Blockchain based access control systems: State of the art and challenges

Sara Rouhani*
sara.rouhani@usask.ca
Department of Computer Science
University of Saskatchewan
Saskatoon, SK, Canada

Ralph Deters
deters@cs.usask.ca
Department of Computer Science
University of Saskatchewan
Saskatoon, SK, Canada

ABSTRACT

Access control is a mechanism in computer security that regulates access to the system resources. The current access control systems face many problems, such as the presence of the third-party, inefficiency, and lack of privacy. These problems can be addressed by blockchain, the technology that received major attention in recent years and has many potentials. In this study, we overview the problems of the current access control systems, and then, we explain how blockchain can help to solve them. We also present an overview of access control studies and proposed platforms in the different domains. This paper presents the state of the art and the challenges of blockchain-based access control systems.

KEYWORDS

blockchain, access control, distributed, privacy

ACM Reference Format:
Sara Rouhani and Ralph Deters. 2019. Blockchain based access control systems: State of the art and challenges. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI '19), October 14–17, 2019, Thessaloniki, Greece.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3350546.3352561

1 INTRODUCTION

Blockchain applications initially were limited to the cryptocurrencies and financial transactions. Invention of smart contracts leads to development of more divers applications [10], such as healthcare [5, 14, 42, 52], IoT [16, 21, 38, 41, 46, 47], supply chain [8, 12, 29]. In our previous study [43], after reviewing many research studies based on blockchain and smart contracts, we noticed that the primary focus of many presented applications is providing an efficient and secure access control mechanism.

Access control is a required security part of almost all applications. Blockchain specific characteristics such as immutability, durability, auditability, and reliability lead to considering blockchain as a supplementary solution for access control systems.

Access control systems are applied to regulate access to the system's resources and it is the fundamental part of computer security. Access control is usually enforced against a set of authorization based on system policies.

In this study we aim to provide the answer for following questions.

- What are the problems with current access control systems?
- How blockchain can help to solve these problems?
- What are the challenges for implementing an access control system based on blockchain?
- What are the gaps in the related studies?

In Section two, we investigate current access control systems problems and explain how blockchain can address them. We overview the related research studies and categorize them based on different domains and applied access control method in section three. In section four, we discuss the challenges of implementing an access control system using blockchain. Finally, in section five, we present the summary of the paper. We aim to provide a comprehensive picture with the details of architecture, implementation, and the challenges.

2 TRADITIONAL ACCESS CONTROL SYSTEM PROBLEMS AND BLOCKCHAIN KEY BENEFITS

In this section, we discuss the problems of current access control systems and how we can address them with blockchain.

Jemel et al. [28] mention a couple of problems in centralized access control systems. As there is a third party, which has access to the data, the risk of privacy leakage exists. Also, a central party is in charge to control the access, so the risk of single point of failure also exists. This study presents an access control mechanism with a temporal dimension to solve these problems and adapts a blockchain-based solution for verifying access permissions.

Attribute-based Encryption method [45] also has some problems such as privacy leakage from the private key generator (PKG) [27] and single point of failure as mentioned before. Wang et al. [51] introduce a framework for data sharing and access control to address this problem by implementing decentralized storage.

Current solutions for managing access control in multi administrative domains are not efficient. Based on Paillisse et al. [40] static approaches are not scalable and granular and PKI-based systems are difficult to manage. They suggest distributing and recording access policies in a permissioned blockchain. Conifer [20] is also another PKI system based on blockchain to achieve security without trusted third parties.

In cloud federation also sharing data between multiple organization is a concern from users privacy perspective [2]. Keeping the

WI '19, October 14–17, 2019, Thessaloniki, Greece

ACM ISBN 978-1-4503-6934-3/19/10…$15.00
https://doi.org/10.1145/3350546.3352561

personal data related to the users' identities private, while giving them access to the shared data, is the main concern. Alansari et al. propose an attribute-based access control system based on symmetric key encryption. The system checks users attributes with access control policies to grant access permissions to the data belong to the federated organization, while it keeps the users attribute private from the federated organization. This study suggests blockchain and trusted execution environment to preserve the integrity of the policy evaluation process.

The users of mobile applications always concern about privacy issues as they usually must give access to their private information. Enigma is an access control management system based on Ethereum blockchain which aims to solve this problem [60]. The presented framework addresses three main concerns: data ownership, data transparency & auditability, and fine-grained access control. The system is designed in a way that users are able to control their own personal data and make the process of access to their data transparent. Also, the users can modify or revoke access permissions to their personal data without uninstalling the mobile application. Figure 1 shows the overview of Enigma framework. The system also contains three distributed databases: a blockchain, a Distributed Hash Table (DHT), and a Multi-Party Computation (MPC), which fragments data into smaller meaningless chunks and distribute it between nodes without replication.

Privacy is not only a problem for the users of the mobile applications, in many access control systems the privacy is not guaranteed when the users grant access to their personal information in order to obtain access to the specific service or share resources. Table one shows research studies that aim to solve the privacy problem in an access control system using blockchain technology.

3 BLOCKCHAIN-BASED ACCESS CONTROL SYSTEM

Blockchain has desirable features that make it a trustable alternative infrastructure for access control systems. The distributed nature of blockchain solves the problem of single point of failure and other centralized management problems. Also, by eliminating third parties, we do not need to be concern about privacy leakage from their side. In addition, we can access to a trustable and unmodifiable history logs. Consensus mechanisms are applied, so only valid transactions are recorded on blockchain. Furthermore, by using smart contracts, we can monitor and enforce access permissions under complex conditions. All of these features have motivated researchers to consider blockchain as an infrastructure for access control systems.

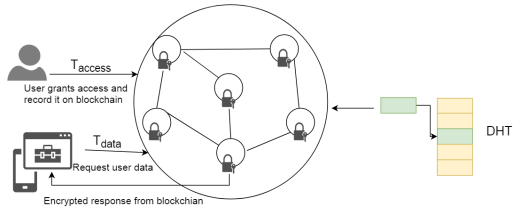

Figure 1: Enigma framework [60]

Table 1: Privacy based research studies

Paper	Privacy Context
Zyskind et al. [60]	Mobile applications.
Alansari et al. [1, 2]	Cloud federation
Ouaddah et al. [39], Pinno et al. [41], Dukkipati [21], Ma et al. [34]	Personal data generated by IoT devices
Dagher et al. [14], Azaria et al. [5], Xia et al. [52]	Healthcare patients data
Le and Mutka [30]	Pervasive environment
Xu et al. [54]	sharing economy applications using public blockchain
Yao et al. [56]	Certificate validation
Es-Samaali and Outchakoucht [22]	Big Data

This section overviews blockchain-based access control studies and decentralized applications. Table 2 shows the these studies classified in different domains, their access control method and their applied blockchain platform.

3.1 Blockchain-based access control from transactions to smart contracts

Maesa et al. [35] initially represented a system by extending Bitcoin, which users can transparently observe access control policies on resources. This study uses attribute-based access control mechanism and eXtensible Access Control Markup Language (XACML) to define policies [24] and store arbitrary data on Bitcoin. They used OP-RETURN script opcode and MULTISIG transactions [49]. In their next study, they considered smart contracts to enforce access control policies instead of simple transactions [17]. They have implemented a proof of concept using XACML policies and Ethereum platform. In their recent study [36], they have added more details and completed their previous works by explaining how the components of an access control system can be adopted in blockchain infrastructure. Also, in order to evaluate the feasibility and performance of the represented system, they have defined a scenario where smart contracts are considered as resources that need to be protected and access to them is restricted. By employing smart contracts, they were able to add more flexibility, details, and efficiency to their implemented system.

3.2 Data sharing access control

Jemel and Serhrouchni [28] suggest using blockchain as an infrastructure for shared data access control management system. A proof of concept has been implemented using Multichain platform and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) access control schema [6]. The analysis result indicates that timely CP-ABE performs better in terms of performance in comparison with timely access control list. As we expected, timely CP-ABE implementation without blockchain is more efficient than blockchain-based solutions, but using blockchain provides security and privacy benefits such as auditing, non-repudiation, as well as no single point of failure.

Table 2: A summary of blockchain-based access control applications

Research paper	Domain	Access control method	Blockchain platform
Maesa et al. [35]	General access control	Attribute-based	Bitcoin
Maesa et al. [17]	General access control	attribute-based	Ethereum
Jemel and Serhrouchni [28]	Data sharing	Attribute-based Encryption	MultiChain
Wang et al. [51]	Data sharing	Attribute-based Encryption	Ethereum
Zhu et al. [58]	Resource sharing	attribute-based	Bitcoin
Hu et al. [26]	Knowledge sharing	Fine-grained	-
Zhu et al . [59]	Digital asset management	Attribute-based	Bitcoin
Ferdous et al. [23]	Cloud federation	-	Hyperledger Fabric
Alansari et al. [2]	Cloud federation	Attribute-base	-
Zhang and Posland [57]	Electronic Medical Record (EMR)	Granular attribute-based	-
Rouhani et al. [42]	Medical data sharing (MediCHain)	Role-based	Hyperledger Fabric
Asaph et al. [5]	Medical data sharing (MedRec)	Fine-grined	Ethereum
Xia et al. [52]	Medical data sharing (MedShare)	-	Bitcoin
Dagher et al. [14]	Medical data sharing (Ancile)	Role-based	Ethereum
Novo [37]	IoT	-	Private Ethereum
Deters [16]	IoT	-	MultiChain
Dukkipati et al. [21]	IoT	Attribute-based	-
Pinno et al. [41]	IoT (ControlChain)	attribute-based	-
Ouaddah et al. [38]	IoT (FairAccess)	Generic	Bitcoin
Rouhani et al. [44]	Physical access control	Role-based	Hyperledger Fabric
Es-Samaali [22]	Big data management	Attribute-based	Bitcoin
Stanciu [50]	Edge computing	-	Hyperledger Fabric
Paillisse et al[40]	Multi-administrative domain	-	Hyperledger Fabric
Maesa et al. [36]	General access control	Attribute-based	Ethereum
Ding et al. [19]	IoT	Attribute-based	Hyperledger Fabric
Ma et al. [34]	IoT	General access control	Multiblockchain
Samaniego et al. [48]	Plant Phenotyping data	General access control	Ethereum

Wang et al. [51] introduce a framework for data sharing and access control. The framework includes IPFS decentralized storage system, Ethereum blockchain, and Attribute-Based Encryption (ABE). The only one who has access to the secret key is the data owner. Ethereum blockchain has been applied for managing the private keys. There are two main smart contracts: data sharing contract that is deployed by the data owner and includes methods to register a user who need access to the specific data belong to the owner of the contract and dataUser contract that is deployed by data requester to invoke the search function defined in data sharing contract to view the search results.

Similarly, Hu et al. [26] propose a Reputation Based Knowledge Sharing system to protect the copyright using fine-grained access control. The system includes three main roles: Questioner, Answerer, and Bystander. The Questioner is the one who designs a question. The answerer is one who is an expert to answer the question and receives rewards from Bystander. The Bystander is the one who is willing to pay a small fee in order to get access to the shared knowledge.

3.3 Access control for cloud federation

Ferdous et al. present a Decentralised Runtime Access Monitoring System (DRAMS) to guarantee the reliability of the access control component in cloud federations dynamically [23]. The represented architecture comprises three components: Logger, Smart contract, and Analyser. Logger component includes "Probing agents" records and forwards data to generate access logs and "Logging interface (LI)". Smart contracts capture logs and carry out monitoring by comparing logs to create dynamic access permissions. Analyzer investigates access permissions based on the system policies.

Similarly, Alansari et al. [2] present an identity and access control management framework for cloud federation while keeps the attributes related to the users' identity private by using the OCBE protocol [31]. Although the federation party, which owns the data, do not have access to the users' attributes, the user can access the requested data if the user has access to the data based on the system policy. The paper suggests the combination of blockchain and Intel SGX (Trusted Execution Environment) [53] for maintaining the integrity of the system. The users' identity attributes and the system access control policies are managed through smart contract and stored on blockchain. The encrypted data should be stored off-chain and in order to preserve the integrity, the cryptographic policy protocol runs in the trusted environment.

3.4 Access control across multiple organizations

Cruz et al. [13] have designed a platform for role based access control to utilize across multiple organization using Ethereum blockchain and Solidity smart contracts. It has implemented a smart contract to initialize the roles and the challenge-response protocol to authenticate the ownership of roles and user verification. The smart contract includes the following functions:

addUsert(u.EOA, u.role, u.notes) and removeUser(u.EOA) to assign a role to or revoke a role from the specific user identified by EOA (Externally owned Account or public key in Ethereum). addEndorser(eu.EOA, eu.notes) and removeEndorser(eu.EOA) to add and remove endorser and function changeStatus() to change the status of deactivated smart contracts.

Challenge-response protocol is utilized for the authentication of the users, who request a service from another organization based on her/his role. This protocol has five steps: declaration, information check, challenge response, and response verification. In summary, a user requests a service corresponding to his/her own roles from another organization. After initial information check, the organization sends an arbitrary data and ask the user to sign it and user responses with the signature. Finally, the authentication confirms after receiving valid signature.

3.5 Access control for shared blockchains

ChainAchor [25] is a blockchain platform that enforces access control for users who submit transactions. This paper introduces ChainAchor as a platform to solve the problem of identity and access control in the shared permissioned blockchains. Shared permissioned blockchain is a permissioned blockchain that is shared between multiple distinct organizations. Identity privacy, access control, and optional disclosure & transaction privacy are challenging issues in shared permissioned blockchains. ChainAnchor consensus method looks for the public-key of the sender of the transaction in a database include all the identities information and it forces access control based on that. The identities of the users are anonymous completely and cannot be disclosed by anyone in the system.

3.6 Access control and self-Sovereign identities

Users of digital identity systems suffer from lacks of privacy. When they request a service, for proving their identities, all the metadata attached to their digital identities become accessible to service provider. In self-sovereign identity system, the owners of digital identities are able to control the data related to their digital identities and their personal data attach to them using blockchain. Yan et al. [55] present a hierarchical secret sharing scheme for general access structure in blockchain to achieve self-sovereign digital identity metadata sharing. Finally, the paper introduces blockchain as a ledger for openPDS (Open Personal Data Store) [15].

4 CHALLENGE DISCUSSION

This section discusses the existing challenges and possible solutions.

Off-chain and on-chain integration: Blockchain is not a suitable structure for storing a big volume of data, so, the data must store in secure off-chain storage and the access policies, the hash of the data, and references to the data record on blockchain. The secure integration between on-chain and off-chain is challenging. Using trusted hardware technology such as intel SGX can be considered to keep the integrity of the system.

Blockchain vulnerability: Besides all the attractive advantages of blockchain, it is still difficult to implement non-vulnerable smart contracts [33]. Subsequently, designing methods and tools to improve the security of smart contracts and blockchain is one of the most competitive fields in blockchain [3, 7, 9].

Transaction transparency: One of the main reasons that blockchain became popular was providing transactional transparency; however, this is not desirable from the enterprise perspective and privacy point of view. That is why we have observed the advent of permissioned platforms, which support transaction privacy and private data. This sacrifices pure decentralization and adopt hybrid centralized and decentralized solutions.

Performance: Blockchain stores all the recorded transactions and data on all peers. The performance of execution and validation of transactions have been improved recently by introducing lighter consensus mechanism and more efficient transaction processing flow in blockchain platforms such as Hyperledger Fabric. Despite recent studies in improving the performance of blockchain [4, 18] still, the performance of the blockchain-based solutions cannot compete with the current centralized solutions. As we can see most of the studies compare the performance of their presented system with other blockchain-based platforms, not current decentralized solutions. In order to solve the performance and scalability problem, Ma et al. [34] suggest an architecture based on multiple blockchains on cloud environment. The represented architecture consists of multiple layers, including device layer, edge networking layer, fog layer, core network layer, and cloud layer. Simulations results indicate that balancing the load of block mining into multiple layers improves the performance of the system by reducing the transaction collection time and block mining time.

Access control methods: Current access control methods which are static might be inadequate for future systems [11] and more dynamic access control methods, one in which resources define their own access control, might be required. Integrating blockchain with dynamic access control approaches could be an interesting area to investigate in the future.

5 SUMMARY AND FUTURE WORKS

In this paper, we explained the required concepts related to blockchain, smart contracts, platforms, and access control methods. The problem of the current access control systems and how blockchain features can solve these problems have been discussed.

Represented blockchain-based access control architectures and systems have been classified based on domain, access control method, and blockchain platforms. These systems have been tailored based on system requirements. These studies [5, 35, 42, 51] have focused on designing a user-centric system, which owners of the data can define and enforce access control policies directly. [23, 36] systems have focused on auditability characteristic and trusted logging provided by blockchain to design a reliable access control system. From the transactional perspective, [28, 35, 59] use only transactions to store access control attributes on blockchain, while [2, 13, 17, 22, 23, 26, 36, 39, 42, 51, 52] applied smart contracts to exploit its advantages such as flexibility and automatically enforcing access control policies. Also, the challenges and future directions have been discussed in this paper.

In our future work, we plan to present an access control service oriented [32] architecture and implementation based on blockchain.

REFERENCES

[1] Shorouq Alansari, Federica Paci, Andrea Margheri, and Vladimiro Sassone. 2017. Privacy-preserving access control in cloud federations. In *Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on*. IEEE, 757–760.

[2] Shorouq Alansari, Federica Paci, and Vladimiro Sassone. 2017. A distributed access control system for cloud federations. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2131–2136.

[3] Sidney Amani, Myriam Bégel, Maksym Bortin, and Mark Staples. 2018. Towards verifying ethereum smart contract bytecode in Isabelle/HOL. In *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs*. ACM, 66–77.

[4] Parwat Singh Anjana, Sweta Kumari, Sathya Peri, Sachin Rathor, and Archit Somani. 2018. An Efficient Framework for Concurrent Execution of Smart Contracts. *arXiv preprint arXiv:1809.01326* (2018).

[5] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. In *Open and Big Data (OBD), International Conference on*. IEEE, 25–30.

[6] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 321–334.

[7] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova, Aseem Rastogi, Thomas Sibut-Pinote, Nikhil Swamy, et al. 2016. Formal verification of smart contracts: Short paper. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*. ACM, 91–96.

[8] Thomas Bocek, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller. 2017. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 772–777.

[9] Santiago Bragagnolo, Henrique Rocha, Marcus Denker, and Stéphane Ducasse. 2018. SmartInspect: solidity smart contract inspector. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 9–18.

[10] Wei Cai, Zehua Wang, Jason B Ernst, Zhen Hong, Chen Feng, and Victor CM Leung. 2018. Decentralized applications: The blockchain-empowered software system. *IEEE Access* 6 (2018), 53019–53033.

[11] Seraphin Calo, Dinesh Verma, Supriyo Chakraborty, Elisa Bertino, Emil Lupu, and Gregory Cirincione. 2018. Self-Generation of Access Control Policies. (2018), 39–47.

[12] Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang. 2017. A blockchain-based supply chain quality management framework. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*. IEEE, 172–176.

[13] Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. 2018. RBAC-SC: Role-Based Access Control Using Smart Contract. *IEEE Access* 6 (2018), 12240–12251.

[14] Gaby G Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society* 39 (2018), 283–297.

[15] Yves-Alexandre De Montjoye, Erez Shmueli, Samuel S Wang, and Alex Sandy Pentland. 2014. openpds: Protecting the privacy of metadata through safeanswers. *PloS one* 9, 7 (2014), e98790.

[16] Ralph Deters. 2017. Decentralized Access Control with Distributed Ledgers. *University of Saskatchewan Cloud Robotics* (2017).

[17] Damiano DI FRANCESCO MAESA, Paolo Mori, and LAURA EMILIA Ricci. 2018. Blockchain based access control services. In *IEEE Symposium on Recent Advances on Blockchain and its Applications, Canada,*.

[18] Thomas Dickerson, Paul Gazzillo, Maurice Herlihy, and Eric Koskinen. 2017. Adding concurrency to smart contracts. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*. ACM, 303–312.

[19] Sheng Ding, Jin Cao, Chen Li, Kai Fan, and Hui Li. 2019. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access* 7 (2019), 38431–38441.

[20] Yuhao Dong, Woojung Kim, and Raouf Boutaba. 2018. Conifer: centrally-managed PKI with blockchain-rooted trust. In *IEEE International Conference on Blockchain (Blockchain)*.

[21] Chethana Dukkipati, Yunpeng Zhang, and Liang Chieh Cheng. 2018. Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. ACM, 61–69.

[22] Hamza Es-Samaali, Aissam Outchakoucht, and J. P. Leroy. 2017. A Blockchain-based Access Control for Big Data.

[23] Md Sadek Ferdous, Andrea Margheri, Federica Paci, Mu Yang, and Vladimiro Sassone. 2017. Decentralised runtime monitoring for access control systems in cloud federations. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2632–2633.

[24] Simon Godik and Tim Moses. 2002. Oasis extensible access control markup language (xacml). *OASIS Committee Secification cs-xacml-specification-1.0* (2002).

[25] Thomas Hardjono and Alex Sandy Pentland. 2016. Verifiable Anonymous Identities and Access Control in Permissioned Blockchains. *manuscript in preparation* (2016).

[26] Shuang Hu, Lin Hou, Gongliang Chen, Jian Weng, and Jianhua Li. 2018. Reputation-based Distributed Knowledge Sharing System in Blockchain. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 476–481.

[27] Junbeom Hur and Dong Kun Noh. 2011. Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Transactions on Parallel and Distributed Systems* 22, 7 (2011), 1214–1221.

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

[29] Kari Korpela, Jukka Hallikas, and Tomi Dahlberg. 2017. Digital supply chain transformation toward blockchain integration. In *proceedings of the 50th Hawaii international conference on system sciences*.

[30] Tam Le and Matt W Mutka. 2018. CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 57–64.

[31] Jiangtao Li and Ninghui Li. 2006. OACerts: Oblivious attribute certificates. *IEEE Transactions on Dependable and Secure Computing* 3, 4 (2006), 340–352.

[32] Dong Liu and Ralph Deters. 2008. Management of service-oriented systems. *Service Oriented Computing and Applications* 2, 2-3 (2008), 51–64.

[33] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 254–269.

[34] Mingxin Ma, Guozhen Shi, and Fenghua Li. 2019. Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. *IEEE Access* 7 (2019), 34045–34059.

[35] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. 2017. Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems*. Springer, 206–220.

[36] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. 2019. A blockchain based approach for the definition of auditable Access Control systems. *Computers & Security* (2019).

[37] Oscar Novo. 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal* 5, 2 (2018), 1184–1195.

[38] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks* 9, 18 (2016), 5943–5964.

[39] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2017. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Springer, 523–533.

[40] Jordi Paillisse, jordi Subira, Alber Lopez, Alberto Rodriguez-Natal, Vina Ermagan, Fabio Maino, and Albert Cabellos. 2019. Distributed Access Control with Blockchain. *arXiv preprint arXiv:1901.03568* (2019).

[41] Otto Julio Ahlert Pinno, Andre Ricardo Abed Gregio, and Luis CE De Bona. 2017. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 1–6.

[42] S. Rouhani, L. Butterworth, A. D. Dimmond, D. G. Humphery, and R. Deters. 2018. MediChainTM: A Secure Decentralized Medical Data Asset Management System. 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)*. IEEE, 14757–14767.

[43] Sara Rouhani and Ralph Deters. 2019. Security, Performance, and Applications of Smart Contracts: A Systematic Survey. *IEEE ACCESS* 7 (2019), 50759–50779.

[44] Sara Rouhani, Vahid pourheidari, and Ralph Deters. 2018. 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)*. IEEE, 1078–1083.

[45] Amit Sahai and Brent Waters. 2005. Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 457–473.

[46] Mayra Samaniego and Ralph Deters. 2016. Blockchain as a Service for IoT. In *2016 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)*. IEEE, 433–436.

[47] Mayra Samaniego and Ralph Deters. 2017. Internet of smart things-iost: Using blockchain and clips to make things autonomous. In *2017 IEEE international conference on cognitive computing (ICCC)*. IEEE, 9–16.

[48] Mayra Samaniego, Cristian Espana, and Ralph Deters. 2019. Access Control Management for Plant Phenotyping Using Integrated Blockchain. In *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*. ACM, 39–46.

[49] Ken Shirriff. 2014. Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software. *Ken Shirriff's blog (accessed July 2017) http://www. righto. com/2014/02/ascii-bernanke-wikileaks-photographs. html* (2014).

[50] Alexandru Stanciu. 2017. Blockchain based distributed control system for edge computing. In *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 667–671.

[51] Shangping Wang, Yinglong Zhang, and Yaling Zhang. 2018. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access* 6 (2018), 38437–38450.

[52] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* 5 (2017), 14757–14767.

[53] Bin Cedric Xing, Mark Shanahan, and Rebekah Leslie-Hurd. 2016. Intel® Software Guard Extensions (Intel® SGX) Software Support for Dynamic Memory Allocation inside an Enclave. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*. ACM, 11.

[54] Lei Xu, Nolan Shah, Lin Chen, Nour Diallo, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. Enabling the sharing economy: Privacy respecting contract based on public blockchain. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 15–21.

[55] Zhu Yan, Guhua Gan, and Khaled Riad. 2017. BC-PDS: protecting privacy and self-sovereignty through BlockChains for OpenPDS. In *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. IEEE, 138–144.

[56] Shixiong Yao, Jing Chen, Kun He, Ruiying Du, Tianqing Zhu, and Xin Chen. 2019. PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management. *IEEE Access* 7 (2019), 6117–6128.

[57] Xiaoshuai Zhang and Stefan Poslad. 2018. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). In *2018 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[58] Yan Zhu, Yao Qin, Guohua Gan, Yang Shuai, and William Cheng-Chung Chu. 2018. 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)*, Vol. 1. IEEE, 535–544.

[59] Yan Zhu, Yao Qin, Zhiyuan Zhou, Xiaoxu Song, Guowei Liu, and William Cheng-Chung Chu. 2018. Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control. In *2018 IEEE International Conference on Services Computing (SCC)*. IEEE, 193–200.

[60] Guy Zyskind, Oz Nathan, et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 180–184.