Conceptualization of A GDPR-Mining Blockchain-Based Auditor: A Systematic Review

Gholamhossein Kazemi
Department of Business, Marketing and Law
University of South-Eastern Norway
Hønefoss, Norway
Email: 238834@usn.no

Shegaw Anagaw Mengiste
Department of Business, History and Social Sciences
University of South-Eastern Norway
Vestfold, Norway
Email: Shegaw.mengiste@usn.no

***Abstract*—This paper is a systematic literature review of the compliance of blockchain with the General Data Protection Regulation act. Although there are contradictory opinions about the compliance of blockchain with General Data Protection Regulation amongst different researchers, in this paper, we conduct a systematic literature review on the topic to get a perspective on previous studies and models to build a conceptual blockchain-based General Data Protection Regulation-mining two-way monetized auditor design upon existing solutions and models for an interactive software auditing the transactions between the data subjects and third parties. This review aims to answer the dilemma of the applicability of blockchain in auditing the transactions between the data subjects and data processors in the General Data Protection Regulation framework. Moreover, this paper discusses the implications and limitations and paves the path for future studies to elaborate on the concept.**

Keywords-blockchain; GDPR; consensus; auditor.

I. INTRODUCTION

Since the emergence of Bitcoin in 2009, based on Blockchain technology, a vast group of academic, industrial, and business innovators have become more and more attracted to using blockchain technology for their purposes such as researches, literature reviews, secure contracts, information sharing, and digital transactions due to its immutable, transparent, secure, and trustworthy characteristics [1][2].

Accordingly, blockchain could be the best solution for privacy protection and data processing transparency regarding its compatibility with the General Data Protection Regulation (GDPR) act that is effective since May 25th 2018 across Europe; however, there are contradictory opinions around its compatibility among scholars [3][4][5]. Numerous pieces of literature introduced the disruptive capabilities of blockchain as the most important revolutionizing invention after the Internet itself, considering its distributed consensus model [6].

A systematic review of more than 260 scholarly articles about blockchain applications from 2014 to the first quarter of 2018 illustrates that only 24 had focused on the privacy and security area, with more than 1000 percent growth in the second half [7]. Hence, regarding the exponential soar in this field, and considering the launch of GDPR in the second quarter of 2018, this study scrutinizes the contrasting notions about the trending less-investigated concept of blockchain-GDPR harmony and develops a conceptual model for an interactive software auditing the interactions between the data subjects and third-party data processors under the supervision of GDPR issuing-parties based on the previous scholarly designs [5]. Hence, the research question is whether a blockchain-based platform is capable of auditing the transactions between the data subjects and third-party data processors in the framework of GDPR or not?

In this regard, this paper analyzes 49 articles and proceedings from 2016 to 2020 to pinpoint the applications and challenges of blockchain and GDPR compatibility of blockchain technologies. This review consists of two main time periods, before the launch of GDPR and after the launch of GDPR, and classifies the applications of GDPR in the mentioned periods to identify the gap for the inception of a blockchain-based GDPR auditing moderator, also at the same time, underpins the issues of implementation of such an application. Moreover, this paper discusses the implications and limitations and paves the path for future studies to elaborate on the concept. This paper contains five parts including introduction as Section I, literature review as Section II covering subtitles of review process, constructs, applications, and compliance, results as Section III, discussion as Section IV, and conclusion as Section V.

II. LITERATURE REVIEW

This study seeks the answer to the dilemma of applicability of blockchain in auditing the transactions between the data subjects and data processors in the GDPR framework that is provided by the EU and imposes strong obligations regarding security and privacy to all of the organizations around the world that collect or process any data related to the people in the EU [3].

Moreover, the findings of this study are related to the context of GDPR articles, and the level of analysis is the applications of blockchain technology, which are highly dependent on its components, mechanisms, and consensuses [8]. Consequently, the low diversity of the mechanisms of blockchain and the translation of the GDPR articles into logical machine algorithms are the limitations of this conceptual model that need further development in future

 ISBN: 978-1-61208-843-3

studies. Finally, the outcome of this study serves the interests of data subjects, third-party data processors, and the auditing organization for the GDPR acts. All the steps of this systematic review are explained in the following sections and depicted in Figure 1.

A. Review Process

To attain a holistic approach towards the proposed model, a preliminary search from 2016 to 2020 with the keywords "Blockchain Applications", "Blockchain Issues", "Blockchain Security", "Blockchain Privacy", and "Blockchain and GDPR" was conducted through Web of Science, Scimago Journal and Country Rank, and Google Scholar to help define the concepts, categorize the applications of blockchain, and assess its compatibility with GDPR. As a preliminary result, 89 articles and proceedings were selected for further investigations while after filtration on source journals and proceedings reliability, H5 index rate, citations rate, abstract and keywords relevancy, and result and conclusion validity and novelty, 40 articles and proceedings were found ineligible and 49 articles and proceedings were selected for the second round of filtration, as illustrated in Table I. Filtered articles and proceedings either have a high citation, a high H5 index from the publisher journal or proceeding, or a valuable content due to its novelty of publishing date. The initial inclusion and exclusion criteria of this systematic review are, respectively, the publication year of the study being between 2016 to 2020, the credibility of the study assessed by the citation rate of the study and H5 index rate of the publisher, the relevancy of the study evaluated by scanning the keywords and abstracts, and the novelty of the results and conclusions. Regarding this criteria, the selected articles and proceedings were assigned into the subcategories of either supportive or key articles and proceedings, resulting in 21 supportive and 28 key articles and proceedings.

TABLE I. DISPERSAL OF THE FOUNDED ARTICLES BY YEAR, H5 INDEX, CITATION, AND KEYWORDS

Year	No of Articles and Proceedings	Min-Max H5 Index	Min-Max Citation	Keywords
2016	5	0-300	118-1098	Applications, Crypto, Issues, Technology
2017	6	0-231	1-518	Applications, Concepts, Consensuses, Crypto, Issues, Privacy Smart Contracts
2018	10	0-231	0-1159	Applications Concept, Consensuses, Crypto, GDPR, Issues, Privacy, Security, Smart Contract
2019	19	0-169	1-339	Applications, Consensuses, Crypto, GDPR, Issues, Privacy Security, Smart Contract
2020	9	0-125	0-545	Applications, Consensuses, Crypto, GDPR, Issues, Privacy, Security, Smart Contract
Overall	49	0-300	0-1159	

The second round of filtration consists of the classification of the 28 key articles and proceedings based on whether they contain information concerning the definition of constructs, the applications of blockchain, or the compatibility of the blockchain and GDPR, resulting in 7 key articles and proceedings concerning constructs, 17 applications, and 4 compatibility aspects. Finally, a three-step literature review reveals the definitions of the constructs, classifies the applications of blockchain, and demonstrates the compatibility of blockchain and GDPR. In each step, the minimum quantitative obligations are a minimum average citation of 150 or a minimum average H5 index of 65, and the minimum qualitative requirement is the verification of a supportive supervisory team including researchers with relevant research experience.

B. Constructs

In the first step of this systematic literature review, this paper derives the definitions of the foundational concepts and mechanisms embedded in blockchain technology and GDPR by reviewing 7 key articles and proceedings from 2016 to 2020 to integrate the notions about the basis of the concepts. These articles and proceedings have an average citation of 150 and an average H5 index of 65 with a citation range of 1 to 518 and an H5 index rate of 19 to 112.

GDPR is one of the largest and most difficult regulations in data privacy history issued by the European Union (EU) party across Europe with data subjects' consent centricity. This regulation applies to all the data processors worldwide offering personal data-related goods and services to the citizens of the EU and the data processors located in the EU providing services for the rest of the world. Besides, the data subject's consent should be withdrawable, the data should be removable, and the processing purpose of the third parties should be clear and accessible to the data subjects [9]. Moreover, one of the applications of the GDPR is the compensation of the data subjects suffering from data privacy violations. This reimbursement takes place by fining the data processors breaking the rules of GDPR, although this is only one-way monetized [3].

Blockchain technology is a synthesis of techniques of cryptography, algorithms, distributed consensuses, immutable databases, and distributed peer to peer networks that propagate blocks containing Hash as the modification notifier and function propagator, Timestamp as the time recorder of the transactions, and data subblocks containing specific programmed data [4][8].

Consensus algorithm enables the establishment of a mutual trust between the users of a blockchain network without any need for an administrative party to verify the transaction between them. In other words, the "consensus function is a mechanism that makes all blockchain nodes have

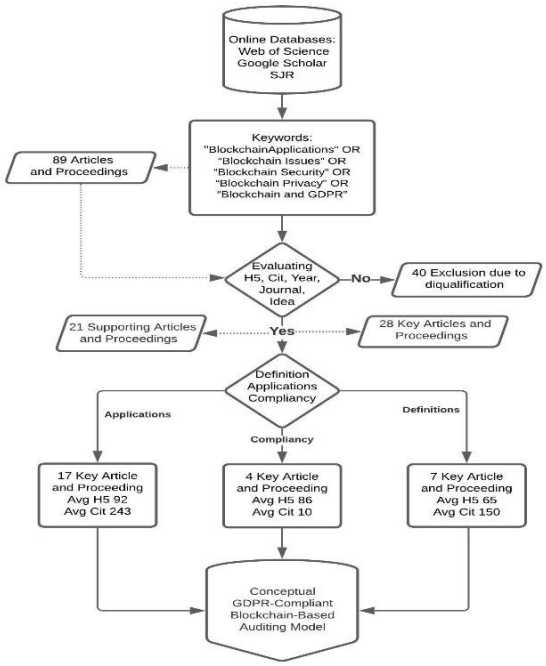

Figure 1. Systematic Review Process.

an agreement in the same message" [10].

Some consensus algorithms are like Proof of Work (PoW) that requires solving a complicated computational process to ensure authentication and verifiability to mine a block of transactions in a blockchain [7][11], Proof of Stake (PoS), which validates the users that present their holdings to generate the next block while another version of PoS is called Delegated Proof of Stake (DPoS), which aims at completing a distributed consensus in the system [7][11], and Zero-Knowledge Proof (ZKP) that in private transactions makes the verifier believe that the target information exists in the transaction, although it does not reveal the real information [11].

Smart contract is an agreement between doubtful members, implemented by the consensus mechanisms in which trusted transactions received by the blockchain can call the contract's public methods to use its data for processing [12].

C. Applications of Blockchain

In the second step, this review divides the target period of the investigation into the before and after the launch of GDPR, which is 2016 to the first quarter of 2018, and the second quarter of 2018 to 2020, and scrutinizes the applications of blockchain in scholarly articles and provides a classification for the covered fields. The classification and dispersal of the applications of blockchain are shown in Table II. This table shows the number of articles and proceedings in each period and the applications that each has mentioned.

In this step, 6 articles from the first period with an average citation of 462 and an average H5 index of 87 were scanned that had a citation range of 11 to 1098 and an H5 index range

TABLE II. APPLICATIONS OF BLOCKCHAIN DISPERSAL AND CLASSIFICATION BY H5 INDEX, CITATION, AND YEAR

Period	No of Articles and Proceedings	Applications	H5 Index	Citation	Year
2016 to 1st quarter of 2018	6	Healthcare, Privacy and Security, Finance, Database, IoT, Other	31	11	2018
		Finance, Privacy and Security, IoT, Health care, Other	35	518	2017
		Healthcare, IoT, Finance, Privacy and Security, Other	19	97	2018
		Finance, Other	231	360	2017
		Finance, Privacy and Security, Other	203	688	2016
		Privacy and Security, Finance, IoT, Other	0	1098	2016
Average			87	462	
2nd quarter of 2018 to 2020	11	Privacy and Security, Database, Healthcare, Other	148	26	2019
		Healthcare, Finance, Privacy and Security, Other	169	95	2019
		Finance, Privacy and Security, Healthcare, Database, IoT	56	395	2019
		Healthcare, IoT, Other	67	13	2020
		Finance, Privacy and Security, Other	24	68	2018
		Other	125	46	2019
		Finance, Healthcare, Privacy and Security, Other	35	0	2020
		Finance, Privacy and Security, Other	174	377	2019
		Database, Other	86	201	2019
		Finance, Database, Privacy and Security, Other	99	128	2019
		Health care, Finance, IoT, Privacy and Security, Other	67	13	2019
Average			95	124	
Overall			92	243	

of 0 to 231, also 11 articles from the second period with an average citation of 124 and an average H5 index of 95 were scanned that had a citation range of 24 to 174 and H5 index range of 0 to 395. The mentioned table classifies the applications of blockchain into Healthcare, Finance, Database, Privacy and Security, Internet of Things (IoT), and others, and illustrates that in these 5 years 17 key articles have mentioned these applications 62 times, although none has mentioned a blockchain-based application for the audition of the transactions between the data subjects and third parties in the framework of GDPR, even after the launch of GDPR.

On the other hand, some articles have discussed the compliance of other blockchain-based applications with the GDPR act that will be investigated in the next section.

D. Compliance of Blockchain With GDPR

In the third step, this review investigates the compliance of the concept of blockchain with the GDPR act. To achieve the result, the contradictory notions are extracted from 4 key scholarly articles and proceedings with an average citation of 10 ranging from 1 to 28 and an average H5 index of 86 ranging from 77 to 112. The dispersal of GDPR inconsistencies of blockchain and their solutions are illustrated in Table III by classification of issues, solutions, H5 index, citation, and year.

On one hand, data immutability in blockchain technology is in contrast with the GDPR act that entitles the users to delete their data, on the other hand, one solution to tackle the crisis of data immutability in the blockchain is using techniques like Accenture that lets a trusted party alter the data block, Monero that makes the data subjects untraceable, and Hyperledger that transforms blockchain to a code executable distributed computer [13]. Moreover, a Hyperledger Fabric permissioned blockchain can use smart contracts to detect trusted parties, an off-chain storage method to reduce data leakage, and eXtensible Access Control Markup Language to impose governance measures to tackle the inconsistency of blockchain and GDPR in a blockchain-based personal data management application [4].

Another prototype overcoming compliance issues is the German Asylum case that uses the layered architecture of information access and storage, private blockchain, and data depersonalization methods to harmonize the ongoing procedures with the GDPR [14].

In another example, Personal Data And Identity Management blockchain-based application, with a human-centric approach, designs layered blockchains with smart contracts, permissioned access, digital identity verification, and off-chain storage for consent and identity management and data monetization [9].

TABLE III. DISPERSAL AND CLASSIFICATION OF BLOCKCHAIN INCONSISTENCIES WITH GDPR AND THEIR SOLUTIONS BY H5 INDEX, CITATION, AND YEAR

No of Articles and Proceedings	GDPR Inconsistency	Solution	H5 Index	Citation	Year
4	Data Erasure, Privacy	Smart Contract, Monero, Accenture Altering Technique, Hyperledger, Etherium	77	7	2019
	Data Erasure, Privacy, Data Governance	Smart Contract, Hyperledger, Etherium, Off-Chain Storage, XACML, SecKit	112	1	2019
	Data Erasure, Privacy	Layered Architecture, Off-Chain Storage, Private Blockchain, Data Depersonalization	77	2	2020
	Data Erasure, Privacy, Data Governance	Layered Blockchain, Smart Contract, Digital Verification, Off-Chain Storage	77	28	2019
Average			86	10	

III. RESULTS

This literature review reveals that although there has been a remarkable increase in the number of scholarly articles exploring the applications of blockchain in the privacy and security area before and after the lunch of GDPR, there is still a gap in unfolding high potential capabilities of blockchain as a GDPR-compatible technology, which is capable of providing the basis for the audition of the transactions between the data subjects and data processors. As disclosed previously, 17 articles and proceedings have mentioned the applications of blockchain 62 times from 2016 to 2020 while only 4 articles and proceedings have investigated its applications in GDPR-related topics like human-centric data management services or one-way monetized personal data management services [4][9][13]. Furthermore, none has indicated blockchain's capability as a basis for a two-way monetized GDPR-mining auditing platform.

After extraction of the concepts and constructs of GDPR and blockchain from the literature, classification of the explored applications of blockchain, and investigation of technical compatibility of GDPR and blockchain, this study explicates that there might be illusive inconsistencies in the definitions of GDPR and blockchain at a superficial level; however, at a technical level techniques and technologies like Smart Contracts, Monero, Accenture, Hyperledger, Off-Chain Storage, etc. reinforce the unseen bonds between the interrelated motifs of GDPR and blockchain [4][14].

Consequently, after clarification of the compatibility of GDPR and blockchain regarding the research's question, and after exploration of the previously proposed solutions and models, this study aims to fill the gap with a conceptual two-way monetized GDPR-mining blockchain-based auditing platform to fulfill the necessity of an effective transaction auditor platform as a supervisory authority, which is capable of fining data privacy violators and rewarding trader data subjects.

 ISBN: 978-1-61208-843-3

IV. DISCUSSION

After three rounds of systematic literature review and analysis containing definition extraction, application gap detection, and blockchain-GDPR compatibility assessment, this study develops a conceptual model based on the previous prominent GDPR-compliant blockchain-based data management applications and builds up the GDPR article mining concept and two-way monetizing contracts upon previous models.

Previous models introduced in the reviewed papers were designed to enhance the security and privacy of managing personal data in the framework of GDPR with the help of blockchain technology, also one-way monetization is mentioned in one of the previously designed models [4][5][9].

Although significant efforts have been made at a technical level for the management of personal data, there is still a need for an auditing platform capable of two-way monetized audition accompanied by the feature of the GDPR-mining concept. Therefore, this study aims to build upon previous models and conceptualize a two-way monetized auditing platform in which data processors can mine the GDPR acts as nodes in the blockchain. In this conceptual three-layered blockchain-based model, an issuing party acts as a supervisory authority that stores, audits, and monetizes the transactions between the data subjects and the third parties based on smart contracts. Figure 2 illustrates the model.

This model consists of a public blockchain for the registration and credit evaluation of the third parties that permits all the data processors to register as a verified member on the blockchain and to interact with the data subjects in order to build up an agreement with them in the framework of a smart contract for the monetization of their relation regarding data processing and data trading [5][9]. This blockchain evaluates the data processors based on PoW consensus after completion of each cycle of transaction that goes through the three-layered blockchain and comes back with the result of the process. Data processors can mine the GDPR nodes and earn value and credit as long as they prove more and more nonconflicting results with the GDPR nodes [7][11].

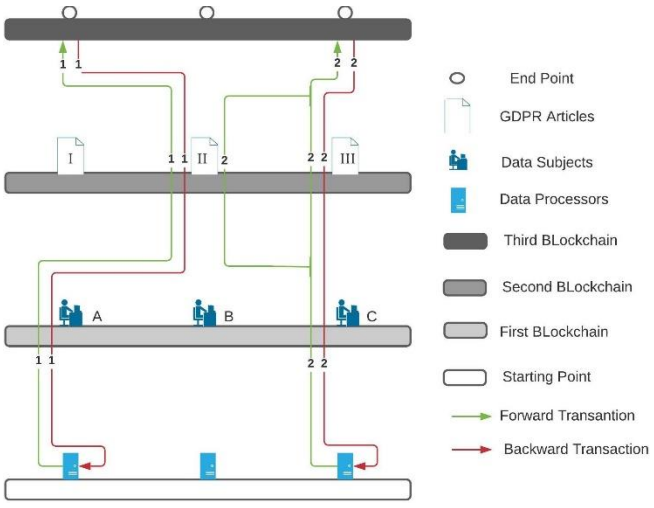

Figure 2. Conceptual model of the three-layered blockchain-based auditor.

Also, a private blockchain of data subjects and their customized governance policies for communication with the third parties is an intermediate layer that stores all the information of the data subjects in blocks of data using consensus algorithms and techniques of data propagation and data alteration in order to empower the data subjects to chose how they want to share their blocks of data and when they want to share or withdraw their blocks of data [4][7][10][11][13]. In this blockchain, smart contracts clarify the agreement of monetization and data accessibility. In this regard, data processors send their request of fetching data with the transparently defined act of GDPR, which is needed to be taken into account, in the form of a PoS or DPoS consensuses. As long as data processors share their act, they can fetch information and mine GDPR nodes to elevate their credits [7][11]. Also, the ZKP consensus ensures the availability of information on the data subject side and the availability of funds on the data processor side for further monetization in the form of data trading or violation fining [11]. Monetization is based on the inputs of involved parties in the agreement of the smart contract.

The third layer is a consortium blockchain of machine-translated GDPR article nodes in which each node presents one specific article of GDPR and its requirements and relations. Requirements obligate the data processors to process the data in the framework of GDPR, and the relations present the possible connection of the different acts of GDPR as nodes in the blockchain. Each time a data processor reaches the information of a data subject through a smart contract, the transaction of fetching and processing of information goes through the GDPR layer for further evaluation and audition of the process. Moreover, a backward transaction containing processed information of the data subject comes back through the GDPR layer and notifies the data subjects about the way their information is being used. This backward transaction helps the evaluation of the third parties in an assessment cycle while the third parties can either enhance their credit as they mine more and more GDPR articles nodes or lose credit due to GDPR violations.

Finally, all the transactions and information are stored on an off-chain server of the auditing issuing party that enables the issuing party to trace the footprints and audit the transactions based on the agreements between the involved parties to either reward the data subjects for selling the data or fine the third parties in case of GDPR-conflicting transactions [4][9]. For instance, as illustrated in Figure 2, at the starting point, data processor number 1 registers on the first blockchain via transaction 1 and requests the establishment of a smart contract with data subject A. After initiation of the monetization agreement and clarification of the act, it fetches the demanded data from the second blockchain and mines the related GDPR act number II. Eventually, after the process of the data at the end point, a backward transaction containing the processed data travels back to the start point, where a supervisory authority stores all the information of the transaction on the off-chain storage and audits the transaction based on the smart contracts in order to validate the GDPR-

 ISBN: 978-1-61208-843-3

act mining of the data processor and monetize the transaction. Similarly, data processor number 2 goes through the same procedure via transaction 2, however it mines two GDPR acts due to the relevancy of its purpose to those acts.

This is an early-stage conceptual design and needs further development due to its technical and practical limitations like the translation of GDPR acts into machine algorithms adjustable in the framework of blockchain, unavailability of customized blockchain mechanisms, and possible refusal of the involved parties for the implementation of such a platform.

V. Conclusion and Future Work

To recapitulate, in three-rounds of systematic analysis, this paper extracts the proper definitions for the understanding of the concepts of blockchain and GDPR, classifies the applications of blockchain, and demonstrates that neither before nor after the launch of GDPR no scholarly article has mentioned the application of blockchain in auditing and monetizing the transactions between the third parties and data subjects. However, after the launch of GDPR, some scholars have investigated the inconsistency of blockchain-based applications with GDPR acts and proposed designed solutions.

Finally, this study builds upon those designs and proposes an interactive conceptual GDPR-mining blockchain-based auditing model capable of GDPR node mining and two-may monetizing. This is an initial conceptual design and further investigation regarding practicality of the model needs to be done, and developments need to be made in the future.

Acknowledgment

This work would not have been possible without the help of the faculty members of the University of South-Eastern Norway. Hence, I would like to thank them all.

References

[1] D. Dasgupta, J. M. Shrein, and K. D. Gupta, “A survey of blockchain from security perspective,” Journal of Banking and Financial Technology, no. 3, pp. 1-17, 2019, doi:10.1007/s42786-018-00002-6.

[2] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, no. 107, pp. 841-853, 2020, doi:10.1016/j.future.2017.08.020.

[3] B. Wolford. GDPR.EU: What is GDPR, the EU’s new data protection law?. [Online]. [Retrieved: March, 2021] Available from: https://gdpr.eu/what-is-gdpr/

[4] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, “GDPR-compliant personal data management: a blockchain-based solution,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1746-1761, 2019, doi:10.1109/TIFS.2019.2948287.

[5] C. Wirth and M. Kolain, “Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data,” Reports of The European Society for Socially Embedded Technologies (EUSSET), vol. 6, no. 2, 2018, doi:10.18420/blockchain2018_03.

[6] M. Crosby, Nachiappen, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: beyond Bitcoin,” Applied Innovation Review, no. 2, 2016. [Online]. [Retrieved: March, 2021] https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

[7] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: current status, classification, and open issues,” Telematics and Informatics, no. 36, pp. 55-81, 2019, doi:10.1016/j.tele.2018.11.006.

[8] A. P. Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” Mathematical Foundations of Computing, vol. 2. no 1, pp. 121-147, 2018, doi:10.3934/mfc.2018007.

[9] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, “BPDIMS: a blockchain-based personal data and identity management system,” The 52nd Hawaii International Conference On System Sciences (HICSS 2019), Hawaii, 2019, pp. 6855-6864, ISBN: 978-0-9981331-2-6. [Retrieved: March, 2021] http://128.171.57.22/bitstream/10125/60121/0681.pdf

[10] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” International Journal of Network Security, vol. 19, no. 5, pp. 653-659, 2017, doi:10.6633%2fIJNS.201709.19(5).01.

[11] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, “Bitcoin and blockchain: security and privacy,” IEEE INTERNET OF THINGS JOURNAL, vol. 7, no. 10, pp. 10288-10313, 2020, doi:10.1109/JIOT.2020.3004273.

[12] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, “Security of cryptocurrencies in blockchain technology: state-of-art, challenges, and future prospects,” Journal of Network and Computer Applications, vol. 163, 2020, doi:10.1016/j.jnca.2020.102635.

[13] S. Farshid, A. Reitz, and P. Robbach, “Design of a forgetting blockchain: a possible way to accomplish GDPR compatibility,” The 52nd Hawaii International Conference On System Sciences (HICSS 2019), Hawaii, 2019, pp. 7087-7095, ISBN: 978-0-9981331-2-6. [Retrieved: March, 2021] http://128.171.57.22/bitstream/10125/60145/0705.pdf

[14] F. Goggenmos, A. Wenninger, A. Rieger, G. Fridgen, and J. Lockl, “How to design a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German Asylum procedure,” The 53rd Hawaii International Conference On System Sciences (HICSS 2020), Hawaii, 2020, pp. 4023-4032, ISBN: 978-0-9981331-3-3. [Retrieved: March, 2021] http://128.171.57.22/bitstream/10125/64234/0397.pdf

[15] R. Stephen, and A. Alex, “A review on blockchain security,” The International Conference on Recent Advancement and Effectual Researches in Engineering Science and Technology (RAEREST 2018), Kerala State, India, 2018, doi:10.1088/1757-899X/396/1/012030.

[16] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu “A survey of blockchain technology applied to smart cities: research issues and challenges,” IEEE Communications Surveys and Tutorials, vol. 21, no. 23, pp. 2794-2830, 2019, doi:10.1109/COMST.2019.2899617.

[17] A. P. Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” Mathematical Foundations of Computing, vol. 1, no. 2, pp. 121-147, 2018. [Retrieved: March, 2021] http://www.aimsciences.org/article/doi/10.3934/mfc.2018007

[18] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: challenges and applications," The 32nd International Conference on Information Networking (ICOIN 2018), Chiang Mai, Thailand, 2018, pp. 473-475. [Retrieved: March, 2021] https://www.researchgate.net/profile/Chian-Techapanupreeda/publication/324725048_Blockchain_Challenges_and_applications/links/5d2ec2d392851cf4408a852c/Blockchain-Challenges-and-applications.pdf

[19] S.Singh and N. Singh, " Blockchain: future of financial and cyber security," The 2nd International Conference on Contemporary Computing and Informatics (IC3I 2016), Noida, India, 2016, ISBN: 978-1-5090-5256-1. [Retrieved: March, 2021] https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FIC3I.2016.7918009

[20] L. Moerel, "Blockchain & data protection…and why they are not on a collision course," European Review of Private Law, vol. 26, no. 6, pp. 825-851, 2018. [Retrieved: March, 2021] https://media2.mofo.com/documents/191019-blockchain-data-protection.pdf

[21] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automative security and privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, 2017, doi:10.1109/MCOM.2017.1700879.

[22] F. Zemler and M. Westner, "Blockchain and GDPR: application scenarios and compliance requirements," The Portland International Center for Management of Engineering and Technology Conference on Technology Management in the World of Intelligent Systems (PICMET 2019), Portland, USA, 2019, ISBN: 978-1-890843-39-7, doi:10.23919/PICMET.2019.8893923.

[23] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, "Blockchain applications in supply chain, transport and logistics: a systematic review of the literature," International Journal of Production Research, vol. 58, no. 7, pp. 2063-2081, 2020, doi:10.1080/00207543.2019.1650976.

[24] S. Underwood, "Blockchain beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-17, 2016, doi:10.1145/2994581.

[25] N. Guar, "Blockchain challenges in adoption," Managerial Finance, vol. 46, no. 6, pp. 849-858, 2020, doi:10.1108/MF-07-2019-0328

[26] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," The Review of Financial Studies, vol. 32, no. 5, pp. 1754-1797, 2019, doi:10.1093/rfs/hhz007.

[27] U. Roth, "Blockchain ensures transparency in personal data usage: being ready for the new EU General Data Protection Regulation," European Research Consortium for Informatics and Mathematics News, no. 110, pp. 32-33, 2017. [Retrieved: March, 2021] https://ercim-news.ercim.eu/images/stories/EN110/EN110-web.pdf

[28] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. A. Fuqaha, "Blockchain for AI: review and open research challenges," IEEE Access, vol. 7, pp. 10127-10149, 2019, doi:10.1109/ACCESS.2018.2890507.

[29] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, "Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda," International Journal of Information Management, vol. 49, pp. 114-129, 2019, doi:10.1016/j.ijinfomgt.2019.02.005.

[30] J. H. Park and J. H. Park, "Blockchain security in cloud computing: use cases, challenges, and solutions," Symmetry, vol. 9, no. 8, 2017, doi:10.3390/sym9080164.

[31] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: a survey on applications and security privacy and challenges," Internet of Things, vol. 8, 2019, doi:10.1016/j.iot.2019.100107.

[32] G. Drosatos, A. Kritsas, C. Ilioudis, A. Papanikolaou, and A. P. Filippidis, "A blockchain-based platform for consent management of personal data processing in the IoT ecosystem," Security and Communication Networks, vol. 2019, 2019, doi:10.1155/2019/1431578.

[33] C. Lima, "Blockchain-GDPR privacy by design: how decentralized blockchain internet will comply with GDPR data privacy." Claudio Lima. [Online]. [Retrieved: March, 2021] https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf

[34] V. Gramoli, "From blockchain consensus back to Byzantine consensus," Future Generation Computer Systems, vol. 107, pp. 760-769, 2020, doi:10.1016/j.future.2017.09.023.

[35] J. Ahmed, S. Yildirim, M. Nowostaki, R. Ramachandra, O. Elezaj, and M. Abomohara, "GDPR compliant consent driven data protection in online social networks: a blockchain-based approach," The 3rd International Conference on Information and Computer Technologies (ICICT 2020), San Jose, USA, 2020, ISBN: 978-1-7281-7283-5, doi:10.1109/ICICT50521.2020.00054.

[36] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security Implications of blockchain cloud with analysis of blockchain withholding attack," The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 2017, doi:10.1109/CCGRID.2017.111.

[37] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18-21, 2018, doi:10.1109/MCE.2017.2776459.

[38] D. Hofman, V. L. Lemieux, A. Joo, and D. A. Batista, "The margin between the edge of the world and infinite possibility: blockchain, GDPR and information governance," Records Management Journal, vol. 29, no. 1/2, pp. 240257, 2019, doi:10.1108/RMJ-12-2018-0045.

[39] R. Teperdjian, "The puzzle of squaring blockchain with the General Data Protection Regulation," Jurimetrics Journal, vol. 60, no. 3, 2020. [Online]. [Retrieved: March, 2021] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3638736

[40] P. Hristov and W. Dimitrov, "The blockchain as a backbone of GDPR compliant frameworks," The 8th International Multidisciplinary Symposium Conference on Challenges and opportunities for sustainable development through quality and innovation in engineering and research management (SIMPRO 2018), Petrosani, Romania, 2018. [Retrieved: March, 2021] https://www.researchgate.net/profile/Peyo-Hristov/publication/328576742_The_blockchain_as_a_backbone_of_GDPR_compliant_frameworks/links/5c27b3d6458515a4c700a92a/The-blockchain-as-a-backbone-of-GDPR-compliant-frameworks.pdf

[41] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 2018, doi:10.1109/TKDE.2017.2781227.

 ISBN: 978-1-61208-843-3

[42] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 33-39, 2018, doi:10.1109/MCOM.2018.1701095.

[43] J. Y. Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?: a systematic review," PLoS One, vol. 11, no. 10, 2016, doi:10.1371/journal.pone.0163477.

[44] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," Paper presented at the IEEE European Symposium on Security and Privacy Workshops (EuroS&W), Paris, France, 2017, doi:10.1109/EuroSPW.2017.43.

[45] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," The IEEE Middle East and North Africa Communications Conference (MENACOMM 2018), Jounieh, Lebanon, 2018, ISBN: 978-1-5386-1254-5, doi:10.1109/MENACOMM.2018.8371010.

[46] G. O. Karame, "On the security and scalability of Bitcoin's blockchain," The ACM/SIGSAC Conference on Computer and Communications Security (CCS 2016), Vienna, Austria, 2016, pp. 1861-1862, doi:10.1145/2976749.2976756.

[47] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," Nature, vol. 563, pp. 465-467, 2018, doi:10.1038/d41586-018-07449-z.

[48] R. Zhang and R. Xue, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 3, 2019, doi:10.1145/3316481.

[49] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," Business Horizons, vol. 62, no. 3, pp. 295-306, 2019, doi:10.1016/j.bushor.2019.01.009.

 ISBN: 978-1-61208-843-3