LUPINE PUBLISHERS

Current Trends in Computer Sciences & Applications

DOI: 10.32474/CTCSA.2023.02.000141

ISSN: 2643-6744

Review article

Towards Consensus Algorithm for Healthcare Management Systems in Blockchains

Fabricio R Freire[1], William F Giozza[2] and Carlo K da Silva Rodrigues[3]*

[1]*Professional Postgraduate Program in Electrical Engineering (PPEE), Brazil*

[2]*Electrical Engineering Department, Brazil*

[3]*Center for Mathematics, Computing and Cognition, UFABC, Brazil*

***Corresponding author:** Carlo K da Silva Rodrigues, Center for Mathematics, Computing and Cognition, UFABC, Brazil

Received: December 21, 2022 **Published:** January 25, 2023

Abstract

Medical-hospital records produced by computational management systems must ensure confidentiality, integrity, and availability of information. Literature studies point to the Blockchain technology as a promising candidate to accomplish these needs. Among the various functionalities existing in Blockchain-based systems, one of them is the consensus mechanism. Within this context, this article proposes enhancing the H-BFT consensus algorithm. The operation of this new algorithm is demonstrated by exploiting two case studies which briefly address the Brazilian SUS and the US Medicare-Medicaid, respectively. At last, general considerations and suggestions for future work close this article.

Introduction

The systems responsible for managing medical information records from patients must allow adequate conditions for storage and analysis, providing subsidies for a better diagnosis and treatment [1-3]. These systems are complex [4,5] and must implement requirements to adequately provide integrity, confidentiality, and availability of medical records, besides processing large data volumes [6]. Blockchain technology shows great promise in the implementation of systems capable of dealing with common problems in the field of healthcare management [7-9]. It is defined as a distributed database, where records are stored in blocks [10], embedding elements such as cryptography, ledger, and consensus algorithms [11], besides owning properties such as immutability, integrity, transparency, availability, decentralization, and disintermediation [12]. Systems developed on Blockchain-based platforms need to establish an agreement between network nodes regarding the validity of transactions then carried out. The consensus occurs from the execution of algorithms that allow communication between the nodes of the Blockchain network, allowing unknown elements, or even competitors, to reach to an agreement regarding the previous and current state of the stored data. Within this context, this article proposes an enhancement of the H-BFT consensus algorithm [13] for use in healthcare management systems. Our proposal is the result of a theoretical study on the most important requirements for healthcare management systems based on Blockchain. The operation of this new algorithm is demonstrated by exploiting two case studies which briefly address the Brazilian SUS [14-16] and the US Medicare-Medicaid [17-19], respectively. The remainder of this article is structured as follows. Section "Literature Proposal" succinctly reviews the H-BFT algorithm. Section "Novel proposal" explains the enhancements we herein propose to the H-BFT algorithm, named as EH-BFT. Section "Performance Analysis" presents an overall discussion to highlight the benefits of the enhanced version of the H-BFT algorithm, by especially delving into two real case studies. This enhancement is named as EH-BFT algorithm. At last, Section "Conclusions and Future Work" present final remarks and gives directions for further research.

Literature Proposal

This Section brings the H-BFT protocol's motivations, briefly explaining its characteristics and advantages of its use in healthcare management systems.

Healthcare Management System based on Blockchain Requirements

In order to understand the biggest concerns in the development of solutions that could meet the needs of a healthcare management system based on Blockchain technology, a plethora of studies were carried out (e.g., [20-26] in which it was found that there was no definition regarding the type of consensus mechanism that could be used, but some characteristics were present in almost all of them. One of those characteristics was the use of private Blockchain networks, resulting from the need to restrict access to this type of information, valuing the privacy of data produced by medical diagnoses. Another feature was the preference for deterministic consensus algorithms over probabilistic models, for reasons such as the number of participants involved and lower computational cost. With the common characteristics identified in the frameworks aimed at healthcare management, five essential requirements were listed, which guided the specification of the H-BFT: confidentiality, integrity, availability, scalability, and security. Confidentiality is the guarantee of protection against undue access to information [27] and was the main focus of concern, both due to constant cyber-attacks and legal issues in countries such as Brazil [28,29] and the USA [30].

Another requirement of great importance was that of integrity, which is linked to the impossibility of changing data by unauthorized individuals, in order to avoid losses due to damage to this asset [31]. The concept of availability refers to the guarantee of access to data by people authorized to do so, whenever necessary, and the system needs to guarantee the continuity of its services and timely responses [8]. Scalability can be defined as the ability of a system to preserve quality in the delivery of its services, even if there is an increase in the number of customers [32], and security pivotally relates to protect the system against any type of attack. For instance, the implementation of a system based on Blockchain technology needs to establish implementations that seek to mitigate already identified vulnerabilities, such as those that allow exploitation of the network by Sybil-type attacks [33,34]. where a node maliciously tries to take control of the network by creating other nodes linked to it [35].

H-B FT algorithm features

The Byzantine Fault Tolerance to Health (H-BFT) consensus mechanism was proposed to meet the identified high-level requirements, incorporating features that aim to meet the already established needs of confidentiality, integrity, availability, scalability and security. It is a voting-based and Byzantine fault-tolerant algorithm, inspired by the PAXOS algorithm [36]. Three distinct roles are presented during the execution of the H-BFT: leader, acceptors and verifiers. The leader receives the values and proposes them to obtain consensus; acceptors are responsible for choosing the proposed value, and verifiers are responsible for the list of reliable nodes in the network. A feature of H-BFT is the creation of a list of reliable nodes, asynchronously by verifiers, applying a reputation algorithm [37]. The purpose of this is to mitigate possible Sybil attacks by establishing quality control over the nature of the elements that will be able to vote and receive votes.

To meet the scalability criterion and solve a common problem in voting-based consensus mechanisms, the H-BFT brings the concept of continuous slicing to obtain consensus, which was inspired by the idea of quorum slicing in the FBA algorithm [38,39]. This principle establishes that consensus occurs from a minimum quorum of reliable nodes in the network, expressed by the formula $[(T - i)/2] + 1$, where T is the total number of individuals verified and i the individuals already selected. If consensus is not obtained in a round, a new execution is performed, applying the same criteria for obtaining the minimum quorum. Moreover, H-BFT uses the reputation concept described in the dB FT algorithm [40] and, added to the list of verified nodes, proposes a Peer-to-Peer (P2P) classification mechanism dynamically selecting respectable nodes [37]. With this, it is possible to replace the leader after a certain time has elapsed.

Algorithm Workflow

The H-BFT is an algorithm with a three-stage flow, which starts when the leader receives a proposal to insert a new record, then messages are exchanged with the verifiers to provide the list of trusted nodes. After the

procedures for obtaining the list, the leader sends a pre-prepare message to the constant acceptors in the quorum slice. The remaining steps may be then noted in the algorithm execution:

a) When an acceptor receives the message, it checks its local database to confirm its integrity, after which it responds to the leader with a pre-prepared response message, informing that it is ready to start the consensus round.

b) The leader evaluates the number of responses received and, if the quorum is still not enough for consensus and there are still honest nodes in the network, it executes the flow from the beginning; otherwise, it sends a prepare message to each acceptor that responded. The acceptors receive the prepared message and acknowledge it to the leader.

c) The leader receives responses from acceptors and sends a commit message to the acceptors that responded. The acceptors confirm the transaction after receiving the commit message sent by the leader, send a response message and update their bases.

Finally, Figure 1 shows message exchanges between network nodes during the execution of H-BFT, representing the routine to obtain consensus among network nodes.

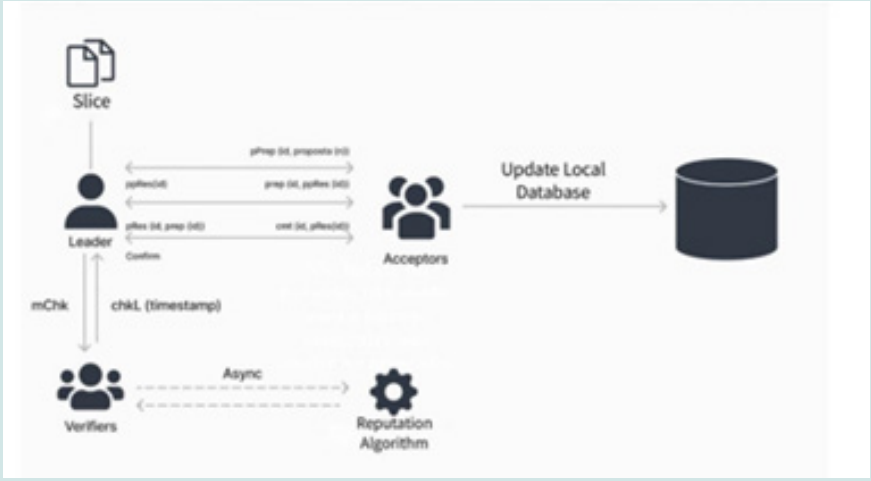

Figure 1: H-BFT workflow (originally presented in [13].

EH-BFT Algorithm

The Byzantine Fault Tolerance to Health Enhanced (EH-BFT) algorithm has two modifications comparing to the H-BFT algorithm. The proposed modifications are associated with the optimization of the database versioning and adjustments in the execution flow to avoid its anomalous functioning during its execution. The two modifications are shown in the following. Additionally, all its steps are detailed in Table 1. One may note that the proposed modifications increase routines, seeking to improve the original algorithm by granting security and consistency of the stored information, without forgetting the original goal of adequately supporting healthcare management systems.

Table 1: H-BFT Algorithm's Specification.

Role	Action
Leader	1. Receives proposal from a client
	2. Send mChk message to network verifiers
Verifier	3. Receive mChk message
	4. Returns chkL(timestamp) and database version
Leader	5. Wait for chkL from verifiers
	6. IF received chkL is expired THEN discard chkL ELSE update local chkL END
	7. Select proposal(n)
	8. Check database version
	9. IF leader database version is outdated THEN update database
Acceptor	10.IF proposal(n) already exists in database THEN discard proposal(n) ELSE send pPrep(id, proposal(n)) to acceptors(slice)
	11. Receives prep (id, proposal(n)) message
	12. Check your local database
Leader	13. IF base is correct THEN send ppRes(id) to leader END
	14. Receive ppRes(id) message
	15. IF quorum is not enough for consensus and there are still reliable nodes in the network THEN Return to Action 2
	ELSE Send prep (id, ppRes(id)) to whoever answered END
Acceptor	16. Get prep (id, ppRes(id)) message
	17. Send pRes (id, prep(id)) to leader
Leader	18. Receive pRes (id, prep(id)) message
	19. Send cmt (id, pRes(id)) message to acceptor
Acceptor	20. Receive cmt (id, prep(id)) message
	21. Confirm the transaction (cRes message)

Leader	22. Update base
	23. Send mUpt (id, timestamp) message to verifier
Verifier	24. Receive mUpt(id, timestamp) message
	25. Store database version

a) The first modification is in the role played by verifiers, which were originally only responsible for maintaining the list of trusted nodes. With the EH-BFT, they gain one more attribution, which is to maintain the most current version of the database, and with that, together with the message requesting the list of suitable nodes, the most recent version of the database will be sent. In the end of the consensus round, the verifiers will keep the current state of the ledger.

b) The second modification is in the routine executed by the leader to verify the current status of the records, the proposal received with the existing records the database received from the verifier, seeking to mitigate problems like double spending.

Performance Analysis

This Section presents a general discussion, highlighting the benefits presented by the EH-BFT. To this end, we consider two real case studies, namely the Brazilian Public Healthcare System [35] [36][37] and US Medicare-Medicaid [18,19].

Case: SUS

The Brazilian Public Healthcare System (SUS) is a healthcare system designed to guarantee medical-hospital care to approximately 215,491,518 people [41] free of charge, from simple medical appointments, exams or transplant of organs [42]. Its performance is based on three pillars: promotion, protection and recovery of health, with activities ranging from promoting quality of life, reducing/eliminating health risks to early diagnoses for timely treatment [37]. The structure of the SUS is organized into Basic Healthcare Units, for outpatient care, Emergency Care Units, for less complex urgent and emergency care, and Public Hospitals or clinics, which provide any type of care and have resources to perform complex procedures [43]. The SUS still has public laboratories and maintains an agreement with private healthcare institutions, to complement the services [36]. An Electronic Health Record-EHR is created for every citizen in their first consultation [38], which will accompany them throughout their lives and will be accessed during consultations by the medical professional responsible for the care, except in cases where that the consultation is carried out at a private institution with an agreement. The current model adopted by SUS for EHR management has some shortcomings, which generate bottlenecks in access to the platform that manages patient information, cause insecurity in the maintenance of diagnoses and procedures performed, in addition to not guaranteeing consistency of data stored in its bases. The data produced during medical appointments are accessible only at the place of care, that is, if the patient moves to another state, the healthcare professional who will assist him will not have access to his medical history and access to patient information is limited, carried out without the use of more robust security mechanisms, restricting itself to the use of username and password.

In the context of SUS, the use of the EH-BFT algorithm (Figure 2), would bring the following benefits.

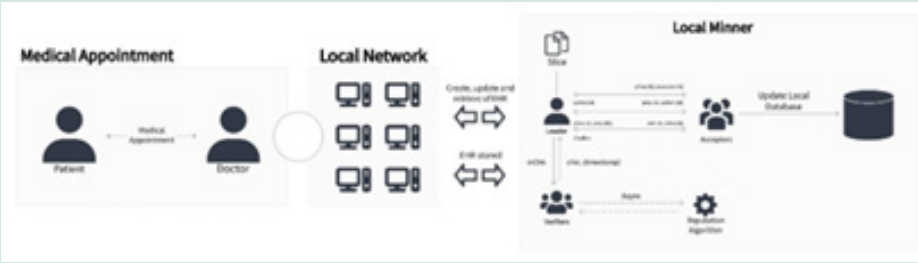

Figure 2: Healthcare Management System Architecture with EH-BFT.

a. The first benefit is linked to the concept of availability of patient information, so that the patient or the healthcare professional responsible for the care can access the medical history quickly, allowing for accurate diagnoses and saving resources, as the treatment would already be more effective, no waste. The decentralized structure, characteristic of Blockchain-based systems, would allow access to the information managed by it anywhere and at any time.

b. Another extremely important factor concerns the integrity of the stored data. The use of EH- BFT would guarantee the consistency and veracity of the records, since the records would be immutable and non-redundant, inserted from the agreement established between the nodes. The consensus mechanism would not only guarantee the veracity of the data, but it would also bring confidence to the professional responsible for the diagnosis.

c. The issue of scalability, something of great impact in a Blockchain network with the size necessary to serve the SUS,

is handled by the EH-BFT when it performs the continuous slicing of the quorum necessary for approval of the insertion of the proposed record, which would solve a difficult problem to measure in a healthcare management system of this size.

d. The confidentiality required of the information, through the LGPD [28], would be fully guaranteed, since the data circulating on the network is encrypted, and accessible only to those who need to do so, including the patient himself.

Case: Medicare and Medicaid

In the United States of America, the healthcare service is private [40], however, there are two assistance programs, maintained by the Federal Government. The first of these is Medicare [41], created in 1966 and aimed at people over 65, people with disabilities or those unable to work for some reason. It provides four types of service: Hospital insurance, medical insurance, extension coverage (maintained by companies to serve their employees) and medication coverage. Medicaid [42], on the other hand, was created to serve people below the poverty line, and is maintained entirely by the Federal Government and by the States. Each hospital or independent healthcare professional that provides care to the insured person will receive the reimbursement due, following a specific cost table, which never mirrors the reality of the market.

This model is extremely bureaucratic, since the government establishes different levels of demand, which means that many people do not get the necessary medical care. As there are no public hospitals, all care is provided by professionals and accredited establishments, which exponentially increases decentralization and redundancy in diagnoses. In the two American forms of public healthcare service, there is a large volume of appointments where professionals need to establish new diagnoses at each consultation, without a reliable base of medical histories, without integration between the two healthcare systems, which does not allow the availability of the data, it is not possible to assess the integrity of the records or the confidentiality of the diagnoses.

a) In the context of Medicare and Medicaid, the use of the EH-BFT algorithm (Figure 2), would bring the following benefits.

a. The first benefit of using a healthcare management system based on Blockchain technology would be the integration between the two public models of medical care, allowing the exchange of information produced by diagnoses made by healthcare professionals.

b. The dispersed nature of the services would make each establishment or healthcare professional a node in the Blockchain network, impacting scalability. This problem has already been solved by the EH-BFT during the routines carried out during its execution, in addition to that, the very decentralized model would guarantee availability for access to authorized persons at any time.

c. Keeping a single EHR available to everyone who needs access to it makes the more economical, faster, and more accurate diagnoses, bringing relief to the patient, in addition to savings and efficiency for the Government. This EHR would also be protected by the cryptography used by the Blockchain, which would guarantee the required confidentiality. In both case studies, the implementation of a healthcare management system based on Blockchain, which implements the EH-BFT, would bring performance benefits, cost reduction, accuracy in diagnoses, availability, and integrity of information, bringing benefits to citizens and for governments.

Conclusions and Future Work

This article presents an improvement proposal for enhancing the Byzantine Fault Tolerance to Health (H- BFT) algorithm. This enhancement, called Byzantine Fault Tolerance to Health (H-BFT), is characterized by optimizations in the flow of the algorithm and on its versioning control of the database. The EH-BFT maintains the specifications regarding continuous quorum slicing, role rotation, and generation of the list of suitable nodes, besides, it also assigns to the verifier the responsibility of controlling the version of the database in use by the system, which will be consulted at each necessary round for establishing consensus among network nodes. Additionally, to exemplify the deployment of EH-BFT, two case studies were herein presented, namely the Brazilian Unified Healthcare System and the US public healthcare systems Medicare and Medicaid, respectively. By means of the exploitation of these two scenarios, the effectiveness of the EH-BFT was demonstrated. As future works and being aware of this research's limitations, we suggest the execution of tests in simulated environments besides the implementation of the EH-BFT algorithm with the goal of validating the processes and results derived herein.

References

1. H Huru, Muhammad Tufailb, Ui Jun Baeka, Jee Tae Parka, Myung SupKima (2022) A novel blockchain-enabled heart disease prediction mechanism using machine learning. Computers and Electrical Engineering 101(1): 108086-108086.
2. E M Adere (2022) Blockchain in Healthcare and IoT: A Systematic Literature Review. Array 14(1): 100139-100142.
3. L Ismail, H Materwala (2020) Blockchain paradigm for healthcare: Performance evaluation. Symmetry 12(8): 1-19.
4. N Reibling, M Ariaans, C Wendt (2019) Worlds of healthcare: A healthcare system typology of oecd countries. Health Policy 123(7): 611-620.
5. M Dabbagh, Mohammad Dabbagh, Kim Kwang Raymond Choo, Amin Beheshti, Mohammad Tahir Nader, et al. (2021) A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. Computers Security 100(1): 102078-102078.
6. H Kaur, M Afshar Alam, Roshan Jameel, Ashish Kumar Mourya, Victor Chang (2018) A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. J Med Syst 42(8): 156-160.
7. S Qahtan, Khaironi Yatim, A A Zaidan, H A Alsattar, Os Albahri, et al. (2022) Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. IEEE Transactions on Industrial Informatics 18(9): 1-1.

8. S Y Lin, Lei Zhang, Jing Li, Li li Ji, Yue Sun (2022) A survey of application research based on blockchain smart contract. Wireless Netw pp. 635-690.
9. H Ghayvat, Munish c Sharma, Prosanta Gope, Pradip Kumar Sharma (2021) SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things. IEEE Transactions on Industrial Informatics 18(8): 5609-5618.
10. Z Zheng, Shaoan Xie, Hong Ning Dai, Xiang Ping Chen, Huaimin Wang (2018) Block chain challenge sand opportunities: survey. International Journal of Web and Grid Services v 14(4): 352-375.
11. F Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Augusto T R Coutinho, Italo Valcy da Silva Brito (2018) Blockchain e a Revolução do Consenso sob Demanda. Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. ed. XXXVI. c. 5.. Sociedade Brasileira de Computação pp. 1-53.
12. K Hasan, Mohammad Jabed Morshed Chowdhury, Kamanashis Biswas,Khandakar Entenam Unayes Ahmed, Md Saiful Islam, et al. (2022) A blockchain based secure data sharing framework for Software Defined Wireless Body Area Networks. Computer Networks 211(6): 109004-109010.
13. F R Freire, W F Giozza and C K S Rodrigues (2023) Proposta de um Algoritmo de Consenso para Plataformas Blockchain em Sistemas de Gestão de Saúde Privados. Revista Ibérica de Sistemas e Tecnologias de Informação.
14. J S Paim (2015) O que é o SUS. Editora Fiocruz. RJ.
15. Brasil (2018) Lei nº 13.787, de 27 de dezembro de 2018. Diário Oficial da República Federativa do Brasil
16. Brasil (2018) Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da República Federativa do Brasil.
17. ISPOR –Improve Healthcare Decision.
18. (2022) Medicare.
19. (2022) Medicaid.
20. K Azbeg, O Ouchetto, S J Andaloussi (2018) BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian Informatics Journal 23(4): 1-15.
21. G Dagher, Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella (2018) Ancile Privacy-preserving frameworkfor access control and interoperability of electronic health record susing block chain technology. Sustainable Cities and Society 39(1): 283-297.
22. S Singh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, Byungun Yoon (2022) A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems 129(2): 380-388.
23. G Tripathi, M A Ahad, S Paiva (2020) S2HS- A blockchain based approach for smart healthcare system. Healthcare 8(1): 100391-100395.
24. Z Bawany, Tehreem Qamar, Hira Tariq, Saifullah Adnan (2022) Integrating Healthcare Services Using Blockchain-Based Telehealth Framework. IEEE Access 10(1): 1-15.
25. K Miyachi , T K Mackey (2021) HOCBS: A Privacy preserving Blockchain Framework for Healthcare Data Leveraging an On-chain and Off-chain System Design. Information Processing & Management 58(3): 102535-102540.
26. M S Rahman, A Alabdulatif, I Khalil (2022) Privacy Aware Internet of Medical Things Data Certification Frameworkon Healthcare Block chain of 5G Edge. Computer Communications 192(1): 373-381.
27. C K S Rodrigues and P C Silva (2019). Uma análise de algoritmos de consenso para Blockchain visando à implementação de Sistemas de Informação Distribuídos e Transparentes. Revista de Sistemas e Computação. Salvador 9(1): 163-188.
28. Brasil (2018) Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da República Federativa do Brasil.
29. Brasil. (2018) Lei nº 13.787, de 27 de dezembro de 2018. Diário Oficial da República Federativa do Brasil.
30. U S (1996) Health Insurance Portability and Accountability Act of 1996. A S (ASPE) Public Law 104-191, 104th Congress. USA.
31. (2018) Iso Central and Secretary. Information technology security techniques information security management systems overview and vocabulary. Standard ISO/IEC TR 27000:2018. International Organization for Standardization. Geneva.
32. S Bouraga (2021) A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Systems with Applications 168(1): 114384-114389.
33. N Neshenko, Elias Bou Harb, Jorge Crichigno, Georges Kaddoum, Nasir Ghani (2019) Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys and Tutorials 21(3): 1-33.
34. F Hashmat, Syed Ghazanfar Abbas, Sadaf Hina, Ghalib A Shah, Taimur Bakhshi, et al. (2022) An Automated Context-aware IoT Vulnerability Assessment Ruleset Generator. Computer Communications 186(1): 133-152.
35. M Iqbal, R Matulevicius (2021) Exploring Sybil and Double-Spending Risks in Blockchain Systems. IEEE Access 4(1): 1-25.
36. L Lamport (1998) The Part-Time Parliament. ACM Transactions on Computer Systems 16(2): 133-169.
37. R Zhou, K Hwang (2007) Power Trust: A Robust and Scalable Reputation System for Trusted Peer-to Peer Computing. IEEE Transactions on Parallel and Distributed Systems 18(4): 460-473.
38. Martin Florian, Sebastian Henningsen, Charmaine Ndolo, Björn Scheuermann (2022) The sum of its parts: Analysis of federated byzantine agreement systems. Distrib. Comput 35(1): 399-417.
39. André Gaul, Ismail Khoffi, Jörg Liesen, Torsten Stüber (2019) Mathematical Analysis and Algorithms for Federated Byzantine Agreement Systems. License pp. 1-42.
40. Q Wang, Rujia Li, Shiping Chen and Yang Xiang (2022) Formal Security Analysis on dBFT Protocol of NEO. Licence pp. 1-14.
41. (2022) Instituto Brasileiro de Geografia e Estatística.
42. (2022) Fiocruz-Pense SUS.
43. C K S Rodrigues (2021) Blockchain-Based Platform for Managing Patients Data in the Public Healthcare System of Brazil. Revista de Sistemas e Computação, Salvador 11(3): 63-72.

DOI: 10.32474/CTCSA.2023.02.000141