Journal of King Saud University – Computer and Information Sciences 34 (2022) 5782–5796

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A systematic literature mapping on secure identity management using blockchain technology

Tripti Rathee [a,b,*], Parvinder Singh [c]

[a] Research Scholar, Department of Computer Science & Engineering, DCRUST, Murthal, Haryana, India
[b] Assistant Professor, Department of Information Technology, Maharaja Surajmal Institute of Technology, Delhi, India
[c] Professor, Department of Computer Science & Engineering, DCRUST, Murthal, Haryana, India

ARTICLE INFO

Article history:
Received 1 February 2021
Revised 15 March 2021
Accepted 16 March 2021
Available online 26 March 2021

Keywords:
Blockchain
Distributed ledger
Digital identity
Access management

ABSTRACT

After the acceptance of blockchain technology, there have been applications which aim to use blockchain in their fields. Various approaches have been proposed in past to build a secure Identity Management (IdM) System. This is a novel systematic literature mapping of IdM in blockchain. This paper provides an extensive review on IdM with emphasis on how the emergence of blockchain has addressed the IdM challenges faced over the years. A thorough study has been done on the existing literature. The primary and secondary "search string" were identified and search was conducted on five databases; and after screening the analysis was done. Out of the total studied literature, 30 primary studies published from 2009 to 2020 were selected. Through this paper, the researchers will be able to: 1) find out the research trends in IdM using blockchain, 2) understand the challenges in IdM and report whether blockchain can solve the IdM challenges, 3) scrutinize and understand how the different frameworks of IdM would deal with security, integrity and privacy problems, 4) know about initiatives taken for IdM using blockchain, 5) which consensus algorithms are popular among blockchains, 6) know about the research projects going on in the field of IdM using blockchain.

Contents

* Corresponding author at: Department of Computer Science & Engineering, DCRUST, Murthal, Haryana, India.
E-mail address: rathee.tripti@gmail.com (T. Rathee).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2021.03.005
1319-1578/

1. Introduction & Motivation

Digital Identity is an online identity which is created by an individual in cyberspace. Just like the information on a passport identifies the owner for a specific purpose, the digital identity recognizes the holder of the identity with some digital identifiers like E-mail address, domain name or some URL. Since we are taking a step forward towards the use of digital technologies therefore require some system which is able to recognize who are the expected users (Lee and Member, 2018) and authorize their name, address and personality (Buchmann et al., 2017; Augot et al., 2017a; Leiding and Norta, 2017; Lemieux and Lemieux, 2016). Nowadays, government services, personalized services and the business services applications hold and transform personal information of the users accordingly. The Digital Identity on the web is still stored on some central repositories and managed by third party people who in turn are tampering and deleting user's data without authorization. This leads to a situation of worry as there can be identity theft, security theft, etc., and therefore requires very vigorous IdM solutions. Digital Identity is a much generous and global issue which needs to be dealt with.

IdM systems are being used by the service providers (SP) so as to authenticate the users and to grant access to the services. Identity and Access Management (IAM) environments include many users and service providers. IAM systems give each user an account and set of capabilities enabling users to go to SP and demonstrate the ownership of accounts and then receive services based on their capabilities. Since the digital identity of the users is crippled and fragmented between various service providers therefore the users have an awful experience because they have monotonous registrations and user name as well as passwords. The situation leads to having an insecure system as the users use same password for many websites. If an effective access control mechanism is missing, then it will definitely hinder the security and privacy of user's confidential information (Qiu et al., 2020). There have been heaps of high profile security hacks and leaks of private data, as well as claims where unencrypted data has been cracked and hacked and put to vulnerable theft. The major problem lies in the fact that the private data is put into central repositories and probably is under the control of intermediaries and third party authorities. The reliance on the central repository servers may prove to be highly ruinous, not only digital but also physical. So there exist many problems with the current state of IdM systems. According to the Economist (Rouven Heck, n.d.) "Trust" is the key to any IdM System. With the availability of public/private key cryptography and distributed ledger technology named Blockchain, the above mentioned problem can be solved (El Haddouti and El Kettani, 2019). The Blockchain Technology can be used to deliver the trust infrastructure to everyone who is a part of the network.

The number of survey papers in blockchain is increasing continuously. Sanka et al. (2021) have surveyed the overall state of art of blockchain technology and its recent development and applications. Toufaily et al. (2021) have scrutinized the challenges and suggestions related to blockchain adoption from entrepreneur's perspective. Asaf et al. (2020) have provided a detailed survey on the adoption of blockchain technology for "The Named Data Networking". Lone and Naaz (2021) have presented a systematic literature review which focuses on the use of blockchain smart contract for securing Internet and IoT. Ali (Ali et al., 2020) have presented a systematic literature review on blockchain in the finance field. Lim et al. (2021) have provided an extensive review on the use of blockchain for supply chain management. Vacca et al. (2020) have used software engineering approach to carry out an extensive study on the techniques, and tools used for development of blockchain based software as well as identified the challenges faced.

There are mainly two landmark literature surveys focusing IdM and blockchain (Mohanta et al., 2019; Liu et al., 2020). However, the studies published by them do not include: 1) the identity management initiatives using blockchain technology, 2) the popularity of consensus mechanisms has not been evaluated so far, 3) the papers published between 2009 and 2016 have not been evaluated, 4) the studies do not involve the research projects undergoing in the field of IdM and blockchain technology. The curiosity among the researchers' for blockchain has led to a need for an analytical evaluation and assimilation of existing literature in the field of IdM using Blockchain technology. Although Systematic mappings are time consuming yet they provide clear and thorough information on the research on going. This paper identifies the key frameworks of IdM on which blockchain has been applied so far, discusses the gaps and suggest opportunities for future researchers.

1.1. Motivation for Work

- Considering Blockchain as a successful technology, the researchers are striving to integrate blockchain in the current generation IdM solutions. Therefore; our study on blockchain and IdM goes beyond source code.
- Upon Assessing state of art on IdM using blockchain technology, we realized the lack of systematic literature mapping. Thus we summarized the existing research on IdM and provided an extensive study of IdM, the challenges faced over time, frameworks of IdM using blockchain, various initiatives taken for IdM using blockchain so far, and the most popular consensus mechanism in blockchain and reported research gaps for further investigation.

The remainder of the paper is formulated as follows: Section 2 describes the background of Identity Management and blockchain

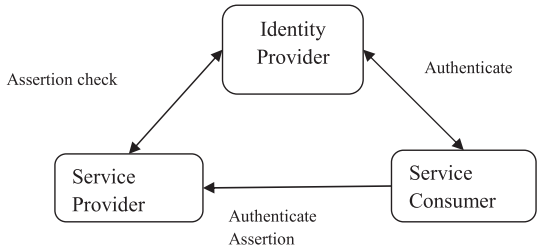

Fig. 1. Identity Federation Model (Stefanova et al., 2010).

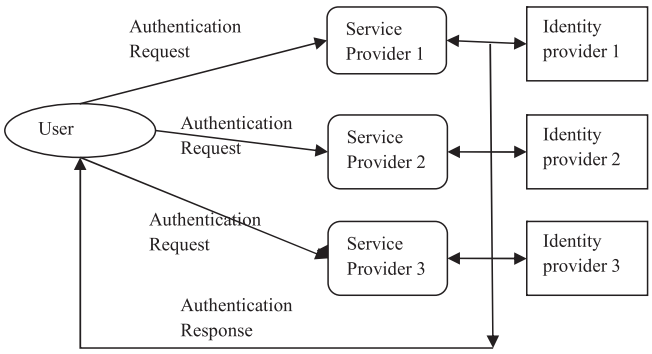

Fig. 2. Isolated IdM Model.

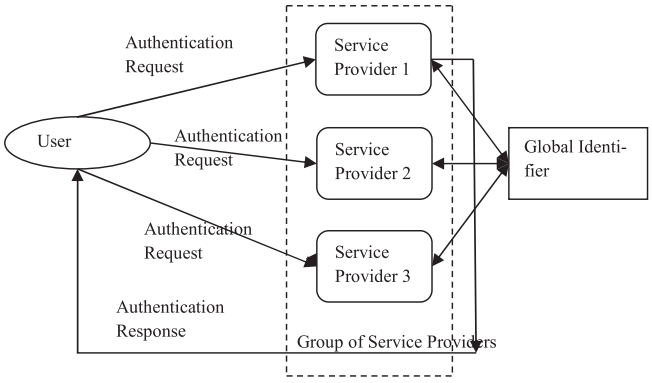

Fig. 3. Federated IdM Model.

technology. Section 3 provides the review methodology used including the research questions. Section 4 provides the result of systematic literature mapping. The important discussion about the research gaps and opportunities are discussed and finally Section 5 concludes the paper.

2. Identity Management and blockchain background

In this section, a brief description about IdM including models used and Identity Management challenges are described. Then a detail description about blockchain, types of blockchain and blockchain application are discussed.

2.1. Identity Management

Identity and Identity Management have always been as emerging topic of research in the literature (Halperin and Backhouse, 2008; Jensen, 2012; Jensen and Jaatun, 2012). Identity Management has become one of the top priorities in this era of Internet because of the presence of digital identity and the people using the digital identities. A majority of the population now days have some or the other form of digital identity because they are spending a lot of time over the Internet and using the services provided through Internet. The traditional IdM models have been designed effective for the service providers but not for the users (Josang et al., 2007) because the users have to remember multiple passwords for accessing multiple web sites. A classification of various IdM strategies is given by (Josang et al., 2007) which includes the aspects like privacy and usability of IdM solutions. At the very basic level, IdM consists of service provider and the service consumer who can perform any kind of transaction without worrying about the security and the privacy associated with each transaction. By including an identity provider can help to establish the trust between the two. The Identity Management architecture described by (Stefanova et al., 2010) is represented in Fig. 1.

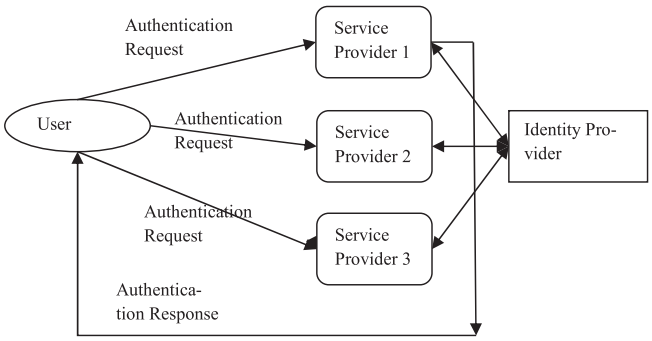

Fig. 4. Centralized IdM Model.

2.2. Identity management models

After studying the existing literature on Identity Management models (Jøsang et al., 2005; Ahn and Ko, 2007), we can classify IdM models into three categories, Isolated IdM, Federated IdM and Centralized IdM. In *Isolated IdM,* every user is provided with a unique identifier by the identity provider so as to have an access to the isolated service requested by the user (example a user name or a password). Isolated IdM is being used by rarely now a day because of the availability of the online services in abundance. Fig. 2 represents the architecture of an Isolated IdM model.

In *Federated IdM*, there is a group of service providers who define a set of protocols and recognizes the identifiers of the users. The services provided by all the service providers in the group can be accessed by an individual user who is the part of that group. Fig. 3 represents the architecture of a Federated IdM model. A user centric identity management model using trusted modules has been proposed by (Vossaert et al., 2013). An extension of already existing Federated IdM using user centric approach is done by (Suriadi et al., 2007). A project PRIME (Leenes, 2014) has implemented a framework for processing personal data (Camenisch et al., 2005).

In *Centralized IdM*, there is only one common Identity provider and the same identifier and credential are used by each service provider. The user has access to all the services using the same credentials. This model is further classified as Common identifier model, *meta*-identifier model and Single Sign On (SSO) model (Jøsang et al., 2005). The architecture of centralized IdM model is represented in Fig. 4.

2.3. Identity management challenges

Traditional IdM systems were centralized and controlled by a single entity. The authentication and authorization was guaranteed by a "Trusted third party". Several IdM models have been proposed in the past (Stefanova et al., 2010). The main function of any IdM system is to bind together the "identifier" and the "attributes" securely (Dunphy and Petitcolas, 2018). According to (Dhamija and Dusseault, 2008) poorly designed IdM systems can aggravate existing security problems and create opportunities to extract personal information from users. *Security, Privacy and Anonymity* are the major challenges while building a successful IdM system (Torres et al., 2012). Experts have considered *Affordability, Integrity, Trustworthiness and Interoperability* as important factors for a good IdM system (Weber et al., 2010). We considered the above seven challenges of IdM and analyzed whether the use of blockchain technology can solve the above mentioned IdM challenges.

In the context of IdM, *Security* can be achieved by avoiding single point of failure and by minimizing the disclosure of user data. Identity Theft is one of the concerns of a successful IdM (Bhargav-Spantzel et al., 2006). The user should have an access to his data and should have control over his private data. Since the digital identities in the cyberspace can be easily copied and stolen, so it is difficult to prevent the attacks in the cyberspace (Bertino et al., 2009). The identity crisis due to lack of security has been studied by (AlpAlpárr et al., 2013). The reaction to the release of Ashley Madison's dossier of more than 30 million people seeking affairs was one of muted resignation (Adee, 2015).

Privacy is another major challenges in IdM System (Shin et al., 2009). It is an essential requirement for a good IdM system. An IdM system involves the sharing of personal information among the user and the service provider. The loss of privacy can result in the inadmissible use of user's private information by the service providers. On the user side, there should be more control over their individual identity attributes so as to increase the individual's privacy provided the security is not compromised. The authors in (Rossudowski et al., 2010) proposes architecture to allow a single smart card to be used in a dynamic multiple application environments. The authors in (Amo et al., 2020) have implemented a plugin in a Moodle system which can solve privacy and identity protection problems in Learning Management Systems. A comparative analysis of various IdM systems has been done in (Ferdous and Poet, 2012) and they found out that none of the compared IdM Systems could be declared as Ideal in protecting privacy but were usable.

Further, it is expected that *Anonymity* should be achieved at all possible levels while designing a successful IdM system. The user should be able to have a control over their private information and how access should be provided to the person who is seeking the information. Protection of user identities and personal information can be achieved by using the principle of pseudo anonymity (Ahn and Lam, 2005). The user should be able to decide which type of identities should be shared further. Various Identity Management solutions have been proposed in the literature ("Future of Identity in the Information Society," n.d.; Leenes, 2014; Pérez-Méndez et al., 2010) which aims to provide technological development to control and monitor identities.

Affordability is categorized as a general requirement while designing an IdM (SNG, 2003). The term affordability itself specifies the meaning i.e whether the technology or the system is affordable enough to be accepted in the future or not. So the cost associated while designing an IdM system should always be kept in mind from the user point. One can say that affordability comes from usability. An IdM system should be simple and it should reduce the boundaries of adoption.

Integrity of an IdM system is essential in order to protect the sensitive identity attributes or to detect any tamper done on the identity attributes. Whenever a user has to authenticate him, he has to provide some identity attributes to the third party. The idea of public key cryptography (Matsumoto and Hellman, 1976) was proposed by Diffie and Hellman so that the integrity can be preserved. However in (Bertino et al., 2009) the authors argued that it may not be satisfactory in terms of identity. The imprudent message security can also lead to identity theft.

Trustworthiness is another factor to be considered while designing a good IdM system. In traditional IdM systems, whenever a transaction takes place between two parties, there is always some degree of confidence between the interacting parties and that confidence can be provided by a "Trusted Third party". This third party is responsible for providing the authentication and integrity of the transaction and hence the interacting parties have to rely on the third party for establishing trust. The level of trust requirement differs for every IdM system and also the cost associated with it, therefore an IdM system with simple level of trust can be maintained. A detailed analysis of trust requirement and trust issues in various IdM models is done in (Jøsang et al., 2005).

Interoperability is considered to be a basic requirement for a good IdM system (Torres et al., 2012) and it is considered to be quite complex in all the aspects ranging from technical, cultural and legal purpose (Backhouse, 2006). Since, the digital identity of a person represent the attributes of the person in real life, it should be able to bind the digital identifier provided to the attributes. The database created should be able to identify the person in all the other systems which have different platforms as well. The identifier created at one system should not be useless to the system. It means that the IdM system should be compatible with the existing protocols and standards. It should implement and follow standard message formats which can be easily accepted in the existing market and are easy to adopt. Interoperability has been a topic of research in the past (Le et al., 2008; "Future of Identity in the Information Society", n.d) Identity in the Information Society," n.d.).

2.4. Blockchain overview

Blockchain concept was introduced in 2008 with "Satoshi Nakamoto" in his white paper wherein he claimed Blockchain as a trust-less technology (Nakamoto, n.d) and bitcoin was the first open source implementation of blockchain technology. Blockchain establishes Trust, Security and Data integrity through Cryptography, Peer reviews, Decentralized transactions which eradicates the role of intermediaries. A Blockchain is a distributed ledger which is immutable, transparent and redefines trust resulting in a fast, secure and trustworthy system. Blockchain is considered to be a set of interconnected technologies which provides the functionality to the framework, as illustrated in Fig. 5

Blockchain follows DLT *(Distributed Ledger Technology)* which is framed on the fundamentals of *Public Key cryptography and Point to Point network* consisting of the participating elements called as *nodes*. The encrypted ledger keeps the detail as private. A Blockchain contains a chain of blocks where the first block is called as genesis block with no parent block. A block is a collection of all the recent transactions that have happened over the point to point network. Every block in the blockchain implements the idea of linked timestamped (merkle tree) with proof of work (Benchoufi, 2017) and a hash code which is used to validate a transaction. The hash code is created in such a manner that it becomes very difficult to reverse engineer. Even a minute change in the block information can change the hash. A valid transaction means that it has been approved by all the members in the participating network. The *Consensus* mechanism is used to achieve the approval task. The block becomes a permanent part of the blockchain only after the transaction has been verified. Since the chain keeps on growing and is linked with immutable blocks it is named as *Blockchain*.

Mining is the process for creating a new block in the network and the people who mine the block are called as miners. Mining process requires a lot of investment and computational power. The miner who validates the transaction as well as complete the next block of blockchain gets some form of incentives. So a tenacious and ever-growing blockchain is formed which is updated constantly to preserve the current state of the distributed ledger (Buterin, 2015).

The distributed ledger thus holds all the transactions that have been done by the nodes in the network and all the nodes hold the copy of the transaction involved. Hence there is no central management of the records and the possibility of being hacked is rare. The need for a blockchain based system is very well defined in (Wust and Gervais, n.d.).

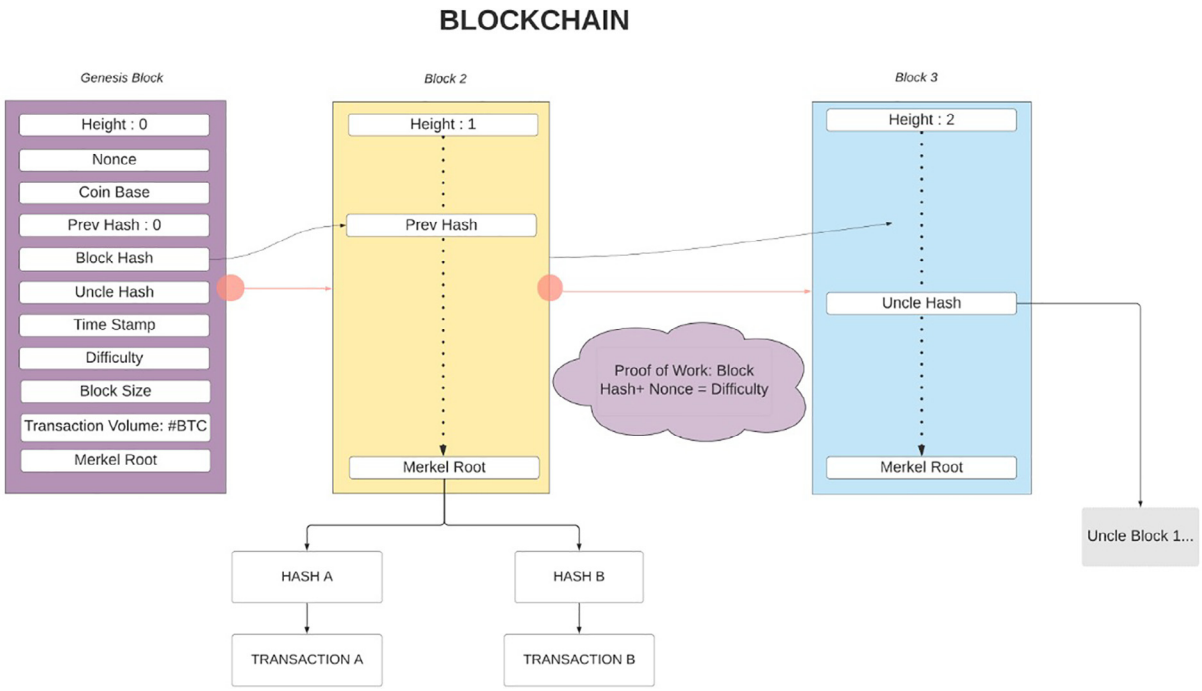

Fig. 5. Blockchain architecture

Characteristics of Blockchain:
The main characteristics of blockchain are described below

- No Centralization: No single party has the control over what information goes in and hence there is no single authority that can turn it off. The information is able to be accessed and replicated by everybody present on the network.
- Secure Transaction: The database can only be extended and previous records cannot be changed. Everyone who participates can see the blocks and the transaction stored in them. The use of cryptography and encryption adds another level of security into the network.
- Transparency: Since the information is distributed over the network, any changes made in the transaction are replicated to the entire participating user and hence every participant knows about the transaction which has been carried out in the network.
- Irreversible: The cryptographic hash used in the blockchain is difficult to alter and it becomes very difficult for the hacker to corrupt the network, as any change made in the network would lead to a complete new transaction.

2.5. Types of Blockchain

The existing literature identifies blockchain into various categories (Zheng et al., 2017; Christidis and Devetsikiotis, 2016; Kravchenko, 2016). We can categorize blockchain into three types: *Public, Private and Consortium.* The base layer technology of the above categorized blockchain becomes the foundation for choosing the blockchain type. In *Public* blockchain anybody in the world can participate, download, read and write the data. It is like an open field in which the users can come and go and therefore the users involved in the network needs to be very active. The well knows examples of public blockchain are given in (Nakamoto, n.d.; Wood, 2018; Ben-Sasson et al., 2014) which include Bitcoin and Ethereum. In *Private* Blockchain, all the permissions are kept central to an organization. The participating users are selected in advance and only those users are granted access to the network. The well-known examples of private blockchain are given in (Brown et al., 2016) which includes BlockStack and Multi Chain. *Consortium* blockchain are semi private blockchain which means they are *permissioned and controlled.* It is distributed among common nodes and privileged members. Ripple and R3 are examples of this type. Table 1 shows the comparison of the above mentioned blockchain types.

2.6. Blockchain applications

Due to the inherent definition, features and structure, blockchain has countless number of applications. If I utter the word blockchain to a group of people, most of them will relate it to bitcoin which is a financial application of blockchain. Initially, there were two prominent categories viz financial and non-financial. The non-financial application got hyped after blockchain 2.0 and blockchain 3.0. A lot of research studies explore and emphasize need of blockchain applications in business, intelligent IOT and e-payments, cybersecurity, and medical field (Kumar and Mallick, 2018; Mohanta et al., 2019; Saha et al., 2019). The most widely used applications of blockchain are shown in Fig. 6.

Table 1
Comparison of Blockchain Types.

Criteria	Public	Private	Consortium
Consensus	All users	A single authority	Group of approved users
Access	Anyone	By invite only	By invite only
Speed	Low	High	High
Security	Low	Medium	High
Identity	Hidden (anonymous)	Trusted	Trusted
De-Centralized	Full	No	Partial

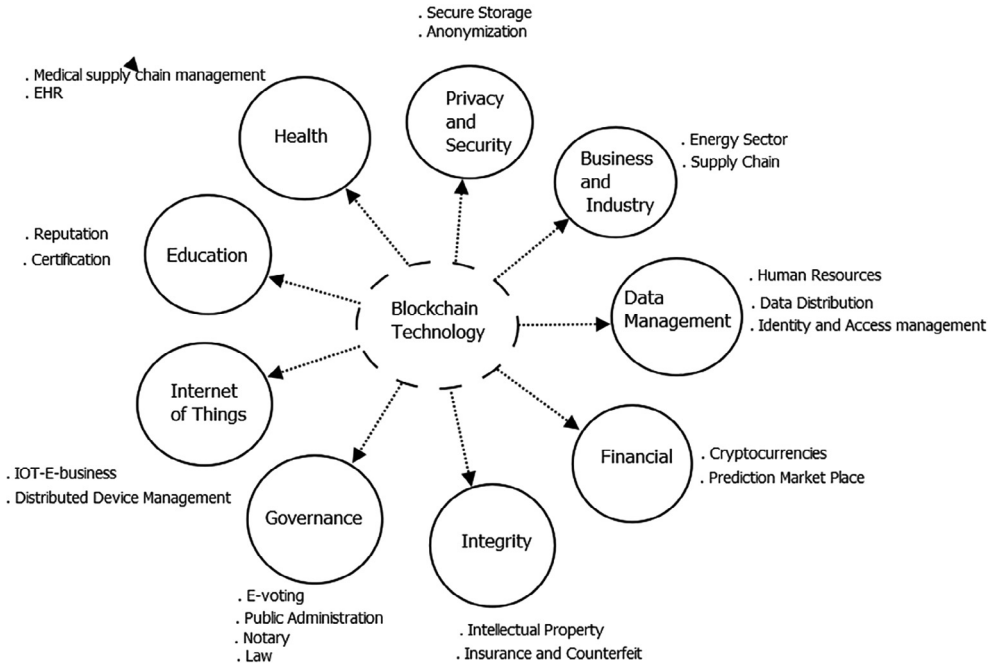

Fig. 6. Applications of blockchain.

Table 2
Research Questions.

RQ1	How are the publications related to blockchain and Identity management distributed over time?
RQ2	What are the initiatives that have been taken for Identity management using blockchain Technology?
RQ3	How can blockchain technology assist effective Identity management and its challenges?
RQ4	Which of the Consensus algorithm of blockchain technology applied to various frameworks of Identity Management?
RQ5	What are the key points which need to be marked sooner or later?
RQ6	What are the research projects undergoing in the field of IdM using blockchain technology?

Table 3
Number of papers found in each database.

Database	Search String	#
IEEE xplore	((blockchain) AND "Index Terms": identity)	272
ACM	[All: blockchain] AND [Abstract: identity]	273
Science direct	Term :Blockchain & Title, abstract, keywords: identity	110
Springer link	blockchain AND "identity management"	398
Wiley	"blockchain" in Keywords and "identity" anywhere	211
Total		1264

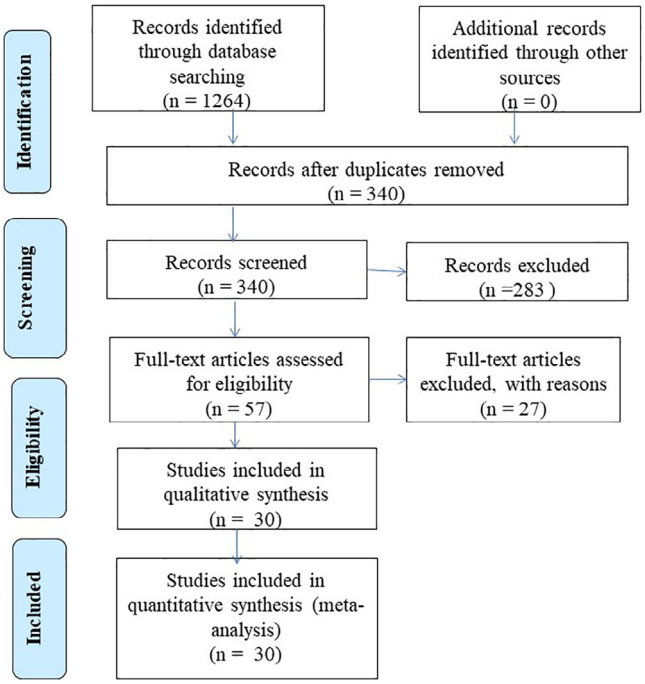

Fig. 7. Flow of Information through the different phases of systematic mapping.

3. Review methodology

Systematic literature mapping is a methodology which provides a coarse-grained overview on any topic. It also facilitate in elucidating existing knowledge gaps and helps in providing future research opportunities. In order to provide a transparent and scientific study the methodology given in (Kitchenham et al., 2011) is followed. The basic steps are described below

3.1. Database

As blockchain is a new technology so the search for relevant publications involving blockchain and Identity Management is scattered over different disciplines and hence we created a relevant protocol to look for admissible papers required for the purpose of fulfilling the research goal. An appropriate set of database must be selected for conducting an efficient search. The studies published between January 2009 to June 2020 in five electronic databases namely IEEE xplore, ACM Digital Library, Science Direct, Springer link and Wiley were collected.

3.2. Research questions (RQ)

Table 2 defines the research questions that have been formulated.

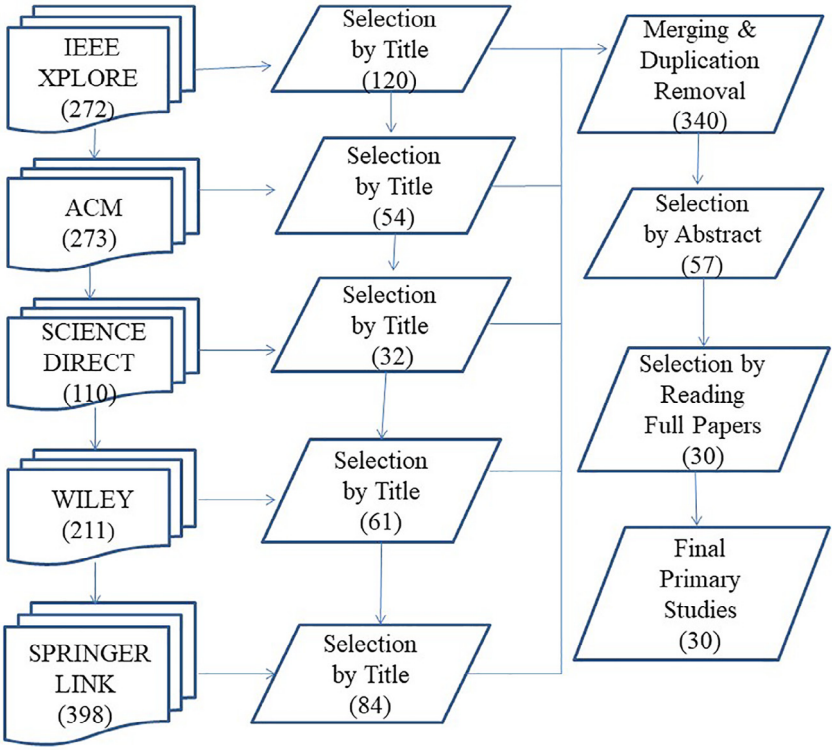

Fig. 8. Selection and screening procedure for the study.

3.3. Search string

For an efficient mapping, search string used and number of papers found in each database is shown in Table 3. The keyword" blockchain" is used in almost all the searches at the initial stage. Then an advanced search is done by constructing the search string for all the e-resources specified above. We tried to obtain as much relevant literature as possible.

3.4. Criteria selection

The search for relevant papers is an important stage. The main objective was to identity and include relevant studies which can help to answer the Research Questions. Since the papers collected through all the five databases were not related to RQ's, they needed to be assessed for their actual relevance. The PRISMA flow graph according to (Moher et al., 2009) is represented in Fig. 7.

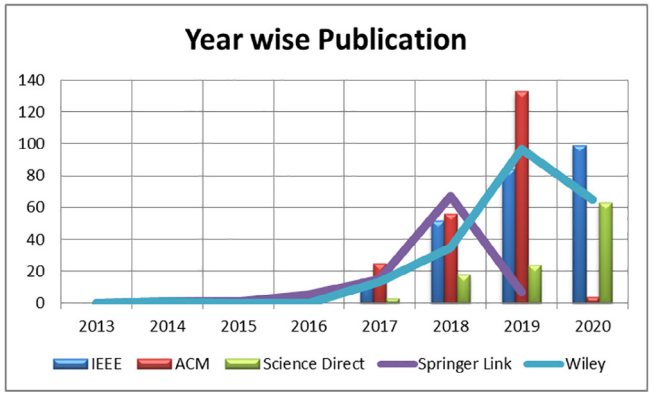

Fig. 9. Time based count of IdM using blockchain.

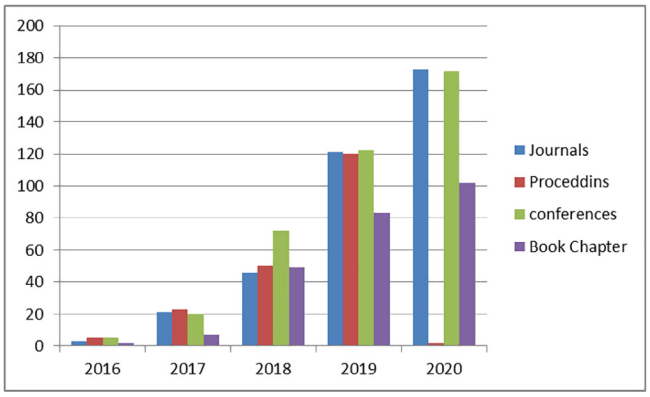

Fig. 10. Year wise analysis per type of publication.

The initial count of the papers was 1264, which was quite big. An Inclusion and Exclusion criteria was then followed to search for more relevant papers. The Inclusion and Exclusion criteria are defined as follows

Inclusion Criteria:

IC1: Empirical study focused on Identity Management and blockchain technology.

IC2: Empirical study focused on Identity Management Challenges.

IC3: Empirical study which focused on consensus mechanisms and types of blockchain used.

IC4: Web portals which included IdM Projects, startups and various other initiatives.

Exclusion Criteria:

EC1: Papers on blockchain without full text availability.

EC2: Studies on blockchain without empirical analysis of results.

Table 4
Identity Management using blockchain technology initiatives.

Solution	Description	Propose type	Blockchain	Network
Authenteq (“Authenteq, n.d:Trust your customers instantly with Authenteq, n.d,”	A platform to create and verify self-sovereign identity.	Company	Permissioned	Lapo Blockchain
BlockAuth, n.d(“BlockAuth-DECENTRALIZED IDENTITY & AUTHENTICATION,” n.d.)	A Federated OpenID provider that lets the user own and control their own identity.	Start-up	Permission- less	Bitcoin
BlockStack(‘Blockstack technical white paper, 2019)	A decentralized computing network and app ecosystem that lets the user to control their identity.	Company	Permission-less	Stack Blockchain based on bitcoin
BlockVerify(Blockverify, n.d)	Introduces transparency to supply chain using anti-counterfeit solutions.	Start-up	Permissioned	Bitcoin
Bloom(Leimgruber et al., 2018)	A blockchain protocol for identity verification and credit scoring.	Open source	Public	Ethereum
Civic (Civic, n.d.)	A platform to protect user identities using multi-factor authentication and biometrics.	Start-up	Permissioned	Ethereum
Cryptid (Cryptid, n.d)	Eliminates Counterfeits in identification by adding factors like encryption and identification.	Hackathon project	Permissioned	Ethereum
Cambridge Blockchain (Cambridge Blockchain, n.d)	Identity Management by adding the facility of KYC and privacy requirement of the users.	Start-up	Permission -less	Ethereum
(CredyCo, n.d)	Document verification SaaS to ensure indisputable and credible statements.	Company	Permissioned	Bitcoin
ConsenSys (ConsenSys, n.d)	Building platform for government for Identity Management	Company	Public	Ethereum
Evernym (Evernym, n.d)	A global decentralized identity network that promotes the use of self-sovereign identity.	Open sourced Company	Public permissioned	Hyper ledger Indy
Existence ID (Existence ID, n.d)	A platform for global identity storage providers the users to have control over their private information	Open source platform	Permissioned	Bitcoin
I/O digital (I/O Foundation, n.d)	Provides secure, fast and user Friendly Decentralized Identity Management over the web	Start up	Private	I/O coin Blockchain
Jolocom (Jolocom, 2019)	Provides a self-sovereign digital identity by providing the users control over their identity.	Open source project	Public	Ethereum
My Health My Data(My Health My Data, 2019)	An EU funded project building dynamic consent interface and personal data account using smart contract	Government Project	Private, Permissioned	Hyper Ledger Indy
Netki (Netki, n.d)	A platform for remote digital identity verification intended to facilitate compliance with KYC and Anti-Money Laundering regulations	Start-up	Private, Permissioned	Hyper Ledger Indy
Namecoin (NameCoin, n.d)	Improves Decentralization of Internet services and Identities.	Open source	Permission -less	Bitcoin
OneName(OneName, n.d)	A decentralized naming and storing system for user identity having the user control of their identity	A web application based on BlockStack	Permission-less	Bitcoin
PeerMountain(Paper, n.d.)	Provides ownership and control over user digital identities using cryptography. Additionally it promotes secure commerce.	Open Source	Public	Blockchain – agnostic
SelfKey (The SelfKey Foundiation, 2017)	A self-sovereign identity platform providing full ownership of the user's digital identity	Non –profit foundation	Public Permissioned, Permission- less	Ethereum
Shocard(Shocard, n.d)	A Platform to establish the identities between user and enterprise securely	Start-up	Public, Permissioned	Blockchain – agnostic
Sovrin (Tobin and Reed, 2016)	A platform for self-sovereign identity management	Non-profit organization	Public, Permissioned	Hyper ledger Indy
UniquID (UniquID, n.d)	Provides Identity as a Service for IOT	Open Source	Public	Litecoin
uPort(Heck et al., 2017)	Provides a platform for Self-sovereign identity by adding identity and messaging protocols.	Company	Public/Private	Ethereum

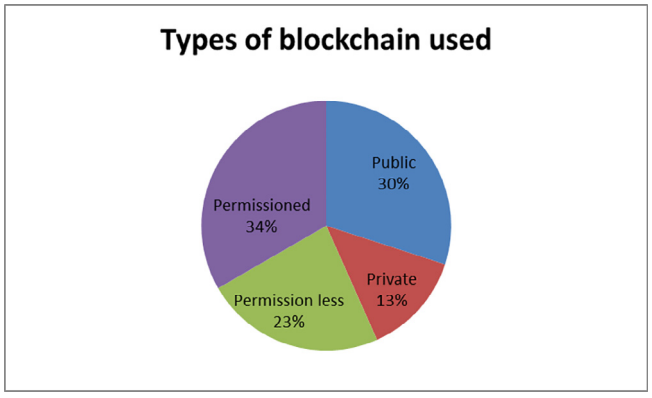

Fig. 11. Types of blockchain used.

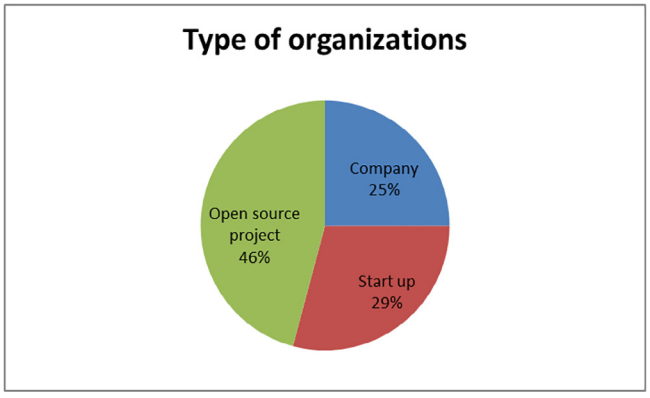

Fig. 12. Types of organizations using blockchain technology for IdM.

EC3: Papers where English was not the main language.

EC4: Papers on blockchain where Identity and Access management was not in context.

After the first exclusion round i.e based on the titles of the retrieved papers, and removal of duplicates, the count was reduced to 340. The main reason for this removal of large number of papers was that the retrieved papers were not related to Identity Management using blockchain technology. For example, many retrieved papers focused on bitcoin and other applications of blockchain and therefore did not help in our study. In the second round of screening the papers, the abstracts of all the previously selected papers were read and the count was reduced to 57. In the final stage the full papers were read and 30 papers were selected as primary studies. Fig. 8 shows the selection process used for the study.

4. Results and discussion

This section presents the analysis done on the basis of RQ's, trend pattern and discussion of the research done in the field of IdM using Blockchain technology.

4.1. Answering research questions

In this section we will answer the Research Questions stated above in Table 2. All the RQ's have been answered.

RQ-1: How are the publications related to blockchain and Identity management distributed over time?

The interpretation of **RQ1** has been done through Fig. 9. Though the research work related to blockchain began in 2009 but the research in blockchain has gained momentum after 2016. Around 65% of the work in blockchain technology and identity management has been done after 2016.

It is also noticeable from Fig. 10 that there is a significant increase in the publication of literature in conferences, book chapters and proceedings.

RQ-2: What are the initiatives that have been taken for Identity management using blockchain Technology?

The **RQ2** is about the initiatives taken for Identity Management using blockchain technology. The government organizations are using permissioned blockchain as a platform to store digital identities. There are few real life examples where blockchain technology is being used by the government for identity management. Blockchain has been used by Estonia government since 2014 to preserve nation data (Sullivan and Burger, 2017). "ID2020 alliance" has ensured digital ID through a multistake holder partnership (id2020, n.d.). The authors in (Turkanović et al., 2018) have applied blockchain in education purpose and proposed a framework "EduCTX" for credit management of students. Table 4 describes in detail about various IdM initiatives using blockchain.

It has been analysed that permissioned blockchain is being used more as compared to various other types of blockchain available. According to General Data Protection Regulation (GDPR) implemented in 2016, blockchain does not have the capability to preserve end user privacy. People are more focused towards keeping their data private. Hence permissioned blockchains are being used more instead of public blockchain. Fig. 11 shows the analysis on types of blockchain used.

It has also been observed in Fig. 12, that there are more open source projects which are working on using blockchain for IdM. Bitnation (Falkvinge et al., 2015) is an open source governance platform based on Ethereum smart contract. Bitnation will lead to the inception of "Decentralized Borderless Voluntary Nation".

RQ-3: How can blockchain technology assist effective Identity management and its challenges?

RQ-3 is whether blockchain technology can solve the identity management challenges described in Section 2.3. Although blockchain has been widely adopted in most of the applications because of its features yet there are distributed opinions about it. The authors in (Gramoli, 2020) claims blockchain to be revolutionary as it solves Byzantine General Problem. Blockchain ensures decen-

Table 5
Analysis on the basis of IdM challenges.

Author	Security	Privacy	Anonymity	Affordability	Integrity	Trustworthiness	Interoperability
(Ma et al., 2018)	√	√	×	√	√	×	×
(Sullivan and Burger, 2017)	√	√	×	√	√	√	×
(Hussein et al., 2018)	√	√	√	√	√	√	×
(Qin et al., 2017)	√	×	×	√	√	√	√
(Zhang et al., 2018)	√	√	×	Low Cost	√	√	√
(Azouvi et al., 2017)	√	×	√	Low Cost	√	Web of trust	×
(Augot et al., 2017b)	√	×	×	High cost	√	√	×
(Sarangal et al., 2019)	√	×	×	Low cost	√	√	×
(Sarier, 2018)	√	√	√	High cost	√	√	×
(Shetty et al., 2019)	√	√	√	High Efficiency at low cost	√	√	×
(Elisa et al., 2018)	√	×	√	Low cost	√	√	√
(Loukil et al., 2018)	Not addressed	√	Not addressed	Not addressed	√	Not addressed	Not addressed
(Buccafurri et al., 2018)	√	√	×	Low cost	√	√	Not addressed
(Ouaddah et al., 2016)	√	√	√	Not mentioned	√	√	×
(Liu et al., 2019)	√	×	√	Not mentioned	√	√	×
(Abbasi et al., 2017)	√	√	√	–	√	√	×
(Gao et al., 2018)	√	×	×	Low cost	√	√	×
(Al-Bassam, 2017)	√	×	×	Low cost	√	√	×
(Liu, 2016)	√	×	√	—	√	×	×
(Friebe and Zitterbart, 2018)	√	√	√	Depends on the system	√	×	×
(Lee and Member, 2018)	√	×	√	Low cost	√	√	×
(Mikula and Jacobsen, 2018)	√	––	×	Low cost	––	—	––
(Alansari et al., 2017)	√	√	×	Low cost	√	×	––
(Sun et al., 2018)	√	√	√	Low cost	√	√	×
(Du et al., 2018)	√	√	———	Low cost	√	———	×
(Kaaniche et al., 2018)	√	√	√	Low cost	×	×	√
(Wang et al., 2017)	√	√	—	—	√	×	×
(Augot, 2017)	√	√	√	Fluctuates based on market forces	√	×	×
(Tian et al., 2019)	√	√	×	Low cost	√	√	√
(Shen et al., 2020)	√	√	√	Small Computational Cost	×	×	×

Table 6
Consensus Mechanisms used in various blockchain based Frameworks.

Author	Consensus Mechanism	Framework Proposed
(Ma et al., 2018)	POW	DRM Chain
(Sullivan and Burger, 2017)	Not mentioned	E-Residency
(Hussein et al., 2018)	MD5 hash	Medical record sharing and access control system
(Qin et al., 2017)	POW	CeCoin
(Zhang et al., 2018)	Not Mentioned	FHIRChain
(Azouvi et al., 2017)	POW	Extension of framework described in (Al-Bassam, 2017)
(Augot et al., 2017b)	Nil	Not mentioned
(Sarangal et al., 2019)	PBFT	Insurance platform
(Sarier, 2018)	Zero Knowledge Proof	Privacy Preserving Biometric Identification
(Shetty et al., 2019)	Not Mentioned	Mobile HealthCare System
(Elisa et al., 2018)	DPOS	e-Government system
(Loukil et al., 2018)	POC	End to end privacy preserving framework
(Buccafurri et al., 2018)	NIL	Crowd shipping
(Ouaddah et al., 2016)	POC	FairAcess for IOT
(Liu et al., 2019)	Not Mentioned	Identity Authentication Scheme
(Abbasi et al., 2017)	POC	VeidBlock
(Gao et al., 2018)	—	BlockId
(Al-Bassam, 2017)	POW	PKI System
(Liu, 2016)	POW	Smart Contract
(Friebe and Zitterbart, 2018)	POW	DecentID
(Lee and Member, 2018)	PBFT	BIDAAS
(Mikula and Jacobsen, 2018)	POC	Hyperledger framework
(Alansari et al., 2017)	____	Access control
(Sun et al., 2018)	PBFT	DABS
(Du et al., 2018)	PBFT	____
(Kaaniche et al., 2018)	POC	Consortium
(Wang et al., 2017)	POC	Ethereum blockchain
(Augot, 2017)	POW	Bitcoin Blockchain
(Tian et al., 2019)	Optimized PBFT	Private/Consortium
(Shen et al., 2020)	Not mentioned	BASA using Consortium Blockchain

tralization, transparency, and ensures low cost transactions (Bunjaku et al., 2017). Since blockchain is still in its developing stage, the privacy issue needs more attention. Table 5 presents a complete analysis based on IdM challenges.

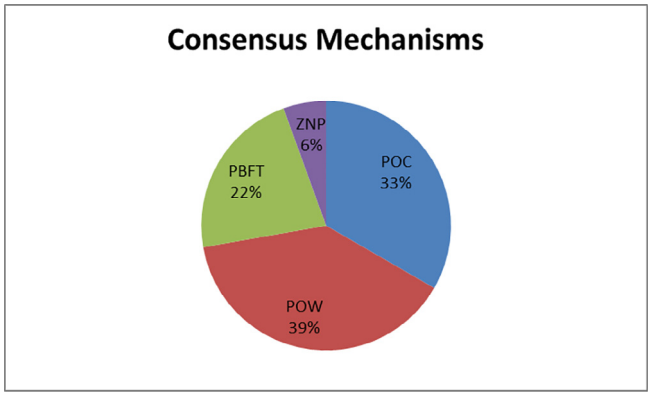

Fig. 13. Types of consensus mechanisms.

From the studies found in Table 5, it can be concluded that blockchain satisfies most of the IdM challenges faced over the time. *Security* is the primary feature of blockchain which has the capability to remove the need of "trusted third party" and the dependence on central organizations for the data(Yli-huumo et al., 2016). The authors (Raju et al., 2017) state that blockchain can be useful in cognitive cellular network for authenticating and securing spectrum sharing. The Blockchain technology addresses the *privacy* challenge of IdM by creating the hash of the transaction. Since the hash is difficult to calculate, hence privacy can be protected. The decentralized nature of blockchain ledger verifies and guarantees that the users, transactions, messages are genuine. The authors in (Zyskind, et al., 2015a) have proposed a decentralized personal data management system that ensures users own and control their data. Enigma, which is an extension of blockchain technology, is a decentralized computation platform with guaranteed privacy (Zyskind et al., 2015b). Storj is a peer-to-peer cloud storage network and claims to be the "most secure and private cloud (Shrier et al., 2016; Storj, 2017). There are surveys in the literature (Bonneau et al., 2015; Tsukerman, 2016; Can et al., 2018; Conti et al., 2017) which focused on the security and privacy issues of blockchain. *Anonymity* is a primary feature in Blockchain because the need of the trusted third party is eliminated in this technology (Yli-huumo et al., 2016; Zheng et al., 2017). There are three frequently-used mechanisms for protecting anonymity in the blockchain and they include: mixing services, ring signature, and non-interactive zero-knowledge proof (Feng et al., 2018). A lot of research has been going on the anonymity feature of the blockchain based systems. The authors in (Heilman et al., 2016) have presented solutions for anonymity in blockchain by using blind signature and smart contract. In (Conoscenti et al., 2016), the authors have identified four distinguished categories of de-anonymization techniques: multiple inputs, change address, associations with IP and usage of centralized services. The Blockchain is a decentralized trust network (Antonopoulos, 2014). The true unique feature of blockchain lies in the fact that it does not require the participating users to trust each other. Since blockchain is a decentralized ledger and any attempt to make changes in the ledger will definitely be rejected by the system, therefore the users can trust this ledger which is shared on various decentralized nodes over the network. Hence blockchain technology can address the *Trustworthiness* challenge of IdM. However the *Interoperability* issue still remains unsolved.

RQ-4: Which of the Consensus algorithm of blockchain technology applied to various frameworks of Identity Management?

In the literature, there are various consensus mechanisms like Proof of Work (POW), Proof of Stake (POS), Practical byzantine fault tolerance (PBFT) and Proof of Concept (POC). It has been identified by analyzing Table 6, that Proof of Work (POW) is the most popular Consensus Mechanisms. POW works on the principle of solving a very complicated computational problem like finding hashes involving specific patterns (Antonopoulos, 2014). Another consensus mechanism which has been widely adopted is Proof of Concept.

It is clear from Fig. 13 that POW consensus algorithm is being used widely as compared to other consensus mechanisms. It has been found that most of the consensus mechanisms are compatible with the existing blockchain systems. It is completely on the user implementation and choice to use the available consensus mechanisms.

RQ5: What are the key points which need to be marked sooner or later?

The major issues which need to be addressed more in the future include: Scalability, Interoperability, Cost associated with release of each transaction, data protection and authentication, data stor-

Table 7
Project initiatives in the field of IdM using blockchain.

S. No	Name	Acronym	From	About	Coordinated In	Overall Budget
1	Secure Cloud Identity Wallet	CREDENTIAL	1–10-2015	Showcases importance of identity and access management and using digital identity for authentication and authorisation. CREDENTIAL tells us how cloud based services can be used for managing and using digital identity.	AUSTRIA	€ 6 686 660
2	My Health - My Data	MH-MD	1–11-2016	The far-fetched goal is to embrace the medical world under the sun of blockchain, helping connect the medical world in a way that facilitates the sharing of confidential data in a safe and secure way, a fact that presupposes developing a comprehensive methodology to guide the implementation of data and identity protection systems.	LYNKEUS , ITALY	€ 1 499 588
3	Decentralised Citizens Owned Data Ecosystem	DECODE	1–10- 2016	A blockchain system being developed in Europe that aims at building an environemt in which people have access to their identity and also give them access to control and manage their data real time. DECODE puts agency and data control in the hands of citizens, to improve citizens' well-being and society for the collective benefit of all.	INSTITUT MUNICIPAL D'INFORMATICA DE BARCELONA , SPAIN	€ 4 987 673,75
4	Global Citizenship Law: International Migration and Constitutional Identity	Global Citizenship Law	1–3-2017	As the global migrations are on rise, so are the fradulent practices that prevail with such migrations. To mitigate the perilious effects of such migrations, MH-MD has embarked on deploying a system that keeps global track of identity of people by measuring them and their histories against severaal benchmarks	EUROPEAN UNIVERSITY INSTITUTE , ITALY	€ 1 499 588
5	The Disrupted Society: mapping the societal effects of blockchain technology diffusion	BLOCKCHAINSOCIETY	1–1- 2018	It talks about society and government and how these factors affect blockchain and how blockchain can affect them	NETHERLANDS	€ 1 499 631
6	Protection and control of Secured Information by means of a privacy enhanced Dashboard	PoSeID-on	1–5-2018	PoSeID-on is aimed at developing a novel Privacy Enhancing Dashboard for personal data protection . In particular, the project will deliver an easily accessible and simple privacy enhancing dashboard useful for monitoring, keeping track record, and controlling all aspects related to data subjects personal data.	ITALY	€ 3 072 586,27
7	Oblivious identitY Management for Private and User-friendly Services	OLYMPUS	1–9- 2018	OLYMPUS will pioneer the concept of distributed oblivious identity management, where the role of the IDP is split over multiple authorities, so that no single authority can track or impersonate their users. The OLYMPUS framework will let users maintain unlinkable identities with different service providers while using standard devices and a single password or biometric.	UNIVERSIDAD DE MURCIA , SPAIN	€ 3 147 837,50
8	Blockchain-based, 100% automated KYC (Know Your Customer) service	BlockchainKYC	1–2- 2019	It start by giving an introduction about KYC and it benifits followed by introducing blockchain enabled KYC shared ledger. Starting from it's applications and how it can be used.	ICELAND	€ 1 758 750
9	Digital Identity Management Platform	LOQR	1–2- 2019	It talks about authentication and authorization using digital identity. It provides identity validation, risk-based adaptable identity authentication along with access management, thought a single trusted identity that can be used by a unique person on all services.	PORTUGAL	€ 71 429
10	Lawful evidence collecting and continuity platform development	LOCARD	1–5-2019	.LOCARD aims to provide a holistic platform for a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain.This will be powered by an immutable storage and an identity management system that will protect privacy and handle access to evidence data using a Trusted Execution Environment.	GRECE	€ 6 833 385
11	Detecting Document frauD and iDentity on the fly	D4FLY	1–9-2019	D4FLY augments current capabilities and capacities of officials in terms of setting benchmark for identity management. The system includes the combined usage of 2D + thermal face, 3D face, iris and somatotype biometrics, making the system, or identity, verbaim, tamper proof.	VERIDOS GMBH, GERMANY	€ 6 984 727,50
12	Brokerage and market platform for personal data	KRAKEN	1–12-2019	KRAKEN project proposes a secure platform that fully preserves the privacy and self-sovereignty of personal data. KRAKEN provides innovating data sharing control based on advanced end-to-end encryption that prevents access to and modification of data.	SPAIN	€ 5 999 787,50

Table 7 (*continued*)

S. No	Name	Acronym	From	About	Coordinated In	Overall Budget
13	TRAnsparency, Privacy and security for European citiZEns	TRAPEZE	1–9-2020	A vision for main framing a system that not only helps make the economy and the world robust but also makes accessing and granting access to private data much more feasible and user friendly, hence giving the control of data in the hands of users, ensuring data integrity and non-repudiation.	TENFORCE BVBA , SPAIN	€ 6 017 950
14	Identity Management in PUbLic SErvices	IMPULSE	1–2- 2021	The following outcome will be produced by the model: Holistic AI and blockchain technology supporting GDPR-compliant eID to complement existing EU identity schemas, ensuring cross-border access and secure and adaptable requirements for actionable integration with other public service providers, and adoption by existing Trust Service Providers (TSP) to ensure marketability.	SPAIN	€ 3 987 593,75

age and replication, risk involved and lack of skilled employees. The major concern over privacy has been a topic of research. The authors in (Amo et al., 2019) have suggested to use smart contacts based on cloud for maintaining the student data privacy instead of blockchain. There are numerous questions which have been referred by the researchers like: How the identities will be stored? How the identification process will be considered as authentic? How identification will be done using passwords? Do we need a separate blockchain for identification purpose etc. (Vandervort et al., 2015). In most of the research papers, privacy and security issues are handled by inherent property of blockchain but some author (Kosba et al., 2016) insists that blockchain helps to attain transactional privacy and correlation can help to reveal the identity of users. The authors in (Stephen and Alex, 2018) emphasizes that the problem of transaction security can be addressed using Elliptical Curve Diffie-Hellman-Merkle Algorithm. Taking in consideration about social media and networking, the decentralization is not preferred over centralization. The problem of data storage, access rights, management of identities, data replication needs to be handled in this case (Bahri et al., 2018). However the authors in (Islam and Kundu, 2019) have suggested that use of pegged sidechain can be used to hide the identity of the users and can help to create a more secure system. Blockchain is considered to be very effective in context of security but the privacy concerns still exists (Budish, 2018; Eyal and Sirer, 2014; Lin and Liao, 2017) because the ledger is still public. The Suitability of blockchain is one key aspect which needs to be dealt with. The public as well as private sectors are eagerly waiting to adopt this technology to solve real life problems (Umeh, 2016). However some IT experts are still trying to visualize the fundamental reason for adopting it. Blockchain is suitable when one needs to have a transaction between trustless sources (Wüst and Gervais, 2018). Therefore one needs to evaluate the suitability of blockchain for their particular use case before trying to just adopt it (Lo et al., 2017). There are various technical challenges which need to be focused on. According to (Swan, 2015), the researchers need to look forward to work upon Latency, Throughput, Size and Bandwidth, Versioning, Hard forks and Multiple Chains.

RQ-6: What are the research projects undergoing in the field of IdM using blockchain technology?

RQ-6 is about the research projects which are undergoing in the field of IdM and blockchain technology. There are many organizations which help in funding of the research projects. We have used the primary public repository to find the information on EU-funded research project i.e the "Community Research and Development Information Services (CORDIS), (https://cordis.europa.eu). Table 7 shows the research projects which are going on using blockchain technology and Identity Management.

4.2. Discussion

Although Identity Management has been examined extensively and accepted in various fields yet it believed to carry many limitations and challenges (Dhamija and Dusseault, 2008). From Table 5, it is clear that blockchain technology has emerged as an effective technology for solving IdM Challenges, but there is dilemma over adoption of blockchain in IdM because of some issues and implications. For example, there are some legal and monetary issues; what if a transaction is found to be criminal and the organization have not verified the identity of the user who performed the transaction; how a pseudonymous user is supposed to prove his reputation to the organization? Some Issues and implications are discussed below:

- *Wallet Leakage:* There is a possibility that the identity wallet is compromised and hence the useful information about the user can be misused. It is suggested to use cold wallets in order to increase the security of the blockchain based IdM systems. The authors (Lu et al., 2020) have proposed an unpacking system "AutoD" which can restore the file which has been decrypted in the reinforced blockchain applications.
- *Identity Reversal:* In Real World, the identity of an individual is not forever, and needs to be changed sometimes. In traditional systems, there is a systematic procedure to be followed in case of any identity reversal process. However in blockchain based IdM Systems, any modifications in the identity will be a challenging task.
- *Key Management:* The participants in a blockchain network acquire a wallet to keep their credentials like private key. It is important to keep the private key very securely. Losing a private key can result in serious loss in case of a bitcoin blockchain. There is no provision like forgot password or rest password. However, a Multi –Party key management suggested by (Feng et al., 2020) can be used.
- *Associated cost:* There is a need to upgrade the existing infrastructure so as to accommodate the blockchain technology in IdM. There will definitely be cost associated with each upgradation. Since blockchain is still in its developing stage and people are not very well trained in this technology, therefore there is a need to provide Certifications, Industrial Training, short term courses etc. to gain insight knowledge.
- *Unlinkability Problem:* There are some design constraints like unlinkability which needs to be re addressed (Zheng et al., 2019; Lee et al., 2019). A solution called Attribute based Encryption has been proposed by (Schanzenbach et al., 2018). The techniques like anonymous signature can also be used to the unlinkability problem in blockchain.

5. Conclusion

A Systematic literature mapping was conducted in order to investigate the use of blockchain technology for IdM. Although the use of blockchain is gaining a lot of attention yet it is advised to check the appropriateness of blockchain against that use case. All the research questions have been answered. It is evident form the study that the use of blockchain in IdM has the potential to overcome the limitations of conventional systems for IdM. It was observed that blockchain is suitable to solve IdM challenges faced over the time. However, privacy and interoperability challenges still need to be solved. Blockchain allows only pseudo anonymity instead of anonymity. There are various successful initiatives taken by the government so as to adopt blockchain in IdM. Based on the studies and discussion, research opportunities like unlinkability problem, key management problem, adoption of blockchain technology, wallet leakage problems have been identified for future research direction in IdM. The Proof of Work Consensus mechanism in blockchain is more famous as compared to the others. There are various key issues like Scalability, Interoperability, Cost associated with release of each transaction, data protection and authentication, data storage and replication and lack of skilled employees. The major concern over privacy has been a topic of research which needs to be dealt with while adopting blockchain for IdM. Since the blockchain technology is still in its developing face, in our future work we will try to focus on the adaptability issue of blockchain.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abbasi, A.G., Acreo, R., Lane, C., 2017. VeidBlock: Verifiable Identity using Blockchain and Ledger in a Software Defined Network 173–179.

Adee, S., 2015. Your data, your rules. New Sci. 227, 10–11. https://doi.org/10.1016/S0262-4079(15)31055-1.

Ahn, G., Lam, J., 2005. Managing Privacy Preferences for Federated Identity Management 28–36.

Ahn, G.J., Ko, M., 2007. User-centric privacy management for federated identity management. In: Proceedings of the 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing. https://doi.org/10.1109/COLCOM.2007.4553829.

Al-Bassam, M., 2017. SCPKI: A smart contract-based PKI and identity system, in: BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Co-Located with ASIA CCS 2017. pp. 35–40. https://doi.org/10.1145/3055518.3055530

Alansari, S., Paci, F., Sassone, V., 2017. A Distributed Access Control System for Cloud Federations. https://doi.org/10.1109/ICDCS.2017.241.

Ali, O., Ally, M., Dwivedi, Y., et al., 2020. The state of play of blockchain technology in the financial services sector: a systematic literature review. Int. J. Inf. Manage. 54, 102199.

AlpAlpárr, G., Hoepman, J.-H., Siljee, J., 2013. The Identity Crisis Security, Privacy and Usability Issues in Identity Management. Journal of Information System. Security 9.

Amo, D., Alier, M., Garc\'\ia-Peñalvo, F.J., Fonseca, D., Casañ, M.J., 2020. Protected users: A moodle plugin to improve confidentiality and privacy support through user aliases. Sustainability 12, 2548.

Amo, D., Fonseca, D., Alier, M., Garc\'\ia-Peñalvo, F.J., Casañ, M.J., 2019. Personal data broker instead of blockchain for students' data privacy assurance, in: World Conference on Information Systems and Technologies. pp. 371–380.

Antonopoulos, A.M., 2014. Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc", ".

Asaf, K., Rehman, R.A., Kim, B.-S., 2020. Blockchain technology in Named Data Networks: A detailed survey. Journal of Network and Computer Applications 171, 102840.

Augot, D., 2017. Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain 25–34. https://doi.org/10.1109/PST.2017.00014

Augot, D., Chabanne, H., Chenevier, T., George, W., Augot, D., Chabanne, H., Chenevier, T., George, W., User-centric, L.L.A., Augot, D., 2017a. A User-Centric System for Verified Identities on the Bitcoin Blockchain To cite this version : HAL Id : hal-01611251 A User-centric System for Verified Identities on the Bitcoin Blockchain.

Augot, D., Chabanne, H., Chenevier, T., George, W., Lambert, L., 2017b. A User-Centric System for Verified Identities on the Bitcoin Blockchain. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (Eds.), Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer International Publishing, Cham, pp. 390–407.

Authenteq:Trust your customers instantly with Authenteq [WWW Document], n.d. URL https://authenteq.com/ (accessed 3.12.21).

Azouvi, S., Al-Bassam, M., Meiklejohn, S., 2017. Who Am I? Secure Identity Registration on Distributed Ledgers. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (Eds.), Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer International Publishing, Cham, pp. 373–389.

Backhouse, J., 2006. Interoperability of identity and identity management systems. Datenschutz und Datensicherheit - DuD 30, 568–570. https://doi.org/10.1007/s11623-006-0145-y.

Bahri, L., Carminati, B., Ferrari, E., 2018. Decentralized privacy preserving services for online social networks. Online Social Networks and Media 6, 18–25.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., 2014. Zerocash: Decentralized anonymous payments from bitcoin. Proceedings - IEEE Symposium on Security and Privacy 459–474. https://doi.org/10.1109/SP.2014.36.

Benchoufi, M., 2017. Blockchain technology for improving clinical research quality 1–5. https://doi.org/10.1186/s13063-017-2035-z

Bertino, E., Martino, L., Paci, F., Squicciarini, A., 2009. Security for web services and service-oriented architectures. Springer Science & Business Media.

Bhargav-Spantzel, A., Squicciarini, A.C., Bertino, E., 2006. Establishing and protecting digital identity in federation systems. J. Comput. Secur. 14, 269–300. https://doi.org/10.3233/JCS-2006-14303.

BlockAuth-DECENTRALIZED IDENTITY & AUTHENTICATION [WWW Document], n.d. URL http://blockauth.org/ (accessed 3.12.21).

Blockstack technical white paper, 2019.

Blockverify, n.d. Blockchain Based Anti-Counterfeit Solution [WWW Document]. URL http://www.blockverify.io/ (accessed 3.14.21).

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W., Foundation, E. F., 2015. SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. https://doi.org/10.1109/SP.2015.14.

Brown, R.G., Carlyle, J., Grigg, I., Hearn, M., 2016. Corda : An Introduction 1–15.

Buccafurri, F., Lax, G., Russo, A., Zunino, G., 2018. Integrating digital identity and blockchain, in: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". pp. 568–585.

Buchmann, N., Rathgeb, C., Baier, H., Busch, C., Margraf, M., 2017. Enhancing Breeder Document Long-Term Security using Blockchain Technology. https://doi.org/10.1109/COMPSAC.2017.119.

Budish, E.B., 2018. The economic limits of bitcoin and the blockchain. SSRN Electron. J. https://doi.org/10.2139/ssrn.3197300.

Bunjaku, F., Gjorgieva-Trajkovska, O., Miteva-Kacarski, E., 2017. Cryptocurrencies–advantages and disadvantages. J. Econ. 2, 31–39.

Buterin, V., 2015. A Next-Generation Smart Contract and Decentralized Application Platform.

Cambridge Blockchain [WWW Document], n.d. URL https://www.cambridgeblockchain.com/ (accessed 3.14.21).

Camenisch, J., Shelat, A., Sommer, D., Fischer-Hüubner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., Tseng, J., 2005. Privacy and identity management for everyone, in. In: Proceedings of the ACM Conference on Computer and Communications Security, pp. 20–27. https://doi.org/10.1145/1102486.1102491.

Can, M., Khalilov, K., Levi, A., 2018. A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems. https://doi.org/10.1109/COMST.2018.2818623.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things, in IEEE Access, vol. 4, no. , pp. 2292-2303, 2016. IEEE Access 4, 2292–2303. https://doi.org/doi: 10.1109/ACCESS.2016.2566339

Civic, n.d. Civic Secure Identity Ecosystem [WWW Document]. URL https://www.civic.com/ (accessed 2.22.20).

Conoscenti, M., Vetro, A., De Martin, J.C., 2016. Blockchain for the Internet of Things: A systematic literature review. In: in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6.

ConsenSys [WWW Document], n.d. URL https://www.consensys.net/ (accessed 3.12.21).

Conti, M., Member, S., E, S.K., Lal, C., 2017. A Survey on Security and Privacy Issues of Bitcoin.

CredyCo [WWW Document], n.d. URL https://www.coindesk.com/trustatom-raises-100k-blockchain-based-due-diligence-service (accessed 3.12.20).

Cryptid [WWW Document], n.d. URL http://cryptid.xyz/

Dhamija, R., Dusseault, L., 2008. The seven flaws of identity management: usability and security challenges. IEEE Secur. Priv. 6, 24–29.

Du, Y., Liu, J., Guan, Z., Feng, H., 2018. A medical information service platform based on distributed cloud and blockchain. IEEE International Conference on Smart Cloud (SmartCloud) 2018, 34–39. https://doi.org/10.1109/SmartCloud.2018.00014.

Dunphy, P., Petitcolas, F.A.P., 2018. A First Look at Identity Management Schemes on the Blockchain. https://doi.org/10.1109/MSP.2018.3111247.

El Haddouti, S., El Kettani, M.D.E.-C., 2019. In: Analysis of Identity Management Systems Using Blockchain Technology, pp. 1–7.

Elisa, N., Yang, L., Chao, F., Cao, Y., 2018. A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Netw., 1–11
Evernym [WWW Document], n.d. URL https://www.evernym.com/ (accessed 3.14.21).
Existence ID [WWW Document], n.d. URL https://existenceid.com/ (accessed 3.13.21).
Eyal, I., Sirer, E.G., 2014. Majority is not enough: Bitcoin mining is vulnerable, in: International Conference on Financial Cryptography and Data Security. pp. 436–454.
Falkvinge, R., Overview, B., Network, A., 2015. B ITNATION Whitepaper by Susanne Tarkowski Tempelhof 1–21.
Feng, Q., He, D., Liu, Z., Wang, D., Choo, K.-K.R., 2020. Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme. IET Inf. Secur.
Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2018. A Survey on Privacy Protection in Blockchain AC. J. Netw. Comput. Appl. https://doi.org/10.1016/j.jnca.2018.10.020.
Ferdous, M.S., Poet, R., 2012. A comparative analysis of identity management systems. In: 2012 International Conference on High Performance Computing & Simulation (HPCS), pp. 454–461.
Friebe, S., Zitterbart, M., 2018. DecentID : Decentralized and Privacy-preserving Identity Storage System using Smart Contracts. In: 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), pp. 37–42. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00016.
Future of Identity in the Information Society [WWW Document], n.d. URL http://www.fidis.net/ (accessed 3.13.21).
Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L., Shi, W., 2018. Blockchain-based Identity management with mobile device blockchain-based identity management with mobile device. https://doi.org/10.1145/3211933.3211945
Gramoli, V., 2020. From blockchain consensus back to byzantine consensus. Future Gen. Comput. Syst. 107, 760–769.
Halperin, R., Backhouse, J., 2008. A roadmap for research on identity in the information society 1, 71–87. https://doi.org/10.1007/s12394-008-0004-0.
Heck, R., Torstensson, J., Mitton, Z., Sena, M., 2017. Uport: a platform for self-sovereign identity.
Heilman, E., Baldimtsi, F., Goldberg, S., 2016. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions, in: International Conference on Financial Cryptography and Data Security. pp. 43–60.
Hussein, A.F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J.M.R.S., de Albuquerque, V.H.C., 2018. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. Cognit. Syst. Res. 52, 1–11. https://doi.org/10.1016/j.cogsys.2018.05.004.
I/O Foundation [WWW Document], n.d. URL https://iodigital.io/ (accessed 3.14.21).
id2020, n.d. We need to get digital ID right [WWW Document]. URL https://id2020.org/ (accessed 12.3.21).
Islam, M.N., Kundu, S., 2019. Enabling ic traceability via blockchain pegged to embedded puf. ACM Trans. Design Autom. Electron. Syst. (TODAES) 24, 1–23.
Jensen, J., 2012. Federated Identity Management Challenges 230–235. https://doi.org/10.1109/ARES.2012.68
Jensen, J., Jaatun, M.G., 2012. Federated identity management-we built it; why won't they come? IEEE Secur. Priv. 11, 34–41.
Jolocom, 2019. A Decentralized , Open Source Solution for Digital Identity and Access Management.
Josang, A., AlZomai, M., Suriadi, S., 2007. Usability and privacy in identity management architectures, in. In: ACSW Frontiers 2007: Proceedings of 5th Australasian Symposium on Grid Computing and e-Research, 5th Australasian Information Security Workshop (Privacy Enhancing Technologies), and Australasian Workshop on Health Knowledge Management and Discovery, pp. 143–152.
Jøsang, A., Fabre, J., Hay, B., Dalziel, J., Pope, S., 2005. Trust requirements in identity management, in: Proceedings of the 2005 Australasian Workshop on Grid Computing and E-Research-Volume 44. pp. 99–108.
Kaaniche, N., Laurent, M., Kaaniche, N., Laurent, M., 2018. A blockchain-based data usage auditing architecture with enhanced privacy and availability To cite this version Availability. In: In Network Computing and Applications (NCA), 2017 IEEE 16th International Symposium on IEEE, pp. 1–5.
Kitchenham, B.A., Budgen, D., Brereton, O.P., 2011. Using mapping studies as the basis for further research–a participant-observer case study. Inf. Softw. Technol. 53, 638–651.
Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: in: 2016 IEEE Symposium on Security and Privacy (SP), pp. 839–858.
Kumar, N.M., Mallick, P.K., 2018. Blockchain technology for security issues and challenges in IoT. Proc. Comput. Sci. 132, 1815–1823.
Le, H., Bouzefrane, S., National, C., Cardspace, A.M.W., 2008. Identity Management Systems and Interoperability in a Heterogeneous Environment 239–242.
Lee, J., Hwang, J., Choi, J., Oh, H., Kim, J., 2019. SIMS: Self Sovereign Identity Management System with Preserving Privacy in Blockchain. IACR Cryptol. ePrint Arch. 2019, 1241.
Lee, J., Member, S., 2018. BIDaaS : Blockchain Based ID As a Service. IEEE Access 6, 2274–2278. https://doi.org/10.1109/ACCESS.2017.2782733.
Leenes, R.E., 2014. PRIME white paper v2.
Leiding, B., Norta, A., 2017. Mapping Requirements Specifications into a Formalized Blockchain-Enabled Authentication Protocol for Secured Personal Identity Assurance Mapping Requirements Specifications into a Formalized Blockchain-Enabled Authentication Protocol for Secured Personal . https://doi.org/10.1007/978-3-319-70004-5.
Leimgruber, J., Meier, A., Backus, J., 2018. Bloom Protocol Decentralized credit scoring powered by Ethereum and IPFS.
Lemieux, V.L., Lemieux, V.L., 2016. Trusting records: is Blockchain technology the answer ? https://doi.org/10.1108/RMJ-12-2015-0042
Lim, M.K., Li, Y., Wang, C., Tseng, M.-L., 2021. A literature review of blockchain technology applications in supply chains: a comprehensive analysis of themes, methodologies and industries. Comput. Ind. Eng. 107133.
Lin, I.-C., Liao, T.-C., 2017. A survey of blockchain security issues and challenges. IJ Network Security 19, 653–659.
Liu, L., 2016. An Online Identity & Smart Contract Management 192–198. https://doi.org/10.1109/COMPSAC.2016.2
Liu, Y.-N., Lv, S.-Z., Xie, M., Chen, Z.-B., Wang, P., 2019. Dynamic anonymous identity authentication (DAIA) scheme for VANET. Int. J. Commun Syst 32, e3892.
Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., Choo, K.-K.R., et al., 2020. Blockchain-based identity management systems: a review. J. Netw. Comput. Appl. 102731.
Lo, S.K., Xu, X., Chiam, Y.K., Lu, Q., 2017. Evaluating suitability of applying blockchain, in: 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS). pp. 158–161.
Lone, A.H., Naaz, R., 2021. Applicability of blockchain smart contracts in securing Internet and IoT: a systematic literature review. Comput. Sci. Rev. 39, 100360.
Loukil, F., Ghedira-Guegan, C., Boukadi, K., Benharkat, A.N., 2018. Towards an end-to-end IoT data privacy-preserving framework using blockchain technology, in: International Conference on Web Information Systems Engineering. pp. 68–78.
Lu, H., Jin, C., Helu, X., Zhu, C., Guizani, N., Tian, Z., 2020. AutoD: intelligent blockchain application unpacking based on JNI layer deception call. IEEE Netw.
Ma, Z., Jiang, M., Gao, H., Wang, Z., 2018. Blockchain for digital rights management reference: future generation computer sys blockchain for digital rights management. Future Gen. Comput. Syst. https://doi.org/10.1016/j.future.2018.07.029.
Matsumoto, T., Hellman, M.E., 1976. New directions in cryptography. IEEE Trans. Inf. Theory 22, 644–654.
Mikula, T., Jacobsen, R.H., 2018. Identity and Access Management with Blockchain in Electronic Healthcare Records. In: 2018 21st Euromicro Conference on Digital System Design (DSD), pp. 699–706. https://doi.org/10.1109/DSD.2018.00008.
Mohanta, B.K., Jena, D., Panda, S.S., Sobhanayak, S., 2019. Blockchain technology: a survey on applications and security privacy challenges. Intern. Things 8, 100–107.
Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J.A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J.J., Devereaux, P.J., Dickersin, K., Egger, M., Ernst, E., Gøtzsche, P.C., Grimshaw, J., Guyatt, G., Higgins, J., Ioannidis, J.P.A., Kleijnen, J., Lang, T., Magrini, N., McNamee, D., Moja, L., Mulrow, C., Napoli, M., Oxman, A., Pham, B., Rennie, D., Sampson, M., Schulz, K.F., Shekelle, P.G., Tovey, D., Tugwell, P., 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement (Chinese edition). Journal of Chinese Integrative Medicine 7, 889–896. https://doi.org/10.3736/jcim20090918
My Health My Data [WWW Document], 2019. . My Health My Data. URL http://www.myhealthmydata.eu/ (accessed 3.12.21).
Nakamoto, S., n.d. Bitcoin: A Peer-to-Peer Electronic Cash System 1–9.
NameCoin [WWW Document], n.d. URL https://www.namecoin.org/ (accessed 2.13.21).
Netki [WWW Document], n.d. URL https://netki.com/ (accessed 3.12.21).
OneName [WWW Document], n.d. URL https://onename.com/ (accessed 11.21.20).
Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A., 2016. FairAccess: a new blockchain-based access control framework for the Internet of Things. Sec. Commun. Netw. 9, 5943–5964.
Paper, W., n.d. Peermountain [WWW Document]. URL https://www.peermountain.com/ (accessed 3.12.21).
Pavel Kravchenko, 2016. Ok, I need a blockchain, but which one? [WWW Document]. URL https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100 (accessed 3.12.21).
Pérez-Méndez, A., Torroglosa-Garc\'\ia, E.-M., López-Millán, G., Gómez-Skarmeta, A. F., Girao, J., Lischka, M., 2010. SWIFT–Advanced Services for Identity Management. Serbian Publication InfoReview joins UPENET, the Network of CEPIS Societies Journals and Magazines 13.
Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., Shi, W., 2017. Cecoin: a decentralized PKI mitigating MitM attacks. Future Gen. Comput. Syst. https://doi.org/10.1016/j.future.2017.08.025.
Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., Fang, B., 2020. A survey on access control in the age of internet of things. IEEE Internet Things J. 7, 4682–4696.
Raju, S., Boddepalli, S., Gampa, S., Yan, Q., Deogun, J.S., 2017. Identity management using blockchain for cognitive cellular networks. In: in: 2017 IEEE International Conference on Communications (ICC), pp. 1–6.
Rossudowski, A.M., Venter, H.S., Eloff, J.H.P., Kourie, D.G., 2010. A security privacy aware architecture and protocol for a single smart card used for multiple services. Comput. Sec. 29, 393–409. https://doi.org/10.1016/j.cose.2009.12.001.
Rouven Heck, n.d. Identity management via blockchain? [WWW Document]. URL https://main-incubator.com/en/identity-management-via-blockchain/ (accessed 6.15.18).
Saha, A., Amin, R., Kunal, S., Vollala, S., Dwivedi, S.K., 2019. Review on "Blockchain technology based medical healthcare system with privacy issues". Sec. Priv. 2, e83.

Sanka, A.I., Irfan, M., Huang, I., Cheung, R.C.C., 2021. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. Comput. Commun.
Sarangal, H., Singh, A., Malhotra, J., Zcc, Á.O.Á.S.Á., 2019. Disrupting Insurance Industry Using Blockchain. Spring. Intern. Publ. https://doi.org/10.1007/978-3-030-03146-6.
Sarier, N.D., 2018. Cyberspace Safety and Security. Springer International Publishing, pp. 254–269.
Schanzenbach, M., Bramm, G., Schütte, J., 2018. reclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption, in: 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). pp. 946–957.
Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., Guizani, M., 2020. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J. Sel. Areas Commun. 38, 942–954.
Shetty, S., Liang, X., Bowden, D., Zhao, J., Zhang, L., 2019. Blockchain-based decentralized accountability and self-sovereignty in healthcare systems business transformation through blockchain. Springer, 119–149.
Shin, D., Lopes, R., Claycomb, W., 2009. Authenticated Dictionary-based Attribute Sharing in Federated Identity Management 0–5. https://doi.org/10.1109/ITNG.2009.193
Shocard [WWW Document], n.d. URL https://shocard.com/ (accessed 3.13.21).
Shrier, D., Wu, W., Pentland, A., 2016. Blockchain & Infrastructure (Identity, Data Security). Massachusetts Institute of Technology-Connection Science, 1–19.
SNG, S.N.G., 2003. Identity Management Systems (IMS): Identification and Comparison Study Independent Centre for Privacy Protection (ICPP)/ Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein.
Stefanova, K., Kabakchieva, D., Nikolov, R., 2010. Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services 8, 189–202.
Stephen, R., Alex, A., 2018. A Review on BlockChain Security. In: IOP Conference Series: Materials Science and Engineering, p. 12030.
Storj, 2017. Storj: Decentralized cloud storage. Storj - Decentralized Cloud Storage.
Sullivan, C., Burger, E., 2017. E-residency and blockchain. Comput. Law Sec. Rev. Int. J. Technol. Law Pract. 1–12. https://doi.org/10.1016/j.clsr.2017.03.016.
Sun, Y., Zhang, R., Wang, X., Gao, K., Liu, L., 2018. A Decentralizing Attribute-Based Signature for Healthcare Blockchain. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–9. https://doi.org/10.1109/ICCCN.2018.8487349.
Suriadi, S., Foo, E., Jøsang, A., 2007. A User-centric Federated Single Sign-on System 101–108. https://doi.org/10.1109/NPC.2007.64
Swan, M., 2015. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc", ".
The SelfKey Foundation, 2017. SelfKey.
Tian, Z., Li, M., Qiu, M., Sun, Y., Su, S., 2019. Block-DEF: A secure digital evidence framework using blockchain. Inf. Sci. 491, 151–165.
Tobin, A., Reed, D., 2016. The inevitable rise of self-sovereign identity. The Sovrin Foundation 29.
Torres, J., Nogueira, M., Pujolle, G., 2012. Future Network 1–16.
Toufaily, E., Zalan, T., Dhaou, S. Ben, 2021. A framework of blockchain technology adoption: an investigation of challenges and expected value. Inform. Manag. 103444.
Tsukerman, M., 2016. The block is hot: a survey of the state of bitcoin regulation and suggestions for the future. Berkeley Technol. Law J. 30, 1127–1169.
Turkanović, M., Hölbl, M., Košič, K., Heričko, M., Kamišalić, A., 2018. EduCTX: a blockchain-based higher education credit platform. IEEE Access 6, 5112–5127.
Umeh, J., 2016. Blockchain double bubble or double trouble? Itnow 58, 58–61.
UniquID [WWW Document], n.d. URL https://uniquid.com/ (accessed 3.14.21).
Vacca, A., Di Sorbo, A., Visaggio, C.A., Canfora, G., 2020. A systematic literature review of blockchain and smart contract development: techniques, tools, and open challenges. J. Syst. Softw. 110891.
Vandervort, D., Gaucas, D., St Jacques, R., 2015. Issues in designing a bitcoin-like community currency, in: International Conference on Financial Cryptography and Data Security. pp. 78–91.
Vossaert, J., Lapon, J., Decker, B. De, Naessens, V., 2013. User-centric identity management using trusted modules 57, 1592–1605. https://doi.org/10.1016/j.mcm.2012.06.010.
Wang, X., Tan, Z., Wang, S., 2017. An Identity Management System Based on Blockchain. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp. 44–4409. https://doi.org/10.1109/PST.2017.00016.
Weber, S.G., Martucci, L., Ries, S., Mühlhäuser, M., 2010. Towards trustworthy identity and access management for the future internet, in: 4th International Workshop on Trustworthy Internet of People, Things & Services.
Wood, G., 2018. A secure decentralized generalized distributed ledger. Ethereum. https://doi.org/10.1017/CBO9781107415324.004.
Wüst, K., Gervais, A., 2018. Do you need a blockchain?, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 45–54.
Wüst, K., Gervais, A., n.d. Do you need a Blockchain ? 1–7.
Yli-huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where Is Current Research on Blockchain Technology ?— A Systematic Review 1–27. https://doi.org/10.1371/journal.pone.0163477
Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T., 2018. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004.
Zheng, Y., Li, Yarong, Wang, Z., Deng, C., Luo, Y., Li, Yixin, Ding, J., 2019. Blockchain-based privacy protection unified identity authentication. In: in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 42–49.
Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Xiangping Chen, H.W., 2017. Blockchain Challenges and Opportunities : A Survey Zibin Zheng Shaoan Xie Hong-Ning Dai Xiangping Chen Huaimin Wang. International Congress on Big Data 14, 1–25. https://doi.org/10.1504/IJWGS.2018.095647.
Zyskind, G., Nathan, O., others, 2015a. Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops. pp. 180–184.
Zyskind, G., Nathan, O., Pentland, A., 2015b. Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471.