Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems

Mongetro Goint, Cyrille Bertelle, Claude Duvallet

mathematics

MDPI

Article

Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems

Mongetro Goint *, Cyrille Bertelle and Claude Duvallet

LITIS, Université Le Havre Normandie, UR 4108, Le Havre, F-76000 Rouen, France; cyrille.bertelle@univ-lehavre.fr (C.B.); claude.duvallet@univ-lehavre.fr (C.D.)
* Correspondence: mongetro.goint@univ-lehavre.fr

Abstract: Data access control is a crucial aspect of data management. Actors who want to share data need systems to manage consent in order to decide who can access their data. This guarantees the privacy of data, which is often sensitive. As a secure distributed ledger, the blockchain is widely used today to manage consent for data access. However, a blockchain is not ideal for storing large volumes of data due to its characteristics. Therefore, it is often coupled with off-chain systems to facilitate the storage of these kinds of data. Therefore, data located outside the blockchain require security procedures. This article proposes a securing mechanism based on data encryption to secure data in off-chain storage in blockchain-based consent systems. The protocol uses a symmetric key system, which prevents the reading of data stored outside the sphere of the blockchain by malicious actors who would have access. The mechanism's set up allows each set of data to be encrypted with a symmetric key that is anchored in a blockchain. This key is then used by the actors who have obtained the consent of the data owner to access and read the data stored outside the blockchain.

Keywords: blockchain; data access; smart contracts; data encryption; distributed ledger

MSC: 68P27

Citation: Goint, M.; Bertelle, C.; Duvallet, C. Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems. *Mathematics* **2023**, *11*, 1592. https://doi.org/10.3390/math11071592

Academic Editor: Jan Lansky

Received: 17 February 2023
Revised: 16 March 2023
Accepted: 20 March 2023
Published: 25 March 2023

1. Introduction

Data sharing is widely regarded as one of the most advantageous aspects of cloud computing. It enables collaborative ecosystems for exchanging information between various parties operating within the same domain. The benefits of data sharing are numerous, as data can be accessed and used by an unlimited number of actors concurrently without losing value or being altered. Numerous research studies have consistently demonstrated the benefits of data sharing [1–3]. Data sharing can facilitate business collaboration, enhance the quality of scientific research, and improve the services offered to users within a system, among other benefits.

Effective management of data is crucial to realizing the benefits of data sharing. Aspects such as privacy, security, and transparency in data management are of increasing concern to data owners, as they seek to ensure that their data are not accessed or utilized without their consent. In addition, companies operating within the same ecosystem may be hesitant to share their data freely due to concerns around competition and other factors. As such, obtaining consent for data access is not only an ethical imperative, but also a legal requirement in many cases [4].

Blockchain technology is increasingly being leveraged to build consent management systems for data access due to its unique intrinsic characteristics. Decentralization, security, transparency, and tamper-proofing are among the key features that make blockchain an ideal technology for managing consent in the data-sharing process. Numerous research studies have demonstrated the effectiveness of the blockchain in setting up consent management systems for data access [5–9]. In a previous research endeavor, we proposed a consent management system for smart territories based on blockchain technology [10]. Consent

management mechanisms generally involve enabling data owners to define an agreement between themselves and potential data accessors, outlining the terms and conditions of data access. By leveraging blockchain technology, these agreements (or consents) can be securely and transparently stored on a tamper-proof ledger. This ensures that the agreement cannot be altered or modified without the knowledge and permission of all parties involved, thus ensuring that data access is governed by a secure and trusted mechanism.

While blockchain is an effective mechanism for securely storing and managing data access consents, it is not always an ideal choice for storing large amounts of data. One of the key challenges of blockchain technology is scalability [11,12], and the transaction costs in a blockchain are also relatively high [13] compared to the volume of data to be stored. To address the challenges associated with storing large amounts of data on the blockchain, it is common practice to couple blockchain technology with off-chain storage systems. In this approach, the blockchain is used to securely manage data access consent, while the actual data are stored in a separate off-chain system. This implies that the blockchain does not necessarily secure the actual data in the off-chain storage system. Therefore, it is necessary to apply strict security mechanisms for data protection in the off-chain system, which will be shared among multiple actors.

The purpose of this article is to propose a data encryption-based security mechanism for off-chain storage in blockchain-based consent systems. The proposed protocol utilizes symmetric key encryption [14,15] to protect data stored off-chain. The symmetric key is securely anchored in the blockchain register and is only used to decrypt the data in the off-chain storage and make them accessible to the authorized data accessor after verifying the established consent. This mechanism provides an additional layer of security to the consent management mechanisms, protecting the data from malicious actors who have not received permission from the data owner. By coupling this encryption-based security mechanism with the consent management mechanisms, the proposed process provides a robust security framework for data access.

The rest of this article is structured as follows: In Section 2, we introduce blockchain technology and provide an overview of how it works. We also discuss the concept of smart contracts. Section 3 focuses on the role of the blockchain in consent management for data access. In Section 4, we propose a data encryption-based security mechanism for securing data access control in off-chain storage. Finally, in Section 5, we conclude the article.

2. Blockchain Overview

Initially developed for the financial sector, specifically the domain of cryptocurrencies, blockchain technology was introduced by Satoshi Nakamoto in 2008 [16]. Blockchain is a secure distributed ledger designed for peer-to-peer digital asset transactions. Public blockchains, which are the first generation of blockchains, are distributed and secure ledgers accessible to all participants. The ledger is shared among all nodes and contains all transactions carried out on the network since its creation, with each node maintaining a copy.

All transactions in a blockchain network are grouped in structures called blocks (cf. Figure 1). To each block created, a hash function is applied, which returns a hash (signature) of all data of the block. Hash function works so that it is impossible to find two distinct inputs that hash the same value. Transactions added in a block on the blockchain are immutable, secure, and verified by the network using cryptography. The hash of the previous block is saved in each current block of the distributed register. This prevents malicious activities, such as modifying a block of transactions. All blocks are then arranged chronologically to form an unalterable chain, as shown in Figure 1.

Blockchains use consensus algorithms to validate transactions, create blocks, and maintain a consistent register. There are several consensus mechanisms in use within the blockchain ecosystem, including Proof of Work (PoW), which is used in various blockchains such as Bitcoin [17]. Ethereum [18] also initially used PoW, and did so until September 2022. Additionally, there are other consensus mechanisms such as Proof of Authority (PoA) and Proof of Stake (PoS), which is currently used by Ethereum [19].

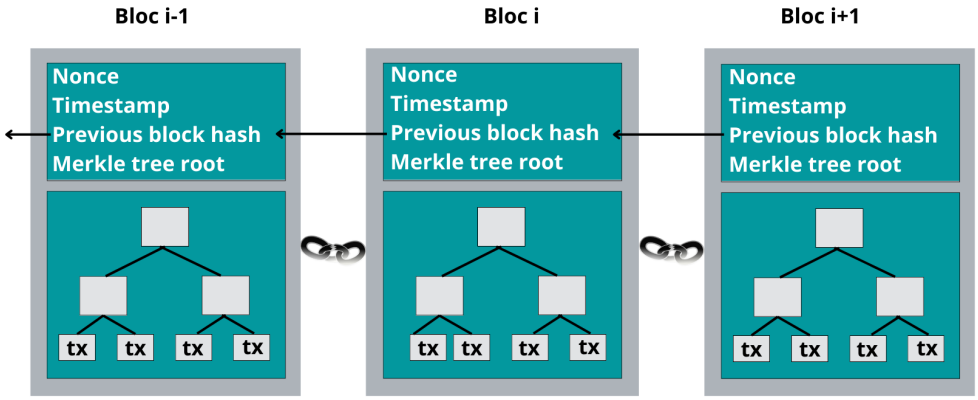

Figure 1. Storage of blocks in a blockchain.

Currently, blockchains can mainly be categorized according to their level of accessibility. Public blockchains, such as Bitcoin [16] and Ethereum [18], are one such category. In public blockchains, the protocol is determined by the entire network of actors, and anyone can access and view the ledger, as all transactions are public. Conversely, permissioned blockchains allow only authorized actors to participate in the network's operation, with transactions, block creation, and validation governed by specific conditions or permissions. The protocol of permissioned blockchains is defined by a restricted community. Private blockchains have their governance limited to a single actor who must approve and declare participants, with the ability to unilaterally change the network protocol. Access to and use of such blockchains is restricted to external users.

Smart Contracts

The concept of smart contracts was originally theorized by scientist Nick Szabo [20] and was subsequently implemented by Vitalik Buterin in the Ethereum blockchain [18]. This represented a significant milestone in the development of blockchain technology.

A smart contract in blockchain (Ethereum particularly) is a program that executes on the blockchain when predefined conditions are met. It consists of a collection of computer code and data, registered at a specific address on the network [18]. To deploy a smart contract, a user must sponsor it using their account on the blockchain. Once that is done, the user can then interact with it by submitting transactions based on the functions defined in the contract. Smart contracts are able to define rules, like a regular contract, but electronically https://ethereum.org/en/developers/docs/smart-contracts/, accessed on 14 January 2023. With the integration of smart contracts, Ethereum promotes the development of new generations of decentralized applications, commonly called DApps https://ethereum.org/fr/developers/docs/dapps/, accessed on 14 January 2023.

While blockchain technology was originally developed to enable the functioning of cryptocurrencies, it has evolved to serve a broader range of use cases. Blockchain now enables the storage and transmission of data in a decentralized, secure, and transparent manner. This has been made possible, in part, by the introduction of smart contracts on the Ethereum network by Vitalik Buterin [18]. Blockchain technology has been used for years in many areas such as personal data protection [21], Internet of Things [5], the healthcare system [6,22–25], the food industry [26], the maritime industry [27], etc.

3. How Blockchain Participates in Consent Management for Data Access

Blockchain technology is widely used for building consent management systems to control data access. This is particularly useful for securing access rights when sharing data. Below, we describe what consent is in the context of blockchain-based systems. Next, we enumerate a list of works using blockchain for consent management for data access, with different approaches. In addition, we discuss our positioning and our contribution to these existing solutions.

3.1. What Is Digital Consent?

Consent refers to the explicit permission given by an individual or organization for the processing and sharing of their personal data. It is a fundamental aspect of data management and is essential for accessing, processing, and sharing data securely and with integrity. The consent process ensures the privacy and security of user data, protecting individuals' rights and preventing unauthorized access to sensitive information [4]. In many ways, digital consent can be compared to a traditional agreement signed between two parties and certified by a notary. However, digital consent is a more complex process that requires a secure and tamper-proof system to act as a trusted third party. In the context of data access, a consent may contain specific items and conditions, such as those described in Table 1.

Table 1. Consent representation.

Attribute	Description
Data owner's ID	Data owner identifier (blockchain wallet address)
Data accessor's ID	Data accessor identifier (blockchain wallet address)
Data ID	A unique identifier for a dataset
Data access conditions	Conditions 1, Conditions 2, Conditions 3, ...

Blockchain, with its original characteristics, especially the immutability of the data stored on it, is now being widely recognized as an effective tool for acting as a notary to certify digital consent. Several works propose using blockchain as a consent management device (as described in Section 3.2). With a consent defined between two parties and anchored in a blockchain, it remains tamper-proof, just like the blockchain itself, as emphasized by Nakamoto [16]. This can be used as a means of verifying access rights before granting data access.

3.2. Related Work Using Blockchain in Consent Management

In this section, we present a chronological list of relevant works that have used blockchain for consent management. Biswas and Muthukkumarasamy [28] proposed a solution that integrates blockchain technology with smart devices, providing a secure communication platform for smart cities. The authors presented an overview of the proposed model, but did not provide technical details. Otherwise, Michelin et al. [29] proposed SpeedyChain. It is a blockchain-based model for data sharing in smart cities. SpeedyChain enables smart vehicles to share data in a decentralized and tamper-proof way. Additionally, the ADvoCATE platform, proposed by Rantos et al. [5], utilizes blockchain technology for processing data from connected devices. ADvoCATE allows device owners to set consents for granting other users access to their data, which are stored on the blockchain. Aldred et al. [30] proposed blockchain as a consent manager, facilitating companies to access user data. The proposed solution is designed to be supported by a certification authority such as ISO/PC 317 to provide an accreditation service to the system. In addition, Mamo et al. [6] proposed an automatic consent management approach using blockchain technology. It has been implemented in Dwarna, a web portal for managing consent on genomic data. The solution was set up for connecting different stakeholders of the Malta Biobank. In Jaiman's work [8], the authors proposed a blockchain-based consent model for controlling access to individual health data. The model uses smart contracts to dynamically represent individual consent on health data and allows data requesters to search and access such data. Agarwal et al. [7] proposed an approach in the Consentio platform, a scalable consent management system. The blockchain is used to keep the history of transactions as well as the consents defined between the different actors for data sharing. Very recently, we proposed a consent management system for establishing digital trust in smart territories [10].

As outlined in the state-of-the-art, various authors have proposed interesting approaches that primarily address the management of consents for data access using blockchain technology. While it is advantageous to utilize a blockchain to store metadata, such as consents for accessing other data, it is not recommended for storing large and recurring data due to several reasons. Firstly, a blockchain has limited scalability compared to other data management systems, making it less efficient for storing large amounts of data. For example, Ethereum [18], one of the most used blockchains to build decentralized applications, processes an average of 15 transactions/s. The problem of scalability in blockchain has also been raised in several research works [11,12]. Otherwise, transaction costs on a blockchain, especially public blockchains, which are the most secure [31], are relatively high. It mainly depends on the volume of data. It can also vary from one blockchain to another. To solve these problems in blockchain-based consent management systems, one solution should be to use, in addition to a blockchain, off-chain storage systems to store large data. Indeed, data stored outside the sphere of the blockchain requires strict security procedures to guarantee their security and integrity.

Most of the existing solutions in the state-of-the-art, such as those proposed by [5,7,8,28], primarily focus on the blockchain consent management process for data access but do not address the issue of securing data that may be stored elsewhere. In contrast, the consent management model presented by Michelin et al. [29] involves storing all data on blockchain nodes. This approach may not be problematic if the system is not built on a public blockchain, where transaction fees can be high, or if it has sufficient storage space to store large amounts of data on the blockchain nodes. However, this approach may not benefit from the high level of security provided by public blockchains. In addition, authors such as [6,30] have discussed the use of off-chain systems for data storage in blockchain-based consent management platforms, but they have not proposed rigorous procedures for securing the data in off-chain storage. In contrast, our proposed model aims to integrate a blockchain as a consent manager for data access, as proposed in the literature, while simultaneously implementing stringent procedures for securing data stored in off-chain storage. This approach provides an additional layer of security for user data against attacks on the off-chain system and is described in detail in Section 4.

4. Securing Access Control to Data in Off-Chain Storage with Encryption Protocols

A blockchain-based consent system utilizes the blockchain as a manager to verify consent for data access, which is hig y beneficial for data sharing. However, as a notary, the blockchain does not necessarily secure the data in off-chain storage, and there is no guarantee that the off-chain storage system being used, such as a cloud system, will adequately protect the stored data. To address this concern, we propose a protocol based on data encryption mechanisms to secure off-chain data in a consent management system.

4.1. Cryptography for Data Encryption

Cryptography is the process of converting data from readable to unreadable form, and it plays a vital role in ensuring security requirements [15,32]. The original objectives of cryptography were to ensure the privacy, integrity, authenticity, and non-repudiation of data [14]. There are various cryptographic mechanisms for encrypting data, including asymmetric encryption, which uses a set of two keys: a public key for data encryption and a private key for data decryption. Another mechanism is symmetric encryption, which uses a single unique key for both encrypting and decrypting data. Figure 2 illustrates how encryption works with a symmetric key system.

Symmetric encryption is particularly useful when data need to be shared with multiple actors. This is the encryption mechanism we utilize in our protocol to secure data in off-chain storage within blockchain-based consent management systems.

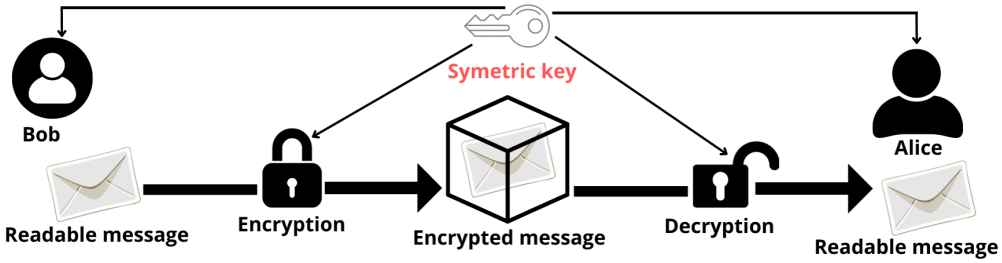

Figure 2. Symmetric key encryption.

4.2. Architecture of the Data Control System Based on Data Encryption

Figure 3 provides a general overview of our proposed secure data access control system in off-chain storage for blockchain-based consent platforms. The architecture is divided into three main components: first, the off-chain system, which includes an API (Application Programming Interface) and an off-chain storage space; second, the blockchain component, which comprises a blockchain API (with smart contracts) and a blockchain storage ledger; and third, the users.

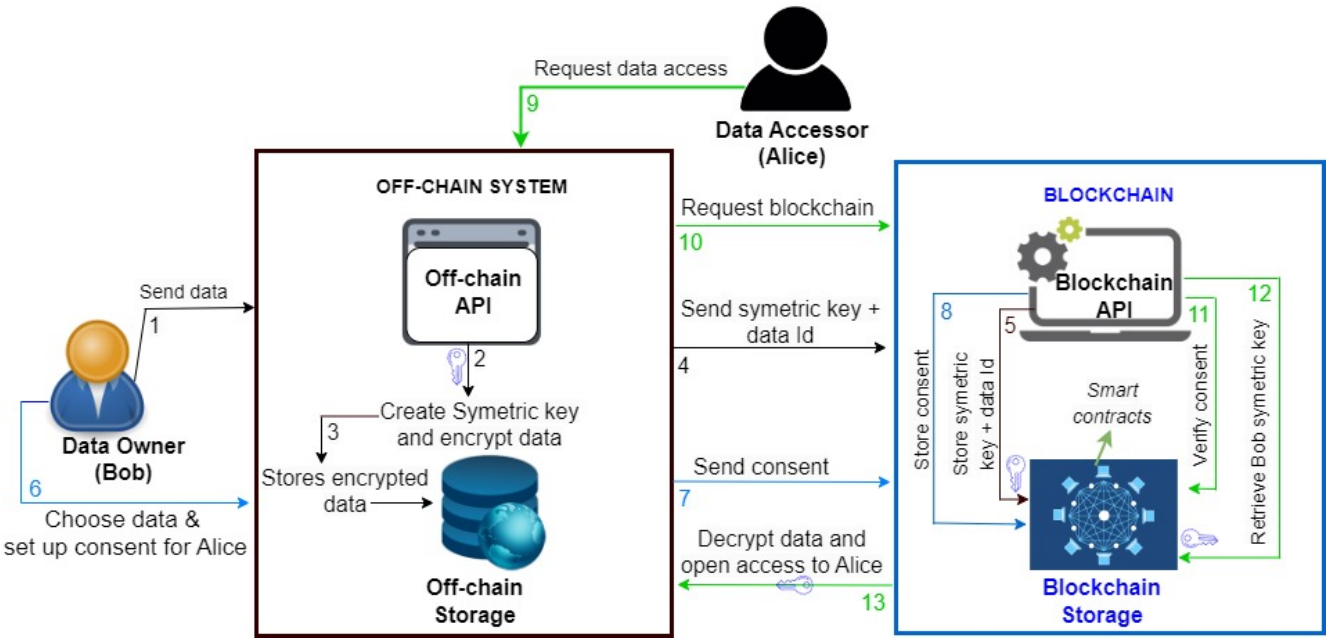

Figure 3. Generic architecture of the data control system based on data encryption.

As a blockchain is not ideal for storing large data, so the data will be stored in an off-chain storage system. This makes it possible to overcome the problems of transaction fees and the scalability of blockchains mentioned previously. Off-chain storage can be any traditional Database Management System, such as MySQL, SQL Server, MongoDB (the one we used), etc. So, in our protocol, large data will be encrypted and then stored in the off-chain system, and the blockchain ledger will be used to securely record the data symmetric encryption key for data decryption; the blockchain will also be used to record the consents for access to this data. Then, whenever someone requests access to data in the off-chain system, it will query the blockchain which will verify the existence of consent for data access. After that, the blockchain retrieves the symmetric encryption key corresponding to the requested data set, which will be used to decrypt it and make it readable.

Moreover, as data are supposed to be shared with several actors, we propose a model based on symmetric keys encryption. This model can be used in consent systems, with a multitude of actors. This model is applicable in various scenarios, including companies

sharing data with other companies and systems that enable users to share data with companies or other users, such as in smart city systems. To ensure true decentralization and take advantage of the robust security features offered by public blockchains, we suggest using the Ethereum blockchain [18] as the underlying technology for our proposed model.

There are several widely used symmetric encryption algorithms today [33]: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), etc. AES is used in our case to encrypt data. The algorithm is known to be more efficient than other algorithms, providing advantages such as large scale data to encrypt and also little resource consumption [34].

4.3. Recording and Encryption Data and Establishing Consent

Suppose a set of actors operating on the blockchain-based consent management system for data sharing. First, these users register according to the rules of the system, before being able to save data, which will be shared on the basis of consent to other users of the system. Once registered, a user can log in and save the data to be shared, as shown in step 1 in Figure 3. When storing data, a symmetric encryption key is generated using AES algorithms and the user data are encrypted before being sent to the off-chain storage, as shown in steps 2 and 3. The symmetric key, along with the data ID, is then sent to the blockchain via a smart contract (step 4), while the encrypted data are registered in the off-chain storage. Finally, in step 5, the blockchain records the symmetric key and the data ID in the blockchain storage.

Once this is done, the data owner can decide in step 6 to choose data and grant consent to another user so that they can access this data. Then, the data owner establishes a consent with the elements mentioned in Table 1. The consent may contain elements such as the data owner's ID (their blockchain wallet address); the data accessor's ID (their blockchain wallet address); the data ID; and the data access conditions. The consent is therefore sent to the blockchain (step 7), which will record it via a smart contract in an immutable way in step 8. This consent will be used to access the user's data by the accessor. This will be the first condition, without which an actor cannot access a user's data.

4.4. Access Data with Consent and Encryption Key

After receiving consent from a data owner, an accessor can make a data subject access request to access data which were shared with them. Consider the example described in Figure 3, where Alice has received Bob's consent to access her data. When Alice tries to consult Bob's data in the off-chain storage, several steps will follow:

1. Alice asks the system to consult Bob's data, as shown in step 9 in Figure 3.
2. In step 10, the off-chain API will ask the blockchain system to check access rights for Alice.
3. In step 11, the blockchain verifies the existence of consent for Alice, regarding Bob's data. If the consent does not exist, no access to the data will be given to Alice. If consent exists, the process will continue.
4. In step 12, the blockchain retrieves Bob's symetric key via a smart contract that manages the consents.
5. Finally, in step 13, the symmetric encryption key will be used to decrypt Bob's data, which will then be available to Alice.

It should be noted that this whole process will happen automatically, without the intervention of the data accessor. In general, the verification of consent is the first layer of data access security in the protocol. Thus, if someone has not received the consent of a data owner, they will not be able to find the symmetric encryption key recorded in the blockchain. As a system that works without a central trusted third party, the blockchain cannot get along with the potential accessor to the data to give them the encryption key. This is also one of the great advantages of using a blockchain, as it is a decentralized and secure ledger operating without a central control entity.

On the other hand, using a data encryption process constitutes a second layer of security, coupled with the consent management. If, despite everything, a hacker manages to use tricks to access the data stored in the off-chain storage, they will not be able to read them. The reason is that the data encryption key is needed for someone to read the data. However, the encryption key, being stored in the blockchain, will not be accessible to someone who has not received consent.

Indeed, this dual process proposed in our protocol, combining consent management and data encryption, complements the consent mechanisms that we have listed in the state-of-the-art. The solutions proposed in the state-of-the-art, which are also very interesting, can be applied in certain contexts, as described by others. However, in our protocol, the consent process on the blockchain side will allow access to the data, while the encryption mechanism protects it and allows consent recipients to read it. This is practical for the implementation of different consent systems managing a lot of data and that want to ensure a high level of security of the data stored in off-chain systems.

5. Conclusions

Secure data access control remains a critical factor in data disposal. This is a non-negligible aspect, especially in systems that generate a lot of data and in which the interactions in terms of data sharing are enormous. Consent management using blockchain technology for data access shows good results, as we have demonstrated here. However, when this technology is coupled with off-chain systems, it requires other data security mechanisms. Consent management by blockchain alone is not enough to ensure a high level of data security outside the blockchain sphere.

This article presents a protocol for secure access control to data stored in off-chain storage within blockchain-based consent systems. We have reviewed different approaches to consent management using blockchain, noting some variations. However, the common approach is to use a blockchain to record consents established between actors for sharing and accessing data. We have also analyzed why it is crucial to ensure the security of data stored outside the blockchain and have explored ways to enhance existing solutions.

Finally, we presented a protocol that enhances data security through a combination of symmetric key systems and consent management mechanisms. This approach offers multi-level security for data in off-chain systems linked to a blockchain system. By using a blockchain, consents for data access can be effectively managed while also enabling the storage of a symmetric key to decrypt data in the off-chain system. This ensures privacy, security, and data integrity.

Author Contributions: Conceptualization, M.G.; methodology, C.B. and C.D.; software, M.G.; validation, C.B. and C.D.; formal analysis, C.D.; writing—original draft preparation, M.G.; writing—review and editing, M.G. and C.B.; visualization, C.D.; supervision, C.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank Le Havre Seine Métropole (LHSM), which supported this work as part of Mongetro Goint's doctoral thesis.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced Encryption Standard
API	Application Programming Interface
DMS	Database Management System
PoS	Proof of Stake
PoW	Proof of Work

References

1. Tenopir, C.; Allard, S.; Douglass, K.; Aydinoglu, A.; Wu, L.; Read, E. Data Sharing by Scientists: Practices and Perceptions. *PLoS ONE* **2011**, *6*, e21101. [CrossRef] [PubMed]
2. Rockhold, F.; Nisen, P.; Freeman, A. Data sharing at a crossroads. *N. Engl. J. Med.* **2016**, *375*, 1115–1117. [CrossRef] [PubMed]
3. Parr, C.S.; Cummings, M.P. Data sharing in ecology and evolution. *Trends Ecol. Evol.* **2005**, *20*, 362–363. [CrossRef] [PubMed]
4. GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. *Off. J. Eur. Union* **2016**, 1–88.
5. Rantos, K.; Drosatos, G.; Demertzis, K.; Ilioudis, C.; Papanikolaou, A.; Kritsas, A. ADvoCATE: A consent management platform for personal data processing in the IoT using blockchain technology. In Proceedings of the 11th International Conference, SecITC 2018, Bucharest, Romania, 8–9 November 2018, *11359*, pp. 1–16.
6. Mamo, N.; Martin, G.; Desira, M.; Ellul, B.; Ebejer, J.-P. Dwarna: A blockchain solution for dynamic consent in biobanking. *Eur. J. Hum. Genet.* **2020** , *28*, 609–626. [CrossRef]
7. Agarwal, R.R.; Kumar, D.; Golab, L.; Keshav, S. Consentio: Managing consent to data access using permissioned blockchains. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–9.
8. Jaiman, V.; Urovi, V. A consent model for blockchain-based health data sharing platforms. *IEEE Access* **2020**, *8*, 143734–143745. [CrossRef]
9. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2019**, *88*, 101653. [CrossRef]
10. Goint, M.; Bertelle, C.; Duvallet, C. Establish Trust for Sharing Data for Smart Territories Thanks to Consents Notarized by Blockchain. In Proceedings of the Blockchain and Applications, BLOCKCHAIN 2021, Salamanca, Spain, 6–8 October 2021; Prieto, J., Partida, A., Leitão, P., Pinto, A., Eds.; Lecture Notes in Networks and Systems; Springer: Cham, Switzerland, 2022; Volume 320. [CrossRef]
11. Chauhan, A.; Malviya, O.P.; Verma, M.; Mor, T.S. Blockchain and scalability. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 122–128. [CrossRef]
12. Kim, S.; Kwon, Y.; Cho, S. A survey of scalability solutions on blockchain. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 17–19 October 2018; pp. 1204–1207. [CrossRef]
13. Laurent, A.; Brotcorne, L.; Fortz, B. Transaction fees optimization in the ethereum blockchain. *Blockchain Res. Appl.* **2022**, *3*, 100074. [CrossRef]
14. Bokhari, M.U.; Shallal, Q.M. A review on symmetric key encryption techniques in cryptography. *Int. J. Comput. Appl.* **2016**, *147*, 43–48.
15. Saranya, K.; Mohanapriya, R.; Udhayan, J. A Review on Symmetric Key Encryption Techniques in Cryptography. *Int. J. Sci. Eng. Technol.* **2014**, *3*, 539–544.
16. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 16 February 2023).
17. Gervais, A.; Karame, G.O.; Wust, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS'16, Vienna Austria, 24–28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 3–16. [CrossRef]
18. Buterin, V. Ethereum. A Next Generation Smart Contract and Decentralized Application Platform. *White Paper* **2014**, *3*, 1–2.
19. Gayte, A. L'Ethereum est Passé à la Proof of Stake Avec the Merge: Tout Comprendre à Cette Révolution des Cryptos. 2022. Available online: https://www.numerama.com/tech/713345-lethereum-passe-a-la-proof-of-stake-tout-comprendre-a-cette-revolution-dans-les-cryptomonnaies.html (accessed on 24 September 2022).
20. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
21. Politou, E.; Alepis, E.; Patsakis, C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *J. Cybersecur.* **2018**, *4*, tyy001. [CrossRef]
22. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
23. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572. [CrossRef]
24. Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. *Sensors* **2021**, *21*, 2462. [CrossRef]
25. Ali, A.; Pasha, M.F.; Ali, J.; Fang, O.H.; Masud, M.; Jurcut, A.D.; Alzain, M.A. Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. *Sensors* **2022**, *22*, 528. [CrossRef]
26. Kamble, S.S.; Gunasekaran, A.; Sharma, R. Modeling the blockchain enabled traceability in agriculture supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 101967. [CrossRef]

27. Abdallah, R.; Besancenot, J.; Bertelle, C.; Duvallet, C.; Gilletta, F. An Extensive Preliminary Blockchain Survey from a Maritime Perspective. *Smart Cities* **2023**, *6*, 846–877. [CrossRef]
28. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; pp. 1392–1393.
29. Michelin, R.A.; Dorri, A.; Lunardi, R.C.; Steger, M.; Kanhere, S.S.; Jurdak, R.; Zorzo, A.F. Speedychain: A framework for decoupling data from blockchain for smart cities. In Proceedings of the MobiQuitous '18: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA, 5–7 November 2018; pp. 145–154.
30. Aldred, N.; Baal, L.; Broda, G.; Trumble, S.; Mahmoud, Q.H. Design and implementation of a blockchain-based consent management system. *arXiv* **2019**, arXiv:1912.09882.
31. Iredale, G. Public Vs Private Blockchain: How Do They Differ? 2021. Available online: https://101blockchains.com/public-vs-private-blockchain/ (accessed on 11 February 2023).
32. Stallings, W. *Network Security Essentials: Applications and Standards*; Pearson Education India: Delhi, India, 2007.
33. Abd Elminaam, D.S.; Abdual-Kader, H.M.; Hadhoud, M.M. Evaluating The Performance of Symmetric Encryption Algorithms. *Int. J. Netw. Secur.* **2010**, *10*, 216–222.
34. Hidayat, T.; Mahardiko, R. A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. *Int. J. Artif. Intell. Res.* **2020**, *4*, 49–57. [CrossRef]