ethereum	Yes	Decentralization	Ethereum Geth Client
Xiaobin Tan et al [RS54]	Generic	No	Decentralization & Tamper-Resistance	—
ADAC [RS26]	Ethereum	Yes	Distributiveness & Trustworthiness	Ropsten test network
Shaddan Ghaffaripour et al [RS27]	Hyperledger Fabric	No	Transparency, Tamper-resistance & Decentralization	—-
BBACS [RS63]	Generic	Yes	Decentralization	MIRACL
BDSS-FA [RS09]	Hyperledger Fabric	Yes	Traceability	Zookeeper, Kafka
BLENDCAC [RS55]	Ethereum	Yes	Decentralization & Smart Contracts	Go-Ethereum
Chao Wang et al [RS28]	Hyperledger Fabric	Yes	Decentralization & Smart Contracts	AWS EC2 cloud host
Uchi Ugobame Uchibeke et al [RS56]	Hyperledger Fabric	Yes	Smart Contracts	Hyperledger Composer Client API
Dwiyan Rezkia Putra et al [RS29]	Ethereum	Yes	Smart Contracts & Consensus Mechanisms	Geth, Remix
Damiano Di Francesco Maesa et al [RS57]	Ethereum	Yes	Smart Contracts	International Educational blockchain academic testnet, Geth
Damiano Di Francesco Maesa et al [RS72]	Bitcoin	Yes	Distributed Auditability	Bitcoin Network
Harsha S. Gardiyawasam et al [RS58]	Generic	No	Delegatability & Tamper-Resistance	—
Shuang Sun et al [RS31]	EOS	Yes	Decentralization	EOS Client
Jin Sun et al [RS07]	Generic	Yes	Non-tamperable & Traceability	Ubuntu Server 15.4
Mathis Steichen et al [RS60]	Ethereum	Yes	Immutability	Go ethereum's abigen, S/Kademlia,
BloCyNfo-Share et al [RS10]	Ethereum	Yes	Transparency, Tamper-Resistance, Verifiability	Go Ethereum (Geth), cpabe

Table 6 continued from previous page

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
CapChain [RS61]	Monero	Yes	Decentralization, Trustlessness & Immutability	ARM Cortex-M0+ MCU, Raspberry Pi Zero W, MSU HPCC network
ControlChain [RS73]	Generic	No	Decentralization	—
DAcc [RS32]	Hyperledger Fabric	Yes	Decentralization & Verifiability	Hyperledger Fabric Cryptogen, Cryptoconfig tools
DCACI [RS33]	IOTA	Yes	Decentralization	Raspberry Pi, Ubuntu 18.04.1 LTS processor
Leepakshi Bindra et al [RS34]	Generic	Yes	Smart Contracts	Query API, Simulated BACnet API
DACBBD [RS35]	Generic	No	Transparency & Traceability	—
Mayssa JEMEL et al [RS74]	Generic	Yes	Decentralized & Verifiability	CP-ABE Toolkit, Multichain
DAM-Chain [RS64]	Generic	No	Verifiability & Traceability	—
Sophie Drame-Maigne et al [RS36]	Generic	No	Distributiveness, Resilience, & Auditability	—
DongYeop Hwang et al [RS62]	Generic	No	Distributiveness	—
EACMS [RS37]	Hyperledger Fabric	Yes	Smart Contracts	Hyperledger Composer
Richa Gupta et al [RS05]	Generic	No	Smart Contracts & Verifiability	—
fabric-iot [RS06]	Hyperledger Fabric	Yes	Decentralization, Tamper-Resistance & Traceability	Docker, Docker compose, Hyperledger fabric
FADB [RS08]	Ethereum	Yes	Smart Contracts	Ubuntu 16.04.4 LTS desktop, Ethereum ganache-cli
GAA-FQ [RS59]	Generic	Yes	Data Integrity	MIRACL, Raspberry Pi 2, Intel i5-4200H Processor
Sara Rouhani et al [RS65]	Hyperledger Fabric	Yes	Tamper-Resistance,	Hyperledger Caliper
BDKMA [RS38]	Generic	Yes	Decentralization, Auditability, Extensibility	OMNeT++ 5.4.1, ECIES, Intel Core i5 CPU
RBAC-HDE [RS39]	Ethereum	Yes	Immutability & Decentralization	Ethereum Remix IDE
RBAC-SC [RS66]	Ethereum	Yes	Decentralization & Smart Contracts	Ropsten Testnet
Yuanyu Zhang et al [RS67]	Ethereum	Yes	Distributiveness, & Trustworthiness	Macbook Pro, Raspberry Pi 3, Dell Inspiron 3650, Geth Clients
SRBAC [RS30]	Generic	No	Delegatability & Smart Contracts	—
TBAC [RS68]	Generic	No	Decentralization, Authenticity & Traceability	—
GUOHUA GAN et al [RS02]	Hyperledger Fabric	No	Fault Tolerance & Trustworthiness	Customized test tools
TrustAccess [RS76]	Generic	Yes	Decentralization & Transparency	Intel (R) Core (TM) i5-8250U CPU
Mirei Yutaka et al [RS40]	Ethereum	Yes	Smart Contracts, Tamper-Resistance & Distributiveness	Intel Xeon CPU E5-1620, Geth, Remix IDE
Oliver Stengele et al [RS48]	Ethereum	Yes	Tamper-Resistance & Verifiability	Remix IDE, Ganache
BACC [RS20]	Ethereum	No	Smart Contracts & Decentralization	—
Mayra Samaniego et al [RS49]	Ethereum	Yes	Decentralization & Smart Contracts	Intel(R) Core(TM) i7-6700 CPU
Afnan Alniamy et al [RS19]	Hyperledger Fabric	Yes	Confidentiality & Integrity	Hyperledger Composer
YongJoo Lee et al [RS50]	Ethereum	Yes	Trustlessness	Geth, Intel Core i7-4790 CPU

Table 6 continued from previous page

Approach	Blockchain Platform	Implementation	Utilized Blockchain Properties	Testbeds/Tools
Chethana Dukkipati et al [RS71]	Generic	Yes	Decentralization, Transparency	—
CapBAC [RS18]	Ethereum	Yes	Decentralization, Smart Contracts & Verifiability	MacBook Pro, MacBook Air, Two Raspberry Pi's
Gabriel Nyame et al [RS16]	Ethereum	Yes	Transparency & Immutability	Ropsten, Remix IDE, MetaMask, Intel Core i7 6700HQ CPU
Santiago Figueroa et al [RS46]	Ethereum	Yes	Decentralization & Smart Contracts	ETH Network Stats, Etherscan Ropsten, Truffle, Infura Dashboard.
Tanzeela Sultana et al [RS17]	Ethereum	Yes	Distributiveness & Smart Contracts	Intel Core i5 CPU
Yan Zhang et al [RS15]	Hyperledger Fabric	Yes	Authenticity & Reliability	Intel core i7-4510U, Intel Core i5-7200U, three Raspberry Pi 3B+, Hyperledger Caliper
Yongjun Ren et al [RS47]	Ethereum	Yes	Decentralization & Tamper-Resistance	Intel Core i7, Raspberry Pi 3
Ancile [RS69]	Ethereum	No	Decentralization & Smart Contracts	—
BACS-IOD [RS04]	Generic	No	Tamper-Resistance	SPAN for AVISPA, Intel Core i5-4460S, Samsung Galaxy S5
BCON [RS41]	Generic	No	Decentralized, Fairness, Verifiability & Tamper-Resistance	Spin Model Checker
BSeIn [RS70]	Generic	Yes	Decentralization, Verifiability & Immutability	JUICE, Intel Core i7-6700 CPU
BACI [RS42]	Generic	No	Trusted, Verifiability, Decentralized	SPIN model checker
Mohsin Ur Rahman et al [RS03]	Ethereum	Yes	Decentralization	Rinkeby Ethereum testnet
Nachiket tapas et al [RS01]	Ethereum	Yes	Immutability, Verifiability & Decentralization	Ganache, Rinkeby
SBAC [RS43]	Ethereum	Yes	Transparency, Smart Contracts & Distributiveness	Intel(R) Core(TM) i5-7200U CPU
Lei Xu et al [RS45]	Hyperledger Fabric	Yes	Decentralization	Cryptogen and Cryptoconfig tools
CBACS-EIOT [RS21]	Generic	Yes	Immutability, Transparency & Decentralization	AVISPA tool, Intel Core i5-4460S, Samsung Galaxy S5
FairAccess [RS75]	Bitcoin	Yes	Distributiveness, Transparency & Smart Contracts	Camera module & Raspberry Pi
Thein Than Thwin et al [RS51]	Hyperledger Fabric	Yes	Tamper-Resistance	Intel Core i7-4510U CPU, Eclipse IDE

The proposed access control systems relying on blockchain technology as a strengthening force is either of theoretic nature only or has prototype implementation with or without simulation carried out on specific platforms. Although, it is important to understand that the proposed model is inherently theoretic in nature if does not provide any prototype implementations or conduct any simulation. However, in Table 7, the "✓" in theoretic column symbolizes the proposed model being strictly of theoretic nature only with no prototype implementations or simulations.

Table 7: Underlying nature of the proposed access control model

Access Control Solution	Theoretic	Simulation	Prototype
Imen Riabi et al [RS22]			✓
AuthPrivacyChain [RS13]			✓
Ting Cai et al [RS14]		✓	
BacCPSS [RS12]			✓
Yuyang Zhou et al [RS44]		✓	
Ilya Sukhodolskiy et al [RS52]			✓
Shangping Wang et al(2018) [RS53]		✓	✓
Sheng Ding et al [RS23]		✓	✓
Jehangir Arshad et al [RS11]			✓
MD Azharul Islam et al [RS24]			✓
Shangping Wang et al(2019)[RS25]		✓	✓
Xiaobin Tan et al [RS54]	✓		
Peng Wang et al [RS26]		✓	
Shaddan Ghaffaripour et al [RS27]	✓		
BBACS [RS63]		✓	
BDSS-FA [RS09]		✓	
BLENDCAC [RS55]		✓	✓
Chao Wang et al [RS28]			✓
Uchi Ugobame Uchibeke et al [RS56]			✓
Dwiyan Rezkia Putra et al [RS29]			✓
Damiano Di Francesco Maesa et al [RS57]		✓	
Damiano Di Francesco Maesa et al [RS72]		✓	
Harsha S. Gardiyawasam Pussewalage et al [RS58]	✓		
Shuang Sun et al [RS31]			✓
Jin Sun et al [RS07]		✓	
Mathis Steichen et al [RS60]		✓	
BloCyNfo-Share [RS10]		✓	
CapChain [RS61]		✓	✓

Table 7 continued from previous page

Access Control Solution	Theoretic	Simulation	Prototype
ControlChain [RS73]	✓		
DAcc [RS32]			✓
DCACI [RS33]			✓
Leepakshi Bindra et al [RS34]	✓		
DACBBD [RS35]	✓		
Mayssa JEMEL et al [RS74]		✓	
DAM-Chain [RS64]	✓		
Sophie Dramè-Maignè et al [RS36]	✓		
DongYeop Hwang et al [RS62]	✓		
EACMS [RS37]			✓
Richa Gupta et al [RS05]	✓		
fabric-iot [RS06]		✓	✓
FADB [RS08]		✓	
GAA-FQ [RS59]		✓	
Sara Rouhani et al [RS65]		✓	
BDKMA [RS38]		✓	
RBAC-HDE [RS39]		✓	
RBAC-SC [RS66]			✓
Yuanyu Zhang et al [RS67]		✓	✓
SRBAC [RS30]	✓		
TBAC [RS68]	✓		
GUOHUA GAN et al [RS02]		✓	
TrustAccess [RS76]		✓	
Mirei Yutaka et al [RS40]		✓	
Oliver Stengele et al [RS48]		✓	
BACC [RS20]	✓		
Mayra Samaniego et al [RS49]			✓
Afnan Alniamy et al [RS19]		✓	

Table 7 continued from previous page

Access Control Solution	**Theoretic**	**Simulation**	**Prototype**
YongJoo Lee et al [RS50]		✓	
Chethana Dukkipati et al [RS71]	✓		
CapBAC [RS18]		✓	✓
Gabriel Nyame et al [RS16]			✓
Santiago Figueroa et al [RS46]		✓	
Tanzeela Sultana et al [RS17]		✓	
Yan Zhang et al [RS15]			✓
Yongjun Ren et al [RS47]			✓
Ancile [RS69]	✓		
BACS-IOD [RS04]		✓	✓
BCON [RS41]		✓	
BSeIn [RS70]		✓	
BACI [RS42]	✓		
Mohsin Ur Rahman et al [RS03]			✓
Nachiket Tapas et al [RS01]		✓	
SBAC [RS43]			✓
Lei Xu et al [RS45]			✓
CBACS-EIOT [RS21]		✓	
FairAccess [RS75]			✓
Thein Than Thwan et al [RS51]	✓		

We chose certain parameters based on their importance and relatability to our study, particularly with the idea of classifying access control systems on a broader level and context. We understand that the parameters can be added based on the relevance and after carefully examining the topic of study. In relevance with our topic, we chose the parameters that we found relevant to our study. We examined the blockchain platforms utilized by the access control systems and 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 Figure 4. Other than that, we also presented test-beds/tools used by each study based on whether the particular study has provided implementation or not. Based upon the type of solution presented by each access control system, we categorized the solutions in Table 7 and presented the whole taxonomy in Table 6.

6. Conclusions

Access control has proven time and again to be an equally important security feature like any other feature in every security system. Certainly, there are flaws with the traditional access control systems, and efforts are in place to overcome the issues one after the other. However, after the inception of blockchain technology, access control systems have started to prepare a different road-map of underlying and upcoming challenges to tackle. The due credit is to the inherently strong blockchain technology itself. In this paper, we presented a systematic literature review of blockchain-driven access control systems. In particular, we presented the relevant key findings from the available proposals and discussed the research themes in perspective and also shed light on them in accordance with their association to the targeted relevant studies. Furthermore, we 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 Hyperledger 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 to address IoT-based applications key security requirements. The field leaves a room for improvement in various directions, particularly in designing access control solutions relying on lightweight, scalable and post-quantum proof-of-works. The enhancement of the underlying blockchain based solutions to a more broader applications domains. A further area of improvement is towards preparation of a generalized evaluation framework covering aspects like security, scalability, lightweightness and proof-based access control systems. As part of the future work, we aim at building a lightweight, scalable, and reliable access control framework for resource constrained devices. Specifically, we aim at building a secure and lightweight consensus mechanism for post-quantum Blockchains, which will act as a building block for developing quantum resistant access control mechanisms.

7. Conflicts of Interest

The authors have no conflict of interest.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Tech. rep., Manubot (2019).

[2] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151 (2014) (2014) 1–32.

[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the thirteenth EuroSys conference, 2018, pp. 1–15.

[4] D. Schwartz, N. Youngs, A. Britto, et al., The ripple protocol consensus algorithm, Ripple Labs Inc White Paper 5 (8) (2014).

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PloS one 11 (10) (2016) e0163477.

[6] F. Casino, T. K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telematics and Informatics 36 (2019) 55–81.

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

[8] I. Riabi, H. K. B. Ayed, L. A. Saidane, A survey on blockchain based access control for internet of things, in: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, 2019, pp. 502–507.

[9] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering (2007).

[10] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, pp. 1–10.

Relevant Studies

[RS01] N. Tapas, F. Longo, G. Merlino, and A. Puliafito. Experimenting with smart contracts for access control and delegation in iot. *Future Generation Computer Systems*, 2020.

[RS02] G. Gan, E. Chen, Z. Zhou, and Y. Zhu. Token-based access control. *IEEE Access*, 8:54189–54199, 2020.

[RS03] M. U. Rahman, B. Guidi, and F. Baiardi. Blockchain-based access control management for decentralized online social networks. *Journal of Parallel and Distributed Computing*, 2020.

[RS04] B. Bera, D. Chattaraj, and A. K. Das. Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment. *Computer Communications*, 153:229–249, 2020.

[RS05] 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 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, pages 338–343, 2020.

[RS06] H. Liu, D. Han, and D. Li. Fabric-iot: A blockchain-based access control system in iot. *IEEE Access*, 8:18207–18218, 2020.

[RS07] J. Sun, X. Yao, S. Wang, and Y. Wu. Blockchain-based secure storage and access scheme for electronic medical records in ipfs. *IEEE Access*, 8:59389–59401, 2020.

[RS08] 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*, 8:85190–85203, 2020.

[RS09] 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*, 8:87552–87561, 2020.

[RS10] S. Badsha, I. Vakilinia, and S. Sengupta. Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0317–0323. IEEE, 2020.

[RS11] J. Arshad, M. A. B. Siddique, Z. Zulfiqar, A. Khokhar, S. Salim, T. Younas, A. U. Rehman, and A. Asad. A novel remote user authentication scheme by using private blockchain-based secure access control for agriculture monitoring. In *2020 International Conference on Engineering and Emerging Technologies (ICEET)*, pages 1–9. IEEE, 2020.

[RS12] L. Tan, N. Shi, C. Yang, and K. Yu. A blockchain-based access control framework for cyber-physical-social system big data. *IEEE Access*, 8:77215–77226, 2020.

[RS13] 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*, 8:70604–70615, 2020.

[RS14] T. Cai, Z. Yang, W. Chen, Z. Zheng, and Y. Yu. A blockchain-assisted trust access authentication system for solid. *IEEE Access*, 8:71605–71616, 2020.

[RS15] 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. *Electronics*, 9(2):285, 2020.

[RS16] G. Nyame, Z. Qin, K. O.-B. O. Agyekum, and E. B. Sifah. An ecdsa approach to access control in knowledge management systems using blockchain. *Information*, 11(2):111, 2020.

[RS17] 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. *Applied Sciences*, 10(2):488, 2020.

[RS18] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara. Exploiting smart contracts for capability-based access control in the internet of things. *Sensors*, 20(6):1793, 2020.

[RS19] A. Alniamy and B. D. Taylor. Attribute-based access control of data sharing based on hyperledger blockchain. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, pages 135–139, 2020.

[RS20] N. Sohrabi, X. Yi, Z. Tari, and I. Khalil. Bacc: Blockchain-based access control for cloud data. In *Proceedings of the Australasian Computer Science Week Multiconference*, pages 1–10, 2020.

[RS21] S. Saha, D. Chattaraj, B. Bera, and A. Kumar Das. Consortium blockchain-enabled access control mechanism in edge computing based generic internet of things environment. *Transactions on Emerging Telecommunications Technologies*, page e3995.

[RS22] I. Riabi, Y. Dhif, H. K. B. Ayed, and K. Zaatouri. A blockchain based access control for iot. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 2086–2091. IEEE, 2019.

[RS23] S. Ding, J. Cao, C. Li, K. Fan, and H. Li. A novel attribute-based access control scheme using blockchain for iot. *IEEE Access*, 7:38431–38441, 2019.

[RS24] M. A. Islam and S. Madria. A permissioned blockchain based access control system for iot. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 469–476, 2019.

[RS25] S. Wang, X. Wang, and Y. Zhang. A secure cloud storage framework with access control based on blockchain. *IEEE Access*, 7:112713–112725, 2019.

[RS26] P. Wang, Y. Yue, W. Sun, and J. Liu. An attribute-based distributed access control for blockchain-enabled iot. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–6, 2019.

[RS27] S. Ghaffaripour and A. Miri. Application of blockchain to patient-centric access control in medical data management systems. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0190–0196, 2019.

[RS28] 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 International Conference on Web Services (ICWS)*, pages 214–218. IEEE, 2019.

[RS29] D. R. Putra, B. Anggorojati, and A. P. P. Hartono. Blockchain and smart-contract for scalable access control in internet of things. In *10th International Conference on ICT for Smart Society, ICISS 2019*, page 8969807. Institute of Electrical and Electronics Engineers Inc., 2019.

[RS30] F. Sabrina. Blockchain and structural relationship based access control for iot: A smart city use case. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 137–140, 2019.

[RS31] 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 International Conference on Data Science in Cyberspace (DSC)*, pages 598–603, 2019.

[RS32] I. Markus, L. Xu, I. Subhod, and N. Nayab. Dacc: Decentralized ledger based access control for enterprise applications. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 345–351. IEEE, 2019.

[RS33] 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 on Internet of Things (WF-IoT)*, pages 13–18. IEEE, 2019.

[RS34] 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 International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, pages 32–38. IEEE, 2019.

[RS35] O. Mounnan, A. Abou El Kalam, and L. El Haourani. Decentralized access control infrastructure using blockchain for big data. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, pages 1–8. IEEE, 2019.

[RS36] 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)*, pages 1582–1587, 2019.

[RS37] A. R. Rajput, Q. Li, M. T. Ahvanooey, and I. Masood. Eacms: emergency access control management system for personal health record based on blockchain. *IEEE Access*, 7:84304–84317, 2019.

[RS38] 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*, 7:34045–34059, 2019.

[RS39] 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 International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, pages 1–2, 2019.

[RS40] 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 Global Communications Conference (GLOBECOM)*, pages 1–6, 2019.

[RS41] G. Ali, N. Ahmad, Y. Cao, Q. E. Ali, F. Azim, and H. Cruickshank. Bcon: Blockchain based access control across multiple conflict of interest domains. *Journal of Network and Computer Applications*, 147:102440, 2019.

[RS42] 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*, 86:318–334, 2019.

[RS43] 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. *Journal of Network and Computer Applications*, 149:102444, 2020.

[RS44] Y. Zhou, Y. Guan, Z. Zhang, and F. Li. A blockchain-based access control scheme for smart grids. In *2019 International Conference on Networking and Network Applications (NaNA)*, pages 368–373, 2019.

[RS45] L. Xu, I. Markus, S. I, and N. Nayab. Blockchain-based access control for enterprise blockchain applications. *International Journal of Network Management*, page e2089, 2019.

[RS46] S. Figueroa, J. Añorga, and S. Arrizabalaga. An attribute-based access control model in rfid systems based on blockchain decentralized applications for healthcare environments. *Computers*, 8(3):57, 2019.

[RS47] 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. *Applied Sciences*, 9(10):2058, 2019.

[RS48] O. Stengele, A. Baumeister, P. Birnstill, and H. Hartenstein. Access control for binary integrity protection using ethereum. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, pages 3–12, 2019.

[RS49] M. Samaniego, C. Espana, and R. Deters. Access control management for plant phenotyping using integrated blockchain. In *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*, pages 39–46, 2019.

[RS50] Y. Lee and K. M. Lee. Blockchain-based rbac for user authentication with anonymity. In *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, pages 289–294, 2019.

[RS51] T. T. Thwin and S. Vasupongayya. Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks*, 2019, 2019.

[RS52] I. Sukhodolskiy and S. Zapechnikov. A blockchain-based access control system for cloud storage. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 1575–1578. IEEE, 2018.

[RS53] 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*, 6:38437–38450, 2018.

[RS54] X. Tan, C. Huang, and L. Ji. Access control scheme based on combination of blockchain and xor-coding for icn. In *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pages 160–165, 2018.

[RS55] R. Xu, Y. Chen, E. Blasch, and G. Chen. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1027–1034. IEEE, 2018.

[RS56] U. Ugobame Uchibeke, K. A. Schneider, S. Hosseinzadeh Kassani, and R. Deters. Blockchain access control ecosystem for big data security. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1373–1378, 2018.

[RS57] D. D. F. Maesa, P. Mori, and L. Ricci. Blockchain based access control services. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1379–1386. IEEE, 2018.

[RS58] H. S. G. Pussewalage and V. A. Oleshchuk. Blockchain based delegatable access control scheme for a collaborative e-health environment. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1204–1211. IEEE, 2018.

[RS59] X. Zhang and S. Poslad. Blockchain support for flexible queries with granular access control to electronic medical records (emr). In *2018 IEEE International conference on communications (ICC)*, pages 1–6. IEEE, 2018.

[RS60] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State. Blockchain-based, decentralized access control for ipfs. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1499–1506. IEEE, 2018.

[RS61] T. Le and M. W. Mutka. Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 57–64. IEEE, 2018.

[RS62] D. Hwang, J. Choi, and K.-H. Kim. Dynamic access control scheme for iot devices using blockchain. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 713–715. IEEE, 2018.

[RS63] X. Zhang, S. Poslad, and Z. Ma. Block-based access control for blockchain-based electronic medical records (emrs) query in ehealth. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2018.

[RS64] 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 International Conference on Services Computing (SCC)*, pages 193–200. IEEE, 2018.

[RS65] S. Rouhani, V. Pourheidari, and R. Deters. Physical access control management system based on permissioned blockchain. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1078–1083, 2018.

[RS66] J. P. Cruz, Y. Kaji, and N. Yanai. Rbac-sc: Role-based access control using smart contract. *IEEE Access*, 6:12240–12251, 2018.

[RS67] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, 6(2):1594–1605, 2019.

[RS68] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, and W. C. 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)*, volume 01, pages 535–544, 2018.

[RS69] 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*, 39:283–297, 2018.

[RS70] 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*, 116:42–52, 2018.

[RS71] C. Dukkipati, Y. Zhang, and L. C. Cheng. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*, pages 61–69, 2018.

[RS72] D. D. F. Maesa, P. Mori, and L. Ricci. Blockchain based access control. In *IFIP international conference on distributed applications and interoperable systems*, pages 206–220. Springer, 2017.

[RS73] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.

[RS74] M. Jemel and A. Serhrouchni. Decentralized access control mechanism with temporal dimension based on blockchain. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pages 177–182, 2017.

[RS75] 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*, 9(18):5943–5964, 2016.

[RS76] 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 Transactions on Vehicular Technology*, 69(6):5784–5798, 2020.