healthcare

MDPI

Review

A Systematic Review of Blockchain for Consent Management

Prasanth Varma Kakarlapudi * and Qusay H. Mahmoud

Department of Electrical, Computer and Software Engineering, Ontario Tech University,
Oshawa, ON L1G 0C5, Canada; qusay.mahmoud@ontariotechu.ca
* Correspondence: prasanthvarma.kakarlapudi@ontariotechu.net

Abstract: Blockchain technology was introduced through Bitcoin in a 2008 whitepaper by the mysterious Satoshi Nakamoto. Since its inception, it has gathered great attention because of its unique properties—immutability and decentralized authority. This technology is now being implemented in various fields such as healthcare, IoT, data management, etc., apart from cryptocurrencies. As it is a newly emerging technology, researchers and organizations face many challenges in integrating this technology into other fields. Consent management is one of the essential processes in an organization because of the ever-evolving privacy laws, which are introduced to provide more control to users over their data. This paper is a systematic review of Blockchain's application in the field of consent and privacy data management. The review discusses the adaptation of Blockchain in healthcare, IoT, identity management, and data storage. This analysis is formed on the principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) and a process of systematic mapping review. We provide analysis of the development, challenges, and limitations of blockchain technology for consent management.

Keywords: blockchain; consent management; privacy

Citation: Kakarlapudi, P.V.; Mahmoud, Q.H. A Systematic Review of Blockchain for Consent Management. *Healthcare* **2021**, *9*, 137. https://doi.org/10.3390/healthcare9020137

Academic Editor: Daniele Giansanti
Received: 28 December 2020
Accepted: 25 January 2021
Published: 1 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Personal data has been added to the long list of precious commodities. Personal information could be anything—a name, an identification number, medical data, or location data. With the world transforming swiftly in terms of technology, every digital activity is registered and collected, which may contain sensitive individual information. According to a survey, there will be approximately 75 billion smart devices by 2025 [1], which will collect user data to monitor. Users give access to these devices to manage their data deliberately or without consent, as they seem reliable, and user profiles are created based on the data provided. This information can be exploited by systems that examine the characteristics and preferences of the user; they attempt to influence decisions by showing content based on aggregated profiles. In 2016, Cambridge Analytica had access to 87 million Facebook users [2], which were acquired via users who were using a third-party application known as "This Is Your Digital Life", where they unknowingly gave access to the app, which collected their information and their friend's network information as well. Using extensive data, the company tried to influence then ongoing voters (US Presidential Election 2016) by various means. There are also other incidents where personal data is misused for illicit reasons. So more than anything, it is crucial to understand the policies and the need for data consent, which brings us to an important topic—consent management.

Consent management is the action or process to manage user and customer consent for processing personally identifiable data. In other words, it ensures that users can select and revoke their consent if desired in different categories (preferences). The main steps in this process are collecting consent from users and storing the consent in a secure database, which allows users to withdraw or revoke and renew their consent. While the process seems simple, it has many challenges, especially for big organizations as individual data is scattered around their business, sitting in company silos. Consent is usually collected using a variety of techniques (websites, mobile applications, and various marketing platforms), making it very difficult to aggregate data (map the data collected to a single person). Once aggregated, the next challenge is to store the data in a single repository (a secure database). Data transparency is another challenge that needs to be focused on, as users do not have the perfect knowledge about how their data is being operated. Organizations should also ensure that proper resources are available so that users can see and modify their data preferences. Identity management is a factor that needs to be considered while collecting the user's consent to the integrity of the information provided. The complexity of implementation becomes harder as privacy rules evolve. These are just a few of the technical challenges with consent management. The other challenge is to inform the user of the purpose of obtaining consent and to make the user aware of it. Additionally, there may be users that approve of the processing of personal information for all reasons and activities, in most instances. However, individuals would like to limit their consent, as a result, with consent management, all these requirements must be addressed while ensuring compliance with the privacy laws.

We believe that consent management with Blockchain makes the process easier, more accessible, and more secure; as it is a decentralized technology, it can make the process more transparent and approachable for users. A blockchain is a digital transaction archive that is duplicated and circulated on the blockchain over the entire computer network. It is indeed important to mention that the tech giants and banking sectors have invested billions of dollars in Blockchain [3]. Bitcoin was the first cryptocurrency to use this technology, and later, more cryptocurrencies such as Monero and Dash started using this technology. In 2013, Vitalik Buterin proposed the idea of Ethereum and started operating on 30 July 2015; Hyperledger was launched by Linux Foundation in December 2015 and had received contributions from IBM, SAP Ariba, and Intel [4]. While Bitcoin, Monero, and Dash are referred to as the first generation of Blockchain, Ethereum comes under the second generation of Blockchain; the third generation of Blockchain are applications that have been developed for various sectors such as healthcare, IoT, supply chain management (SCM), identity management, etc. The third section explains how Blockchain helps with the consent management process.

The purpose of this paper is to systematically collect and classify all related Blockchain research papers from a renowned organization (IEEE), and to achieve the desired purpose, we carried out a systematic review of the Blockchain literature to show some useful insights. There are a few insightful analyses of this subject in the literature, our methodologies and objectives vary from one another, and most of the reviews focus on one application of Blockchain (healthcare, education, or data management). We focused on various applications of Blockchain (in the field of consent management) such as healthcare, IoT, identity management, and data storage. In the review conducted by Ali Alammary et al. [5], the prime focus was on the applications of Blockchain in the field of education. Healthcare was the main application of the systematic review that was conducted by Cornelius C. Agbo et al. [6] and Tsung-Ting Kuo et al. [7]. While Fran Casino et al. [8] discussed the various applications of Blockchain, their review was not in the area of consent management. Therefore, to the best of our knowledge, this is the first systematic review covering a few areas in the field of consent management. Our systematic review follows the guidelines set by PRISMA [9]. It is a well-structured research protocol for systematic review ensuring a thorough and impartial analysis of all published peer-reviewed papers that apply to the topic.

The rest of the paper is structured as follows. Consent management and its importance and challenges are presented in Section 2. An overview of blockchain is presented in Section 3. Section 4 presents the research methodology we have followed. The results are presented in Sections 5, and a discussion of the challenges and possible solutions are presented in Section 6. Finally, Section 7 concludes the paper and offers ideas for future work.

2. Consent Management

Consent is strictly related to a processing purpose, which is the purpose that the personal data of an individual is processed for, such as marketing, analysis, or healthcare [10]. Consent management is a method, procedure, or collection of policies to enable users to specify what information they are willing to allow access to various care providers [11]. The main steps in consent management involve:

1. Collection of consent;
2. Storage of consent;
3. Use of collected consent and data.

2.1. Collection of Consent

Consent can be collected from a variety of sources—websites, mobile applications, CRM (Customer Relationship Management) systems, marketing platforms, contact centers, and sales points. The most traditional way of obtaining consent is through terms of conditions/services or CMP (consent management platform). The main challenge is the process of collecting informed consent from the user. For an instance, a patient might be willing to share his data with a physician but not willing to share his data with a medical researcher. In this scenario, the user provided partial consent to share his data. Therefore, the consent management system should also be designed to capture partial consent from the user. Another example could be a user using an IoT device. Initially, the user provided consent for sharing his preferences of a smart device with the service provider but could decide against sharing at any point in time. Considering the change, the system should also allow the user to revoke the consent at any period.

With the introduction of GDPR (General Data Protection Regulation) and other privacy laws in various countries, companies must make sure the user is entirely aware of the consent they are giving. The company must provide precise information regarding the situations where their data will be utilized; in other words, there should be transparency.

2.2. Storage of Consent

As indicated above, consent is collected using a variety of methods, the main task after collecting consent is to aggregate the data. Once properly collected, consent should be stored in a single source of truth, which should be a secure database. Data storage is very important, as it should be stored in a secure location. Data should also be modeled based on the requirement.

The period of data storage is another important case, as the data cannot be stored for longer periods, only for the shortest possible time the data must be stored. The organizations usually come up with the period of data storage, and they must also ensure correct and up-to-date information is maintained. According to GDPR, the time for which personal data are kept should be strictly limited to Recital 39 of the GDPR [12], and the data controller shall set limits for deleting information.

2.3. Use of Collected Consent and Data

The following questions arise and need to be addressed after receiving and storing the consent:

- How is the obtained consent used for data access regulation?
- Are all policies such as GDPR and CCPA (California Consumer Privacy Act) met?
- Are there sufficient resources to maintain the transparency of data?

Data of a user can be shared with any third-party organizations based on the consent that is collected. Overall, the main challenging part of the consent management system is to get and maintain consent in a customizable, effective, and transparent way. Ensuring all the conditions set out in the various privacy laws is also very important, as failure could lead to severe penalties. Organizations should also inform users of the purpose of their data, and users should also be informed if their data is sold to third parties for marketing/research purposes. By following all these, the process will be very transparent, which, in turn, will help the organization to build trust with its customers. After ensuring all the policies are met, there should also be resources to help the customer if they want to revoke/withdraw their consent.

Failure in following the regulations can lead up to 10 million Euros or two percent of the annual turnover of the company [13]. In the following section, we explained how Blockchain works and how it helps to achieve consent management.

2.4. Efficiency Challenges of Current Consent Management

There are multiple data sources such as patient health information, social media data, data collected from the IoT devices, etc. Since all of these data sources contain sensitive information of individual users, they need to be maintained securely. More importantly, we should also have a systematic and transparent consent collection by the present systems. Some challenges identified in the current systems include:

- Methodologies used for consent collection. The current systems are not capable of collecting or requesting specific consent from the users. They use sophisticated single terms and conditions (T&C). Instead of that, consent should be collected for specific purposes, and it must be presented in a simplified manner.
- Data Regulation. After the consent is collected, the data sharing must be regulated to avoid unwanted sharing of the data. Additionally, current systems do not have a standard platform where the data could be shared among them. Another challenge in the present system is the ability to inform the patients when their data is shared. When there is an exchange of information between hospitals or organizations, the users are generally unaware of the data exchange
- Data handling. The existing healthcare infrastructure should be developed to process the huge volumes of data and should make sure accurate information is being collected from the patients. Storing and collecting inaccurate healthcare information could lead to a fatality when the patient is treated.

To avoid challenges, Blockchain can be used to maintain a flexible and transparent consent management system. Its immutability and decentralized features will make the system trustworthy for the users.

3. Overview of Blockchain

Before blockchain technology, transactions were recorded using a centralized model that consists of server-side and client-side applications. In 1990, Haber, S and Stornetta, W. S. came up with the idea of a secured chain of time-stamps [14]. They aspired to create a system where the timestamps of a document cannot be tampered with. However, Blockchain's concept earned its acclaim in 2008 when it was used as a distributed ledger technology in Bitcoin (Bitcoin white paper published in October 2008 [15]). The mysterious Satoshi Nakamoto introduced Bitcoin, where we can trade electronic coins without a centralized party (banks, for example). In a typical transaction, a third party must be involved in transferring money; third parties are not always reliable, as there is a chance of them getting compromised, and there are transfer limits as well; also, additional amounts are charged when a third party is involved. With the introduction of Bitcoin, we can avoid these confinements. Bitcoin is a virtual currency exchange that takes place without a third party between peers. It is immune to counterfeiting and is preserved by complex algorithms.

Around 2014, cryptocurrency exchanges were not the only application of fascinating blockchain technology. It was explored and used in many other fields. Blockchain uses the SHA-256 algorithm to maintain the data changes in the network and asymmetric cryptography to achieve enhanced security.

3.1. Working of Blockchain

As mentioned earlier, Blockchain is used to make sure the documents have not been tampered with, it stores the information in terms of blocks. Usually, each block comprises three things:

- Data
- Hash of block
- Hash of the previous block

Information stored within a block depends on the Blockchain type; for example, a bitcoin includes financial data (details of a transaction) stored in its blocks. The hash value of a block will be generated when a block is created; its value will not be the same if the data of the block is changed and it also contains the previous block's hash value. As seen in Figure 1 below, the first block in a blockchain is called a Genesis Block, and it won't have the hash value of any previous block; instead, it starts from zero.

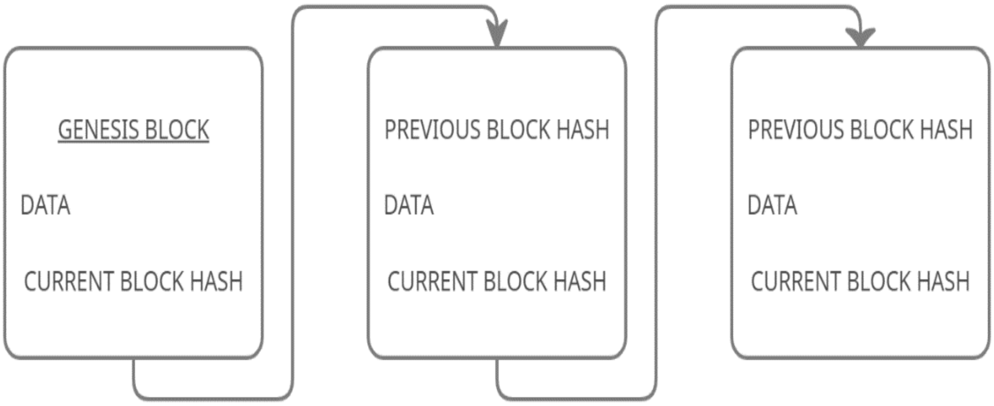

Figure 1. A basic block contains a hash, a previous block hash, and data.

When there is a new transaction, a block will be added with the corresponding data. Therefore, a new block will be attached, and it establishes a chain in the process, hence the name Blockchain. Due to its immutable property, the data in the Blockchain cannot be modified.

In an instance where data is changed in a block, as the information is changed, its hash value also changes. Therefore, this block's hash value and the previous hash value of the next blocks will not be the same, resulting in breaking the chain and making it invalid, but there is a chance of recalculating the remaining block's hash values to make it valid again with the help of advanced supercomputers; to avoid this, we use the concept of proof of work.

The initial consensus algorithm in a Blockchain network is the proof of work (PoW) [16]. PoW is done by people who are called miners to ensure that the transactions made are authentic. This validation method of the transactions is called mining; once transactions are verified valid, they can be added to the Blockchain.

A smart contract is a program that can act as a protocol or an agreement, which cannot be tampered with. This concept is introduced by Nick Szabo in 1994 [17]. In the case of Blockchain, these play a very crucial role. Once deployed on the network, these can be invoked or triggered with the help of a unique address that is assigned to them. Therefore, when a smart contract is deployed, the information is stored on the network, which is accessible to the nodes that are participating. The other nodes on the network cannot change the information on the smart contract. There are many use cases of the smart contract. For instance, when we want to sell a particular object (car, house, etc.,), a potential buyer can be found on the network, thus eliminating the need for a third party. Therefore, smart contracts are self-verifiable. Solidity is one of the main programming languages that is used to create and execute. Ethereum and Zeppelin are Blockchain platforms that use the Solidity programming language.

There are three crucial Blockchain types—public, private, and consortium. All the transactions are made available to the public in public Blockchain; anyone can participate, create, or mine. Private Blockchain or permissioned Blockchain—in this kind, users should have consent to join the group, and it is more centralized than that of public Blockchain. The third kind is consortium blockchain, and it is indistinguishable from private Blockchain, but the key difference between a private and a consortium Blockchain is in a consortium blockchain, it is controlled or regulated by a group instead of a single person, as is the case in a private Blockchain.

3.2. Applications of Blockchain Technology

Healthcare. An important issue in the healthcare industry is the privacy of the patients. Patient consent is the key point in the healthcare ecosystem. The technology brings a more secure model for patient information exchange. Considering its distributed ledger feature, it provides more ease of operations between the hospitals. It has the capability to achieve nationwide interoperability between the hospitals for EHR (electronic health records). MedChain [18] was introduced as a data-sharing system. In this system, the data is collected from the medical devices and sensors. There are two events that are created on the network in this model. The first event is created when the healthcare provider adds the data to patient inventory, and the second event is created when a patient provides access to the requestor. Another blockchain application in the medical field is [19], the proposed design is a private blockchain network with Ethereum as its platform and a back end distributed file system. In this prototype, the smart contracts are created as a representation of health records and contain metadata of the ownership, permissions, and data integrity. The prototype deals with various use cases of smart contracts such as the process of issuing the medicines, sharing the lab results with doctors, and for clinical trials, etc.

Internet of Things (IoT). This is will enable businesses to make insights from data collected from IoT devices, which will help them provide improved service to the users. Devices such as Fitbit collect information from the user. In the framework [20], advanced cryptography methods are used to make the design secure and suitable for IoT devices. The prototype deals with off-chain storage, and data is stored on the cloud. The main idea is to have the cloud servers send the hash of the data to the overlay network. When the data is shared to the cloud, the sender adds a digital signature. The overlay network sends an alert to healthcare providers. When the healthcare provider has received an alert, they will have full access to the patient's data.

Machine Learning. An insurance company could benefit from the integration of ML and blockchain, as identity fraud can be detected before entering the details on the network. In [21], the authors have introduced an algorithm to find the better configurations of weights in a neural network using Blockchain and its concepts. The model was developed on a local network, where the multiple devices are connected. Each node on the network will have the same controls. Transactions can be viewed by each node itself. This avoids unnecessary access to the other nodes. Here, each demand is considered as a transaction, and in the event of a conditional stopping, miners will be awarded based on the better results.

3.3. Blockchain for Consent Management

The following comprises an effective consent management system:

- Data transparency
- Secure storage
- Accurate data management

Blockchain is a decentralized network where all users have access to the data available on it. For instance, any transaction/movement made by the organization can be seen by all users, making the process completely transparent. Any exchanges made between the organizations can be recorded and can be made available to users so that they can track their data movement. Its decentralized nature will make sure that systems are not dependent on one central authority. Instead, it is distributed across the nodes or members on the network for various approvals or acceptance, making it more trustworthy. The most interesting and essential feature of Blockchain is its immutability. Once a record is added to the network, the consent of a user cannot be modified. If there is a change of consent, it can be added one more time as a different block. Combining or mapping data from all sources is one of the most difficult tasks and can be done using Blockchain. Data can be aggregated in Blockchain using a distributed hash table (DHT) [22]. The encrypted consent data created by DHT can be stored on Blockchain, and the actual data can always be retrieved easily, which also resolves the size issue of the Blockchain, as more data cannot be stored in a block.

Another main application of Blockchain is identity management, where user's data can be validated by an organization. For instance, an educational organization can validate a student's final degree and store it on Blockchain, which can also be used to validate user data so that accurate data can be collected and stored. Therefore, using Blockchain, the consent management process can be made easier and more compliant.

4. Research Methodology

We also followed the recommendations for a systematic review of the literature [23] and the criteria outlined in the PRISMA statement [9]. In the first step, we have identified the critical research questions that would help us to understand what level blockchain-based technologies (related to consent/privacy data management) were built. The questions help us in examining the issues and constraints. The basic steps involved in conducting a systematic review are shown in the below Figure 2.

Description of Research Objectives

We identified four research questions that we wanted in the review.

RQ1: How does Blockchain protect user privacy and data consent across different sectors?

- This is one of the primary questions in this research to understand how Blockchain is used to implement consent management in various sectors such as healthcare, education, IoT, etc. We have reviewed multiple research papers and articles to understand different problems that blockchain applications could solve as PII (Personal Identifiable Information) policies went through a lot of change after the introduction of GDPR.

RQ2: What Blockchain-based applications have been built of the described use cases?

- Although this technology was introduced in 2008 by the enigmatic Satoshi Nakamoto as an essential technology for Bitcoin, it is still a relatively new technology in other sectors such as healthcare, IoT, and education. Many application proposals were given in the scientific reviews, but very few discussed the working prototypes. Therefore, it is vital to learn and understand the real-world implementations.

RQ3: How are the limitations of current solutions addressed?

- Here our objective is to find out the limitations of the technology based on the prototypes that have been developed? We will also examine the steps taken to avoid such limitations.

RQ4: What are the major challenges for future research?

- With the introduction of GDPR rules in the EU, we have many restrictions on the use of PII. With this question, we identify the research gaps and challenges that need to be addressed so that the applications follow the new rules and policies.

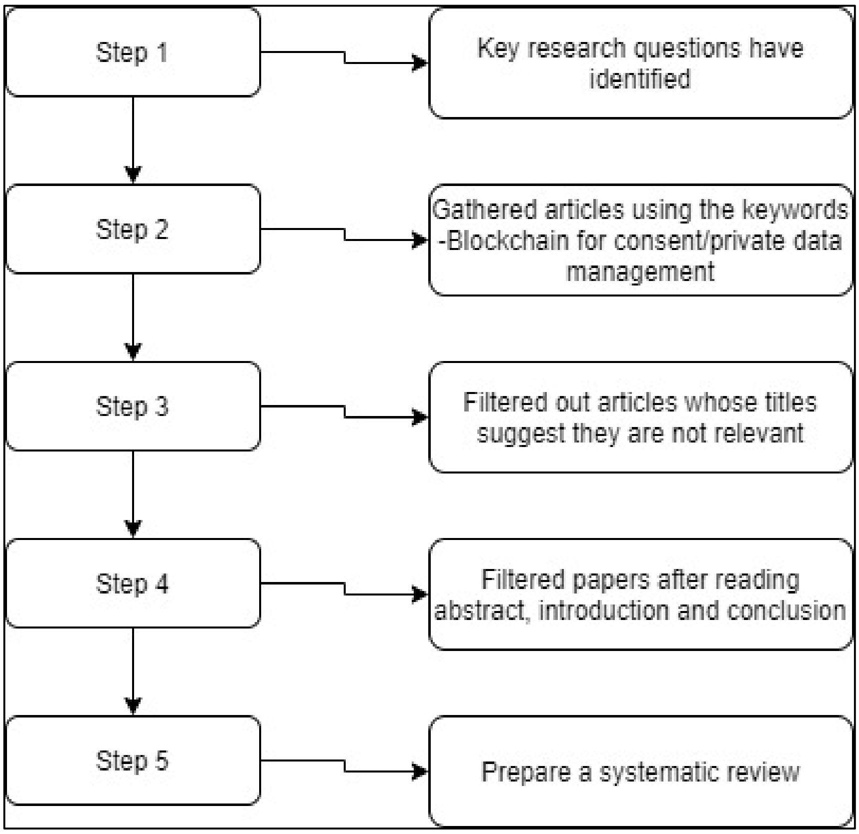
Step 1
Key research questions have identified
Step 2
Gathered articles using the keywords -Blockchain for consent/private data management
Step 3
Filtered out articles whose titles suggest they are not relevant
Step 4
Filtered papers after reading abstract, introduction and conclusion
Step 5
Prepare a systematic review

Figure 2. The process followed to conduct this review.

Figure 3 shows the PRISMA flow of this systematic review.

In the next step, we have searched for research papers in a reputable database (IEEE) with the keywords "Blockchain for consent management" and "Blockchain for private data management" and collected research papers. In the following step of the filtering, we have removed those documents whose title indicated that they were not of relevance to the topic. A few papers, for instance, were about Blockchain, but not related to the field of consent management.

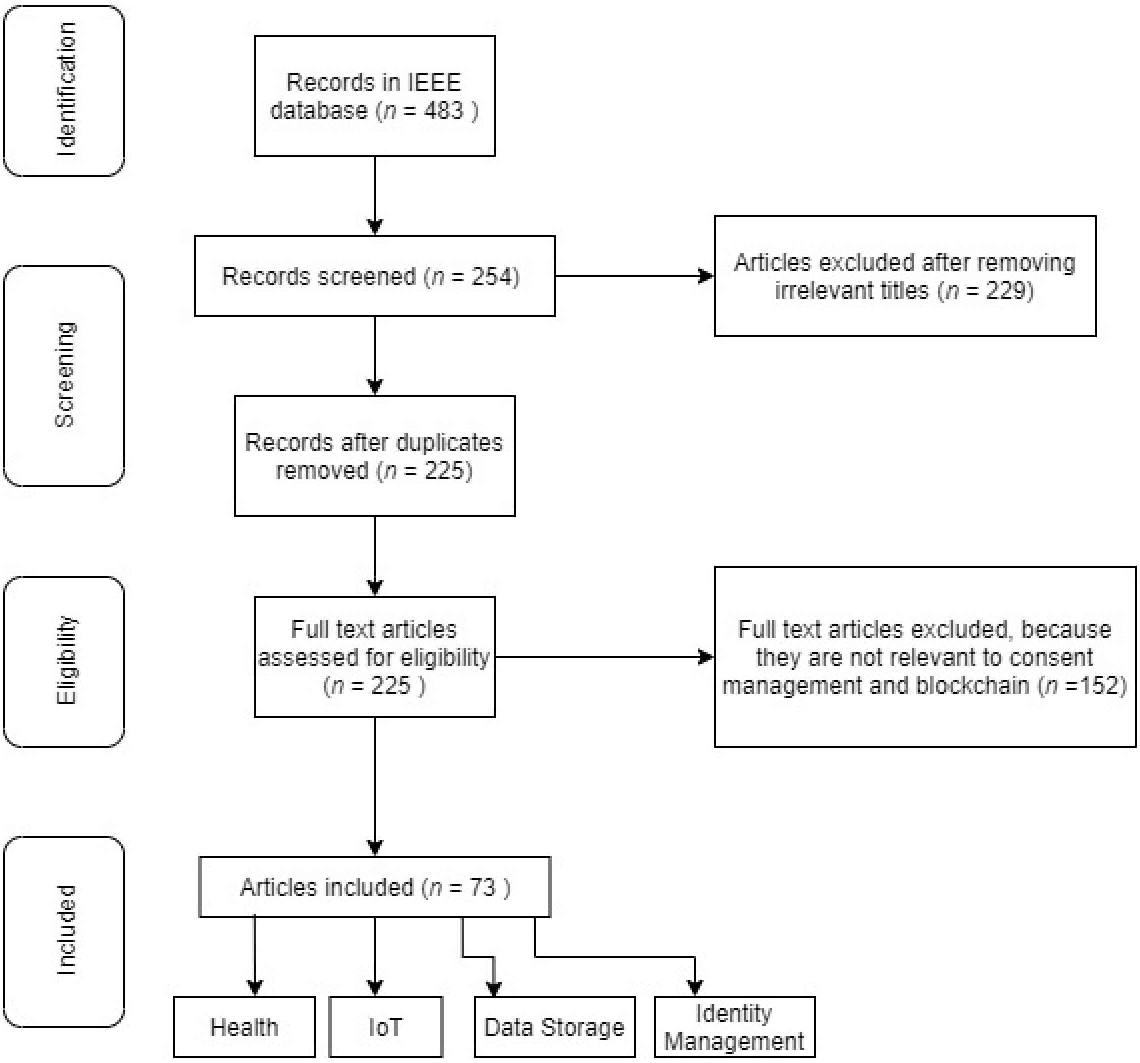
Identification
Screening
Eligibility
Included
Records in IEEE database (n = 483)
Records screened (n = 254)
Articles excluded after removing irrelevant titles (n = 229)
Records after duplicates removed (n = 225)
Full text articles assessed for eligibility (n = 225)
Full text articles excluded, because they are not relevant to consent management and blockchain (n =152)
Articles included (n = 73)
Health
IoT
Data Storage
Identity Management

Figure 3. A PRISMA flow of this systematic review.

In the next step, the following exclusion criteria were used after reading the abstract thoroughly:

- If the paper is not in the English Language
- Duplicate papers were removed
- If the paper is not related to consent/private management

In the next step, we have analyzed the remaining papers thoroughly and divided them into categories such as healthcare, IoT, etc. As shown in Table 1 below, we have also extracted the following data from the papers.

Table 1. Classification of papers.

Data Item	Description
Authors	Authors of the paper
Title	Title of the paper
Year	Paper year publication
Publication Type	Journal/Conference/Magazine
Prototype	Yes or No

5. Results

The findings of the systematic review are summarized in this section. Using the mentioned keywords, we have gathered 483 research papers where we filtered out the paper whose titles suggested that they were not relevant to the research. After this step, we were left with 254 papers of various researchers, which were combined into a single file to check for duplicates; we found around 29 duplicate papers and removed them from the list. After reading the abstract, introduction, and conclusion extensively, we had to remove 152 papers, as they had nothing to do with Blockchain for consent/privacy management. The outcome was 73 papers selected. The full list of final papers is shown in Table 2 below.

Table 2. Selected papers.

Author	Year	Publication Type
Guy Zyskind. et al. [24]	2015	Conference
Asaph Azaria. et al. [25]	2016	Conference
Marco Conoscenti. et al. [26]	2016	Conference
Elena Karafiloski. et al. [27]	2017	Conference
Fangfang Dai. et al. [28]	2017	Conference
Shinsaku Kiyomoto. et al. [29]	2017	Conference
Jatinder Singh. et al. [30]	2018	Conference
Kaiwen Zhang. et al. [31]	2018	Conference
Klaus Zaerens [32]	2018	Conference
Liping Liu. et al. [33]	2018	Conference
M. Alessi. et al. [22]	2018	Conference
Mohammad Jabed Morshed Chowdhury. et al. [34]	2018	Conference
Nasr Al-Zaben. et al. [35]	2018	Conference
Paul Dunphy. et al. [36]	2018	Magazine
Pranita Upadhyaya. et al. [37]	2018	Conference
Qianyi Dai. et al. [38]	2018	Conference
R. ANGELINE [39]	2018	Conference
Reza Soltani. et al. [40]	2018	Conference
Sandro Amofa. et al. [41]	2018	Conference
Saqib Ali. et al. [42]	2018	Conference
Sebastian Friebe. et al. [43]	2018	Conference
Shanto Roy. et al. [44]	2018	Conference
Shi-Cho Cha. et al. [45]	2018	Journal
Shirley Crompton. et al. [46]	2018	Conference
Sushmita Ruj. et al. [47]	2018	Conference
Vero Estrada-Galinanes. et al. [48]	2018	Conference
Ahmed Afif Monrat. et al. [49]	2019	Journal
Ahmed Raza Rajput. et al. [50]	2019	Journal
Ajay Kumar Shrestha. et al. [51]	2019	Conference
Anang Hudaya Muhamad Amin. et al. [52]	2019	Conference
Bhabendu K. Mohanta. et al. [53]	2019	Conference
Bhabendu Kumar Mohanta. et al. [54]	2019	Conference
Dipti Ashok Belurgikar. et al. [55]	2019	Conference
Fariza Sabrina [56]	2019	Conference
Florian Zemler. et al. [57]	2019	Conference
Hongzhi Li. et al. [58]	2019	Journal
Huang Bowen. et al. [59]	2019	Conference
Hye-Young Paik. et al. [60]	2019	Journal
Ingo Weber. et al. [61]	2019	Conference

Malak Parmar. et al. [62]	2019	Conference
Martin Florian. et al. [63]	2019	Conference
Nilima D. Pai. et al. [64]	2019	Conference
Nitin Sukhija. et al. [65]	2019	Conference
Nitish Andola. et al. [66]	2019	Conference
Ping Zhong. et al. [67]	2019	Conference
Ronald Doku. et al. [68]	2019	Conference
Rujuta Shah. et al. [69]	2019	Conference
Shadan Ghaffaripour. et al. [70]	2019	Conference
Taylor Hardin. et al. [71]	2019	Conference
Thang X. Vu. et al. [72]	2019	Conference
Thorsten Weber. et al. [73]	2019	Conference
Tiffany Hyun-Jin Kim. et al. [74]	2019	Conference
Vinay Mahore. et al. [75]	2019	Conference
Wie Liang Sim. et al. [76]	2019	Conference
Xiaoguang Liu [77]	2019	Journal
Yiheng Liang. et al. [78]	2019	Conference
Yongseon Ji. et al. [79]	2019	Conference
Abdulbadi Sabir. et al. [80]	2020	Conference
Emanuele Bellini. et al. [81]	2020	Journal
James P. Howard. et al. [82]	2020	Magazine
Jãnis Grabis. et al. [83]	2020	Conference
Javed Ahmed. et al. [84]	2020	Conference
Kai Fan. et al. [85]	2020	Journal
Ma Zhaofeng. et al. [86]	2020	Journal
Manaf Zghaibeh. et al. [87]	2020	Journal
Mingxiao Du. et al. [88]	2020	Journal
Nguyen Binh Truong. et al. [89]	2020	Journal
Randhir Kumar. et al. [90]	2020	Conference
Richa Gupta. et al. [91]	2020	Conference
Saifull ah Khan. et al. [92]	2020	Conference
Shahriar Badsha. et al. [93]	2020	Conference
Soe Myint Myat. et al. [94]	2020	Conference
Yan Zhuang. et al. [95]	2020	Journal

5.1. Analysis of the Papers

We found that more relevant papers were published after 2015, and very few papers were published in the years 2016 and 2017. Additionally, 27% of the papers were published in 2018, and most papers, which amounts to 43%, were published in 2019. From 2020 onwards, we have 22 percent of the papers that are considered for review. The following Figure 4 gives us more details on the distribution of papers on a year-to-year basis.

Almost a few percent of the papers only discussed the technical part of the technology without a working prototype, out of all the papers which discussed an implementation, the most used technology is Ethereum, followed by Hyperledger Fabric. Figure 5 below shows the percentage of the technologies used for implementation.

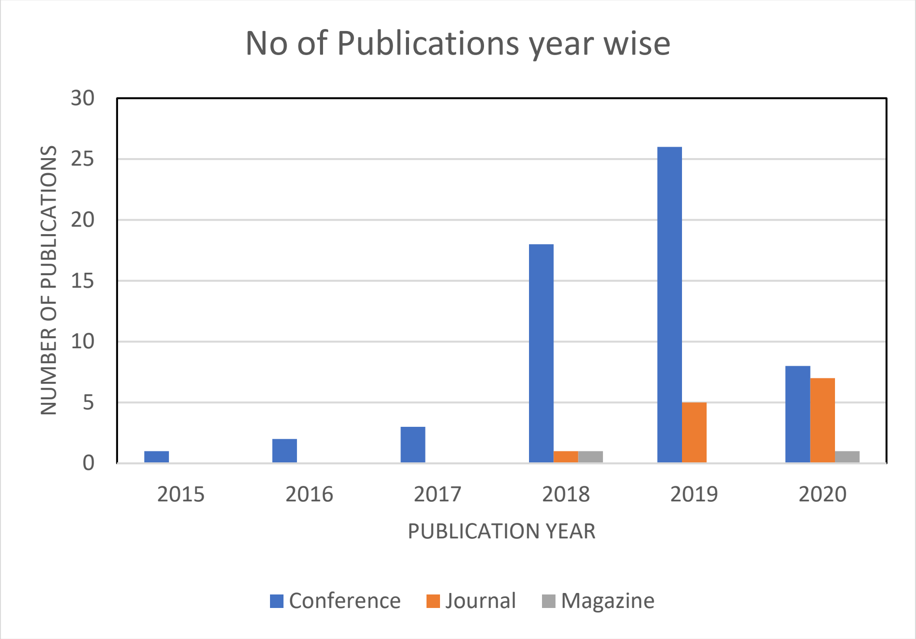

Figure 4. The number of publications per year.

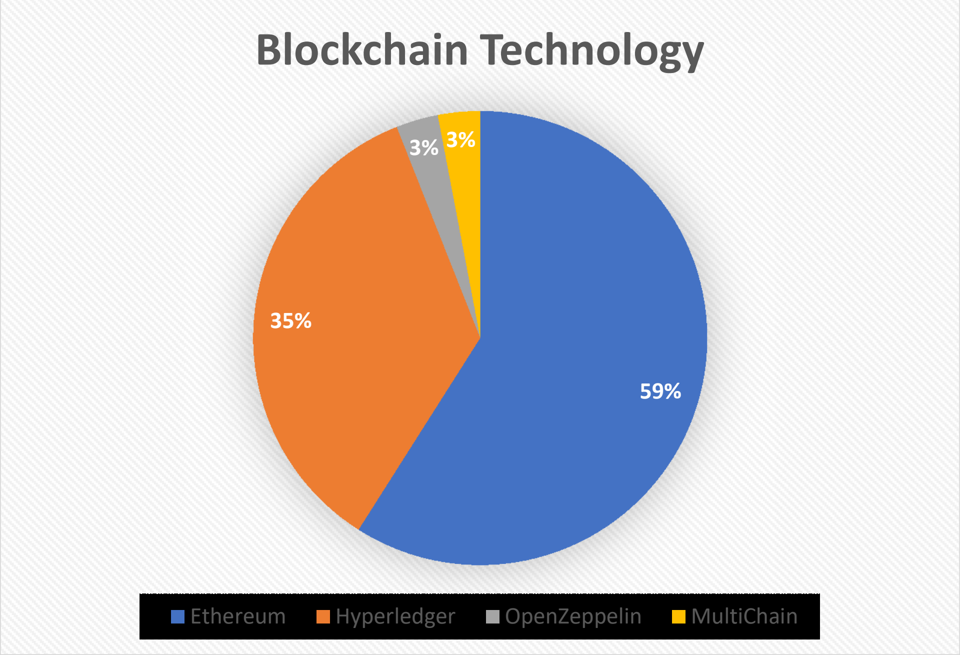

Figure 5. Choice of Blockchain platforms.

The papers we have reviewed included idea papers, idea papers with prototypes, and review papers. as shown in Figure 6. Many papers had technical details of the prototype implementation. Some papers included design ideas but no implementation or evaluation details. Review papers focused on various applications in the field.

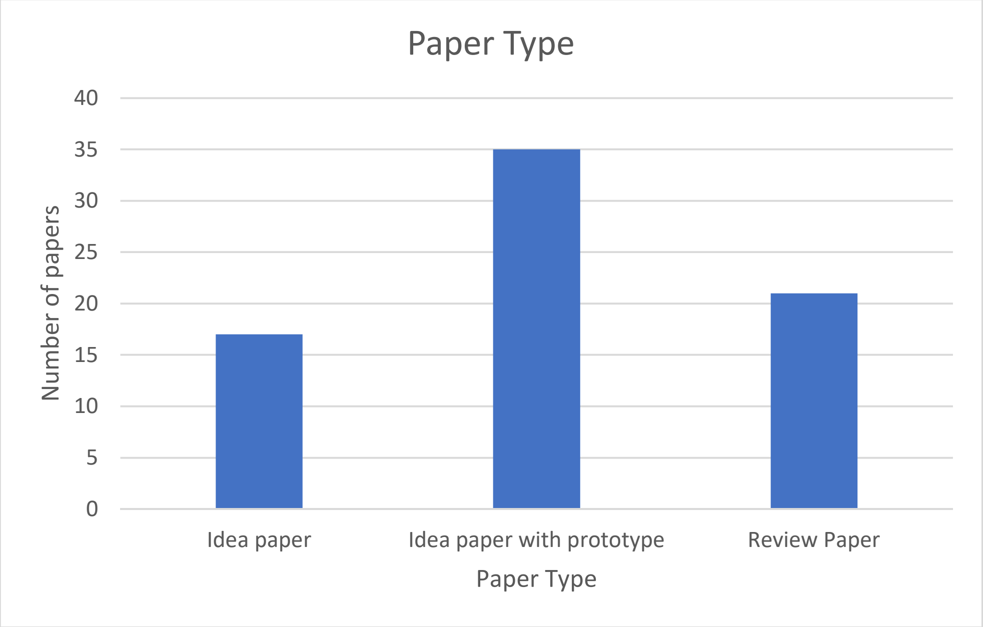

Figure 6. Paper types.

Finally, we have used the locations (countries) of those organizations of which writers of selected papers are associated to get an idea of the regional distribution of research group members interested in blockchain research. We have taken the lead author country details if the authors are from different countries. The geographical distribution of the papers chosen for the study is shown in Figure 7. From the figure, we can observe that authors in China, India, and the USA published most of the papers. They are followed by Australia, Canada, Germany, the UK, and Italy, respectively. Authors from the rest of the countries submitted less than two research papers.

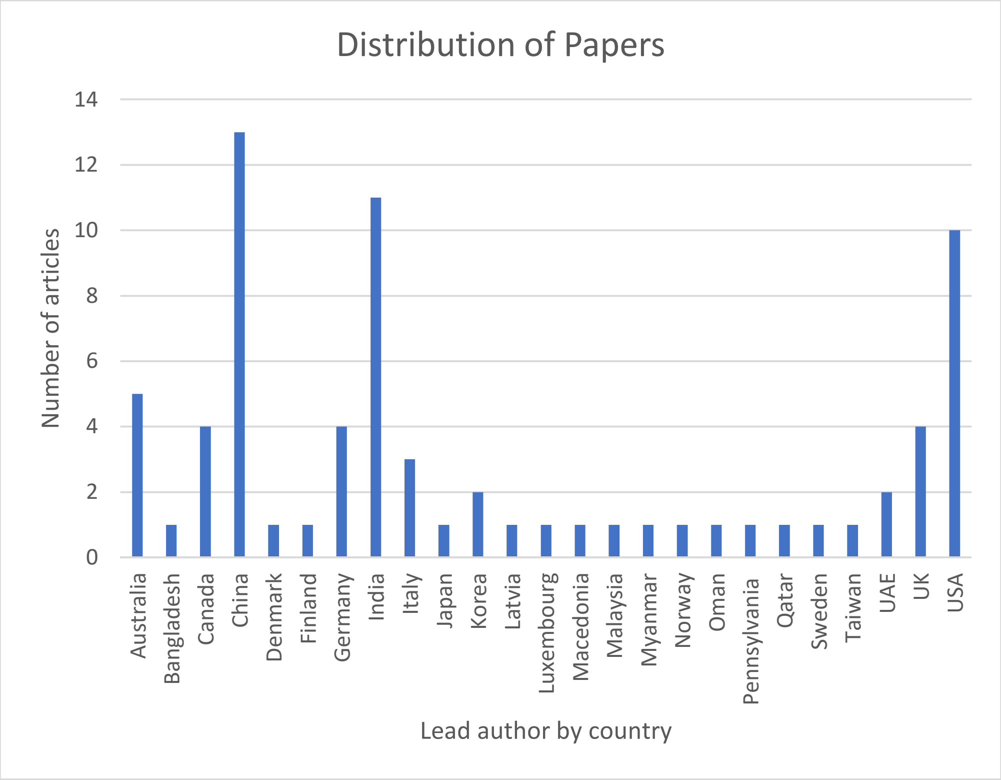

Figure 7. Distribution of papers by country of the lead author.

5.2. Classification of the Papers

Most of the selected papers were conference papers, and the next significant type of selected papers are journal type papers. We have also identified the industry sectors such as healthcare, IoT, identity management and storage, to classify the use cases of the papers and have discussed a few main sectors where Blockchain is implemented.

5.2.1. Healthcare

Researchers have identified that the healthcare industry is one of the primary industries that can benefit from Blockchain technology. As it follows the distributed ledger concept, medical records can be shared easily between the hospitals/doctors/researchers for various reasons, which can easily be used for managing a patient's data. Counterfeiting medicines are a big concern for the pharmaceutical industry [49]. Health research funding studies have shown that 10% to 30% of drugs sold in developing countries are counterfeit [96]. The WHO reports that 16% of counterfeit products have the wrong ingredients, while 17% have an imprecise amount of necessary ingredients [49]. The use of these can lead to severe health problems and sometimes cause death. Blockchain can be used to avoid this, as it is digitally timestamped, and information cannot be changed/tampered with.

As stated, the main advantage of Blockchain in the healthcare industry is that it can be used to track and manage the patient's data. Severe diseases require a personalized treatment, and a person cannot consult a single doctor for every disease. Hence, Blockchain is a platform where we can share this sensitive data, and we can make sure that it is safe and secure. Asaph Azaria and the team have proposed a framework called MedRec to share the medical information, which also has storage solutions [25]. They also introduced the incentives concept by asking the stakeholders to participate in the network and verify as miners [25]. S. Amofa also discussed the importance of sharing the data between doctors and built a framework using Ethereum [41]. In [37], Blockchain was implemented in a developing country, Nepal, where, with the implementation, there was a financial gain of 63%.

While it is important to share the data between the organizations, it is also important for researchers to access and analyze health information. Vero Estrada-Galinanes and K. Wac discussed such importance in [48] and proposed the development of an Open Health Archive (OHA), a shared forum for maintaining and archiving personal health records. The importance of the research in the health care sector is discussed in the articles [75,88] by the respective authors. The research articles [77,80] discussed the importance of sharing the data in the Cloud, as PII is not allowed directly in Blockchain because of GDPR, and they have also explained it with their respective working prototypes.

The research papers [70,95] examined the importance of user control over the data, which is shared, and working models have been built using Ethereum and Hyperledger Fabric, respectively. Emergency access to health records is discussed in [50]; it can be achieved with help of smart contracts. The author suggested having a smart contract that will give access to information in case of an emergency for a limited period. SHEMB is an Ethereum-based solution that requires a third party in storing data using a symmetrically searchable encryption technique to speed up access to information using the patient's search query [66].

5.2.2. IoT

This is another field where Blockchain implementation can revolutionize the world. IoT applications are those that are connected to the Internet and can communicate with each other. Though there are many advantages of IoT devices, the main concern is that they collect sensitive information like our location, etc., and they can be used to make or understand the behavioral patterns of a user. Therefore, Blockchain technology integration with IoT devices will result in privacy issues being nullified.

The papers [26,45] discussed the implementation of Blockchain in the IoT field and the limitations that come along with it. Cha, S.C. and others have suggested the design of a blockchain linked gateway that preserves user privacy preferences for IoT devices on the blockchain network adaptively and securely [45].To make sure the IoT data is secure, Fariza Sabrina came up with a solution that discusses the privacy data challenge. An approach is a service-oriented approach and a mix of public Blockchain (with smart contracts) and local off-chain data for entitlement management and control [56]. The architecture is implemented using Ethereum and helps to secure confidential data. In the article authored by [53], the paper discusses the importance of trust while integrating Blockchain and IoT. Here, the implementation is done using Ethereum Framework, and the decentralized network is laid between the patient, insurance provider, and hospital instead of a traditional centralized network. The main disadvantage of a centralized network is that it is a time taking process, and there is no proper transparency.

5.2.3. Identity Management

Usually, personal identity is verified using documents such as Social Number, license, and passport. However, there is hardly an efficient equivalent method for protecting online identities [49]. Using Blockchain, a digital identity/ID can be created and can be used for online transactions instead of using real identities. This way, we can eliminate the possibility of online fraud. Blockchain-based identity management solutions may allow customers to access and validate online purchases by simply using an authentication app instead of using a username and password or biometric system [97]. Additionally, the self-sovereign identity concept in Blockchain is introduced by D. Baars to eliminate identity theft [98]. A new way of storing important documents related to education is explained by Alan Colman and the team in [34], and it is implemented using Ethereum. The author proposed a framework that can store the data and authenticate the education-related documents where the authentication of documents is done by the University or College and stored on the Blockchain. As the data in Blockchain cannot be tampered with, we can always request authentication. Paul Dunphy et al. introduced a framework for identity management, using distributed ledger technology to improve decentralization, accountability, and user control [36].

5.2.4. Storage

Though direct PII cannot be stored in a Blockchain network, this can be used to store encrypted data. One of the main applications of Blockchain is the ability to combine with third parties like Cloud, etc., to store the data. This enables users to have data transparency and the ability to track the usage of their data. In [68], they introduced a new technique called interest groups, where each group will hold to a field data. Now the groups can sell/borrow/rent the data that they hold. They also spoke about the rewards that could be given for a group that offers the most relevant data. Data transparency is the main feature. As stated before, the size of a block and GDPR make it difficult to store data on Blockchain. Therefore, Saqib Ali and others came up with the idea of Pinger [42]. It stores the metadata of the files, while the original files are stored in various locations with the aid of a DHT (distributed hash table). Using Ethereum and IPFS (InterPlanetary File System), M. Alessi and the team came up with a prototype [34], which can store personal data and also has requested data service.

These are the main classifications that we found in the process. There are other fields like agriculture, where Blockchain is used. The importance of farmer's consent using Blockchain is mentioned in [99]. Consentio [100] is a general consent management system that is built on Hyperledger Fabric that can be used for various cases such as EHR (Health), small infrastructure (IoT), and social media. Few papers also discussed the main applications, challenges, and issues [27,60,63,64,81].

6. Discussion

In this section, we utilize our findings to cross-examiner the research questions we have identified in Section 4. We provide a discussion of our analysis and address the limitations of the review.

RQ1: How does Blockchain protect user privacy and data consent across various sectors?

Blockchain is used in various types of industries—healthcare, IoT, Identity Management, etc. The most common use cases are mentioned below in Table 3.

Table 3. Use cases in various sectors.

Field	Usage
Healthcare	To share the medical information securely between doctors/organizations/researchers
IoT	To have the user's privacy preference for IoT Devices
Identity Management	Management of identity verification
Storage	Tamper-proof activity monitoring and data access control protection

RQ2: What Blockchain-based applications have been built of the described use cases?

Although the concept of Blockchain was introduced in 2008, it is still a new technology for other sectors except for Finance. Many of the papers presented technical implementation; very few papers had a practical implementation, and few of those details are given in Table 4.

Table 4. Existing applications.

Field	Application
Healthcare	MedRec [25], SHEMB [66]
IoT	Blockchain-enabled Security Architecture [56]
Identity Management	Blockchain as a Notarization Service [34]
Storage	Pinger [42], Pledge [68]

Out of the implementations that have been developed, we have observed that Ethereum is the most used framework, and it is followed by Hyperledger Fabric. The concept of Smart Contracts in Ethereum is one of the main reasons it is the most used Framework.

RQ3: How are the limitations of current solutions addressed?

The main challenges are interoperability, block size, regulations, response time, and the GDPR rule "right to be forgotten". Interoperability is a big challenge that is being faced, as we cannot operate between two frameworks, and the integration of Blockchain with legacy systems is still an issue. After interoperability, the size of the network is a concern, as the Bitcoin network is around 270 GB, and Ethereum size already crossed 1 TB [101]. The main challenge with the size of these networks is the transaction speed and validation process. Due to the increasing size of the networks, the main challenge is to the validators/contributors who need to spend more money to make their nodes run. Not only the cost but also the response time of the network is impacted due to this. Now bigger blocks are very much challenging to running the network, whereas smaller blocks are feasible to run and work well with a third-party solution like Cloud. As a decentralized system, it does not have standard regulations making it vulnerable. Coming to another challenge in Blockchain technology is the GDPR rules that were introduced in 2018 to protect the PII of European Nations. It means that a person is entitled to ask the data to be erased. But Blockchain being immutable, it is impossible to erase data from the network. Finally, there are a few security concerns with the existing applications. A potential breach could leak all the user's data, as there have been several attacks on certain Blockchain applications. There is also a risk of identifying a user when there is adequate information available on the network.

There are few networks such as Cosmos [102] and Polkadot [103] that came up with the solution for interoperability. As a part of the Cosmos network, independent networks (called zones) are connected through the Cosmos Hub. Additionally, Ethereum 2 (also known as Serenity) solves a few critical issues with the introduction of concepts such as subchain and POS (Proof of Stake) [104]. These features now enable a person to maintain small transactions without mining, which reduces the bloating problem. With the help of the subchain, now the transactions will be cheaper and quicker. Additionally, the 51% percent attack can be avoided with the POS concept, as a person/miner with more than 51 percent of control would not want to attack their network. Additionally, erasing data from local storage is possible, as we do not store the PII on the network. This has been explained by M. Florian in [63]. The author suggested an approach where we can completely delete the undesirable data from local nodes. By this, we can ensure the GDPR rule, which is the right to be forgotten. Additionally, only a few nodes can participate in the consensus and validation processes to boost the efficiency of the system and increase the processing speed [105]. Currently, more extensive research is going to improve the current standards and conditions of Blockchain technology to make it more useful. Permissioned Blockchain should be used instead of the public Blockchains to avoid attacks and sharing of the data. To protect the user information on the network, encryption technologies are being used, and techniques are also to be updated periodically.

RQ4: What are the major challenges for future research?

Blockchain solves many real-world problems, such as data authentication, data storage, and data privacy. It is still in the early stages of implementation, as there are not many working prototypes at this moment. Therefore, extensive research is going in every field to implement this technology, especially in the field of data management, as we believe that it can eliminate the process of filling up forms, as the data can be shared between any departments/organizations securely. More working models are needed to come up with the best practice to implement for managing the data; for this reason, the prototypes must be tested thoroughly. We believe it will play a crucial role in the future healthcare, IoT, data storage, identity management, and Telecom sectors, respectively. Additionally, to make sure the new working prototypes are approachable to the people, there is a need for a few regulations to be introduced.

One of the main focuses is also on the interoperability of the frameworks. Apart from interoperability, the other main challenges that need to be worked upon are security and privacy; the speed of adding blocks to a network is one constant area that also needs to be checked. These are a few areas where there are open research questions. It is also highly essential that Blockchain complies with all the regulations set by GDPR. By meeting all the requirements, it will give a boost to the companies to integrate into their existing solutions.

Limitations of the Review

Despite the various benefits of conducting a systematic analysis, certain drawbacks need to be considered: bias in the collection, bias in publication, imprecision in the extraction of data, and misclassification [23]. To eliminate the bias, we investigated the papers irrespective of novelty or unremarkable outcomes. To achieve a maximum possible number of papers, an efficient search protocol was developed for research papers, followed by a search with all alternative keywords. Moreover, criteria for inclusion and exclusion have been established to ensure that the papers included are focused on research topics that are well linked to the research goals.

Inaccuracies in the extraction of data and misjudgments may be attributed to the reviewer's failure to accurately retrieve information and data from its records. We have used an Excel sheet throughout the process to make sure all the extracted data have been properly recorded.

7. Conclusions and Future Work

Blockchain is an evolving technology that will revolutionize the information technology world, because it can be applied in many applications domains where an immutable ledger is useful. To evaluate the applications of blockchain to consent management and private data management, we have conducted this systematic review using the PRISMA guidelines to identify the current solutions, limitations and research challenges. Overall, 73 papers were studied in detail to perform this review.

Our study indicates that Blockchain has been implemented in various fields such as healthcare, IoT, data storage, and management. Many prototypes have been developed and are already tested in real-world scenarios. More research is being conducted on this, and in the future, more research will be done to understand and evaluate the implementations. Further research is aimed at solving the issues associated with the use of blockchain technology such as scalability, latency, interoperability, privacy, and security.

Author Contributions: Writing—original draft preparation: P.V.K.; supervision and writing—review and editing: Q.H.M. All authors have read and agreed to the published version of the manuscript.

Funding: We acknowledge the support of the Office of the Privacy Commissioner of Canada (OPC) Contributions Program 2020–2021.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Number of IoT Devices 2015–2025. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed on 21 June 2020).
2. Isaak, J.; Hanna, M.J. User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer* **2018**, *51*, 56–59, doi:10.1109/MC.2018.3191268.
3. Top 10 Tech Giants Are Diving into Blockchain. Available online: https://medium.com/aelfblockchain/top-10-tech-giants-are-diving-into-blockchain-a2e7d9b44697 (accessed on 21 June 2020).
4. Hyperledger Blockchain, "Hyperledger". Available online: https://www.hyperledger.org/ (accessed on 21 August 2020).
5. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400, doi:10.3390/app9122400.
6. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56, doi:10.3390/healthcare7020056.
7. Kuo, T.T.; Rojas, H.Z.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478, doi:10.1093/jamia/ocy185.
8. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81, doi:10.1016/j.tele.2018.11.006.
9. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; Altman, D.; Antes, G.; Atkins, D.; Barbour, V.; Barrowman, N.; Berlin, J.A.; et al. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med*. **2009**, *6*, 336–341.
10. Overview of Consent Management. Available online: https://www.ibm.com/support/knowledgecenter/SSWSR9_11.6.0/com.ibm.mdmhs.overview.doc/consentmanagementoverview.html (accessed on 10 June 2020).
11. Consent Management. Available online: https://www.gartner.com/en/information-technology/glossary/consent-management (accessed on 12 June 2020).
12. Privacy Regulation "Recital 39 EU GDPR". Available online: https://www.privacy-regulation.eu/en/recital-39-GDPR.htm (accessed on 21 August 2020).
13. GDPR 'What Are the GDPR Fines. Available online: https://gdpr.eu/fines/ (accessed on 2 September 2020).
14. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography Springer, Berlin/Heidelberg, Germany, 11 August 1990.

15. Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System". Available online: https://bitcoin.org/bitcoin.pdf (accessed on 22 August 2020).
16. Tar, A. Proof-of-Work, Explained. 2018. Available online: https://cointelegraph.com/explained/proof-of-work-explained (accessed on 12 June 2020).
17. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*, 9.
18. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207, doi:10.3390/app9061207.
19. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94, doi:10.3390/electronics9010094.
20. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326, doi:10.3390/s19020326.
21. Winnicka, A.; Kęsik, K. Idea of Using Blockchain Technique for Choosing the Best Configuration of Weights in Neural Networks. *Algorithms* **2019**, *12*, 163, doi:10.3390/a12080163.
22. Alessi, M.; Camillo, A.; Giangreco, E.; Matera, M.; Pino, S.; Storelli, D. Make users own their data: A decentralized personal data store prototype based on ethereum and ipfs. In Proceedings of the 2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia, 26–29 June 2018.
23. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering, Version 2.3*; EBSE Technical Report, EBSE-2007-01; Keele University: Newcastle, UK; University of Durham: Durham, UK, 2007.
24. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 22 May 2015.
25. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016.
26. Conoscenti, M., Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 Dececember. 2016.
27. Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017–17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017.
28. Dai, F.; Shi, Y.; Meng, N.; Wei, L.; Ye, Z. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In Proceedings of the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, 11–13 November 2017.
29. Kiyomoto, S.; Rahman, M.S.; Basu, A. On blockchain-based anonymized dataset distribution platform. In Proceedings of the 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, UK, 7–9 June 2017.
30. Singh, J.; Michels, J.D. Blockchain as a service (BaaS): Providers and trust. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 23–27 April 2018.
31. Zhang, K.; Jacobsen, H.A. Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018.
32. Zaerens, K. Concept for controlled business critical information sharing using smart contracts. In Proceedings of the 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 24–26 October 2018.
33. Liu, L.; Piao, C.; Jiang, X.; Zheng, L. Research on Governmental Data Sharing Based on Local Differential Privacy Approach. In Proceedings of the 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), Xi'an, China, 12–14 October 2018.
34. Chowdhury, M.J.M.; Colman, A.; Kabir, M.A.; Han, J.; Sarda, P. Blockchain as a notarization service for data sharing with personal data store. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
35. Al-Zaben, N.; Onik, M.M.H.; Yang, J.; Lee, N.Y.; Kim, C.S. General data protection regulation complied blockchain architecture for personally identifiable information management. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018.
36. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29, doi:10.1109/MSP.2018.3111247.
37. Upadhyaya, P.; Upadhyay, S.K.; Subedi, B.; Subedi, B.; Gaire, A. Revolutionizing healthcare systems of a developing country using Blockchain. In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018.
38. Dai, Q.; Xv, K.; Guo, S.; Dai, L.; Zhou, Z. A private data protection scheme based on blockchain under pipeline model. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018.
39. Angeline, R. An immortal database system for the decentralized internet. In Proceedings of the 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 15–16 October 2018.

40. Soltani, R.; Nguyen, U.T.; An, A. A new approach to client onboarding using self-sovereign identity and distributed ledger. In Proceedings of the 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), Halifax, NS, Canada, 30 July–3 August 2018.
41. Amofa, S.; Sifah, E.B.; Kwame, O.B.; Abla, S.; Xia, Q.; Gee, J.C.; Gao, J. A blockchain-based architecture framework for secure sharing of personal health data. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018.
42. Ali, S.; Wang, G.; White, B.; Cottrell, R.L. A blockchain-based decentralized data storage and access framework for pinger. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
43. Friebe, S.; Sobik, I.; Zitterbart, M. Decentid: Decentralized and privacy-preserving identity storage system using smart contracts. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
44. Roy, S.; Ashaduzzaman, M.; Hassan, M.; Chowdhury, A.R. Blockchain for IoT security and management: Current prospects, challenges and future directions. In Proceedings of the 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 18–20 December 2018.
45. Cha, S.C.; Chen, J.F.; Su, C.; Yeh, K.H. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access* **2018**, *6*, 24639–24649, doi:10.1109/ACCESS.2018.2799942.
46. Crompton, S.; Jensen, J. Towards a secure and gdpr-compliant fog-to-cloud platform. In Proceedings of the 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), Zurich, Switzerland, 17–20 December 2018.
47. Ruj, S.; Rahman; M.S.; Basu, A.; Kiyomoto, S. Blockstore: A secure decentralized storage framework on blockchain. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018.
48. Estrada-Galinanes, V.; Wac, K. Visions and challenges in managing and preserving data to measure quality of life. In Proceedings of the 2018 IEEE 3rd International Workshops on Foundations and Applications of Self* Systems (FAS* W), Trento, Italy, 3–7 September 2018.
49. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151, doi:10.1109/ACCESS.2019.2936094.
50. Rajput, A.R.; Li, Q.; Ahvanooey, M.T.; Masood, I. EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access* **2019**, *7*, 84304–88431, doi:10.1109/ACCESS.2019.2917976.
51. Shrestha, A.K.; Vassileva, J. User Acceptance of Usable Blockchain-Based Research Data Sharing System: An Extended TAM-Based Study. In Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Los Angeles, CA, USA, 12–14 December 2019.
52. Amin, A.H.M.; Siddartha, S.; Almehairi, R.K.M.O.M.; Albalooshi, Y.H.M.A.; Alsuwaidi, S.A.S.A.; Shamsi, J.O.S.O.K.; Almatrooshi, A.N.T.R. Permissioned Blockchain Design for Integrated Healthcare Data Management. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019.
53. Mohanta, B.K.; Panda, S.S.; Satapathy, U.; Jena, D.; Gountia, D. Trustworthy Management in Decentralized IoT Application using Blockchain. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019.
54. Mohanta, B.K.; Satapathy, U.; Panda, S.S.; Jena, D. A Novel Approach to Solve Security and Privacy Issues for IoT Applications Using Blockchain. In Proceedings of the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 19–21 December 2019.
55. Belurgikar, D.A.; Kshirsagar, J.K.; Dhananjaya, K.K.; Vineeth, N. Identity Solutions for Verification using Blockchain Technology. In Proceedings of the 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 19–20 March 2019.
56. Sabrina, F. A Novel Entitlement-based Blockchain-enabled Security Architecture for IoT. In Proceedings of the 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, 27–29 November 2019.
57. Zemler, F.; Westner, M. Blockchain and GDPR: Application scenarios and compliance requirements. In Proceedings of the 2019 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 25–29 August 2019.
58. Li, H.; Han, D. EduRSS: A blockchain-based educational records secure storage and sharing scheme. *IEEE Access* **2019**, *7*, 179273–179289, doi:10.1109/ACCESS.2019.2956157.
59. Bowen, H.; Yi, L.; Li, F.; Xinhua, D.; Ping, C. Blockchain-based Access Control Data Distribution System. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019.
60. Paik, H.Y.; Xu, X.; Bandara, H.D.; Lee, S.U.; Lo, S.K. Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance. *IEEE Access* **2019**, *7*, 186091–186107, doi:10.1109/ACCESS.2019.2961404.

61. Weber, I.; Lu, Q.; Tran, A.B.; Deshmukh, A.; Gorski, M.; Strazds, M. A platform architecture for multi-tenant blockchain-based systems. In Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 25–29 March 2019.
62. Parmar, M.; Shah, S. Reinforcing Security of Medical Data using Blockchain. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May 2019.
63. Florian, M.; Henningsen, S.; Beaucamp, S.; Scheuermann, B. Erasing data from blockchain nodes. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019.
64. Pai, N.D.; Mondal, S. A study on Blockchain enabled Applications and its Security Issues. In Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 29–31 March 2019.
65. Sukhija, N.; Bautista; E.; Moore, M.; Sample, J.G. Employing Blockchain Technology for Decentralized Crowdsourced Data Access and Management. In Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 19–23 August 2019.
66. Andola, N.; Prakash, S.; Venkatesan, S.; Verma, S. SHEMB: A secure approach for healthcare management system using blockchain. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019.
67. Zhong, P.; Zhong, Q.; Mi, H.; Zhang, S.; Xiang, Y. Privacy-Protected Blockchain System. In Proceedings of the 2019 20th IEEE International Conference on Mobile Data Management (MDM), Hong Kong, China, 10–13 June 2019.
68. Doku, R.; Rawat, D. Pledge: A private ledger based decentralized data sharing framework. In Proceedings of the 2019 Spring Simulation Conference (SpringSim), Tucson, AZ, USA, 29 April–2 May 2019.
69. Shah, R.; Sridaran, R. A Study on Security and Privacy related Issues in Blockchain Based Applications. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019.
70. Ghaffaripour, S.; Miri, A. Cryptographically Enforced Access Control in Blockchain-Based Platforms. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019.
71. Hardin, T.; Kotz, D. Blockchain in Health Data Systems: A Survey. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019.
72. Vu, T.X.; Chatzinotas, S.; Ottersten, B. Blockchain-based Content Delivery Networks: Content Transparency Meets User Privacy. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019.
73. Weber, T.; Prinz, W. Trading User Data: A Blockchain Based Approach. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019.
74. Kim, T.H.J.; Lampkins, J. SSP: Self-Sovereign Privacy for Internet of Things Using Blockchain and MPC. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019.
75. Mahore, V.; Aggarwal, P.; Andola, N.; Venkatesan, S. Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019.
76. Sim, W.L.; Chua, H.N.; Tahir, M. Blockchain for Identity Management: The Implications to Personal Data Protection. In Proceedings of the 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 19–21 November 2019.
77. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A blockchain-based medical data sharing and protection scheme. *IEEE Access* **2019**, *7*, 118943–118953, doi:10.1109/ACCESS.2019.2937685.
78. Liang, Y. Identity Verification and Management of Electronic Health Records with Blockchain Technology. In Proceedings of the 2019 IEEE International Conference on Healthcare Informatics (ICHI), Xi'an, China, 10–13 June 2019.
79. Ji, Y.; Bae, S.; Shin, Y. A personal information management using blockchain. In Proceedings of the 2019 International Conference on Information Networking (ICOIN), Kuala Lumpur, Malaysia, 9–11 January 2019.
80. Sabir, A.; Fetais, N. A Practical Universal Consortium Blockchain Paradigm for Patient Data Portability on the Cloud Utilizing Delegated Identity Management. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020.
81. Bellini, E.; Iraqi, Y.; Damiani, E. Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access* **2020**, *8*, 21127–21151, doi:10.1109/ACCESS.2020.2969820.
82. Howard, J.P., II; Vachino, M.E. Blockchain Compliance with Federal Cryptographic Information-Processing Standards. *IEEE Secur. Priv.* **2020**, *18*, 65–70, doi:10.1109/MSEC.2019.2944290.
83. Grabis, J.; Stankovski, V.; Zariņš, R. Blockchain Enabled Distributed Storage and Sharing of Personal Data Assets. In Proceedings of the 2020 IEEE 36th International Conference on Data Engineering Workshops (ICDEW), Dallas, TX, USA, 20–24 April 2020.
84. Ahmed, J.; Yildirim, S.; Nowostaki, M.; Ramachandra, R.; Elezaj, O.; Abomohara, M. GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020.

85. Fan, K.; Pan, Q.; Zhang, K.; Bai, Y.; Sun, S.; Li, H.; Yang, Y. A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5826–5835, doi:10.1109/TVT.2020.2968094.
86. Zhaofeng, M.; Xiaochang, W.; Jain, D.K.; Khan, H.; Hongmin, G.; Zhen, W. A blockchain-based trusted data management scheme in edge computing. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2013–2021, doi:10.1109/TII.2019.2933482.
87. Zghaibeh, M.; Farooq, U.; Hasan, N.U.; Baig, I. SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities. *IEEE Access* **2020**, *8*, 70030–70043, doi:10.1109/ACCESS.2020.2986789.
88. Du, M.; Chen, Q.; Chen, J.; Ma, X. An optimized consortium blockchain for medical information sharing. *IEEE Trans. Eng. Manag.* **2020**, 1–13, doi:10.1109/TEM.2020.2966832.
89. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1746–1761, doi:10.1109/TIFS.2019.2948287.
90. Kumar, R.; Marchang, N.; Tripathi, R. Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain. In Proceedings of the 2020 International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 7–11 January 2020.
91. Gupta, R.; Shukla, V.K.; Rao, S.S.; Anwar, S.; Sharma, P.; Bathla, R. Enhancing Privacy through "Smart Contract" Using Blockchain-Based Dynamic Access Control. In Proceedings of the 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 9–10 January 2020.
92. Ah Khan, S.; Jadhav, A.; Bharadwaj, I.; Rooj, M.; Shiravale, S. Blockchain and the Identity based Encryption Scheme for High Data Security. In Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020.
93. Badsha, S.; Vakilinia, I.; Sengupta, S. Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020.
94. Myat, S.M.; Soe, T.N. Preserving the Privacy for University Data Using Blockchain and Attribute-based Encryption. In Proceedings of the 2020 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 27–28 February 2020.
95. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176, doi:10.1109/JBHI.2020.2993072.
96. Glass, B.D. Counterfeit drugs and medical devices in developing countries. *Res. Rep. Trop. Med.* **2014**, *5*, 11–22, doi:10.2147/RRTM.S39354.
97. Jacobovitz, O. Blockchain for Identity Management. Available online: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf (accessed on 19 August 2020).
98. Baars, D.S. Towards self-sovereign identity using blockchain technology. Master's Thesis, University of Twente, Eschede, The Netherlands, 2016.
99. Topart, L.; Genestier, P.; Picaud, Y. Blockchain brings confidence to facilitate the flow of data in the agricultural field. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020.
100. 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.
101. Nitish Singh. Blockchain Size: Things You Should Know. Available online: https://101blockchains.com/blockchain-size/ (accessed on 10 June 2020).
102. Cosmos Network. Available online: https://cosmos.network/ (accessed on 19 August 2020).
103. Polkadot. Available online: https://polkadot.network/ (accessed on 19 August 2020).
104. Ethereum, "Ethereum Whitepaper". Available online: https://ethereum.org/en/whitepaper/ (accessed on 19 August 2020).
105. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain Technology Innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.