Blockchain and Identity Management

Xin Yang and Johnny Chan(✉)

The University of Auckland, Auckland, New Zealand
jh.chan@auckland.ac.nz

Abstract. On one end of the world, we have a billion people who do not have any registered identity or bank account. On the other end, there are billions of people registered with multiple digital identities, who are having their personal information and privacy being invaded on a daily basis. The objective of this paper is to explore opportunities in addressing both problems through the application of blockchain-based identity management. A systematic review is conducted, and 53 papers are summarised and analysed. It discusses how blockchain technology could process sensitive and large identity dataset among different domains.

Keywords: Blockchain · Identity · Privacy · Identity management · Cybersecurity · IoT · Healthcare

1 Introduction

On one end of the world, we have a billion people who do not have any registered identity [1], and 1.7 billion adults are living without a bank account [2]. Most of them reside in rural areas or war zones that lack the means for persistent and trustworthy identity management [3, 4]. On the other end, there are billions of people registered with multiple identities for numerous digital services, worrying about their identity-associated information and privacy could be invaded by hackers, corporations and governments [5]. This problem will always be there if identities are managed by a single institution at the centre. We desperately need a solution to solve the identity crises on both ends.

Blockchain, the underlying technology behind Bitcoin [6], has shown some promises by replacing traditional centralised systems with decentralised and distributed systems and networks [7]. The decentralised structure offers two main benefits: tamper-proof data immutability and disintermediation. Blockchain is a technology that combines cryptography, mathematical algorithms and peer-to-peer networking [8]. The objective of this paper is to explore the opportunities of blockchain-based identity management through a systematic review of the existing literature [9].

P. Cong Vinh and A. Rakib (Eds.): ICCASA 2021, LNICST 409, pp. 192–204, 2021.
https://doi.org/10.1007/978-3-030-93179-7_15

2 Literature Review

2.1 Search String

To select the relevant papers from the literature systematically, a series of keywords in identity management and blockchain technology are considered for composing a search string. As it turns out, "identity" is not an ideal search phrase on its own, because research publication databases often equate that with "identify" in which the context is usually irrelevant to personal identity or identity management. After a few trial-and-error attempts, this issue could be remedied by adding the word "privacy" with "identity" as a combined keyword to search for identity management. Therefore, the finalised search string is composed as [(Identity AND Privacy) AND Blockchain].

2.2 Screening Process

The screening process is carried out in two steps. The first step aims to eliminate papers associated with irrelevant fields. An abstract and keyword screening is applied to all selected papers. Some relevant papers could be identified by abstract screening alone. However, when the abstract does not remotely correspond to blockchain and identity management, a keyword screening is followed to minimise the chance of eliminating papers with valuable information. Some of these papers do not focus on blockchain-based identity management systems, but they have some detailed description of such a system as part of the project, product or service they study or propose. For instance, a paper on Internet of Things (IoT) may include a full description of a blockchain-based identity management system for secured identity data storage, even though its abstract does not mention anything about it.

The second step is a full-text screening of all papers considered relevant from the first step, and it removes any paper that does not discuss blockchain-based identity management systems within the body of the article. Through the full-text screening, the final list of papers is classified into different research areas.

2.3 Result

After applying the composed search string, 267 papers are initially collected from six databases including ABI/Inform, Business Source Premier, Emerald Insight, IEEE, JSTOR and ScienceDirect. Only studies published in academic and practitioner journals are selected for quality control reasons [10]. It is worth noting that a significant portion of the literature is collected from ABI/Inform and Science Direct, including 74 and 162 papers, respectively. All papers are separated into two categories. Category A represents the candidate papers of the systematic review, and Category B stores the filtered papers at the end of the screening process. During the abstract and keyword screening, 77 papers are placed in Category A and 190 papers are placed in Category B. The majority of papers from Category B are associated with network security which contains the keywords "privacy" and "identity". However, they do not discuss identity management and hence are categorised as irrelevant. The full-text screening stage further moves 24 papers from Category A to Category B. Most of them are

associated with the security improvement of the cryptocurrency ecosystem, or reviews of popular blockchain technologies. Although these papers have mentioned blockchain-based identity management, they do not provide enough detail to be part of the knowledge base built from the systematic review. Figure 1 captures the screening process and the resulting Review Knowledge Base.

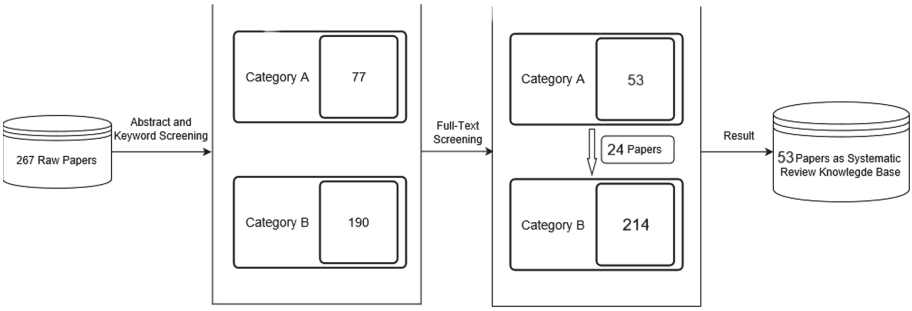

Fig. 1. Screening process and review knowledge base

Based on the Screening Process, there are 214 identity management irrelevant papers, and most of these papers discuss the identity and privacy problems in cryptocurrency. Compared to cryptocurrency, blockchain-based identity management is significantly under explored, even though it might be one possible solution to the severe identity management problem.

3 Analysis of Existing Solutions

The knowledge base of the systematic review contains 53 papers with 10 primary domains emerging as shown in Table 1. Even a paper could be related to multiple domains, they are being classified by their strongest association. The 10 primary domains are: IoT (19), healthcare (9), cyber-identity (8), data management (5), energy (3), cloud service (3), manufacturing (2), social network (2), cybersecurity (1) and financial service (1).

The top three primary domains are IoT, healthcare and cyber-identity, and they represent almost 70% of the knowledge base from the study. All papers from the IoT and healthcare domains also associate with the identity management domain. The proportionally large number of papers from the IoT domain indicates the role and importance of smart devices and connectivity to our identity management in the future, centralised or decentralised. The stronger thematic association to healthcare among those papers shows that identity management in this specific context is the most critical one being studied by researchers and scholars. The following subsections would focus on these three primary domains, to discuss the identity management problems they are facing, and how blockchain technology was integrated and enhanced their identity management.

Table 1. The knowledge base

No	Title	Reference	Primary domain
1	Trustworthy data-driven networked production for customer-centric plants	[11]	IoT
2	E-residency and blockchain	[12]	Cyber-Identity
3	A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors	[13]	Cyber-Identity
4	Designing microgrid energy markets	[14]	Energy
5	BIDaaS: Blockchain Based ID As a Service	[15]	Cyber-Identity
6	Blockchain's roles in strengthening cybersecurity and protecting privacy	[16]	IoT
7	Toward open manufacturing	[17]	Manufacturing
8	OmniPHR: A distributed architecture model to integrate personal health records	[18]	Healthcare
9	Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector	[19]	Healthcare
10	Cecoin: A decentralized PKI mitigating MitM attacks	[20]	Cybersecurity
11	Access control in the Internet of Things: Big challenges and new opportunities	[21]	IoT
12	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	[22]	Healthcare
13	A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform	[23]	Healthcare
14	CreditCoin: A Privacy-Preserving Blockchain-based Incentive Announcement Network for Communications of Smart Vehicles	[24]	IoT
15	Decentralized privacy preserving services for Online Social Networks	[25]	Social Network
16	A Social-Network-Based Cryptocurrency Wallet-Management Scheme	[26]	Social Network
17	An OpenNCP-based Solution for Secure eHealth Data Exchange	[27]	Healthcare
18	A Privacy-Preserving Trust Model Based on Blockchain for VANETs	[28]	IoT
19	Digital identity – From emergent legal concept to new reality	[29]	Identity Management
20	Internet of things security: A top-down survey	[30]	IoT
21	Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform	[31]	Cloud Service

(*continued*)

Table 1. (*continued*)

No	Title	Reference	Primary domain
22	A Case Study for Blockchain in Manufacturing: "fabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes	[32]	Manufacturing
23	Blockchain for digital rights management	[33]	Cyber-Identity
24	Decentralized enforcement of document lifecycle constraints	[34]	Data Management
25	A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems	[35]	Cyber-Identity
26	Block-secure: Blockchain based scheme for secure P2P cloud storage	[36]	Cloud Service
27	Bubbles of Trust: A decentralized blockchain-based authentication system for IoT	[37]	IoT
28	Blockchain technology for security issues and challenges in IoT	[38]	IoT
29	Blockchain mechanisms for IoT security	[39]	IoT
30	A blockchain future for internet of things security: a position paper	[40]	IoT
31	A Survey on Essential Components of a Self-Sovereign Identity	[41]	Cyber-Identity
32	A first look at identity management schemes on the blockchain	[42]	Cyber-Identity
33	FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data	[43]	Healthcare
34	Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability	[44]	Healthcare
35	Authenticating Health Activity Data Using Distributed Ledger Technologies	[45]	Healthcare
36	Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities	[46]	Energy
37	A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval	[47]	Healthcare
38	Blockchain and the future of energy	[48]	Energy
39	A TISM modeling of critical success factors of blockchain based cloud services	[49]	Cloud Service
40	Towards decentralized IoT security enhancement: A blockchain approach	[50]	IoT
41	A remote attestation security model based on privacy-preserving blockchain for V2X	[51]	IoT
42	Smart-toy-edge-computing-oriented data exchange based on blockchain	[52]	Data Management

(*continued*)

Table 1. (*continued*)

No	Title	Reference	Primary domain
43	On blockchain and its integration with IoT. Challenges and opportunities	[53]	IoT
44	Multi-tier blockchain framework for IoT-EHRs systems	[54]	IoT
45	IoT security: Review, blockchain solutions, and open challenges	[55]	IoT
46	Machine learning based privacy-preserving fair data trading in big data market	[56]	Data Management
47	Controllable and trustworthy blockchain-based cloud data management	[57]	Data Management
48	Blockchain's adoption in IoT: The challenges, and a way forward	[58]	IoT
49	A survey on internet of things security from data perspectives	[59]	IoT
50	A secure versatile light payment system based on blockchain	[60]	Financial Service
51	Renovating blockchain with distributed databases: An open source system	[61]	Data Management
52	A blockchain-based location privacy-preserving crowdsensing system	[62]	IoT
53	MOF-BC: A memory optimized and flexible blockchain for large scale networks	[63]	IoT

3.1 IoT

The rapid growth of smart devices and high-speed internet have made the IoT become one of the most popular topics recently. As more devices like smartwatches and smart surveillance cameras are being connected, more identity data would be generated and flowing through the web, creating new challenges for identity management among IoT systems [58].

A common architecture of an IoT system has smart devices collecting data in a distributed manner, and they report to a centralised cloud service through multiple network layers. However, this setting is vulnerable and susceptible to malicious attacks. For example, an attacker could pretend to be one of the smart devices, monitor the instructions from the centralised server, and steal the backup data. Additionally, the centralised server itself could also become a victim from cyberattacks [55].

Many researchers have investigated the integration of the IoT system with blockchain technology. They discuss the possibility, and they develop and evaluate new IoT models by adopting blockchain technologies. Most of the review papers discuss the scalability and robustness of the centralised and the decentralised systems. Makhdoom et al. [58] have constructed a table to compare the differences between the system structures of a centralised cloud and a decentralised blockchain. Cloud service is under

the centralised control of one trusted entity. If that trusted entity encounters an accident or a malicious attack, the entire IoT system could break down. However, the blockchain technology provides an edge storage feature with each miner node containing a full copy of the blockchain. So even if one node is taken down, the other nodes will become its back up to ensure the IoT system will stay functional.

Many papers discuss different consensus protocols among blockchain-based systems. A consensus protocol can reduce the data communication overhead between the nodes and the centralised server by allowing node to node activities, such as data exchange and authentication, to be carried out in a distributed manner. In addition, decision-making programmes can be embedded as smart contracts in a blockchain to allow the nodes of an IoT system to make decisions without a server, and hence enabling a rapid data exchange among all the nodes. Ouaddah et al. [21] point out that a decentralised blockchain authentication system for identity management in an IoT system would be less dependent on a trusted entity.

However, system performance could become an issue. Reyna et al. [53] explain that as the data stored in each node increases and the size of the blockchain grows, the nodes would consume more resources and affect system performance. For instance, the synchronisation time of adding a new node will increase. There could be gigabytes of data generated by IoT systems within an hour, but many current blockchain-based systems could only process a few transactions per second. Hammi et al. [37] present a decentralised blockchain-based authentication system called the Bubble of Trust. One of the issues they identify is that their system could not be adapted to real time application because the consensus time for validating one transaction would take 14 s from the Ethereum main chain.

Some researchers try to integrate a decentralised blockchain with the traditional centralised IoT system to tackle the performance issue. Xu et al. [51] develop a remote attestation security model with a blockchain for IoT systems in vehicles. Each node of this blockchain stores the access control information and its current status. As the nodes take over the access control and status monitoring, the workload of the server is reduced. Also, the security risks are now distributed to all the nodes and therefore the possibility of the entire system being compromised drops. The performance evaluation of their system shows a 97% success rate of updating their status with a confirmation time of 3 s on real vehicles. Similarly, Lu et al. [28] propose a blockchain-based anonymous reputation system for Vehicle ad hoc Networks (VANET) which stores the authentication keys for the access control of the VANET system to avoid the escrow problem in centralised IoT authentication systems with a decentralised blockchain identity storage.

3.2 Healthcare

With the traditional centralised systems, the management and exchange of health records and identities have been raised as a common problem in the healthcare domain. One reason is that health records and identities are often distributed among various third parties, including the hospitals, the clinics, and the insurance companies, who do not have a shared data repository. Therefore, when applying a medical treatment to a patient, certain data exchanges among the third parties may be required to gather the

necessary health data. However, the health identities of patients are private, and it is important for them to be informed where, when and who their health identities are stored, exchanged and accessed.

Gordon and Catalini [44] propose that the current institute-driven health identity management should be transformed to patient-driven. The concept of patient-driven identity management encourages third parties to hand over the health identity sovereignty back to the individuals. For instance, in a case where an institute needs the health identity of a patient for medical treatment, the institute will ask the patient for permission to access the data. The patient can choose to authorise the institute and give them a key to the other third parties' databases to access his entire health record and identity. The institute is only allowed to access, update or transfer the health identity based on the level of permissions it has been given by the patient. Dagher et al. [22] create a framework for the access control and data exchange of health identity called Ancile. In this framework, a blockchain is used to store the permissions of different institutes for a patient. Once an institute requests an access to the patient's health identity, the blockchain will first check its permission level. If the institute does not hold the permission to access, the blockchain will ask the patient for authorisation. As only the patient has the right to alter the permission level, the health identity management is now driven by the patient. Additionally, the framework has a transaction log to record all the institutes' activities, therefore a patient can monitor any activities to their health record and identity.

Beside the issue of sovereignty, others have proposed new channels for the data exchange to happen between different institutes. For instance, Zhang et al. [43] introduce a framework called FHIRChain to store the encrypted database addresses of patients' health identities. For one institute requesting to exchange a patient's health identity with another, the digital keys from both institutes are required to decrypt the database addresses. Hence, the institute can review, retrieve or update the data by accessing the database through the decrypted addresses.

The data exchange between different institutes could also bring security challenges. The traditional unsecured data exchange channels may be attacked and result in data leakage. Blockchain-based systems could provide a more secure data exchange channel with lowered network overhead [43]. Even if data is leaked, the encrypted addresses still leave the attackers a formidable challenge. Furthermore, because of the lowered network overhead, that could benefit health identity management in rural areas. The health identity of the patients living in rural areas can therefore be transferred to a place with better internet infrastructures. For the health institutes in rural areas, instead of updating or downloading the full documents, they can visit or update a patient's health identity directly from a remote database. By exchanging the lightweight database addresses, the health identity management in rural areas will become more accessible.

Compared to IoT, the healthcare domain only manages a relatively smaller amount of identity data. However, the identity management in healthcare still needs to store the patients' health records and identities in the databases off-chain, and it cannot avoid the involvement of the third parties. Therefore, the identity management could not be fully decentralised.

3.3 Cyber-Identity

Contrary to the research from domains of IoT and healthcare, papers from cyber-identity focus mainly on systems aiming to manage individual identity in a more secure and convenient way without a specific context.

Lee [15] proposes a framework called BIDaaS to support the identity verification process. BIDaaS has three entities, namely the BIDaaS provider, the partner and the user. The BIDaaS provider stores the identity information of users off-chain and manages a Virtual ID generator on-chain. The partners are the trusted third parties which may require a user's identity information. They can be any legal entity like the banks, the hospitals, and the councils, which require the identity of a user for social services; or small-sized institutions such as online shopping providers which require the identity information of a user for subscription. The users hold a digital key for authentication and Virtual ID generation. Traditionally, a user provides his identity information directly to the partners for verification. However, with the support of BIDaaS, the user can use the digital key to generate a Virtual ID on the blockchain and send it to the partners. The partners can then obtain the identity information from the BIDaaS provider by sending this Virtual ID to the BIDaaS server. The users can specify which identity information is shared during the key generation so that they are still in control of the shared content. This framework provides convenience to both the partners and the users. For the partners, instead of maintaining an identity verification system, they can now retrieve verified identity information directly from the BIDaaS system. For the users, without the need of managing various identity documents, they only need to bring a digital key for the identity verification from any third parties.

The capability of a blockchain-based cyber-identity system is not limited to identity verification. For instance, Estonia has established an e-residency program with Bitnation [12]. The purpose of this program is to encourage the e-resident to access social and commercial activities and services in Estonia, including banking services, and company formation and taxation services. Bitnation, as the e-residency provider, issues an e-identity and a series of documents storage services based on the blockchain technology. Therefore, the Bitnation users can create their new identity and store their documents such as marriage certification, insurance policy and land title on-chain to access the public services.

The blockchain-based identity management in healthcare reveals a pattern of having both a decentralised decision-making structure and a centralised data storage. A similar trend could also be observed among general blockchain-based cyber-identity system design as well, dealing with all kinds of identities including financial records, vehicle registrations or criminal records.

4 Discussion and Conclusion

To conclude, the decentralised blockchain-based system has shown significant potentials in fast authentication, secured data exchange and improved self-sovereignty with user identity. These potentials can benefit the management of the large quantity of identity data from IoT, as well as the sensitive and private records such as healthcare

records and cyber-identity. Unfortunately, as a potential solution to many identity management problems among different domains, blockchain-based identity management is still under explored. It is the time to shift some focus from cryptocurrency to blockchain-based identity management. The future works for blockchain-based identity management can be concluded into two aspects. The first aspect is to increase the level of decision-making from the decentralised nodes, and the node functions should not be limited to authentication and data exchanges but including a registration system to let users create new identities. The second aspect is to introduce the current blockchain-based identity management frameworks to more domains and areas.

References

1. The World Bank Group: Identification for Development (ID4D) Global Dataset. https://datacatalog.worldbank.org/dataset/identification-development-global-dataset
2. Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., Hess, J.: The Global Findex Database 2017 - Measuring Financial Inclusion and the Fintech Revolution: Overview. The World Bank (2018). https://doi.org/10.1596/978-1-4648-1259-0
3. Harbitz, M., del Carmen Tamargo, M.: The Significance of Legal Identity in Situations of Poverty and Social Exclusion: The Link between Gender, Ethnicity, and Legal Identity (2009)
4. Williams, R., Drury, J.: Personal and collective psychosocial resilience: implications for children, young people and their families involved in war and disasters. In: Cook, D.T., Wall, J. (eds.) Children and Armed Conflict. SCY, pp. 57–75. Palgrave Macmillan UK, London (2011). https://doi.org/10.1057/9780230307698_5
5. Samarati, P., di Vimercati, S.D.C.: Data protection in outsourcing scenarios: issues and directions. In: The 5th ACM Symposium on Information, Computer and Communications Security, pp. 1–14. ACM, New York, USA (2010). https://doi.org/10.1145/1755688.1755690
6. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). https://doi.org/10.1007/s10838-008-9062-0
7. Underwood, S.: Blockchain beyond bitcoin. Commun. ACM. **59**, 15–17 (2016). https://doi.org/10.1145/2994581
8. Lin, I.-C., Liao, T.-C.: A survey of blockchain security issues and challenges. IJ Netw. Secur. **19**, 653–659 (2017)
9. Tranfield, D., Denyer, D., Smart, P.: Towards a methodology for developing evidence-informed management knowledge by means of systematic Review. Br. J. Manage. **14**, 207–222 (2003). https://doi.org/10.1111/1467-8551.00375
10. Crossan, M.M., Apaydin, M.: A multi-dimensional framework of organizational innovation: a systematic review of the literature. J. Manage. Stud. **47**, 1154–1191 (2010). https://doi.org/10.1111/j.1467-6486.2009.00880.x
11. Preuveneers, D., Joosen, W., Ilie-Zudor, E.: Trustworthy data-driven networked production for customer-centric plants. Ind. Manage. Data Syst. **117**, 2305–2324 (2017). https://doi.org/10.1108/IMDS-10-2016-0419
12. Sullivan, C., Burger, E.: E-residency and blockchain. Comput. Law Secur. Rev. **33**, 470–481 (2017). https://doi.org/10.1016/j.clsr.2017.03.016

13. Wolfond, G.: A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. Technol. Innov. Manage. Rev. **7**, 35–40 (2017). https://doi.org/10.22215/timreview/1112
14. Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., Weinhardt, C.: Designing microgrid energy markets. Appl. Energy. **210**, 870–880 (2017). https://doi.org/10.1016/j.apenergy.2017.06.054
15. Lee, J.H.: BIDaaS: blockchain based ID as a service. IEEE Access. **6**, 2274–2278 (2017). https://doi.org/10.1109/ACCESS.2017.2782733
16. Kshetri, N.: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecomm. Policy. **41**, 1027–1038 (2017). https://doi.org/10.1016/j.telpol.2017.09.003
17. Li, Z., Wang, W.M., Liu, G., Liu, L., He, J., Huang, G.Q.: Toward open manufacturing. Ind. Manage. Data Syst. **118**, 303–320 (2017). https://doi.org/10.1108/imds-04-2017-0142
18. Roehrs, A., da Costa, C.A., da Rosa Righi, R.: OmniPHR: a distributed architecture model to integrate personal health records. J. Biomed. Inform. **71**, 70–81 (2017). https://doi.org/10.1016/j.jbi.2017.05.012
19. Engelhardt, M.A.: Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol. Innov. Manage. Rev. **7**, 22–34 (2017). https://doi.org/10.22215/timreview/1111
20. Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., Shi, W.: Cecoin: a decentralized PKI mitigating MitM attacks. Futur. Gener. Comput. Syst. (2017). https://doi.org/10.1016/j.future.2017.08.025
21. Ouaddah, A., Mousannif, H., Abou Elkalam, A., Ait Ouahman, A.: Access control in the Internet of Things: big challenges and new opportunities. Comput. Networks. **112**, 237–262 (2017). https://doi.org/10.1016/j.comnet.2016.11.007
22. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018). https://doi.org/10.1016/j.scs.2018.02.014
23. Hussein, A.F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J.M.R.S., de Albuquerque, V.H.C.: A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cogn. Syst. Res. **52**, 1–11 (2018). https://doi.org/10.1016/j.cogsys.2018.05.004
24. Lun, L., Jiqiang, L., Lichen, C., Shuo, Q., Wei, W., Xiangliang, Z.: CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. **19**, 2204–2220 (2018). https://doi.org/10.1109/TITS.2017.2777990
25. Bahri, L., Carminati, B., Ferrari, E.: Decentralized privacy preserving services for online social networks. Online Soc. Networks Media. **6**, 18–25 (2018). https://doi.org/10.1016/j.osnem.2018.02.001
26. He, S., et al.: A social-network-based cryptocurrency wallet-management scheme. IEEE Access. **6**, 7654–7663 (2018)
27. Staffa, M., et al.: An OpenNCP-based solution for secure eHealth data exchange. J. Netw. Comput. Appl. **116**, 65–85 (2018). https://doi.org/10.1016/j.jnca.2018.05.012
28. Liu, W., Lu, Z., Liu, Z., Wang, Q., Qu, G.: A privacy-preserving trust model based on blockchain for VANETs. IEEE Access. **6**, 45655–45664 (2018). https://doi.org/10.1109/access.2018.2864189
29. Sullivan, C.: Digital identity – from emergent legal concept to new reality. Comput. Law Secur. Rev. **34**, 723–731 (2018). https://doi.org/10.1016/j.clsr.2018.05.015
30. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Comput. Networks. **141**, 199–221 (2018). https://doi.org/10.1016/j.comnet.2018.03.012

31. Li, Z., Barenji, A.V., Huang, G.Q.: Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Robot. Comput. Integr. Manuf. **54**, 133–144 (2018). https://doi.org/10.1016/j.rcim.2018.05.011
32. Angrish, A., Craver, B., Hasan, M., Starly, B.: A case study for blockchain in manufacturing: "fabRec": a prototype for peer-to-peer network of manufacturing nodes. Procedia Manuf. **26**, 1180–1192 (2018). https://doi.org/10.1016/j.promfg.2018.07.154
33. Ma, Z., Jiang, M., Gao, H., Wang, Z.: Blockchain for digital rights management. Futur. Gener. Comput. Syst. **89**, 746–764 (2018). https://doi.org/10.1016/j.future.2018.07.029
34. Hallé, S., Khoury, R., Betti, Q., El-Hokayem, A., Falcone, Y.: Decentralized enforcement of document lifecycle constraints. Inf. Syst. **74**, 117–135 (2018). https://doi.org/10.1016/j.is.2017.08.002
35. Khalilov, M.C.K., Levi, A.: A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Commun. Surv. Tutorials. **20**, 2543–2585 (2018). https://doi.org/10.17654/cs017010035
36. Li, J., Wu, J., Chen, L.: Block-secure: blockchain based scheme for secure P2P cloud storage. Inf. Sci. (Ny) **465**, 219–231 (2018). https://doi.org/10.1016/j.ins.2018.06.071
37. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018). https://doi.org/10.1016/j.cose.2018.06.004
38. Kumar, N.M., Mallick, P.K.: Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. **132**, 1815–1823 (2018). https://doi.org/10.1016/j.procs.2018.05.140
39. Minoli, D., Occhiogrosso, B.: Blockchain mechanisms for IoT security. Internet of Things. **1–2**, 1–13 (2018). https://doi.org/10.1016/j.iot.2018.05.002
40. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for internet of things security: a position paper. Digit. Commun. Networks. **4**, 149–160 (2018). https://doi.org/10.1016/j.dcan.2017.10.006
41. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. **30**, 80–86 (2018). https://doi.org/10.1016/j.cosrev.2018.10.002
42. Dunphy, P., Petitcolas, F.A.P.: A first look at identity management schemes on the blockchain. IEEE Secur. Priv. **16**, 20–29 (2018). https://doi.org/10.1109/MSP.2018.3111247
43. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **16**, 267–278 (2018). https://doi.org/10.1016/j.csbj.2018.07.004
44. Gordon, W.J., Catalini, C.: Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. **16**, 224–230 (2018). https://doi.org/10.1016/j.csbj.2018.06.003
45. Brogan, J., Baskaran, I., Ramachandran, N.: Authenticating health activity data using distributed ledger technologies. Comput. Struct. Biotechnol. J. **16**, 257–266 (2018). https://doi.org/10.1016/j.csbj.2018.06.004
46. Zhang, X., et al.: Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun. Mag. **56**, 82–88 (2018). https://doi.org/10.1109/mcom.2018.1700401
47. Kleinaki, A.S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P.S., Kaldoudi, E.: A blockchain-based notarization service for biomedical knowledge retrieval. Comput. Struct. Biotechnol. J. **16**, 288–297 (2018). https://doi.org/10.1016/j.csbj.2018.08.002
48. Brilliantova, V., Thurner, T.W.: Blockchain and the future of energy. Technol. Soc. (2018). https://doi.org/10.1016/j.techsoc.2018.11.001

49. Prasad, S., Shankar, R., Gupta, R., Roy, S.: A TISM modeling of critical success factors of blockchain based cloud services. J. Adv. Manage. Res. **15**, 434–456 (2018). https://doi.org/10.1108/JAMR-03-2018-0027
50. Qian, Y., et al.: Towards decentralized IoT security enhancement: a blockchain approach. Comput. Electr. Eng. **72**, 266–273 (2018). https://doi.org/10.1016/j.compeleceng.2018.08.021
51. Xu, C., Liu, H., Li, P., Wang, P.: A remote attestation security model based on privacy-preserving blockchain for V2X. IEEE Access. **6**, 67809–67818 (2018). https://doi.org/10.1109/ACCESS.2018.2878995
52. Yang, J., Lu, Z., Wu, J.: Smart-toy-edge-computing-oriented data exchange based on blockchain. J. Syst. Archit. **87**, 36–48 (2018). https://doi.org/10.1016/j.sysarc.2018.05.001
53. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/j.future.2018.05.046
54. Badr, S., Gomaa, I., Abd-Elrahman, E.: Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput. Sci. **141**, 159–166 (2018). https://doi.org/10.1016/j.procs.2018.10.162
55. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018). https://doi.org/10.1016/j.future.2017.11.022
56. Zhao, Y., Yu, Y., Li, Y., Han, G., Du, X.: Machine learning based privacy-preserving fair data trading in big data market. Inf. Sci. (Ny) **478**, 449–460 (2019). https://doi.org/10.1016/j.ins.2018.11.028
57. Zhu, L., Wu, Y., Gai, K., Choo, K.K.R.: Controllable and trustworthy blockchain-based cloud data management. Futur. Gener. Comput. Syst. **91**, 527–535 (2019). https://doi.org/10.1016/j.future.2018.09.019
58. Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W.: Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. **125**, 251–279 (2019). https://doi.org/10.1016/j.jnca.2018.10.019
59. Hou, J., Qu, L., Shi, W.: A survey on internet of things security from data perspectives. Comput. Networks. **148**, 295–306 (2019). https://doi.org/10.1016/j.comnet.2018.11.026
60. Zhong, L., Wu, Q., Xie, J., Li, J., Qin, B.: A secure versatile light payment system based on blockchain. Futur. Gener. Comput. Syst. **93**, 327–337 (2019). https://doi.org/10.1016/j.future.2018.10.012
61. Muzammal, M., Qu, Q., Nasrulin, B.: Renovating blockchain with distributed databases: an open source system. Futur. Gener. Comput. Syst. **90**, 105–117 (2019). https://doi.org/10.1016/j.future.2018.07.042
62. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Futur. Gener. Comput. Syst. **94**, 408–418 (2019). https://doi.org/10.1016/j.future.2018.11.046
63. Dorri, A., Kanhere, S.S., Jurdak, R.: MOF-BC: a memory optimized and flexible blockchain for large scale networks. Futur. Gener. Comput. Syst. **92**, 357–373 (2019). https://doi.org/10.1016/j.future.2018.10.002