ANALYSIS OF DATA GOVERNANCE IN BLOCKCHAIN-BASED SYSTEMS

B. SEVA NAIK
Research Scholar,
Dept. of CSE,
Rayalaseema University,Kurnool.
Email:sevanaikb@gmail.com

M.SREENIVAS REDDY
Assistant Professor
Dept. of CSE,
Mahaveer Institute Of Science & Technology, Hyderabad.
Email:sreenivas.ml@gmail.com

ABSTRACT

In a blockchain-based system, data and the agreement-based process of recording and modifying them over distributed nodes are central to enabling the untrust multi-party transactions. Thus, completely understanding what and how the data are stored and manipulated finally determines the degree of usefullness, performance, and cost of a blockchain-based application. While blockchains enhance the quality of the data by providing a transparent, constant, and consistent data store, the technology also brings new challenges from a data management viewpoint. In this paper, we analyse blockchains from the perspective of a developer to highlight important concepts and considerations when incorporating a blockchain into a larger software system as a data store. The work focuses to increase the level of understanding of blockchain technology as a data store and to promote a methodical approach in applying it to large software systems. Firstly, we identify the common architectural layers of a typical software system with data stores and conceptualize each layer in blockchain terms. Secondly, we examine the placement and flow of data in blockchain-based applications. Thirdly, we explore data administration aspects for blockchains, especially as a distributed data store. Fourth one, we discuss the analytics of blockchain data and trustable data analytics enabled by blockchain. Finally, we examine the data governance issues in blockchains in terms of privacy and quality assurance.

KEYWORDS: Analytics, blockchain, databases, data governance, data handling, distributed data management, distributed databases, software architecture, transaction databases.

I. INTRODUCTION

The transformative capability of blockchain technology is often compared to that of the World Wide Web. In just a few years, besides the initial cryptocurrency applications, the foundations of blockchain technology are now being utilized for many other classes of applications, such as asset management, medical/health, finance, banking, and insurance. From the viewpoint of such applications, blockchain enhances the quality of the data through transparency, immutability, and consistency [1].However, the precise nature of blockchains that gives these benefits also brings new challenges from a data management perspective.

For example, in terms of the blockchain as a datastore and a processing network, following open issues could be observed:

The data models used in blockchains vary from key value to document stores and are generally combined with ``off-chain" data stores. Therefore, searching and retrieving heterogeneous data in blockchain-based systems takes hand-crafted and ad-hoc programming efforts, unlike the abstract and declarative query techniques in conventional databases. Considering the increasing demand for blockchain data analytics at scale, understanding how to efficiently access, integrate, and analyze data in this heterogeneous environment is essential.

The volume of data that blockchain system networks store and manage will only grow with time. However, many modern implementations show low throughput, low scalability, and high latency. Besides, to offset the high cost of building trust among transacting parties through consensus, as well as to discourage dormant data, fees are charged in public blockchains for both storing and manipulating data. Properly evaluating the on-chain/off-chain data architectural choices of a blockchain application can help resolve some of these issues.

The data stored in blockchains are permanent and transparent to the whole network. This brings about a range of data governance issues such as privacy and quality assurance. While storing data in encrypted form is recommended, it could be subject to brute-force decryption attacks in the future (e.g., breakthroughs in quantum computing might render current encryption technologies ineffective) or lead to unintended privacy leakages. Therefore, it is imperative to carefully review these issues to help develop adequate frameworks for blockchain data governance to promote effective management and proper use of blockchain technology.

Given these challenges, we trust there is a need to examine the use of a blockchain as a data store in the context of data management. A good understanding of blockchains in terms of how the data are stored and managed can help application developers and database administrators good design and manage a large software system where a blockchain and a complementary database may co-exist. It could also avoid sub-optimal designs, errors, and bugs due to idealistic expectations on how blockchains behave.

Blockchain has been briefly compared with databases in other work regarding functionality and unique properties [2][5]. Our work is complementary to these efforts, where we further conceptualize the differences according to how the application developers would generally perceive the software system layers.

In this paper, we systematically examine blockchain technology through a database lens. We aim to enhance the understanding of blockchains as a data store with the objective of enhancing the utility and correct use of blockchains in large software systems. To achieve this, we identify and analyze data management issues that are crucial in building and managing blockchain-based applications. We make the following contributions.

1) Suggest a new interpretation of blockchain as an application's data store.

2) Identify and evaluate good practices in blockchain data architectures and operational issues.

3) Explore data administration aspects of blockchains.

4) Current practical insights into the emerging topic of blockchain data analytics and trustable data analytics using blockchain.

5) Examine present issues and future directions in the governance of blockchain data privacy and quality.

The rest of the paper is organized as follows;

Section II presents fundamental properties of blockchains that are relevant from a data and software system perspective.

Section III presents blockchain system terminology and interpretation of blockchain-based applications from a database viewpoint. How the data could be integrated and stored in a blockchain are discussed in Section IV.

Governance aspects of data privacy and quality are presented in Section V.

II. BLOCKCHAIN PROPERTIES

Blockchains can provide a trustworthy and neutral data storage platform for a large software system that uses blockchain as a component. Trust and neutrality come from the following properties, which are resulting from the unique design of the ledger structure, the network, consensus protocol, and cryptographic mechanisms it uses:

Transparency: Data stored on a blockchain are accessible to all participants within the blockchain network. Thus, the data on a public blockchain is visible to everyone on the Internet.

Immutability: Due to the distributed consensus process, once data are subjoined to the blockchain, they cannot be changed or deleted. However, immutability might be probabilistic for blockchains using certain consensus protocols. All the transactions in the blockchain network are stored as immutable records. These immutable records become a public audit trail for regulatory purposes.

Consistency: Distributed consensus and immutability ensure all committed data are visible to all future data manipulations establishing a single truth across the blockchain network.

Equal rights: Due to disintermediation, every participant of the network has the same rights to manipulate and access the blockchain. With different consensus protocols, these rights may be weighted by the computation power or stake owned by the participant.

Availability: Every participates within the blockchain network may host a full replica of the blockchain data.

Hence, from the system perspective, the data are available if at least one node is in the blockchain network.

From the software architecture perspective, every design decision of a system is a trade-off among multiple properties. Likewise, Condentiality and Performance are the two main perception arising from the design of blockchain. As there is no privileged user within the blockchain network, every participant can access all data on blockchain compromising condentiality. Performance refers to the transaction processing rate and the latency of adding and confirming new records.

The throughput is limited by the block size configuration and block generation rate. Further, the latency between the submit and commit of a transaction is affected by the consensus protocol, which is around 1 hour (10-minute block interval with6-block confirmations) on Bitcoin [6] and around 3-minutes(15-second block interval with 12-block confirmation) on Ethereum [7].

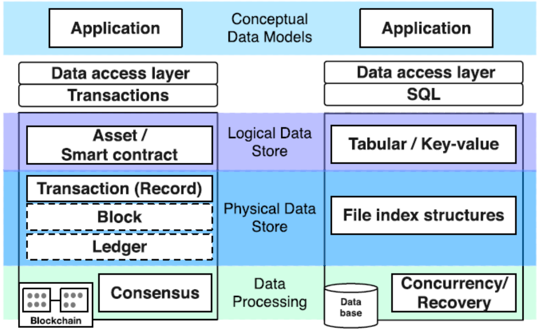

FIGURE 1. Application architectures: Blockchains vs. Database.

III. BLOCKCHAIN ARCHITECTURE AS A DATA STORE

In Fig. 1, we define a conceptual architecture of a software system, detailing a blockchain as its data store layer [5]. On the right, we show a conventional database to highlight our interpretation on how a blockchain data store can be explained from the conventional view of a database-backed application architecture.

Broadly, three different types of applications utilize

blockchain technology at its basics, namely, currency (e.g., Bitcoinand micropayments), contracts (e.g., escrow and automated insurance process based on agreed terms), and asset management (e.g., land registry and digital coupons). Just like in a conventional database-backed application, the conceptual data model underpinning a blockchain-based application needs to be mapped to the logical and physical levels of the data store to persist.

GOVERNANCE

Governance refers to comprehensive control including processes, policies, and structures, which could be applied to, e.g., IT or data assets to support right decision making in organisations. As a new technology that breaks many conventional norms (e.g., removing of a central mediator), blockchains have not yet come to terms with many areas of governance. Take cryptocurrencies, for instance. They are essentially ''tokens'' issued within a blockchain platform (e.g., BTC on Bitcoin and ETH on Ethereum) and there are more than 2,500 cryptocurrencies in operation. Most of the transactions on these cryptocurrency-enabled blockchains are financial; hence, have corresponding financial regulation issues. It is debatable whether cryptocurrency can be considered as cash or cash equivalent because it lacks broad acceptance as a means of value exchange. It may also not be considered a financial asset because there is no contract between the holder of cryptocurrency and another partner. Thus, none of the existing standards applies to cryptocurrencies, according to the International Accounting Standard Board (IASB).[31] Nonetheless, there is an obvious need for governance on cryptocurrencies as they are currently used to pay for transaction fees (e.g., smart contract executions). It is also worth pointing out that these governance concerns are applicable to any tokenised asset that represents some form of value or equity. For example, micropayments, loyalty programs, raffles, and benefit dispersion applications built around blockchains may need to comply with financial regulations of respective geographies. Moreover, metadata of such payments may need more controlled manipulating and storing as outlined in standards such as Payment Application Data Security Standard (PA-DSS) [41].

Notwithstanding the broader governance concerns in blockchain platforms, in this section, we focus our governance discussion around the issues relating to data management. A blockchain as data store brings up a range of governance issues, first as a unique data processing platform that removes the need for a centralised authority and second as an append-only, permanent data storage. In the following, we examine data governance concerns and challenges in blockchains, in particular regarding privacy and data quality. For the discussion to be meaningful, we first need to point out that the original design goals of blockchain technology never aimed to meet the contemporary privacy and data quality concerns being raised by the data management community. However, considering the increasing depth and breadth of the applications the technology is being considered and adopted for, we believe it is important and timely to explore to what extent the current blockchain technology as a data store satisfies the concerns and potential approaches to mitigate them.

A. PRIVACY AND LEGAL COMPLIANCE

The concept of a data-sharing ecosystem, where multiple participants interact to provide, use, and share data, is widely adopted by many organizations. However, there is a pervasive problem of the potential data breach (data abuse or misuse) in such environments due to the complicated nature of the interactions and sophisticated information diffusion schemes within the systems[42].

Recognising this problem, recently, new regulations and amendments aiming for better protection of the user information and rights of data subjects have been introduced. One of the significant schemes is the European General Data Protection Regulation (GDPR) which became law in May 2018 [43] and applies to any organisations that interact with data subjects based in the EuropeanUnion(EU). The My Health Records Amendment Act 2018 by the Australian government is another example of regulatory efforts to strengthen privacy [44]. Although not comprehensive, we can derive some common and significant privacy requirements from these regulations as follows:

- *Access/Timeliness* – The data subject has the right to access and view their personal data. Also, a data subject's request for any information relating to their personal data should be responded to without undue delay.
- *Rectification*–The data subject should be able to correct inaccurate data concerning him or her.
- *Restriction of usage* – Personal data can only be processed with the data subject's consent.
- *Portability of the personal data* – The data subject has the right to receive the personal data in a structured, commonly used and machine-readable format and to transmit the data to another service.

- *Right to be forgotten* – The data subject has the right of the erasure of personal data concerning him/her without undue delay.

- Blockchain technology is actively promoted for inclusion in various data-sharing ecosystem architectures, citing the increased data quality and openness as a reason to trust the technology. However, there are growing concerns about whether blockchains can comply with these recent regulations, as data privacy is still an open issue for a blockchain-based system.

- In terms of the requirements identified above, access (and timeliness of it) in blockchains depends on the permissions. In a public blockchain, the data subject is free to access and obtain their personal data stored on the blockchain network on time. In fact, as there is no ''privileged'' participant in a public blockchain, where it is also referred to as a permissionless blockchain. In a permissioned blockchain, however, access and timeliness could be restricted to those with the appropriate access rights in the network. Whether any inaccurate data could be corrected or not depends on the ownership of the transaction record. If the data subject owns the transaction, he/she could issue another transaction which will rectify the error. If not, rectifying an error will depend on how the owner of the transaction would respond to a rectification request. Although there is no inherent method in blockchains to impose user consent for data usage, smart contracts provide a transparent means to encode and enforce access policies. Also, a recent development such as self-sovereign identity management scheme[32]could give a sophisticated solution for ensuring ''user-controlled'' data usage. As the blockchain data is machine-readable, it satisfies portability. Moving the data to another blockchain platform is not yet straightforward. Since the introduction of GDPR, the term right to be forgotten has received considerable attention. The records in a blockchain are immutable by design; hence, removing data to comply with this requirement is not feasible. There is a need for discussion on how to deal with the limitations to comply with privacy regulations.

B. DATA QUALITY

The value of data rely on its *quality*, which could be defined as ''the ability to satisfy the usage requirements'' [52], [53]. The data quality is often regarded as one of the key management areas in data governance [53], [54] because through the assessment and management of data quality a managing body can also correctly identify and manage data risks. Data quality can be assessed using a range of dimensions, some of which are detailed below[55]:

- *Consistency* – The degree to which data have attributes that are free from contradiction and are coherent with other data.
- *Traceability* – The degree to which data have attributes that provide an audit trail of access to data and any changes made to the data.
- *Availability* – The degree to which data have attributes that enable them to be retrieved by authorized users and applications.
- *Compliance* – The degree to which data have attributes that stick to standards, conventions, or regulations in force and similar rules relating to data quality.
- *Confidentiality* – The degree to which data have attributes that ensure that they are only accessible and interpretable by authorized users.
- *Credibility* – The degree to which data have attributes that are regarded as true and believable by users.

The use of blockchain technologies for data sharing is a double-edged sword in terms of managing data quality. While it guarantees better consistency, traceability, and availability, it lacks support in providing compliance, confidentiality, and credibility. As a distributed database, a blockchain provides strong consistency mechanisms, reliable services, and transparency to the participants. It, therefore, increases *consistency*, *traceability*, and *availability*. In blockchain applications, *credibility* depends on the level of trust on the external data providers (e.g., oracles). As anyone can access the data stored in a public blockchain without explicit permissions, it becomes difficult for the governing body to meet the desired level of data quality when it comes to *compliance and confidentiality*.

CONCLUSION:

We are seeing the growth of blockchain applications reaching far beyond the initial craze of Bitcoin. A consequence of the fast adoption of the technology is that, in many cases, a blockchain is often used as an architectural component in a large-scale distributed software system to store data, which not only vary widely in both format and content, but also express arrange of complex application domain requirements. Therefore, carefully examining blockchains to understand and assess its capabilities and issues as a data store is a timely and relevant topic to the academic and industry communities who are looking to use the technology.

To conclude, we would like to highlight some of the main lessons. First, having a clear understanding of a blockchain as a data store, and be able to comprehend and evaluate the characteristics of blockchains with regards to the conventional data stores will help application developers design and implement a blockchain-based application more effectively.

Our contributions In this regard are three folds:

(i)we offered a fresh view of a blockchain as a data store, conceptualising its logical and physical layer functions compared to the conventional data stores, (ii) we analysed the various data placement options, emphasising the impact of each design option on an overall system,(iii) we showed the critical tasks and tools involved in administering/operating a blockchain as a data store. Second, if one looks beyond digital currencies, contemporary data management issues for blockchains pose both risks and opportunities. We particularly identified two categories for discussions; data analytics and data governance. Much of the focus on blockchain technology has mostly been on methodologies to develop new applications. Methods and tools for analysing blockchain data at scale, and using blockchains to enable new types of data analytics are emerging topics. Data governance is another area of importance that warrants more interests from there search and industry communities.

REFERENCES:

[1] J. Yli-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, Art. no. e0163477.

[2] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, ''Blockchain versus database: A critical analysis,'' in Proc.17th IEEE Intl. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Intl. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018, pp. 1348–1353.

[3] S. Tai, J. Eberhardt, and M. Klems, ''Not ACID, not BASE, but SALT: A transaction processing perspective on blockchains,'' in Proc. 7th Intl. Conf. Cloud Comput. Services Sci. (CLOSER), Apr. 2017.

[4] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, ''A taxonomy of blockchain-based systems for architecture design,'' in Proc. IEEE Intl. Conf. Softw. Archit. (ICSA), May 2017, pp. 243–252.

[5] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, ''The blockchain as a software connector,'' in Proc. 13th Working IEEE/IFIP Conf. Softw. Archit., Apr. 2016, pp. 182–191.

[6] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] G. Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger: Byzantium Version, Ethereum Project Yellow Paper. Accessed: Mar. 2019. [Online]. Available: https://ethereum.github.io/ yellowpaper/paper.pdf

[8] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, ''Blockchain-oriented software engineering: Challenges and new directions,'' in Proc. IEEE/ACM 39th Intl. Conf. Softw. Eng. Companion (ICSE-C), May 2017, pp. 169–171.

[9] H. Rocha and S. Ducasse, ''Preliminary steps towards modeling blockchain oriented software,'' in Proc. 1st Intl. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB), May/Jun. 2018, pp. 52–57.

[10] M. Marchesi, L. Marchesi, and R. Tonelli, ''An agile software engineering method to design blockchain applications,'' in Proc. 14th Central Eastern Eur. Softw. Eng. Conf. Russia, Oct. 2018, pp. 3:1–3:8.

[11] A. B. Tran, Q. Lu, and I. Weber, ''Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset

management,'' in Proc. 16th Intl. Conf. Bus. Process Manage. (BPM), 2018, pp. 56–60.

[12] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, ''Ethereum query language,'' in Proc. 1st Intl. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB), May 2018, pp. 1–8.

[13] T. Haerder and A. Reuter, ''Principles of transaction-oriented database recovery,'' ACM Comput. Surv., vol. 15, no. 4, pp. 287–317, Dec. 1983.

[14] S. Gilbert and N. Lynch, ''Brewer's conjecture and the feasibility of consistent, available, partition-tolerant Web services,'' ACM SIGACT News, vol. 33, no. 2, pp. 51–59, Jun. 2002.

[15] M. Herlihy, ''Atomic cross-chain swaps,'' in Proc. ACM Symp. Princ. Distrib. Comput., 2018, pp. 245–254.

[16] V. Zakhary, D. Agrawal, and A. El Abbadi, ''Atomic commitment across blockchains,'' 2019, arXiv:1905.02847. [Online]. Available: https://arxiv.org/abs/1905.02847

[17] M. Borkowski, C. Ritzer, D. McDonald, and S. Schulte, ''Caught in chains: Claim-first transactions for cross-blockchain asset transfers,'' Vienna Univ. Technol., Vienna, Austria, white paper, version 4, Feb. 2018.

[18] X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications. Cham, Switzerland: Springer, 2019.

[19] D. N. Dillenberger, P. Novotny, Q. Zhang, P. Jayachandran, H. Gupta, S. Hans, D. Verma, S. Chakraborty, J. J. Thomas, M. M. Walli, R. Vaculin, and K. Sarpatwar, ''Blockchain analytics and artificial intelligence,'' IBM J. Res. Develop., vol. 63, nos. 2–3, pp. 5:1–5:14, Mar. 2019.

[20] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, ''Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive,'' IEEE Trans. Depend. Sec. Comput., Nov. 2019, doi: 10.1109/TDSC.2019.2952332.

[21] J. Eberhardt and J. Heiss, ''Off-chaining models and approaches to offchain computations,'' in Proc. 2nd Workshop Scalable Resilient Infrastructures Distrib. Ledgers (SERIAL), Dec. 2018, pp. 7–12.

[22] I. Weber, Q. Lu, A. B. Tran, A. Deshmukh, M. Gorski, and M. Strazds, ''A platform architecture for multi-tenant blockchain-based systems,'' in Proc. IEEE Int. Conf. Softw. Archit. (ICSA), Mar. 2019, pp. 101–110.

[23] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, ''Blockbench: A framework for analyzing private blockchains,'' in Proc. ACM Intl. Conf. Manage. Data, May 2017, pp. 1085–1100.

[24] M. Schäffer, M. di Angelo, and G. Salzer, ''Performance and scalability of private Ethereum blockchains,'' in Proc. Blockchain Forum, 17th Int. Conf. Bus. Process Manage. (BPM), Sep. 2019, pp. 1085–1100.

[25] Hyperledger Performance and Scale Working Group.Hyperledger Blockchain Performance Metrics.Accessed:Oct.2018.[Online]. Available:https://www.hyperledger.org/resources/publications/blockchainperformance-metrics

[26] N. Heudecker and A. Chandrasekaran. Debunking the Top 3 Blockchain Myths for Data Management. Accessed: Apr. 2018. [Online].Available:https://www.gartner.com/en/documents/3871956

[27] H. D. Bandara, X. Xu, and I. Weber, ''Patterns for blockchain migration,'' Jun. 2019. arXiv:1906.00239. [Online]. Available: https://arxiv.org/abs/1906.00239

[28] H. Kalodner, S. Goldfeder, A. Chator, and M. Möser, and A. Narayanan, ''BlockSci: Design and applications of a blockchain analysis platform,'' 2017, arXiv:1709.02489. [Online]. Available: https://arxiv.org/abs/1709.02489

[29] F. Reid and M. Harrigan, ''An analysis of anonymity in the Bitcoin system,'' in Security And Privacy In Social Networks. New York, NY, USA: Springer, 2013, pp. 197–223.

[30] D. Ron and A. Shamir, ''Quantitative analysis of the full Bitcoin transaction graph,'' in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2013, pp. 6–24.

[31] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, ''When the cookie meets the

blockchain: Privacy risks of Web payments via cryptocurrencies,'' Proc. Privacy Enhancing Technol., vol. 2018, no. 4, pp. 179–199, 2018.

[32] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, ''Tracking ransomware end-to-end,'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2018, pp. 618–631.

[33] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, ''Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology,'' in Proc. World Wide Web Conf. (WWW), 2018, pp. 1409–1418

[34] C. Klinkmüller, A. Ponomarev, A. B. Tran, I. Weber, and W. van der Aalst, ''Mining blockchain processes: Extracting process mining data from blockchain applications,'' in Business Process Management: Blockchain and Central and Eastern Europe Forum, C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar Stemberger, A. Ko, and M. Staples, Eds. Nature Switzerland: Springer, 2019, pp. 71–86. 186106 VOLUME 7, 2019 H.-Y. Paik et al.: Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance

[35] G. Zyskind, O. Nathan, and A. S. Pentland, ''Decentralizing privacy: Using blockchain to protect personal data,'' in Proc. IEEE Secur. Privacy Workshops, San Jose, CA, USA, May 2015, pp. 180–184.

[36] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, ''Towards a novel privacy-preserving access control model based on blockchain technology in IoT,'' in Proc. Eur. MENA Cooperation Adv. Inf. Commun. Technol., Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2017, pp. 523–533.

[37] J. D. Harris and B. Waggoner, ''Decentralized & collaborative AI on blockchain,'' in Proc. IEEE Intl. Conf. Blockchain (Blockchain), Jul. 2019, pp. 180–184.

[38] A. Baldominos and Y. Saez, ''Coin.AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning,'' Entropy, vol. 21, no. 8, p. 723, 2019.

[39] Q. Wang, M. Li, W. Zhang, P. Wang, Z. Shi, and F. Xu, ''BDML: Blockchain-based distributed machine learning for model training and evolution,'' in Proc. 2nd Intl. Symp. Found. Appl. Blockchain, Apr. 2019, pp. 10–21.

[40] A. B. Kurtulmus and K. Daniel, ''Trustless machine learning contracts; evaluating and exchanging machine learning models on the Ethereum blockchain,'' 2018, arXiv:1802.10185. [Online]. Available: https://arxiv.org/abs/1802.10185

[41] PCI Security Standards Council. (May 2016). Payment Application Data Security Standard—Requirements and Security Assessment Procedures. [Online]. Available: https://www. pcisecuritystandards.org/document_library

[42] S. U. Lee, L. Zhu, and R. Jeffery, ''A data governance framework for platform ecosystem process management,'' in Proc. Int. Conf. Bus. Process Manage. (BPM), 2018, pp. 211–227.

[43] The European Parliament and of the Council. General Data Protection Regulation, GDPR. Accessed: Oct. 1, 2019. [Online]. Available: https://gdpr-info.eu/

[44] Australian Government. (2018). My Health Records Amendment (Strengthening Privacy) Act. [Online]. Available: https://www.legislation.gov.au/Details/C2018A00154

[45] A. Cavoukian, ''Privacy by design: The 7 foundational principles,'' Inf. Privacy Commissioner, Ontario, ON, Canada, Tech. Rep., 2009, vol. 5.

[46] S. Schwerin, ''Blockchain and privacy protection in the case of the European general data protection regulation (GDPR): A delphi study,'' J. Brit. Blockchain Assoc., vol. 1, no. 1, p. 3554, 2018.

[47] M. de Vos, M. Olsthoorn, and J. Pouwelse, ''Devid: Blockchain-based portfolios for software developers,'' in Proc. IEEE Intl. Conf. Decentralized Appl. Infrastructures (DAPPCON), Apr. 2019, pp. 158–163.

[48] P. Dunphy and F. A. P. Petitcolas, ''A first look at identity management schemes on the blockchain,'' IEEE Security Privacy, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[49] A. Dorri, S. S. Kanhere, and R. Jurdak, ''MOF-BC: A memory optimized and flexible blockchain for large scale networks,'' Future Gener. Comput. Syst., vol. 92, pp. 357–373, Mar. 2019.

[50] Y. Yu, Y. Li, J. Tian, and J. Liu, ''Blockchain-based solutions to security and privacy issues in the Internet of Things,'' IEEE Wireless Commun., vol. 25, no. 6, pp. 12–18, Dec. 2018.

[51] M. C. K. Khalilov and A. Levi, ''A survey on anonymity and privacy in bitcoin-like digital cash systems,'' IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2543–2585, Mar. 2018.

[52] Information Technology—Governance of IT—Governance of Data— Part 1: Application of ISO/IEC 38500 to the Governance of Data, Standard ISO/IEC 38500, Apr. 2017. [Online]. Available: https://www.iso.org/standard/56639.html

[53] V. Khatri and C. V. Brown, ''Designing data governance,'' Commun. ACM, vol. 53, no. 1, pp. 148–152, 2010.

[54] K. Weber, B. Otto, and H. Österle, ''One size does not fit all—A contingency approach to data governance,'' J. Data Inf. Qual., vol. 1, no. 1, p. 4, 2009.

[55] ISO/IEC Data Quality Model. [Online]. Available: https://iso25000. com/index.php/en/iso-25000-standards/iso-25012?limit=5&limitstart=0

[56] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, ''Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,'' in Proc. 17th IEEE/ACM Intl. Symp. Cluster, Cloud Grid Comput. (CCGRID), May 2017, pp. 468–477.

[57] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, ''Astraea: A decentralized blockchain oracle,'' in Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), Jul./Aug. 2018, pp. 1145–1152.

[58] S. U. Lee, L. Zhu, and R. Jeffery, ''Data governance for platform ecosystems: Critical factors and the state of practice,'' in Proc. 21st Pacific–Asia Conf. Inf. Syst., 2017.