CEUR-WS.org/Vol-3145/paper03.pdf

Towards Blockchain-based Smart Systems

Hamza Baniata[1], Dragi Kimovski[2], Radu Prodan[2] and Attila Kertesz[1]

[1] Software Engineering Department, University of Szeged, Hungary
[2] Institute of Information Technology, University of Klagenfurt, Austria

Abstract

The unprecedented pace of technological development in smart systems, incorporating sensing, actuation, and control functions, have the following properties and needs: (i) they are interconnected and need scalable, virtualized resources to run, store and process data, (ii) they are mobile and can potentially access and build on user data made available by smartphones and tablets, and (iii) they are getting smarter, so they may get access to user data provided by connected smart devices. As the number of smart devices in smart systems grows, the vast amount of data they produce requires high-performance computational and storage services for processing and analysis and other novel techniques and methods that enhance these services and their management. Blockchain applications have been proposed in a wide variety of environments such as distributed voting, eHealth, Mobile Computing, Internet of Vehicles, etc. We believe that integrating Blockchain technology with smart applications for managing data of mobile devices can further enhance the privacy and security requirements of current complex systems. In this paper, we discuss Blockchain-integration possibilities for smart systems to support the efficient, secure, and privacy-aware execution of smart applications. We propose a design space where issues need to be solved in different layers of such integrated systems. Accordingly, we envision a Blockchain-enabled simulation framework capable of analysing the integration possibilities with fog/edge and cloud infrastructures at different layers of smart systems. The framework will be able to model and analyse the behavior of Blockchain networks in large-scale fog-enhanced smart systems while using different AI methods.

Keywords

Blockchain, Smart Systems, Cloud Computing, Internet of Things

1. Introduction

Nowadays, we are witnessing an unprecedented pace of technological development in smart systems. A Smart System (SS) incorporates the functions of sensing, actuation, and control in order to describe and analyze a situation and make decisions based on the available data in a predictive or adaptive manner, thereby performing smart actions [1]. A Smart Device (SD) is a fundamental component of a SS generally connected to other devices or networks via different wireless protocols (such as Bluetooth, Zigbee, NFC, Wi-Fi, LiFi, 5G, etc.). They can operate to some extent interactively and autonomously [2]. SSs address environmental, societal, and economic challenges like limited resources, climate change, population aging, and globalization. They are for this reason increasingly used in a large number of sectors, such

1st Workshop on Connecting Education and Research Communities for an Innovative Resource Aware Society (CERCIRAS Cost Action CA19135), September 2, 2021, Novi Sad, Serbia

baniatah@inf.u-szeged.hu (H. Baniata); dragi.kimovski@aau.at (D. Kimovski); radu.prodan@aau.at (R. Prodan); keratt@inf.u-szeged.hu (A. Kertesz)

© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

as transportation, healthcare, energy, safety and security, logistics, ICT, and manufacturing. One can also categorize SSs via regions by referring to smart homes and smart cities. The management of SDs and their data in SSs require smart applications, raising many requirements and open issues.

The current SS services and applications have the following properties and needs: they are interconnected and need scalable, virtualized resources to run, store and process data; they are mobile and can potentially access and build on user data made available by smartphones and tablets, and they are getting smarter, so they may get access to user data provided by connected SDs.

As the number of SDs interconnected within a SS grows, the vast amount of data they produce requires high-performance computational and storage services for processing and analysis and other novel techniques and methods that enhance these services and their management. To support these needs, Cloud Computing [3] services started to be utilized almost a decade ago by responding to the growing data management needs of large scale systems. Meanwhile, the miniaturisation of electronic devices and improvements in battery lifetime led to the development of small computational devices with communication capabilities giving birth to the Internet of Things (IoT) paradigm [4]. From a different point of view, different integration options of IoT devices with cloud-based services have become the reference models of SSs. To cope with the possibly massive number of communicating entities, Fog (FC) and Edge Computing (EC) [5], born around five years ago, enhance data management operations by providing computational services placed close to their origins within SSs. A group of such edge nodes of a network forms the fog, which enables data processing and analysis to be performed with reduced service latency and improved service quality compared to a remote cloud utilisation. The application of these innovative technologies in smart cities led to the creation of a powerful ecosystem among public administrations, private companies and citizens to improve the quality of life by implementing new communication strategies, policies and solutions for their active involvement in the service management [6]. Such a smart, citizen centric management of urban services allows each city to reduce costs, and to increase security by keeping data locally (off the cloud) and ensure citizens satisfaction with reduced service latencies at the same time.

Blockchain (BC) [7] is the backbone technology for many Distributed Ledger (DL) and Distributed Computing (DC) applications, such as digital cryptocurrencies and digital smart contracts. Solutions integrated with BCs excel the provenance of high levels of security and trust, and guarantee fully-immutable log of transactional history without the interference or control of a central authority. BC applications have been proposed in a wide variety of environments such as distributed voting, eHealth, Mobile Computing, Internet of Vehicles, etc. We believe that integrating the BC technology with smart applications for managing data of mobile SDs can further enhance the privacy and security requirements of current SSs. Sharma et al. [8] were the first to integrate BC technology into fog-enabled systems by addressing privacy challenges.

Critical implementation and deployment decisions in such complicated, blockchain-assisted SSs cannot be made by system administrators and need various sophisticated methods. Furthermore, the big data produced in SSs by SDs cannot be handled and analyzed via traditional methods. The data handled by COVID-19-related applications, for instance, represents a much higher potential to fight the pandemic, once these applications are made smarter. On top of this, recent advances in the field of Artificial Intelligence (AI) [9] are also being actively deployed in both SSs and BC-based systems. AI deployment implies that system entities are able to act for maximizing the chances of successfully achieving their common goals and provide better services and enhanced data propagation. The deployment of AI in SSs indeed was proven to exponentially raise system abilities in terms of smartness. That is, system entities may learn what to do and when, in an automated environment that allows sensors, actuators, and other SDs to optimize their collaboration. AI deployment in BC-based systems, on the other hand, equips BC entities (usually referred to as miners, which mint and confirm new blocks and verify users and transactions) with methods to determine optimized collaboration practices for different purposes, such as optimal selection of peers and optimized data verification/confirmation. Such deployment in highly dynamic BC networks (e.g. public-permissionless BC) can increase, or decrease the propagation time of new blocks, leading to lower/higher consistency of the distributed ledger or latency of data retrieval. Despite all of these advantages of AI-BC-FC-SS integration, these systems still inherit the trade-offs that appear in BC and SSs, which requires further research regarding optimization and privacy-awareness.

To address all these issues and challenges, we propose a framework including novel integrated methods for SSs using a BC-based edge and fog-enabled distributed infrastructure to handle latency, single-points-of-failure and mobility issues, while AI technologies can optimize collaboration between these elements. To facilitate the use of such complex BC-based AI-enhanced Edge/Fog-enabled SSs, we need to strengthen trust and to provide novel techniques to ensure privacy, while optimizing the integration of these different technologies within different layers of the SS. In the future, we plan to provide enhancements to COVID-19-related applications and use them to validate our proposal.

The remainder of the paper is organized as follows: in Section 2 we present the state-of-the-art, and in Section 3 we introduce our proposed and envisioned integrated architecture. Finally, in Section 4 we state our future direction, and conclude the paper in Section 5.

2. State-of-the-art

The support for the future decentralized platforms for medical data storage and analysis in BC with autonomous and democratic practices is still immature. Nevertheless, promising research initiatives have started in the European research community, focused towards solving issues related to medical data management with BC. One of these initiatives is the Horizon 2020 MyHealth – MyData[1] project that aims at the development of decentralised marketplace for open sharing of anonymized sensitive medical data for research purposes. The project provides secure ecosystem that encourages hospitals and medical centers to share their data, while making the citizens the ultimate owners and controllers of this data. Furthermore, the Horizon 2020 FeatureCloud[2] project focuses on creating a federated AI platform with centralized, yet transient Cloud for shared intelligence in medical systems. The platform utilizes DLT technologies for data access control and to secure features sharing.

Generally, BC have been utilized in the literature for providing a reliable distributed database, where several parties collaborate for handling/managing sensitive data and controlling the

[1] http://www.myhealthmydata.eu/

[2] https://featurecloud.eu/

access to it. BC represents a database that need not be administered by a central authority. Furthermore, all parties of the system can confirm or reject any piece of data added to it, while no data can be deleted from it. This provides a full history of all transactions appeared on the BC, giving system users a method to insure the correctness of retrieved information.

In the literature, Kuo and Ohno-Machado [10] propose a cross-institutional healthcare predictive model for quality improvement initiatives by predicting the risk of re-admission of a group of patients using data from multiple institutions. This approach sets the ground for developing privacy-preserving ML technology in BC. Furthermore, Mettler [11] provides an initial medical data management approach through BC, empowering patients and fighting counterfeit drugs in the pharmaceutical industry. Jenkins et al. [12] discuss a distributed unsupervised learning framework based on BC for bridging the gap between security and large medical data analysis with functional bio-markers to identify possible inherited diseases. Recently, a feasibility study, presented in [13], explores the idea of applying federated learning[3] for secure multi-institutional data analysis, with multiple local models coordinated by a centralized aggregation server. Although the concept is promising, it still requires centralized model to gather all updates, which can be prone to failures and undemocratic decisions. Moreover, a recent research [14] proposes a BC-based healthcare data gateway architecture to enable rudimentary control and secure share possibilities of patient data without violating privacy. The data is stored in a private blockchain, thus not anonymized. Lastly, Omidshafiei et al. [15] present a generalized linear ML models for the first time, which are able to perform model training in a fully decentralized setting. The approach, termed COLA, provides communication-efficient decentralized framework, without any requirement for parameter tuning.

Utilizing the BC technology has its own drawbacks and challenges [16]. Although BC is considered the current state-of-the-art solution to reliably handle DC applications, privacy and standardization issues are still major concerns for BC deployment. One problem is the use of pseudonyms, which does not fully preserve privacy, even when combined with advanced privacy-preserving methods (e.g. mixing services [17]). Additionally, BC deployment implies higher latency for data aggregation and for maintaining DL consistency compared with centralized systems, depending on various methods employed in different BC-based applications to reach consensus among system elements. However, SSs may suffer from heterogeneity, which hardships the maintaining of data concurrency and credibility, and limits the computing and storage abilities. BC-integrated systems can solve such problems, while maintaining high security. On the other hand, infrastructure requirements of BCs, such as distributed and highly connected Peer-to-Peer networks, resource management platforms/algorithms, standardized computing entities, and fast communication channels through various scalable network topologies, are provided in nearly all SSs.

Concerning the state-of-the-art for utilizing the BC technology to address challenges related to the COVID-19 pandemic, we identified initial related literature, e.g. BeepTrace [18] for global infection tracing, PPMF [19] for nationwide infection tracing. Biometric and identity management companies, such as SCIPA, Mvine and iProov announced the trials of their Covid-19 immunity and vaccination passport in the beginning of 2021. Meanwhile, European national efforts have been reported by the European Commission regarding mobile contact tracing apps

[3] https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[20]. Although such applications are being approached vigilantly by both governments and non-practitioners, it was argued by Barsocchi et al. [21] that a more transparent approach for data treatment would benefit the adoption of such services. Accordingly, digital Verifiable Credentials (VCs) using ZKPs were argued to be the most suitable approach for these applications. Digital VCs can be instantly approved, no central authority collects private data of users, and the verification process is more accurate, up-to-date, and thus more reliable than paper-based schemes. To address the challenges of a successful, globally-trusted, and reliable digital VCs application, a collaboration of different national projects is required.

3. Our proposal

BC deployment in a wide range of applications was proven as an enhancement factor in terms of security [22], decentralization [23], reliability [24], and optimization of multi-party decision making [25]. Generally, these criteria enhanced by successful BC integration, are considered the main challenges in IoT, fog, and cloud based SSs.

In this position paper, we present a set of research questions and envisioned methods to tackle them. Our future research focus mainly targets these questions, and we will apply different methods to efficiently address their challenges. We aim to answer the following questions:

1. What are the best practices for integrating SS-IoT technologies with BC technology?
2. How to combine AI, BC, Cloud and FC in SSs to better serve the requirements of smart applications?
3. What BC methods and consensus algorithms are most suitable for optimizing services provided by FC-enhanced SSs?
4. How can the integration of fog/edge, AI, and BC technologies advance user experience, trust and privacy protection at the same time?
5. What is the potential enhancement of COVID applications driven by the integration of SS, IoT and BC technologies?

Figure 1 depicts the design space of our vision and research methodology for performing research in BC technology integration. The main entities are: (i) blockchains, (ii) smart systems and (iii) applications. Each of the entities in the demonstrated design space has unique identification layers, where different services and protocols can be placed and investigated, be it the end-user devices, servers/APs in the fog tier, or VMs in the cloud. Generally, a BC-based system can be defined according to the infrastructure it is occupied with, the local protocols that define how transactions and blocks are mined, validated and shared, the algorithms that control how system entities confirm a mined block and verify each other, and the purpose of the BC deployment (in the application). The infrastructure, specifically, can be studied according to different P2P connection models with technical consideration referred to by the OSI network model. Finally, a smart system is defined by edge devices (mainly corresponding to end-user devices in an IoT enabled system), edge gateways that locally control and secure communications among edge devices and with upper layers, edge servers (corresponding to the fog nodes in the lowest layer of the fog), and global servers, clouds or upper fog layers. To answer the research questions raised earlier, our research aims at analyzing the requirements of COVID-19-related

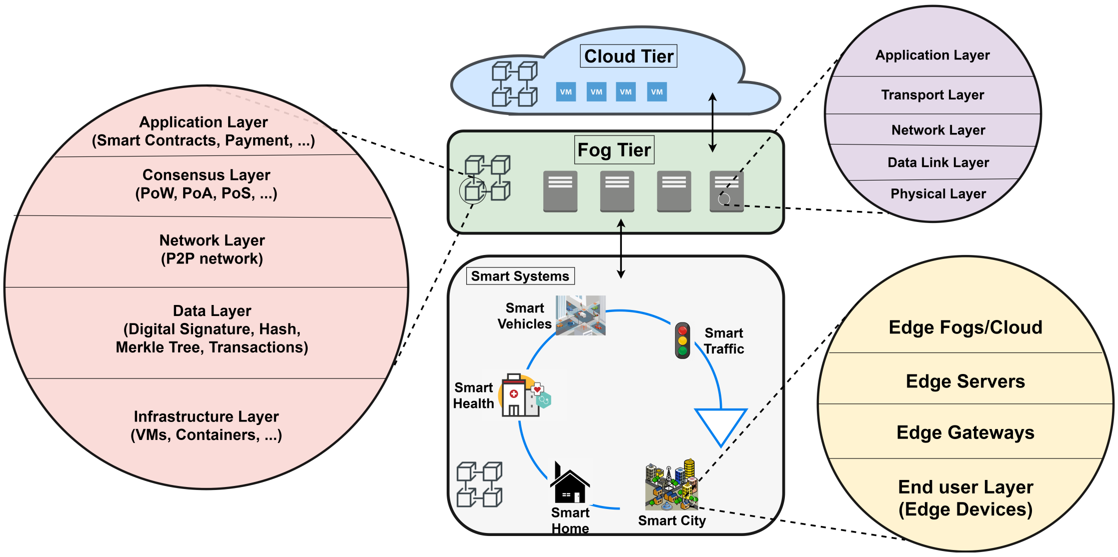

Figure 1: Design Space for Blockchain and Smart Systems integration within a fog-enhanced cloud architecture

smart applications to guide our research, and investigating and developing sophisticated AI methods to be applied within individual layers of each of the combined technologies, then validating them with smart applications by means of simulation. Consequently, we aim at the optimization of our methods for technology integration, so that practitioners can decide, at the time of systems deployment, which protocol, algorithm, infrastructure, etc. to adopt for maximizing the efficiency of those systems, meanwhile fulfilling GDPR-compliance. To this end, we plan to investigate how the GDPR regulation affects BC-integrated smart systems. We plan to address these challenges by applying privacy and data protection by design methods of GDPR for application data storage and processing. We believe that applying our proposed BC- and AI-based methods in these applications can significantly improve their privacy and trust reputation.

We will therefore research a simulation environment for the integration of AI, BC, Cloud and FC supported by a visual user interface. An integrated template library will provide reusable templates for simulation of complex smart applications and smart systems over BC technology. The template library will be extensible with user-defined simulation models and actions. The extensible templates will support simulation of various smart applications through the injection of step-specific code provided by application owners. This solution regulates the inter-step communication using a race-condition-free mixture of message-oriented consensus algorithm over distributed file systems. Apart from the injected code, the simulation will support the definition and simulation of SSs by considering the hardware requirements, application parameters and scaling the number of concurrent instances of each component of the application. The simulator will enable serialization and deserialization (saving and loading) of application definitions using the standard output format (JSON, XML or YAML). The serialized application definitions will produce a deployment service configuration for the services, including the requirements of the smart systems and inter-application communication code as part of the simulation scenario.

Besides, the simulator will utilize the application definition from the template library and extract step definitions. Therefore, the users only need to provide a sample input for the entire application used for simulation purposes. The tool will simulate each component in the smart application by instantiating container-based templates and deploying an instance in a sandbox. Additionally, it will automatically provide input to the sandbox tool, that will estimate the throughput and performance of each component in the application. The estimated throughput and execution properties will be used to simulate the entire application and mathematically calculate its performance under configurable load conditions with high accuracy.

We have previously proposed an extensible tool for simulating integrated Fog-BC applications, called FoBSim [26]. FoBSim provides easy configuration through its Command Line Interface (CLI) for selecting BC deployment model, data model, Consensus algorithm and application model suitable for scenarios to be simulated. To test and evaluate our future proposed solutions for addressing our research questions, we will build up and extend FoBSim so that different realistic AI-BC-FC-SS integrated scenarios can be configured and simulated.

The current version of FoBSim allows to utilize the PoW, PoS and PoA consensus algorithms. It allows for simulating different BC services namely Digital payments, Identity Management, Smart Contracts and Data Management. Additionally, FoBSim allows for different deployment models of the BC in the Fog tier or end-user tier, where massive number of fogs and edge devices can be simulated using multithreaded interactive networks realized using the networkx library and a message-driven approach. Specifically, we plan to enhance FoBSim implementation by adding AI methods and deploy easy-to-modify smart components to FoBSim, represented by adding a module to the 'Miner' component where AI code can be injected and deployed by AI practitioners without the need of previous knowledge on the other technical aspects of FoBSim. FoBSim miners then regularly check this module and run its code, while the tool automatically presents its results (if applicable) at the end of each simulation run. Additionally, we plan to add mobility properties to end-user devices, which is represented by adding a mobility module to the 'End-user' and 'Fog' components, similar to [27], which allows the simulation and evaluation of system behaviour when end-users and fogs are mobile.

We also plan to add new consensus algorithms such as PoSign and pBFT, to FoBSim that are more suitable for different BC models (permission -ed/-less) and DL models (e.g. DAG). This extension will be represented by adding new consensus algorithms to the 'Consensus' Module that can be selected through the simulation run. Furthermore, we plan to add new benchmark methods that are needed for evaluating different SS infrastructure (Edge devices, Things, Fogs) such as energy consumption and QoS. This extension will be represented by adding more variables to the tool throughout the code, as well as allowing FoBSim users to configure the simulated machines in terms of power consumption according to their roles. As the current version of FoBSim is not able to simulate mining pools, and only allows the utilization of one BC system that runs one predefined consensus algorithm, we plan to allow these by adding a clustering module to the 'Network' component of FoBSim. The extension will allow sharding, pooling, as well as utilizing different BCs that uses different consensus algorithms at the same simulation run. Finally, we plan to utilize previous simulation tools to allow the provision of realistic cloud scenarios where critical decisions need to be made for enhanced overall system efficiency.

4. Future work

As our future work, we plan to extend the simulator to support complex models for simulating the scheduling and provisioning process of the entire application. The simulation models will adaptively respond to significant changes in the pool of available SDs (Cloud or Fog instances) during application execution and identify provisioned devices that do not provide good performance for a given smart application component. They will further enable the replacement of low-performing SDs, e.g., provisioned as VMs or containers that no longer meet the application requirements, or reconfigure existing ones (increase number of CPUs to a VM running).

The application scheduling and provisioning models will enable the simulation of decentralized data-aware resources scheduling over multiple control and network domains with increased trust. The model will utilize the transaction logs, stored in the simulated BC, to manage the SDs in an efficient manner. The approach will use semantics to describe the simulated SDs and check their compatibility through an Application Definition Machine (ADM). The ADM will describe the recommended resources for a given smart application.

We also plan to model different migration techniques to provide accurate simulation of the deployment and communication overhead for using smart devices from multiple providers. In case of over-provisioning, we will simulate the release or downgrading of resources to minimize the overall resource consumption without violating application requirements. Finally, the model will enable the simulation of resources provisioning through ADM for each individual application defined in the simulator.

We aim to focus our research on smart applications related to the prevention of virus spreading or to the management of societal problems, such as travel restrictions caused by the pandemic. The vast majority of such applications are mainly centralized and non-smart, which makes them carry single-point-of-failure, privacy, high latency, and legal issues, along with the lack of efficient handling of mobile SDs. The adoption and mass acceptance of such applications, e.g. COVID-19-related applications, are greatly hindered by the general lack of trust associated with the nature of tracing apps, and the reluctance of people to share their personal data. To overcome these issues, we need to revise current solutions, and design methods addressing privacy-preserving, privacy-awareness, explainability and interoperability.

5. Conclusions

Integrating the Blockchain technology with smart applications for managing data of smart devices can enhance the management of current complex systems. In this paper, we proposed Blockchain-integration possibilities for smart systems to support the efficient and secure execution of smart applications. As the heart of our solution, we envisioned a Blockchain-enabled simulation framework capable of analysing the integration possibilities with fog and cloud infrastructures at different layers of smart systems. Such a framework will be able to model and analyse the behavior of Blockchain networks in large-scale fog-enhanced smart systems, while using different AI methods.

Acknowledgments

The research leading to these results is partially supported by the European COST programme under action identifier CA19135 (CERCIRAS), and by the National Research, Development and Innovation Office within the framework of the Artificial Intelligence National Laboratory Programme.

References

[1] G. Akhras, Smart materials and smart systems for the future, Canadian Military Journal 1 (2000) 25–31.

[2] S. Gong, E. Tcydenova, J. Jo, Y. Lee, J. H. Park, Blockchain-based secure device management framework for an internet of things network in a smart city, Sustainability 11 (2019) 3889.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation computer systems 25 (2009) 599–616.

[4] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future generation computer systems 29 (2013) 1645–1660.

[5] B. Di Martino, K.-C. Li, L. T. Yang, A. Esposito, Internet of everything: Algorithms, methodologies, technologies and perspectives, Springer, 2017.

[6] M. Fazio, R. Ranjan, M. Girolami, J. Taheri, S. Dustdar, M. Villari, A note on the convergence of iot, edge, and cloud computing in smart cities, IEEE Cloud Computing 5 (2018) 22–24.

[7] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Business & Information Systems Engineering 59 (2017) 183–187.

[8] P. K. Sharma, M.-Y. Chen, J. H. Park, A software defined fog node based distributed blockchain cloud architecture for iot, Ieee Access 6 (2017) 115–124.

[9] T. Marwala, B. Xing, Blockchain and artificial intelligence, arXiv preprint arXiv:1802.04451 (2018).

[10] T.-T. Kuo, L. Ohno-Machado, Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, arXiv preprint arXiv:1802.01746 (2018).

[11] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2016, pp. 1–3.

[12] J. Jenkins, J. Kopf, B. Q. Tran, C. Frenchi, H. Szu, Bio-mining for biomarkers with a multi-resolution block chain, in: Independent Component Analyses, Compressive Sampling, Large Data Analyses (LDA), Neural Networks, Biosystems, and Nanoengineering XIII, volume 9496, International Society for Optics and Photonics, 2015, p. 94960N.

[13] M. J. Sheller, G. A. Reina, B. Edwards, J. Martin, S. Bakas, Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation, in: International MICCAI Brainlesion Workshop, Springer, 2018, pp. 92–104.

[14] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, Journal of medical systems 40 (2016) 218.

[15] S. Omidshafiei, J. Pazis, C. Amato, J. P. How, J. Vian, Deep decentralized multi-task multi-agent reinforcement learning under partial observability, in: Proceedings of the 34th International Conference on Machine Learning-Volume 70, JMLR. org, 2017, pp. 2681–2690.

[16] H. Baniata, A. Kertesz, A survey on blockchain-fog integration approaches, IEEE Access 8 (2020) 102657–102668.

[17] L. Chen, L. Xu, N. Shah, N. Diallo, Z. Gao, Y. Lu, W. Shi, Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, pp. 23–28.

[18] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, M. A. Imran, Beeptrace: blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond, IEEE Internet of Things Journal (2020).

[19] M. Whaiduzzaman, M. R. Hossain, A. R. Shovon, S. Roy, A. Laszka, R. Buyya, A. Barros, A privacy-preserving mobile and fog computing framework to trace and prevent covid-19 community transmission, IEEE Journal of Biomedical and Health Informatics 24 (2020) 3564–3575.

[20] D. Zeinalipour-Yazti, C. Claramunt, Covid-19 mobile contact tracing apps (mcta): A digital vaccine or a privacy demolition?, in: 2020 21st IEEE International Conference on Mobile Data Management (MDM), IEEE, 2020, pp. 1–4.

[21] P. Barsocchi, A. Calabrò, A. Crivello, S. Daoudagh, F. Furfari, M. Girolami, E. Marchetti, Covid-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing, Array 9 (2021) 100051.

[22] S. Singh, A. S. Hosen, B. Yoon, Blockchain security attacks, challenges, and solutions for the future distributed iot network, IEEE Access 9 (2021) 13938–13959.

[23] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, L. Chen, A survey of decentralizing applications via blockchain: The 5g and beyond perspective, IEEE Communications Surveys & Tutorials (2021).

[24] C. Zhang, L. Zhu, C. Xu, C. Zhang, K. Sharif, H. Wu, H. Westermann, Bsfp: blockchain-enabled smart parking with fairness, reliability and privacy protection, IEEE Transactions on Vehicular Technology 69 (2020) 6578–6591.

[25] B. Cao, X. Wang, W. Zhang, H. Song, Z. Lv, A many-objective optimization model of industrial internet of things based on private blockchain, IEEE Network 34 (2020) 78–83.

[26] H. Baniata, A. Kertesz, Fobsim: an extensible open-source simulation tool for integrated fog-blockchain systems, PeerJ Computer Science 7 (2021) e431.

[27] R. Mahmud, S. Pallewatta, M. Goudarzi, R. Buyya, Ifogsim2: An extended ifogsim simulator for mobility, clustering, and microservice management in edge and fog computing environments, arXiv preprint arXiv:2109.05636 (2021).