Blockchain Trust Mechanism in Named Data Networking: A Systematic Literature Review

Athirah Rosli[*]
Faculty of Ocean Engineering Technology and Informatics
Universiti Malaysia Terengganu
Kuala Terengganu, Malaysia
athirah.rosli@umt.edu.my

Suhaidi Hassan
InterNetWorks Research Laboratory
School of Computing
Universiti Utara Malaysia
Sintok, Kedah, Malaysia
suhaidi@uum.edu.my

Mohd Hasbullah Omar
InterNetWorks Research Laboratory
School of Computing
Universiti Utara Malaysia
Sintok, Kedah, Malaysia
mhomar@uum.edu.my

***Abstract*— Blockchain has been reported as one of the technologies that could change the Internet architecture in the future. By offering better mechanism that increases trust in the network, it gives possibilities for the future Internet, Named Data Networking (NDN) to adapt such mechanism. This paper focuses to look into the potential trust mechanisms of Blockchain to be adapted in NDN. Systematic Literature Review (SLR) is used as a technique to dig into current researches to identify research that supports the research question. From the findings, the consensus mechanism has been seen as the potential mechanism that offers trust in Blockchain.**

Keywords—Blockchain, Named Data Networking, trust mechanism, consensus mechanism

I. Introduction

The Blockchain has been known to provide better security and trust throughout the network. The protected database which is called chain will distribute between the users in the network. The distributed ledger has made Blockchain to provide transparent and trusted transaction. Every user in the chain will have the authority to check and validate the block. However, the block is not editable and cannot be tampered without the consensus of another member in the network.

Trust has always been the main concern in network, especially in Named Data Networking (NDN) environment where everything is distributed and there is no central authority that will control the authentication. Thus, Blockchain has been seen as a suitable mechanism to be paired with NDN since both are distributed and Blockchain offers a trust mechanism that can make the network more secure. Trustless in Blockchain mean a system that can be trusted rather than the reputation of a central authority.

This paper presents a review of trust in Blockchain technology by using a systematic literature review (SLR) method. The review focuses on the trust mechanisms in Blockchain and NDN. The aim of SLR is not just to answer and provide evidence to the research question, but also gives guidelines on how the literature searches can be done strategically. This paper is organized as follows. Firstly, this paper describes the steps used in the Systematic Literature Review method. Next, the formulation of the research question takes place and the literature search is done. Inclusion-exclusion criteria is described in the next section. Then, quality assessment of the literature searches is done, and the literature is collected. After that, the data is analyzed in the next section. Lastly, conclusions and suggestion for this paper is presented in the last section.

II. Methods

The review process is a process on how the systematic literature review is done. There are four processes to be taken. The process can be seen in Fig 1.

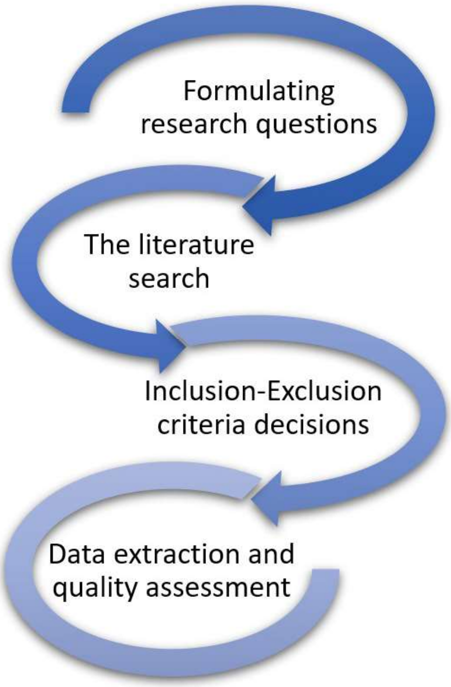

Formulating research questions
The literature search
Inclusion-Exclusion criteria decisions
Data extraction and quality assessment

Fig 1. Review process of the systematic literature review.

The review process starts by formulating the research questions. The research question needs to answer the research objective and reflect the body of knowledge of the research. The next step is the literature search that will be based on the searching process steps. After searching the literature, the literature

[*]The author is currently a doctoral researcher at the InterNetWorks Research Laboratory, School of ComputingUniversiti Utara Malaysia,Sintok, Kedah, Malaysia

A. Research Question

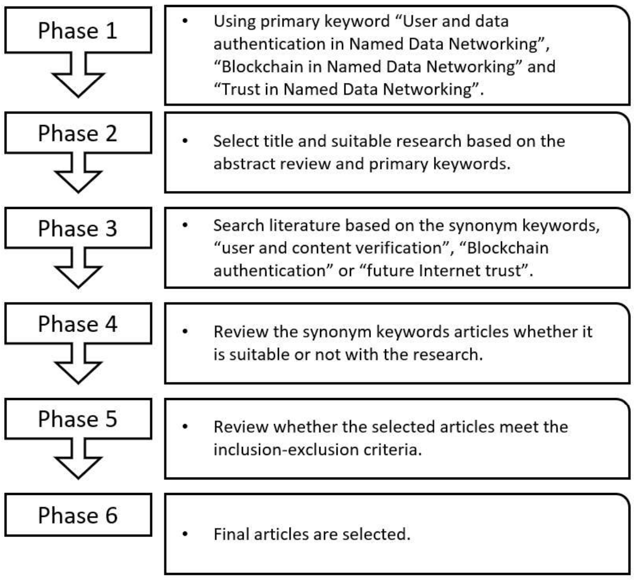
Research questions are built to answer the aim of the objectives of this paper. The objective of this paper is to analyze the trust mechanism in Blockchain technology to be adapted to the Named Data Networking environment. Thus, the research question to this objective is,

What is the potential mechanism in Blockchain that can offer trust in Named Data Networking?

To answer the research question, related articles and publications from 2015 to 2020 were searched. From the searched articles, the keywords, research problem and the objective of the articles are accessed.

B. Search Process

The search process is a process of searching the related articles from journals, proceedings, and published work. Electronic databases like ACM Digital Library, IEEE Xplore Digital Library, SpringerLink and Google Scholar are contributed in this searching process. Fig 2 shows the steps in the searching process.



Phase 1
- Using primary keyword "User and data authentication in Named Data Networking", "Blockchain in Named Data Networking" and "Trust in Named Data Networking".

Phase 2
- Select title and suitable research based on the abstract review and primary keywords.

Phase 3
- Search literature based on the synonym keywords, "user and content verification", "Blockchain authentication" or "future Internet trust".

Phase 4
- Review the synonym keywords articles whether it is suitable or not with the research.

Phase 5
- Review whether the selected articles meet the inclusion-exclusion criteria.

Phase 6
- Final articles are selected.

Fig 2. Searching process step in systematic literature review.

C. Inclusion and Exclusion Criteria

After the searching process has been done, all the searched articles will be filtered by using inclusion-exclusion criteria. This process is done to ensure that the searched articles fulfilled the requirement of the research and suitable in the area of knowledge. Through the results of the filtered articles, the research can acknowledge its key study and deliver a strong solution or suggestion to answer the RQs [1]. The inclusion-exclusion criteria of this research can be seen in Table I and Table II respectively.

D. Quality Assessment

After the articles and publications being finalized, the data will be extracted to avoid any bias in determining papers to be reviewed. Quality assessment of the articles and publications will be done to each of them to get the assessment score. The higher the assessment score, the valid the articles on this research. The quality assessment score is rated by Yes=1, Partly=0.5 and No=0. This score is based on Dyba & Dingsoyr [2], Kitchenham et. al [3] and Shakeel et. al [4]. The checklist of the score can be seen in Table III.

TABLE I. INCLUSION CRITERIA

INCL#	**Inclusion Criteria**
INCL1	Major topic to be searched will focuses on authentication mechanism, user and data authentication, authentication in NDN, trust in the future Internet, trust mechanism.
INCL2	Articles and publications need to have a clear objective, problem and methods.

TABLE II. EXCLUSION CRITERIA

EXCL#	**Exclusion Criteria**
EXCL1	Articles and publications that did not focus on authentication mechanism, user and data authentication, authentication in NDN, trust in the future Internet, trust mechanism.
EXCL2	Survey journal.
EXCL3	Short articles, lecture notes, and not peer-reviewed journals.

TABLE III. ASSESSMENT QUESTIONS AND SCORE FOR QUALITY ASSESSMENT

Num.	**Assessment Questions (QA)**	**Assessment Score**
1	Is the articles or publication is peer-reviewed or refereed?	Yes/No
2	Do the articles or publications clearly state the objectives, problems and the appropriate keywords?	Yes/Partly/No
3	Is there any experiment being done in the research?	Yes/Partly/No
4	Is there any data collected from the experiment?	Yes/Partly/No
5	Is there any data analysis being done with parameters/metrics to evaluate?	Yes/Partly/No

E. Data Collection

Table IV shows lists of related publications on users and data authentication based on the quality assessment score.

TABLE IV. LIST OF PUBLICATIONS BASED ON QUALITY ASSESSMENT SCORE

Num	Publications	QA 1	QA 2	QA 3	QA 4	QA 5	QA Score
1.	[5]	Y	T	T	P	Y	4.5
2.	[6]	Y	Y	P	Y	Y	4.5
3.	[7]	Y	Y	Y	P	Y	4.5
4.	[8]	Y	P	P	Y	Y	4.0
5.	[9]	Y	P	Y	P	P	3.5
6.	[10]	Y	P	P	Y	P	3.5
7.	[11]	Y	P	Y	Y	P	4.0
8.	[12]	Y	Y	Y	Y	Y	5.0
9.	[13]	Y	P	P	Y	Y	4.0
10.	[14]	Y	P	Y	Y	Y	4.5
11.	[15]	Y	Y	Y	P	Y	4.5
12.	[16]	Y	Y	Y	P	Y	4.5
13.	[7]	Y	P	Y	Y	Y	4.5
14.	[17]	Y	P	Y	P	Y	4.0
15.	[18]	Y	Y	P	P	Y	4.0
16.	[19]	Y	P	N	N	N	1.5
17.	[20]	Y	P	N	P	P	2.5
18.	[21]	Y	P	N	P	P	2.5
19.	[22]	Y	P	Y	P	Y	4.0
20.	[23]	Y	Y	P	P	Y	4.0
21.	[18]	Y	Y	N	P	Y	3.5
22.	[16]	Y	Y	Y	Y	Y	5.0
23.	[24]	Y	Y	Y	P	P	4.0

III. DATA ANALYSIS

From Table IV, Conti, Hassan & Lal [12] and Hamdane & Fatmi [24] mark the highest QA scores of 5.0. According to this score, the highest score means the research is closely related to this research and fulfill the requirement needed.

In [12], Conti, Hassan & Lal have suggested an authentication protocol that supports Blockchain technology for mobile distribution called BlockAuth. BlockAuth works as producers' prefix authentication mechanism to guarantee only legitimate routine updates have the permission to advertise. Issues arise in the current authentication mechanism are often related to handoff latency, increasing in packet loss, signaling overhead and cause insecure connection when handling the network forwarding information. These issues can be mitigated by using Blockchain technology that offers security, privacy and access control.

The consensus is one of a promising mechanism offers by Blockchain to ensure trust distribution and transparent transactions to the network. Trust and authentication relate to each other. Authentication has been discussed in many researches and there are many methods that have been introduced by other researchers. However, the authentication types and requirements differ between them. Table V shows the difference authentication requirement between Blockchain and other authentication methods.

Based on Table V, mutual authentication specifies mutual decision from participating members on authenticating members entering the network. Otherwise, it will become one-way authentication if it involves only one party to do the authentication. No additional hardware specifies the authentication process does not need any add on devices to do the authentication process. Examples of authentication that need additional devices to do the authentication process are biometric and token authentication. For the multiple credentials, it presents several levels in authenticating the user or data identity and registration. During those levels, the user or data will need to introduce themselves and keep the

TABLE IV. AUTHENTICATION METHODS AND REQUIREMENTS

	Password authentication [25], [26]	Two-factors authentication [27]–[29]	Token authentication [30]–[32]	Biometric authentication [33], [34]	SSL/TLS [35]–[37]	CAPTCHAs [38], [39]	Single sign-on [40]–[42]	Karberos [43], [44]	Blockchain [45]–[47]
Mutual authentication		/	/		/			/	/
No additional hardware	/				/	/	/	/	/
Multiple credential		/		/	/				/
Registration	/	/	/	/					
Offline phase	/						/	/	
Decentralized									/
User to Machine	/	/	/	/	/	/	/		/
Machine to Machine	/		/						/

record before the authentication process happens. For the offline requirement, it will allow the authentication method to be used without the availability of Internet connectivity.

While decentralized means, there is no central server or third-party involvement needed to do the authentication process. User to machine means the authentication process occurs from the user to the server or central authority.

Meanwhile, machine to machine happen between the servers and the authentication process will not involve any human intervention.

IV. RESULTS

From Table V, it is clearly stated that Blockchain offers more advantages than the other authentication methods.

Blockchain provides a mutual agreement between user to machine and machine to machine. To do the authentication process, there are no additional devices require to in order to accomplish the process and in Blockchain authentication, it involves multiple credentials from the participating parties in the consortium before any changes made to the data. The most essential characteristics of Blockchain is, it is decentralized which is suitable to the NDN environment. This brings advantages to Blockchain as it can solve the single point of failure issues and data tempering issues [48]. Contrary to the existing server-based network, there is no central authority and third-party authentication needed. Thus, the security and the privacy of the network will be enhanced [49].

Blockchain has been a sensational technology considering its security mechanism and trustworthy service, specifically at the time of doing the transaction that being documented through distributed cryptographic protocol [50]. There are four types in Blockchain which are, permissionless Blockchain, permissioned Blockchain, consortium Blockchain, and private Blockchain. Each type of Blockchain works differently according to their accessibility and how the authenticate transaction in the network. The technological advancement of Blockchain offers more chances, particularly in the financial sector, notary services, management, management, insurance, industrial sector, automotive, healthcare, education, government, foster security, and IoT [51].

Trust has been highlighted as the strongest mechanism in Blockchain because of its potential to identify the identity of the producer and consortium members without knowing the identity of them. In research by Kim et al. [52], they highlighted trust between the nodes in Wireless Sensor Network (WSN) that adapt Blockchain as the mechanism to increase trust. Another research by Conti et al. [12] has suggested BlockAuth that act as the authentication mechanism for producer before they produce any content. Thus, in this paper, it shows that Blockchain offers a trust mechanism to the NDN network through its consensus mechanism. Several researchers also have been adapted consensus as their authentication mechanism to increase trust and security in their network.

V. CONCLUSIONS

As a promising technology that offers valid transaction agreement of transaction, Blockchain consensus also imposes trust as one of its advantages [53]. Up until now, a numerous consensus mechanism has been introduced by the researcher. Some of them are, Proof-of-Work (PoW), Proof-of-Stake (PoW), Proof-of-Authority (PoA) and Proof-of-Trust (PoT). Through this consensus mechanism, trust can be built in the trustless environment by trusting the structure of the network. Thus, in the environment of NDN, the trust will be achieved by authentication of the publisher with is an unknown entity that publishes the content and later will be kept in the cache. It is answering the research question that being asked in Section A which is a consensus mechanism in Blockchain is the potential mechanism that offers trust in the NDN network.

This paper believes that Blockchain technology is suitable to be adapted to NDN network. Through the consensus mechanism in Blockchain, it will increase the trust level in NDN especially to the producer and the content in the cache. Thus, this can avoid any consequences and attacks such as content poisoning and cache pollution attack in the NDN network. In the future, we will investigate other mechanisms of Blockchain that can be adapted in the NDN network.

REFERENCES

[1] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, no. 2004, pp. 1–26, 2004.

[2] T. Dybå and T. Dingsøyr, "Empirical studies of agile software development: A systematic review," *Inf. Softw. Technol.*, vol. 50, no. 9–10, pp. 833–859, 2008.

[3] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[4] Y. Shakeel, J. Krüger, I. Von Nostitz-Wallwitz, G. Saake, and T. Leich, "Automated Selection and Quality Assessment of Primary Studies: A Systematic Literature Review," *J. Data Inf. Qual.*, vol. 12, no. 1, pp. 1–26, 2019.

[5] D. Kim, S. Nam, J. Bi, and I. Yeom, "Efficient content verification in named data networking," in *Proceedings of the 2nd International Conference on Information-Centric Networking*, 2015, pp. 109–116.

[6] Y. Wang, Z. Qi, K. Lei, B. Liu, and C. Tian, "Preventing bad content dispersal in named data networking," in *Proceedings of the ACM Turing 50th Celebration Conference-China*, 2017, p. 37.

[7] T. Refaei, M. Horvath, M. Schumaker, and C. Hager, "Data authentication for NDN using hash chains," in *IEEE Symposium on Computers and Communication (ISCC), 2015*, 2015, pp. 982–987.

[8] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surv. tutorials*, vol. 20, no. 1, pp. 566–600, 2017.

[9] M. Raykova, H. Lakhani, H. Kazmi, and A. Gehani, "Decentralized authorization and privacy-enhanced routing for information-centric networks," in *Proceedings of the 31st Annual Computer Security Applications Conference*, 2015, pp. 31–40.

[10] Y. Yu, A. Afanasyev, D. Clark, K. Claffy, V. Jacobson, and L. Zhang, "Schematizing Trust in Named Data Networking," in *Proceedings of the 2nd International Conference on Information-Centric Networking - ICN 2015*, 2015, pp. 177–186.

[11] R. Li, H. Asaeda, J. Li, and X. Fu, "A verifiable and flexible data sharing mechanism for information-centric IoT," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–7.

[12] M. Conti, M. Hassan, and C. Lal, "BlockAuth: BlockChain based distributed producer authentication in ICN," *Comput. Networks*,

vol. 164, p. 106888, 2019.

[13] X. Wang and S. Cai, “An efficient named data networking based IoT cloud framework,” *IEEE Internet Things J.*, 2020.

[14] M. Wazid, A. K. Das, V. Bhat, and A. V Vasilakos, “LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment,” *J. Netw. Comput. Appl.*, vol. 150, p. 102496, 2020.

[15] S. K. Ramani, R. Tourani, G. Torres, S. Misra, and A. Afanasyev, “NDN-ABS: Attribute-Based Signature Scheme for Named Data Networking,” in *Proceedings of the 6th ACM Conference on Information-Centric Networking*, 2019, pp. 123–133.

[16] H. Nakano, H. Kato, S. Haruta, M. Yoshida, and I. Sasase, “Trust-based Verification Attack Prevention Scheme using Tendency of Contents Request on NDN,” in *2019 25th Asia-Pacific Conference on Communications (APCC)*, 2019, pp. 159–164.

[17] R. Li, H. Asaeda, and J. Wu, “DCAuth: Data-centric authentication for secure in-network big-data retrieval,” *IEEE Trans. Netw. Sci. Eng.*, 2018.

[18] J. Lou, Q. Zhang, Z. Qi, and K. Lei, “A blockchain-based key management scheme for named data networking,” in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018, pp. 141–146.

[19] T. Song, B. Cui, R. Li, J. Liu, and J. Shi, “Smart Contract-Based Trusted Content Retrieval Mechanism for NDN,” *IEEE Access*, vol. 8, pp. 85813–85825, 2020.

[20] Z. Zhang *et al.*, “An overview of security support in named data networking,” *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 62–68, 2018.

[21] Y. Yu, Y. Li, X. Du, R. Chen, and B. Yang, “Content protection in named data networking: Challenges and potential solutions,” *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 82–87, 2018.

[22] Y. Yu, A. Afanasyev, J. Seedorf, Z. Zhang, and L. Zhang, “NDN DeLorean: An authentication system for data archives in named data networking,” in *Proceedings of the 4th ACM Conference on Information-Centric Networking*, 2017, pp. 11–21.

[23] L. Wang *et al.*, “Naxos: A Named Data Networking Consensus Protocol,” in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, pp. 986–991.

[24] B. Hamdane and S. G. E. Fatmi, “A credential and encryption based access control solution for named data networking,” in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015, pp. 1234–1237.

[25] T. Mick, R. Tourani, and S. Misra, “LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities,” *IEEE Internet Things J.*, 2017.

[26] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, “A password authentication scheme over insecure networks,” *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, 2006.

[27] Y. Lu, L. Li, H. Peng, and Y. Yang, “Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment,” *Secur. Commun. Networks*, vol. 9, no. 11, pp. 1331–1339, 2016.

[28] M. Qi and J. Chen, “An efficient two-party authentication key exchange protocol for mobile environment,” *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3341, 2017.

[29] P. Gope and B. Sikdar, “Lightweight and privacy-preserving two-factor authentication scheme for IoT devices,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, 2018.

[30] H. Polat and S. Oyucu, “Token-based authentication method for M2M platforms,” *Turkish J. Electr. Eng. Comput. Sci.*, vol. 25, no. 4, pp. 2956–2967, 2017.

[31] P. K. Rayani, B. Bhushan, and V. R. Thakare, “Multi-Layer Token Based Authentication Through Honey Password in Fog Computing,” *Int. J. Fog Comput.*, vol. 1, no. 1, pp. 50–62, 2018.

[32] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, “Token-based lightweight authentication to secure IoT networks,” in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019, pp. 1–4.

[33] Z. Rui and Z. Yan, “A survey on biometric authentication: Toward secure and privacy-preserving identification,” *IEEE Access*, vol. 7, pp. 5994–6009, 2018.

[34] G. L. Masala, P. Ruiu, and E. Grosso, “Biometric authentication and data security in cloud computing,” in *Computer and Network Security Essentials*, Springer, 2018, pp. 337–353.

[35] A. N. El-Kassar, R. Haraty, and H. Otrok, “Improving the Secure Socket Layer Protocol by modifying its Authentication function,” 2017.

[36] S. Shakya, “An efficient security framework for data migration in a cloud computing environment,” *J. Artif. Intell.*, vol. 1, no. 01, pp. 45–53, 2019.

[37] H. Otrok, R. Haraty, and A. N. El-Kassar, “Improving the secure socket layer protocol by modifying its authentication function,” in *2006 World Automation Congress*, 2006, pp. 1–6.

[38] B. Souley and H. Abubakar, “A captcha–based intrusion detection model,” *Int. J. Softw. Eng. Appl.*, vol. 9, no. 1, pp. 29–40, 2018.

[39] G. Ye *et al.*, “Yet another text captcha solver: A generative adversarial network based approach,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 332–348.

[40] Y. Zhang, C. Xu, H. Li, K. Yang, N. Cheng, and X. S. Shen, “PROTECT: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage,” *IEEE Trans. Mob. Comput.*, 2020.

[41] Y. Atwady and M. Hammoudeh, “A survey on authentication techniques for the internet of things,” in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.

[42] T. Bazaz and A. Khalique, “A review on single sign on enabling technologies and protocols,” *Int. J. Comput. Appl.*, vol. 151, no. 11, pp. 18–25, 2016.

[43] Z. Tbatou, A. Asimi, Y. Asimi, Y. Sadqi, and A. Guezzaz, “A New Mutuel Kerberos Authentication Protocol for Distributed Systems.,” *IJ Netw. Secur.*, vol. 19, no. 6, pp. 889–898, 2017.

[44] G. Yuan, L. Guo, and G. Wang, “Security Analysis and Improvement on Kerberos Authentication Protocol,” in *International Conference on Big Data and Security*, 2019, pp. 199–210.

[45] I. Bashir, *Mastering Blockchain*. Packt Publishing Ltd, 2017.

[46] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” 2008.

[47] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A decentralized blockchain-based authentication system for IoT,” *Comput. Secur.*, vol. 78, pp. 126–142, 2018.

[48] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digit. Commun. Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[49] N. Z. Benisi, M. Aminian, and B. Javadi, “Blockchain-based decentralized storage networks: A survey,” *J. Netw. Comput. Appl.*, p. 102656, 2020.

[50] C. Cachin and M. Vukolić, “Blockchains Consensus Protocols in the Wild,” *arXiv Prepr. arXiv1707.01873*, 2017.

[51] V. Gatteschi, F. Lamberti, and C. Demartini, “Blockchain Technology Use Cases,” in *Advanced Applications of Blockchain Technology*, Springer, 2020, pp. 91–114.

[52] T.-H. Kim *et al.*, “A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks,” *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[53] G.-T. Nguyen and K. Kim, “A Survey about Consensus Algorithms Used in Blockchain.,” *J. Inf. Process. Syst.*, vol. 14, no. 1, 2018.