



Convergence of Blockchain, Autonomous Agents, and Knowledge Graph to Share Electronic Health Records

Yao Yao^{1,2*†}, Meghana Kshirsagar^{1,2*†}, Gauri Vaidya^{3†}, Jens Ducrée⁴ and Conor Ryan^{1,2*}

¹ Biocomputing and Developmental Systems Group, University of Limerick, Limerick, Ireland, ² Lero, The Science Foundation Ireland Research Centre for Software, Limerick, Ireland, ³ Principal Global Services, Pune, India, ⁴ School of Physical Sciences, Dublin City University (DCU), Dublin, Ireland

OPEN ACCESS

Edited by:

Jane Thomason,
University College London,
United Kingdom

Reviewed by:

Wendy M. Charles,
BurstIQ, United States
Ingrid Vasiliu Feltes,
University of Miami, United States

*Correspondence:

Yao Yao
Yao.Yao@ul.ie
Meghana Kshirsagar
Meghana.Kshirsagar@ul.ie
Conor Ryan
conor.ryan@ul.ie

[†]These authors have contributed
equally to this work

Specialty section:

This article was submitted to
Blockchain for Good,
a section of the journal
Frontiers in Blockchain

Received: 30 January 2021

Accepted: 08 March 2021

Published: 06 April 2021

Citation:

Yao Y, Kshirsagar M, Vaidya G,
Ducrée J and Ryan C (2021)
Convergence of Blockchain,
Autonomous Agents, and Knowledge
Graph to Share Electronic Health
Records. *Front. Blockchain* 4:661238.
doi: 10.3389/fbloc.2021.661238

In this article, we discuss a data sharing and knowledge integration framework through autonomous agents with blockchain for implementing Electronic Health Records (EHR). This will enable us to augment existing blockchain-based EHR Systems. We discuss how major concerns in the health industry, i.e., trust, security and scalability, can be addressed by transitioning from existing models to convergence of the three technologies – blockchain, agent-based modeling, and knowledge graph in a decentralized ecosystem. Each autonomous agent is responsible for instantiating key processes, such as user authentication and authorization, smart contracts, and knowledge graph generation through data integration among the participating stakeholders in the network. We discuss a layered approach for the design of the proposed system leading to an enhanced, safer clinical decision-making system. This can pave the way toward more informed and engaged patients and citizens by delivering personalized healthcare.

Keywords: EHR data, blockchains, knowledge integration, knowledge graphs, agent based modeling, data sharing, smart healthcare

INTRODUCTION

Information for a given individual comprises many aspects, such medical history, genetic issues, medications, vital signs, immunizations, surgeries and progress reports, laboratory data, radiology reports, drug allergies, etc. This information is scattered across various healthcare service providers and the challenge is to integrate the necessary data and knowledge from these diverse organizations to improve the interoperability between different discrete functional entities in the whole healthcare ecosystem. This has the potential to reduce medical errors caused by issues of incompleteness in traditional EHR (Capece and Lorenzi, 2020; Tandon et al., 2020) systems.

Daraghmi et al. (2019) has proposed a cloud-based solution to address the interoperation among the stakeholders but the system has the limitation of uploading the documents manually in the data streams. The government of Estonia has deployed blockchain based Estonian National Health Information System (ENHIS) (Heston, 2017) that provides a patient platform named “My E-Health” for sharing medical records in the form of digitized data and accessible to hospitals, doctors, governments and patients. To secure the privacy of the health information on the network, healthcare professionals are issued with a personalized identification card which can be read only by a specialized device, thus blocking any alternate means of logging and accessing the network. While it is not mandatory to use ENHIS for “My E-Health,” it is a regulation in Estonia to upload

all the data in the private EHR on the EHNIS portal to ensure a centralized data repository when needed. For instance, if a patient performs an X-ray of any body organ, the respective data on the remote EHR will be uploaded to the EHNIS account of the patient so that it is accessible in some other healthcare center when needed¹. However, some issues identified by healthcare professionals in this deployed system were lack of quality data and the need for a more user-friendly interface.

We augment the existing deployed blockchain (Nakamoto, 2009) based healthcare systems by proposing the integration of knowledge graphs and autonomous agents with blockchains for facilitating sharing of EHR records. This will permit the patient to control access to their records and knowledge graphs by giving different types of permissions for the various stakeholders in the network (Medicalchain.Com, 2018). Furthermore, by incorporating agent-based modeling the key processes of the system are automated by creation of agents at different layers for embedding protocols that will adhere to the Patient Access Final Rule² that will take effect from July 1, 2021. Patient Access Final Rule is a patient-centric rule in the healthcare system allowing the administrators to give access to the patient data when they require it. This rule facilitates the interoperability among stakeholders as well as delivers access to patient health information.

The integration of data achieved through automated agents will model the knowledge in the form of a semantic knowledge graph and, with the knowledge integration, a global knowledge base will be established to describe the related resource and data sharing regulation. **Data integrity** will be achieved by incorporating a referential matching technology which will ensure uniqueness among all the network users (here, user refers to different stakeholders within the blockchain network) as well as provide access to the network. Through blockchain's consensus mechanism, the consensus on the knowledge can be achieved by a secure and flexible communication process and supported by multiple agents and smart contracts. The agent-based modeling leads to the *automation* of key processes of the framework. The various functionalities contained in commercial health record systems will be incorporated in our proposed system through agents which will be stored separately on discrete nodes of blockchain.

In our framework, we store the data and knowledge separately. The knowledge shared with all stakeholders only includes the necessary information of accessing the data but it doesn't maintain and include the corresponding data copy itself. The data and related functional tools will be developed and maintained by the corresponding stakeholders locally, while the knowledge will describe the way of using these resources through the blockchain. By sharing the knowledge on blockchain, we protected the consensus of data sharing and led to **trustworthiness** among stakeholders. Moreover, linkage of knowledge graph databases with Resource Description Framework (RDF) stores will lead to **scalable architecture**

optimized for speed, leading to fast transactions with ultra-high parallelization, giving high throughput even as the data grows. The different components of the proposed framework such as blockchain and knowledge graph (KG) will pave the way to deliver a sustainable and highly secured solution in a decentralized and highly dynamic environment.

The proposed framework can also be helpful to integrate knowledge for various current AI-based or data-driven applications, such as Covid-19 tracing apps which are in line with European Union's (EU) data protection rules (Van Der Sloot et al., 2019) thus ensuring privacy. By providing a common semantic description and customized data regulation policies, the heterogeneous data collected from these applications can be interpreted and shared by others. Such cross-platform knowledge can improve the power and efficiency of the corresponding applications and also holds the promise of a comprehensive view that may be derived from sharing data. For example, through providing knowledge derived from all related shared data, a data-driven diagnosis approach could serve to identify the severity of patients' current health condition, their underlying conditions, their allergy information and their past clinical as well as mental health history, which, when merged with the information from the various Covid-19 tracing apps (Julienne et al., 2020; Morley et al., 2020) can effectively lead to safe decision making.

Digital twin simulations can also use such data sharing to perform predictions based on a particular patient profile. Moreover, complicated decisions often depend on efficient data sharing crossing multiple stakeholder's platforms; for example, the prioritization of various population groups for vaccination programs, or safeguarding the frailest and most vulnerable in society by dedicating or identifying potential isolation areas for advanced caretaking resource planning. This can be done both in terms of personnel and administrative resources, as well as critical resources such as ICU beds and high end equipment for better monitoring of patients' condition. Such complex and potentially life-altering decisions need AI applications or experts capable of accessing comprehensive data which usually is not stored with any single stakeholder. By providing interpretable knowledge of all needed cross-platform data through blockchain, our proposed framework can help public health service providers for better preparedness with respect to current and unforeseen future pandemics as well as endemics.

LINKAGE OF KNOWLEDGE INTEGRATION AND AUTONOMOUS AGENTS WITH BLOCKCHAIN

Permissioned Blockchains

Permissioned blockchains differ from public and private blockchains as they have an additional blockchain security system, which maintains an access control layer to allow certain actions to be performed only by certain identifiable participants, such as the adding and validation of transactions. Similarly, transactions can only be viewed by nodes that have been given access; permissioned blockchain examples include Corda (Brown

¹<https://e-estonia.com/solutions/healthcare/e-health-record/>

²<https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index#CMS-Interoperability-and-Patient-Access-Final-Rule>

et al., 2016), Hyperledger Fabric (Androulaki et al., 2018), Multichain (Greenspan, 2013).

Ethereum (Buterin, 2015) can be configured both as private and public blockchain; we use the private version as it is possible to implement permissioning in its application layer. Using Ethereum, we propose to control data access where the system can be configured to generate different dynamic knowledge graphs depending upon the authorization rights validated through multiple smart contracts. For example, a patient may decide to share only medication prescriptions with a pharmacist, dental records with a dental surgeon, etc., or can disclose an integrated knowledge pertaining to a more detailed past history, current medications, mental health history, allergy conditions, and medications, genetic disorders etc. Hence, a patient always controls different views of their own data (privacy) that can be shared among different stakeholders. The level of access control will be achieved according to the FHIR 4.0.1 standard of data exchange.

Knowledge Graph

Knowledge Graphs (KGs) are a powerful data science technique to mine information from diverse data formats (Ehrlinger and Wöß, 2016; Afanasyev et al., 2019). It can be regarded as a knowledge base used by diverse AI programs to enhance their understanding and learning efficiency with information gathered from a variety of sources (Fensel et al., 2020). A KG provides a graph-structured topology to organize data and it can present interlinked descriptions of its entities, i.e., objects, events and situations, as well as abstract concepts with free-form semantics. With this feature, a KG has the ability to integrate diverse data into a common format.

Ontology Based Knowledge Representation

An ontology means a representation, formal naming and definition of the various categories, properties and relations between the concepts, data and entities that make one, many, or all domains of discourse (Gayathri and Uma, 2018). The Resource Description Framework (RDF) (Tripathi, 2001) is a family of World Wide Web Consortium (W3C) specifications originally designed as a metadata data model. In the RDF model, a semantic triple, or RDF triple, or simply triple, is the atomic data entity. As its name indicates, a triple is a set of three entities that codify a statement about semantic data in the form of subject–predicate–object expressions. We propose to use Neosemantics as a linked toolkit for Neo4j and RDF-linked data ontologies to extract knowledge from data before converting it into a semantic KG. The agents can be programmed to extract knowledge from data and convert that knowledge into semantic triples which it then stores in a hierarchical KG. These will be integrated to provide ontology-based background knowledge about the medical domain in the proposed framework.

Agent Based Model (ABM)

An agent is a computer program that can adapt to a certain kind of environment and is capable of autonomous actions to meet its designed objectives (Bolliger, 2006); multiple agents can

cooperate on collective and complex tasks. When a distributed system needs to synchronize its behavior with multiple entities, an agent-based approach is general and powerful (Niazi and Hussain, 2011) as it enables complex interaction between different stakeholders. The dynamic consensus of the system arises from the interaction of agents whereby the behavior of the agent is determined by the common cognitive structure. In addition, the ubiquity and multilateral view of the agents results in a larger vision and often offer a better overall result in terms of quality.

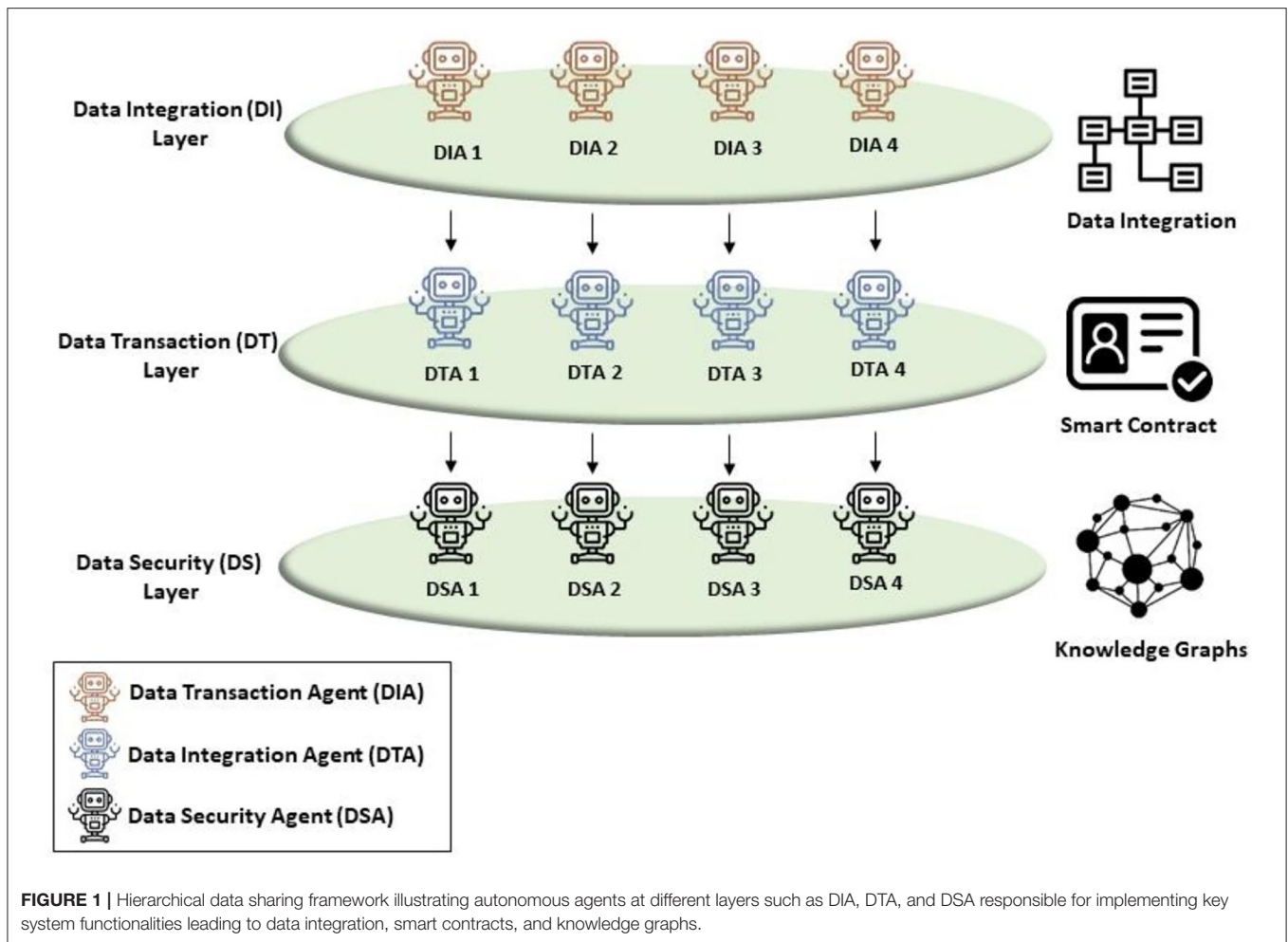
In many recent research projects, using agent-based systems to help the blockchain application has been proposed (Kaligotla and Charles, 2018; Pinheiro et al., 2018; Braga et al., 2019). The data-sharing processes of our framework are defined by the knowledge from hierarchical knowledge graphs. The top level of knowledge concerns the profile of each stakeholder, the corresponding permission credentials and the types of interaction between stakeholders. This knowledge is stored on the global KG, which is shared with all stakeholders on the blockchain.

In this study, the role of stakeholders is corresponding to the particular type of users in the data-sharing framework. For instance, the possible roles can be patient, doctor, pharmacist, lab researchers, and so on. An individual user may have multiple roles, as someone could be both a patient and a doctor at different times, but each of the roles has a unique way of sharing and regulating their own data. This means the users need to create a particular schema of data for each of their roles even if it may point to the same local data. For example, a user who is both a patient and a doctor would likely have the same personal name for both roles. Each given role of possible stakeholders has to comply with the consensus on blockchain, but the individual user also can customize data regulation rules based on the given template and functions. All these data schema setting descriptions will be packed into the local KG which will be updated as a node on the global KG. Through this, each user will control the view of their data under the particular role of stakeholders in data sharing.

Each stakeholder can develop its own local knowledge at a lower level and subsequently update any sharable knowledge, which includes setting the related smart contracts (Bhargavan et al., 2016; Knecht and Stiller, 2017; O'Connor, 2017), agents that can manipulate the knowledge on the hierarchical KGs, and any data descriptions into the global KG. All updated knowledge from stakeholders will be regarded as transactions on the blockchain and all such knowledge will then be processed by integration agents into the global KG, before broadcasting the update to all nodes in the network.

After the stakeholders have approved the new transaction, the new principles and knowledge will be updated and confirmed on the blockchain. Based on the corresponding permission credential, each stakeholder may receive a different updated version of KGs and that gives a hierarchical structure of the KG. However, for common global knowledge, all stakeholders always keep a compatible version on the blockchain. For different transactions, the system will activate different agents to respond.

The agent-based modeling of the proposed framework will lead to the automation of certain key processes, such



as integrating knowledge from different databases at the data integration layer, establishing consensus-oriented communication and regulation at the data transaction layer, and generating semantic knowledge graphs at the data security layer as shown in **Figure 1**. When a user submits an application or request, the corresponding agents on the client side will be activated by the behavior of users and start to collect the data from its accessible local dataset. After reading the data from datasets and users, they decide if there is a need to make a transaction. If so, the corresponding agent will extract knowledge from the data and convert it into semantic triples.

Such semantic triples can describe the context and entities that are related to the corresponding transaction. In our proposal, the semantic triples will be encrypted and packed into a blockchain transaction with the signature of agents. The transactions will be broadcasted to all nodes on the blockchain and verified with these nodes. A Practical Byzantine Fault Tolerance (PBFT) (Castro and Liskov, 2002) algorithm can ensure congruence of every transaction. PBFT is the recommended consensus mechanism for strongly secure domains such as healthcare to help avoid any system failures.

Layered Implementation of Proposed Approach

The layered approach of the proposed system (see **Figure 2**) adheres to universal standards followed in the healthcare ecosystem. The application layer is responsible for collecting data from multiple sources which will be represented by the standard vocabulary terms according to Systematized Nomenclature of Medicine - Clinical Terms (SNOMED-CT) (Lee et al., 2014). These nomenclatures will be embedded in the data transaction agents responsible for initializing and establishing smart contracts among various stakeholders of the ecosystem. The Health Insurance Portability and Accountability Act (HIPAA) protocol, designed in 1996 (Institute of Medicine (US) Committee on Health Research the Privacy of Health Information: The HIPAA Privacy Rule et al., 2009), caters to the possibility of patients predefining a set of records that may be shared amongst clinicians in the event of them being unconscious or otherwise rendered incapable of granting permissions.

The agents of the system are embedded with instructions to carry out this protocol so that, in such scenarios, they will automatically initiate a session on behalf of the patient and attend clinicians to enable data sharing. The interoperation

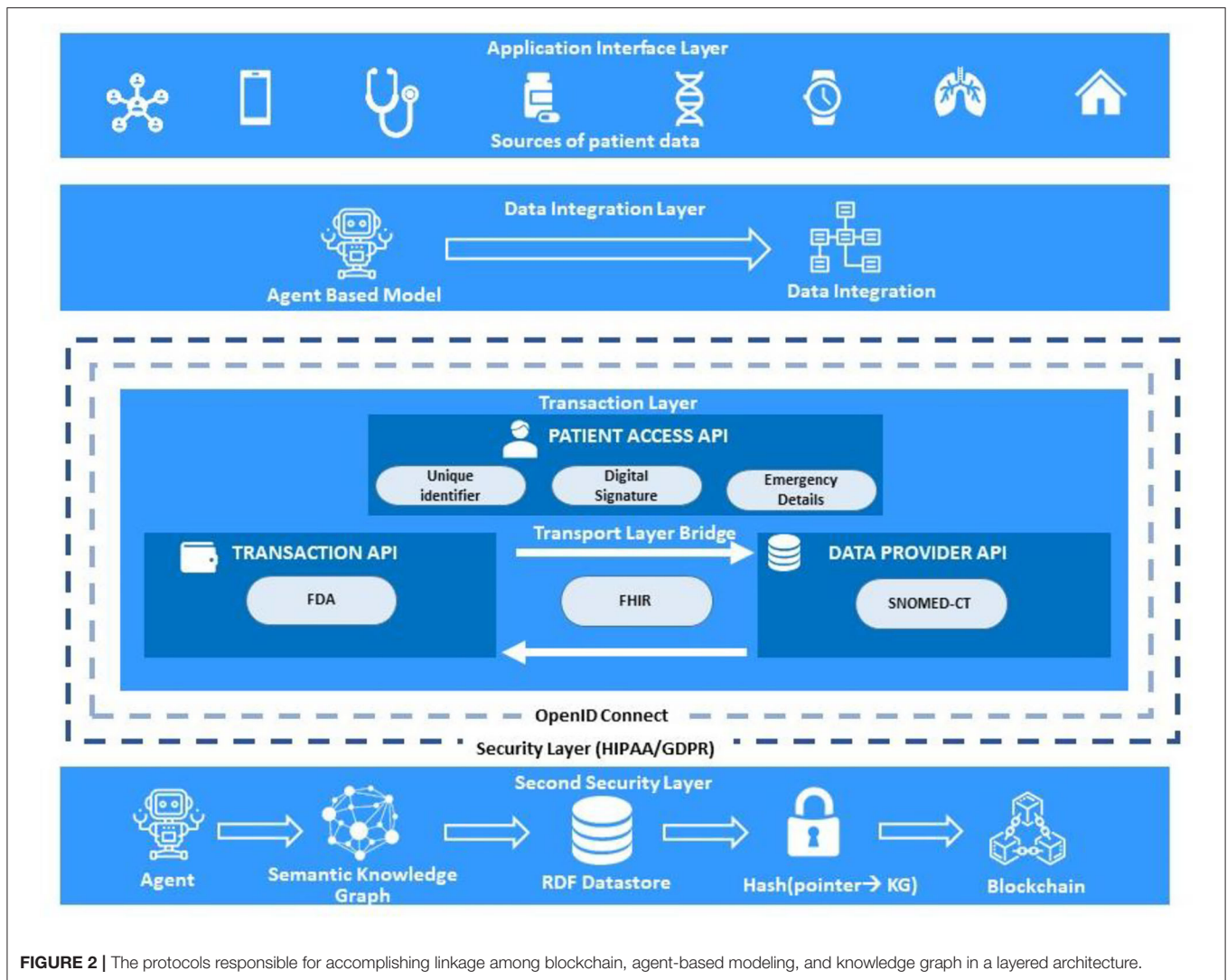


FIGURE 2 | The protocols responsible for accomplishing linkage among blockchain, agent-based modeling, and knowledge graph in a layered architecture.

among stakeholders would be achieved through embedding the data integration agents with the protocol rules as specified in Fast Healthcare Interoperability Resources (FHIR) (Walinjkar, 2018). Access to the permissioned Ethereum network would be authenticated through by OpenID Connect³ to ensure the sharing of data for a specified limit of time with a token-generation system which will be further automated by multi-agent systems. The transactions as submitted and confirmed on blockchain will be immediately accessible to the patient by the nodes in the network. Unauthorized access of data will also be stored in audits to keep track of any malicious access. All these events occur at the transaction layer. The data sharing will follow either the General Data Protection Rule (GDPR) for European continent and HIPAA for the United states of America.

These protocols will enable the stakeholders to implement sophisticated data sharing transactions. The data accessing regulation, approaches and format can be customized by the

stakeholders and the concrete application will be implemented, respectively as it is described on knowledge by smart contracts. For large data sharing issues, the storage cost could be shared based on the consensus between the potential customers who are the users who request data. Such consensus can be reached through negotiation of stakeholders and this negotiation process will be also updated as transactions on blockchain. Once consensus is reached and approved by all stakeholders, it will be implemented by the corresponding smart contracts and programs. The framework only provides users a platform to reach the consensus and protect data sharing between stakeholders.

DISCUSSIONS

Integration of blockchain with KG driven by automated agents make the proposed system robust with multi-layer security offering the following enhanced features:

- *Data sharing:* Derivation of KGs by automated multi-agent systems makes data sharing possible while maintaining data

³Recordon, D., Fitzpatrick, B.: OpenID Authentication 2.0 | Final. (2007) http://openid.net/specs/openid-authentication-2_0.html.

security and confidentiality. The KG only extracts the relevant data related to the patient transaction while the multi-agents are responsible for maintaining authentication, authorization, and integration.

- **Three-fold security architecture:** The proposed system ensures 3-fold security validations of the patient data along the three tiers of the framework.
 - **Encryption of data:** The data stored in off-chain storage or centralized cloud is encrypted with the private key of the patients, ensuring they have full access to and rights over their personal data. The encryption also ensures the data cannot be accessed even if the network is hacked. Only the partial details will be available to the hacker as only the index is stored on the blockchain. For viewing the data, only a patient's ID and permission will be needed to access the data.
 - **User authentication:** The authentication mechanism is designed to establish a connection between different stakeholders, and they are validated through smart contracts. The smart contract verifies permissions through an access control list defined at the configuration level which maintains a database of valid unique identifiers of all the stakeholders participating in the network.
 - **Session integrity with smart contracts:** The transaction details between patient and healthcare provider are stored in the form of smart contracts in the off-chain storage with encryption that can only be accessed with patient's consent.

The proposed system will augment or interact with existing information technology systems that perform gatekeeping (such as firewalls, user authentication systems) and there are critical third-party programs that perform these functions. The proposed model can easily be converted to a business architecture with the introduction of assets or incentive mechanisms (Bierer et al., 2017) in the network. Possible incentive mechanisms in our proposed systems could be any or all of the below:

- **Generation and validation of quality data:** Various sources of data like the use of smart apps related to healthcare tracking can help in generation of quality patient data to upload on the network. The data generated will be validated using algorithms such as information entropy (Xiaoyan et al., 2019) to measure the usefulness and uniqueness of the shared information. If the quality of data meets the prescribed standards, the patient can be incentivised by issuing tokens or credits on insurance policies.
- **Fast retrieval of stored data:** The efficiency of the nodes to retrieve the data when needed, following the Proof of Retrievability (PoR) (Ren et al., 2018) will be directly proportional to the number of credits or tokens earned by the node.

In this article, we present a framework that uses an agent-based system and a KG to improve customized data sharing using blockchain. This proposed framework provides a potential interdisciplinary solution for data sharing in healthcare. Due to the high sensitivity, privacy, and complexity of health

records, sharing data among multiple healthcare stakeholders is very challenging, but important to implement. Our proposed framework has the potential to provide a safe and secure sensitive EHR data sharing by allowing distributed storage. Here each owner customizes data accessing policies. The system can thus be configured to provide a secure, efficient, transparent, and tractable data sharing schema with multiple stakeholders through blockchain. With the high Byzantine fault tolerance and agent-based knowledge integration, the discussed structure will show a great robustness, flexibility, and extensibility for the general EHR data sharing under a complicated context.

This paper provides a promising solution for data sharing in healthcare that is broad enough to be useful for data sharing tasks in other sensitive domains. The proposed framework has the potential to overcome challenges in the current healthcare system and help to extend the efficiency of the system by sharing the data and knowledge safely. This will be especially helpful to society when confronting significant public health issues such as the Covid-19 pandemic. The trade-off between privacy, security and efficiency is an increasingly important balance for modern society, however, with this framework, we introduce a patient-centric model to enable data interchange among all stakeholders of the health ecosystem, which could enable collaborative clinical decision-making in telemedicine and precision medicine.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

YY provided inputs on agents and knowledge integration framework. MK provided inputs on EHR with blockchain. GV provided inputs on ethical issues. JD advised on blockchain concepts. CR advised on the structure of manuscript and reviewed the final manuscript. All authors coordinated equally in writing manuscript and approved the manuscript.

FUNDING

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie). This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 754489.

ACKNOWLEDGMENTS

We are thankful to the Chief Editor and the Reviewers for providing critical insights towards developing the manuscript.

REFERENCES

- Afanasyev, I., Kolotov, A., Rezin, R., Danilov, K., Mazzara, M., Chakraborty, S., et al. (2019). Towards blockchain-based multi-agent robotic systems: analysis, classification and applications. *arXiv [preprint]*. abs/1907.07433
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of The Thirteenth Eurosys Conference* (Porto: Association for Computing Machinery), 1–15. doi: 10.1145/3190508.3190538
- Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., et al. (2016). "Formal verification of smart contracts: short paper," in *Proceedings of ACM Workshop on Programming Languages and Analysis for Security* (Vienna). doi: 10.1145/2993600.2993611
- Bierer, B. E., Crosas, M., and Pierce, H. H. (2017). Data authorship as an incentive to data sharing. *N. Engl. J. Med.* 376, 1684–1687. doi: 10.1056/NEJMs1616595
- Bolliger, J. (2006). "Individual-based modeling and ecology," in *Landscape Ecology*, eds V. Grimm and S. F. Railsback (New York, NY: Springer), 317–318. doi: 10.1007/s10980-006-9008-z
- Braga, J., Silva, J. N., Endo, P. T., Ribas, J., and Omar, N. (2019). Blockchain to improve security, knowledge and collaboration inter-agent communication over restricted domains of the internet infrastructure, with human interaction. *Braz. J. Dev.* 5, 9013–9029. doi: 10.34117/bjdv5n7-103
- Brown, R., Carlyle, J., Grigg, I., and Hearn, M. (2016). Corda: An Introduction. Buterin.
- Buterin, V. (2015). A Next-Generation Smart Contract and Decentralized Application Platform.
- Capece, G., and Lorenzi, F. (2020). Blockchain and healthcare: opportunities and prospects for the EHR Sustainability 12:9693. doi: 10.3390/su12229693
- Castro, M., and Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* 20, 398–461. doi: 10.1145/571637.571640
- Daraghmi, E., Daraghmi, Y., and Yuan, S. (2019). Medchain: a design of blockchain-based system for medical records access and permissions management. *IEEE Access.* 7, 164595–164613. doi: 10.1109/ACCESS.2019.2952942
- Ehrlinger, L., and Wöß, W. (2016). *Towards a Definition of Knowledge Graphs*. Leipzig: SEMANTICS.
- Fensel, D., Simşek, U., Angele K, Huaman, E., Kärle, E., Panasiuk, O., et al. (2020). "Introduction: what is a knowledge graph?" in *Knowledge Graphs*, eds G. Qi, H. Chen, K. Liu, H. Wang, Q. Ji, and T. Wu (Cham: Springer), 1–10. doi: 10.1007/978-3-030-37439-6_1
- Gayathri, R., and Uma, V. (2018). Ontology based knowledge representation technique, domain modeling languages and planners for robotic path planning: a survey. *ICT Express.* 4, 69–74. doi: 10.1016/j.ict.2018.04.008
- Greenspan, G. (2013). *MultiChain Private Blockchain - White Paper*, 1–17.
- Heston, T. (2017). A case study in blockchain health care innovation. *Int. J. Current Res.* 9, 60587–60588. doi: 10.22541/au.151060471.10755953
- Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, Nass, S. J., Levit, L. A., and Gostin, L. O. (eds.). (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: National Academies Press.
- Julienne, H., Lavin, C., Belton, C., Barjaková, M., Timmons, S., and Lunn, P. D. (2020). *Behavioural Pre-testing of COVID Tracker, Ireland's Contact-Tracing App*. doi: 10.31234/osf.io/9cguq
- Kaligotla, C., and Charles, M. M. (2018). "A generalized agent based framework for modeling a blockchain system," in *2018 Proc Winter Simul Conf (WSC)* (Gothenburg). doi: 10.1109/WSC.2018.8632374
- Knecht, M., and Stiller, B. (2017). "SmartDEMAP: a smart contract deployment and management platform," in *Security of Networks and Services in an All-Connected World* (Zurich: Springer International Publishing), 159–164. doi: 10.1007/978-3-319-60774-0_15
- Lee, D., Keizer, N., Lau, F., and Cornet, R. (2014). Literature review of SNOMED CT use. *J. Am. Med. Inform. Assoc.* 21, e11–e19. doi: 10.1136/amiajnl-2013-001636
- Medicalchain.Com (2018). Available online at: <https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf> (accessed March 02, 2021).
- Morley, J., Cowsls, J., Taddeo, M., and Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature* 582, 29–31. doi: 10.1038/d41586-020-01578-0
- Nakamoto, S. (2009). *Bitcoin P2P E-cash Paper*. *The Mail Archive*. Available online at: <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html> (accessed February 08, 2021).
- Niazi, M., and Hussain, A. (2011). Agent-based computing from multi-agent systems to agent-based models: a visual survey. *Scientometrics* 89, 479–499. doi: 10.1007/s11192-011-0468-9
- O'Connor, R. (2017). "Simplicity: a new language for blockchains," in *Proceedings of the 2017 Workshop on Programming Languages and Analysis for Security* (Dallas, TX: ACM). doi: 10.1145/3139337.3139340
- Pinheiro, P., Macedo, M., Barbosa, R., Santos, R., and Novais, P. (2018). "Multi-agent systems approach to industry 4.0: enabling collaboration considering a blockchain for knowledge representation," in *PAAMS* (Toledo). doi: 10.1007/978-3-319-94779-2_14
- Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., and Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mobile Inform. Syst.* 2018, 1–10. doi: 10.1155/2018/6874158
- Tandon, A., Dhir, A., Islam, N. A. K. J., and Mäntymäki, M. (2020). Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* 122:103290. doi: 10.1016/j.compind.2020.103290
- Tripathi, A. (2001). Resource Description Framework (RDF) for organised searching on internet. *DESIDOC Bull. Inf. Technol.* 21, 3–7. doi: 10.14429/dbit.21.4.3545
- Van Der Sloot, B., Hoofnagle, C. J., and Zuiderveen Borgesius, F. J. (2019). The European Union general data protection regulation: what it is and what it means. *Inf. Commun. Technol. Law* 28, 65–98. doi: 10.1080/13660834.2019.1573501
- Walinjkar, A. (2018). FHIR tools for healthcare interoperability. *Biomed. J. Sci. Tech. Res.* 9:1863. doi: 10.26717/BJSTR.2018.09.001863
- Xiaoyan, L., Wanghu, C., Jing, L., Yuxiang, M., and Zhen, T. (2019). Incentive mechanism of medical data sharing based on information entropy in the blockchain environment. *J. Phys.* 1302:022056. doi: 10.1088/1742-6596/1302/2/022056

Conflict of Interest: GV was employed by company Principal Global Services, Pune, India.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright © 2021 Yao, Kshirsagar, Vaidya, Ducreé and Ryan. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.