Journal of Electrical Engineering and Information Technologies, Vol. **7,** No. 1, pp. 33–42 (2022)
Article 194
In print: ISSN 2545–4250
Received: April 2, 2022
On line: ISSN 2545–4269
Accepted: April 29, 2022
UDC: 004.89:614.21
https://doi.org/10.51466/JEEIT2271194033k

Original scientific paper

DESIGN OF THE FUNCTIONAL ENTITIES OF THE BloHeS SYSTEM

Jovan Karamačoski, Liljana Gavrilovska

Faculty of Electrical Engineering and Information Technologies,
"Ss. Cyril and Methodius" University in Skopje,
Rugjer Bošković bb, P.O. box 574, 1001 Skopje, Republic of North Macedonia
jovankaramac@yahoo.com

A b s t r a c t: The increased number of Internet services and the exposure of the personal information to the public network, create a problem with the privacy of the personal data. This problem is extremely impactful in the healthcare systems where the sensitive medical data circulate in the network. The emerging Blockchain technologies offer properties and tools for better personal data access management. The integration of the Blockchain technologies into the healthcare systems can provide better data privacy. However, beside the attractive properties, the current Blockchain technologies cannot achieve sufficient scalability to serve a global public healthcare system and cannot provide compatibility with the GDPR and HIPAA regulations. To overcome these limitations, this paper introduces new deducted Blockchain-based public healthcare system, the BloHeS, with main focus on several functional entities, such as optimal consensus mechanism, better storage organization, improved network organization and compatibility with GDPR and HIPAA regulations. It also defines a procedure for patient-centric data access management, protocols for Island management and new block structure.

Key words: BloHeS; island management protocols; PBS structure; block structure; data access management

ДИЗАЈН НА ФУНКЦИОНАЛНИТЕ ЕНТИТЕТИ КАЈ СИСТЕМОТ BloHeS

А п с т р а к т: Зголемениот број сервиси на Интернетот и изложеноста на личните информации во јавната мрежа создаваат проблем со приватноста на личните податоци. Овој проблем е особено влијателен во здравствените системи, каде што чувствителни медицински податоци циркулираат низ мрежата. Новите Blockchain технологии нудат карактеристики и алатки за подобро управување со пристапот до личните податоци. Интеграцијата на технологиите Blockchain во здравствените системи може да обезбеди поголема приватност на податоците. Сепак, покрај атрактивните карактеристики, тековните Blockchain технологии не можат да постигнат доволна скалабилност за да опслужат глобален јавен здравствен систем и не можат да обезбедат компатибилност со регулативите GDPR и HIPAA. За да се надминат овие ограничувања, во овој труд се воведува нов дедуктивен на Blockchain базиран јавен здравствен систем, BloHeS, со посебен осврт на неколку главни функционални ентитети: дефинирање на оптимален консензуален механизам, подобра организација на складиштата, подобрена мрежна организираност и компатибилност со регулативите на GDPR и HIPAA. Во трудот исто така се дефинираат постапката на пристапот до основните податоци за пациент, протоколите за управување со нив и новата блок-структура.

Клучни зборови: BloHeS; протоколи за управување со острови; PBS структура; блокструктура; управување со пристап до податоци

INTRODUCTION

The decade of huge expansion of Blockchain technologies and their implementation in a wide variety of applications exposes a challenge to design an appropriate application for a global healthcare system. The promising characteristics of the Blockchain technologies and the immense problems to obtain privacy over the medical data are the main reasons for the fusion between the Blockchain technologies and

the healthcare systems. The public healthcare systems are especially attractive due to generated and stored sensitive personal medical records. The current public healthcare systems are cloud-based solutions, which cast a shadow to the privacy protection of the medical records.

The merge of the Blockchain technologies and the public healthcare systems can provide enhanced data protection, better private data management, longevity of the medical records, inability for deletion and modification of personal data, availability of the medical records anytime and anywhere. The general solutions for data access management built on top of the existing Blockchain technologies enable the *patient-centric* approach to this paradigm.

The patient-centric data access management will motivate and allow the development of new business ideas for the insurance companies and pharmaceutical companies. The insurance companies can offer new insurance packages based on the complete health status of the patient. Pharmaceutical companies can determine the effectiveness and potential side effects of their medication. Artificial intelligence agents can also contribute to the enhanced individual or group diagnostics.

This paper introduces the design of main functional entities for a global healthcare system solution that enables the patients to manage their private data, increase the mobility of the patients by enhancing the availability of the medical records, decentralizing the healthcare services and centralizing the data access management in the domain of the patient. This system can support the increased mobility of the patients and can provide universal services globally, allowing patients to receive medical care out of their home country. The implementation of a standard form of medical records and universal codes for diagnostics will allow automated translation of records and better interoperability. Furthermore application of machine learning algorithms can support better diagnostics. Additionally, the solution provides enhanced privacy, compliant with the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) regulations.

RELATED WORKS

The development of the healthcare systems went through several generations [1]. The last generation of the healthcare systems is generally *cloud-based*, but also introduces *Blockchain based mechanisms* for improving the data access management in order to enhance the data privacy. As reported in [2], the pure cloud-based solutions provide enhanced scalability but inferior security, privacy and real-time data access. Contrary, the pure Blockchain-based applications provide enhanced security, privacy and real-time data access, but with inferior scalability. The fusion of the Blockchain technology with the cloud-based applications can be designed in *encapsulated* approach (with improved scalability) or in *non-encapsulated* approach (with improved security, privacy and scalability). However, both approaches lack the real-time data access capabilities.

The Blockchain-based healthcare systems are either build as applications on top of the existing general-purpose Blockchain platforms or as a dedicated system solution. Among the Blockchain platforms, the Ethereum platform [3] is one of the most prominent. The applications use the Ethereum infrastructure and the benefits from the smart contracts to implement mechanisms for enhancing security, privacy and data access management. Additionally, the Ethereum network is widely known for low transaction throughput performance, expensive costs for transaction generation and long waiting times for transaction verification. Some of the most prominent solutions based on the Ethereum platforms are: Patientory [4] for electronic healthcare records management, MedRec [5] for medical record access management and FHIRChain [6] for clinical data sharing. However, sharing a general-purpose Blockchain platform with a healthcare system usually cannot deliver optimal solutions.

The development of a dedicated healthcare system based on a Blockchain technology in most of the cases relies on the Hyperledger Blockchain solutions [7]. The Hyperledger-based system uses the Blockchain-as-a-Service paradigm for solution development, where the major part of the necessary infrastructure is stored in a cloud-like fashion and it is under control of the Hyperledger Foundation. The development of a healthcare system based on some of the Hyperledger solutions can enable the system to have optimal performances, but the cloud-based approach for system development casts a shadow to the provided security and privacy of the personal data. Some of the Hyperledger-based healthcare systems are [8], [9], [10] and [11].

The next generation optimal Blockchain-based healthcare system requires development of a dedicated patient-centric data access management solution capable of providing enhanced data security and privacy [1]. It also needs to provide availability of

medical records anytime and anywhere with sufficient scalability and transaction throughput. The newly designed dedicated Blockchain-based healthcare system, called BloHeS, fulfills these goals. This paper provides design for main functional entities of the BloHeS. It defines several novel paradigms, such as: a new and optimal consensus mechanism that will allow improved scalability of the system, a description of an optimal storage organization that will improve the efficacy of the system storage, a definition of a patient-centric approach for enhanced privacy and data access management, definitions of clustering protocols for self-organizing validators, and a description of a new block structure and Personal vault with a wallet.

BloHeS CONSENSUS MECHANISM

The BloHeS is dedicated healthcare system solution based on Blockchain technology with hierarchical cluster-based architecture organization defined in [12]. The BloHeS system is organized from independent Federated networks which resemble the state border or healthcare system organization. The cooperation between the Federated networks is organized with smart contracts.

The BloHeS consensus mechanism [13] manages the Federated networks that implements hierarchical consensus cycling between the two types of independent consensus mechanisms, arranged in a two-layer organization. The BloHeS consensus mechanism is presented in Figure 1. The two independent consensus mechanisms are *Archiving* consensus mechanism and *Island* consensus mechanism. The Archiving consensus mechanism is the higher layer consensus mechanism implemented in the Archiving domain. The Archiving domain consists of a single Archiving cluster in the system. The Island consensus mechanism is the lower layer consensus mechanism implemented in the Island domain. The Island domain consists of multiple self-organized clusters called Islands. Every Island manages independent consensus cycle. The Island participants obligated to conduct the validation process are the healthcare practitioners' agents.

The Archiving and Island consensus mechanisms are based on the Tendermint consensus mechanism [14]. They are implementing the Tendermint's three-stage process for consensus achievement, but are introducing new entities such as: commitpool memory, dissemination and finalization phase and forwarding links for intercluster communication.

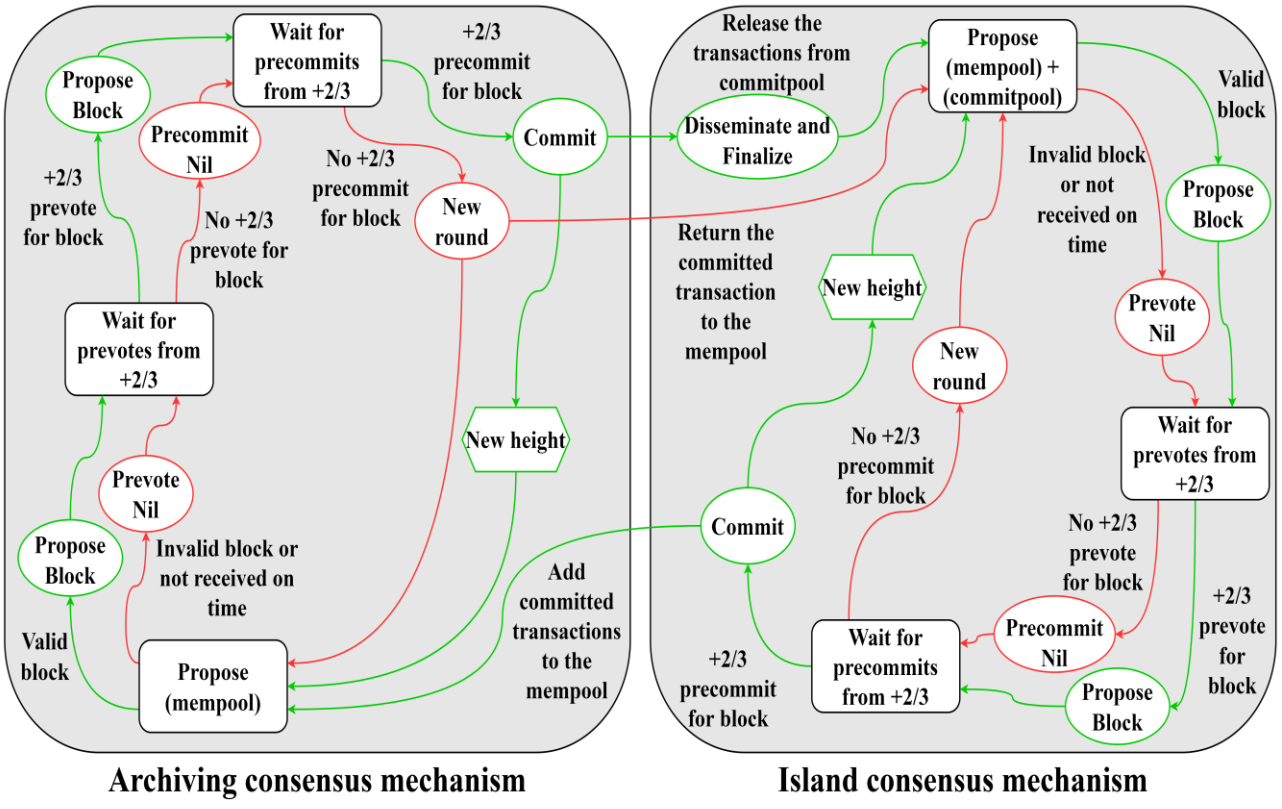

Fig. 1. BloHeS consensus mechanism

The *commitpool memory* is a new type of memory alongside the mempool memory (defined in the Tendermint consensus mechanism [15]) that is part of the Island consensus mechanism. The commitpool memory keeps the blocks that are committed by the Island consensus mechanism until the Island participants receive confirmation from the Archiving cluster for successful finalization of the block. The commitpool memory is independent for every Island.

The *dissemination and finalization* phase is a part of the Island consensus mechanism. During this phase, the Island proposer conducts a dissemination of the information from the Archiving consensus mechanism's committed block to every participant in the Island (in order to finalize the transactions that are part of that committed block).

The *forwarding links* connect the two types of consensus mechanisms. The lower layer Island consensus mechanism forwards committed blocks to the higher layer Archiving consensus mechanism for finalization. The higher layer Archiving consensus mechanism forwards notification for the outcome of the finalization process to the lower layer Island consensus mechanism. There are two possible outcomes from the finalization process: accepting the committed block or rejecting the committed block. Accordingly, the information is shared with the Island participants.

The BloHeS consensus mechanism, even based on Tendermint consensus mechanism, performs superior [13]. It shows decreased *message count* for transaction finalization leading to better scalability. The *protection capacity P* reflects the system ability to cope with the faulty nodes:

$$P = \sum_{k=1}^{n_i} f_k,$$

where the f_k is the maximum number of faulty nodes that can be tolerated by every Island and n_i is the number of Islands in the network. The BloHeS consensus mechanism asymptotically approaches the slightly better protection capacity achieved by the Tendermint consensus mechanism, in scenarios with larger Islands. The evaluation of the ratio between the message count and the protection capacity shows that the BloHeS consensus mechanism obtains much smaller message count compared to the Tendermint consensus mechanism, for similar protection capacity. A detailed analysis of the BloHeS consensus mechanism and its comparison to the Tendermint consensus mechanism considering several relevant parameters is available in [13].

BloHeS ISLAND MANAGEMENT PROTOCOLS

The organization of the validators in clusters has dynamic nature following the validators' activity. The validators are self-organizing to participate in the Island clusters implementing the *Island management protocols*. There are three Island management protocols: Node addition, Island splitting and Island merging protocol. The detailed procedures of the Island management protocols are introduced in [16].

The *Node addition protocol* main goal is to attach the newly added node to the most optimal cluster from a list of randomly selected clusters. This protocol allows the new node to become a validator in a cluster based on the network metric between the users and maximizing the performance of the Island consensus mechanism.

The main goal of the *Island splitting protocol* is to provide a mechanism to limit the maximum size of the Islands. The goal is to create Islands with acceptable performances and no more than 100 validators in the cluster [17, 18]. This protocol defines the maximum numbers of validators in an Island in order to avoid the network congestion from voting message exchanges.

The *Island merging protocol* main goal is to provide protection for the Island cluster from at least one faulty node. Such scenario considers that the smallest number of validators in the Island is four. At the moment when the number of validators in the Island falls to three, the Island is disintegrated and the validators from that Island are redistributed in other clusters.

The Island management protocols provide mechanisms for the validators enabling them to:

- Attach to the most optimal Island in order to improve the overall consensus mechanism performance;
- Manage Islands that are not over-sized in order to avoid problem of network congestion from voting message exchange;
- Manage Island consensus mechanism that can provide protection from at least one malicious validator.

Block structure

The block structure of the Island consensus mechanism and Archiving consensus mechanism are based on the Tendermint block structure [14] with essential changes introduced to adapt it to the BloHeS consensus mechanism design. The block structure of the Island consensus mechanism and the Archiving consensus mechanism are presented in Figures 2 and 3, respectively.

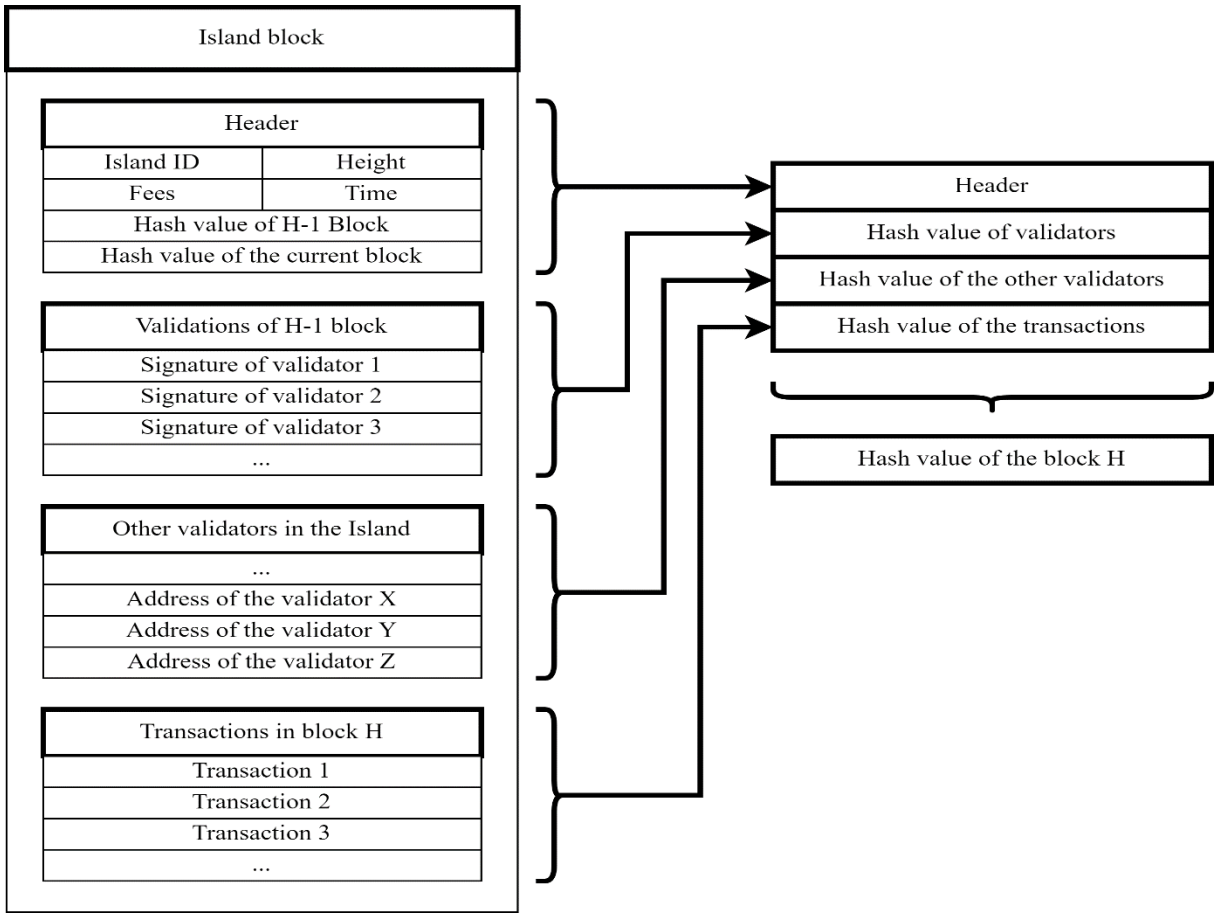

Fig. 2. Island Block structure

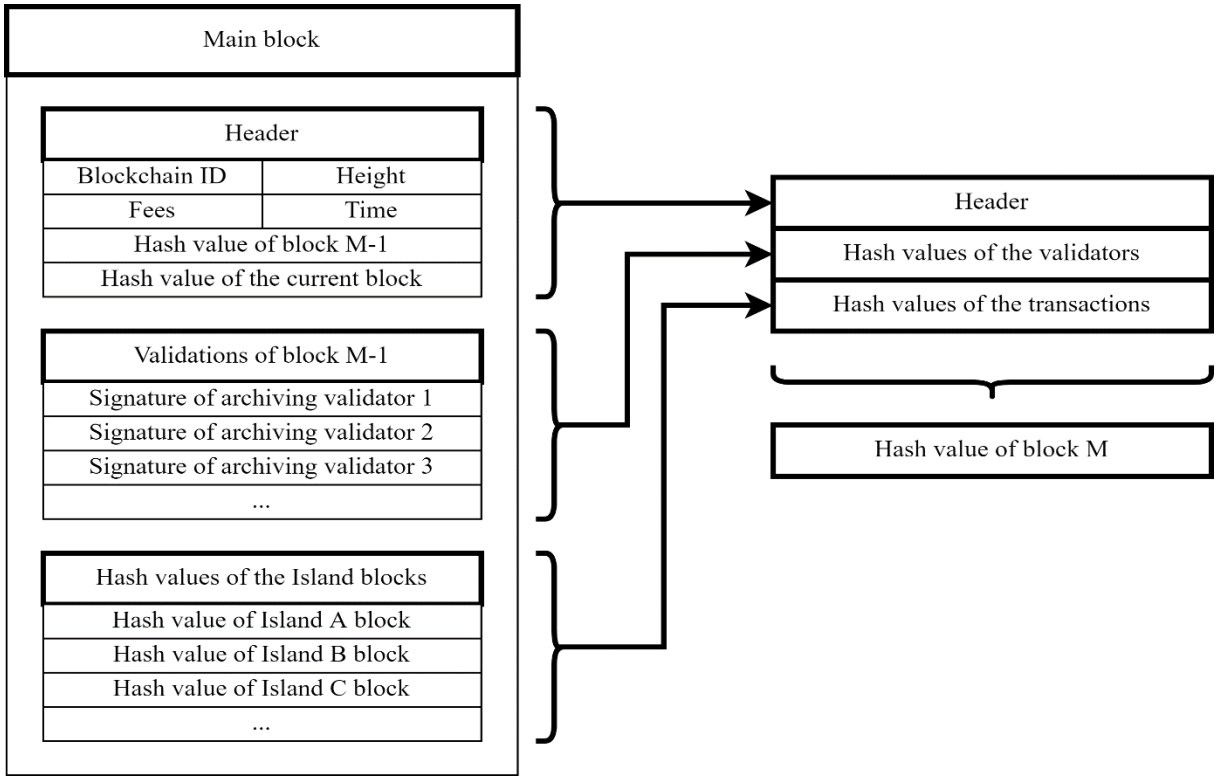

Fig. 3. Archiving cluster block structure

Every Island in the BloHeS network has a unique identifier, generated as a random number by the first proposer in the Island. The Island identification is important during the phase of transaction consolidation and block finalization, to mark the unique source of the block of information. The header of the block structure contains the height of the block, so the validators will be able to trace the consecutiveness of the generated and validated blocks. The height of the Island block structure has internal usage only and it is not correlated to the height of the main Blockchain. The hash value of the current state is also integrated into the header. The current state represents the Merkle root of the validators in the Island, the accounts of the participants in the Island, the additional information for validators and the registered names for the validators.

The Island block structure contains the signatures of the validators that support the validated block, but also the addresses of the validators that do not support the block, but are part of the Island. This extra information strengthens the security of the network and contributes to better defense from double-voting attack.

The Archiving cluster is managing the main Blockchain line, actually the main Blockchain database. The main Blockchain database is the Federal network database where the finalized block of transactions is stored. The records of the Federal network database are generated from the accepted committed blocks received from the Islands. Actually the records from the block of the Federated network database are the addresses from the validated transactions from the Islands. This approach allows the record to keep the location of the actual transaction, but not the content of the transaction. The committed blocks from the Archiving cluster are added to the Federal network database and are sent to the Island proposers. The proposers will disseminate the Archiving cluster committed blocks to the participants in the Island. If the proposer does not respond, the committed block is sent to the proposer from the previous round.

The distinct organization of the Island block structure and Archiving cluster block structure increases the security of the network and protects the network from double-voting attack. The introduction of complete list of participants in the Island block structure helps the Archiving cluster validators to check the Islands' committed blocks for malicious validators that are participating or voting in more than one Island. Furthermore, the Archiving cluster block structure offers significant storage space savings by keeping only addresses of the transactions, instead of the complete content of the transactions. The content of the transaction can be reviled upon request.

Personal Blockchain Stream and the BloHeS storage organization

The size of the global healthcare system requires smart storage organization. The data storage organization of the current Blockchain technologies assumes replication of the system data in every agent in the system. That approach enables the system to offer robust and reliable services, but it is a burden to scalability.

To improve the storage scalability, the BloHeS system introduces redefined approach for data storage, described in [12]. The data storage in the BloHeS system consists of two main databases: *Patients database* and *Common database*, where the Common database is further divided into: *Island database* and *Federated network database*. The most essential part of the data storage organization is the *Personal Blockchain Stream (PBS)* [19]. The PBS represents a separate database for storing personal medical records. The medical records have form of transactions within a Blockchain-like structure. The PBS structure is presented in Figure 4. The independence of the PBS database offers easier database relocation and access management. The PBS is a personal database of the patient, but only the healthcare practitioner has the ability to insert records under patient consent. Also, the whitelisted IoT devices may also insert data in the PBS.

Making the system to be more robust and reliable requires at least three mandatory replicas of the PBS stored in the patient agent, healthcare provider agent and governmental agent. Introducing other reliable storage points optionally increases the number of replicas.

The PBS record consists of a *header*, *content* of the record and *hash* value of the finalized block in the Federal network database where the address of the record is stored. The header contains basic fields for a hash value of the previous record, wallet address of the patient, height of the block, version of the standard in use, and a hash value of the current block. The hash value of the finalized block from the Federal network database is not part of the current hash value field. The form of the medical record follows one of the available standards for medical records, described in [12], which allows the system to be future-proof and have broader interoperability.

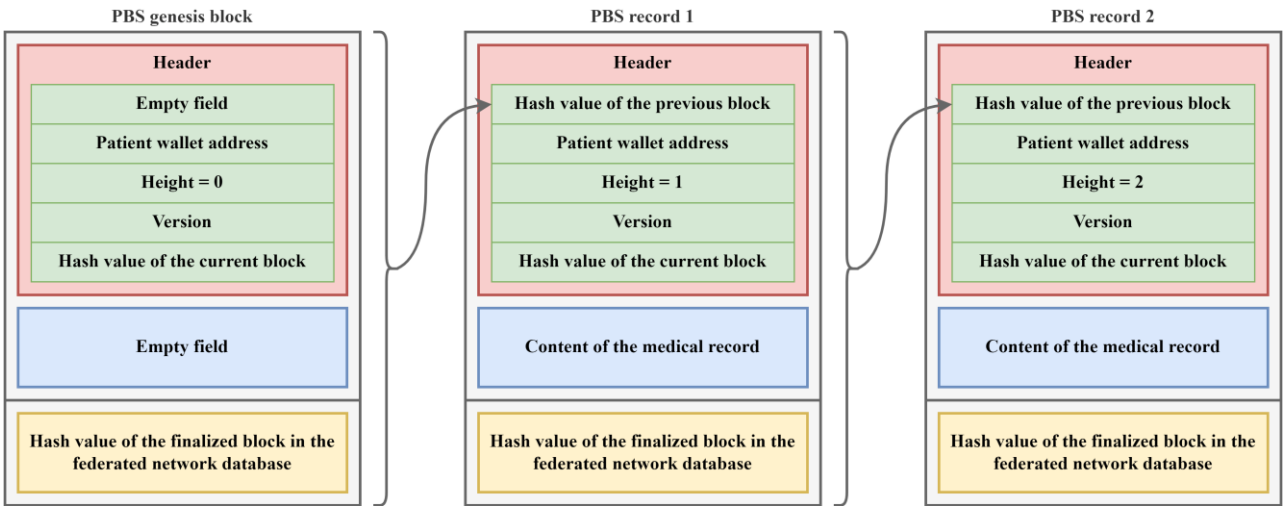

Fig. 4. PBS structure

The implementation of PBS as a record carrier has a twofold benefits. The first benefit of the PBS structure and characteristics is the ability to make a system that is *GDPR compliant*. The new approach for data storage enables the patients to protect their personal data from the unauthorized access from third parties. By definition, PBS is an independent and separate database at any place where it is replicated. Any change to the PBS will not affect the global Blockchain structure and will not require hash value recalculation from all past blocks. The PBS has container-like characteristic so any change will be only reflected inside the PBS itself.

The second benefit of the PBS implementation is the increased *scalability factor* that is achieved by the decreased replication of the same data in the system. The data of the PBS is kept in encrypted form so there is no need for a replica to be stored in third-party nodes that are not in any relation with the patient. A replica of the PBS will be readily available in unencrypted form for the patient and the healthcare provider depending on the patient's preferences. The content of the PBS can be unencrypted upon request, for the governmental node or any other third parties.

Personal vault and wallet

The BloHeS system defines the *Personal vault* to make secure management with the private data. Figure 5 presents the content of the Personal vault. The Personal vault is an encrypted data container, where the patient stores the PBS data, personal wallet, list of access profiles and list of third parties who have access to the personal data. The Personal vault is an application protected with a password to be easily accessible for the patient.

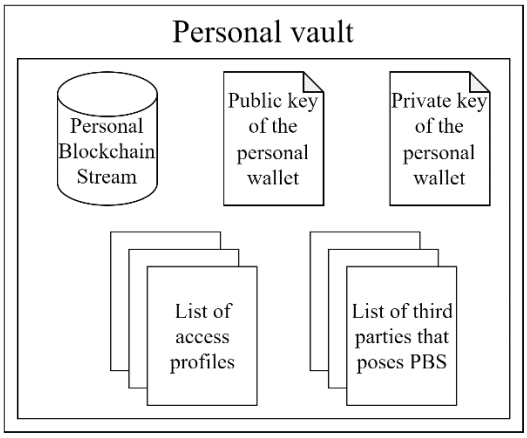

Fig. 5. Personal vault and wallet

The *smart contract* that is located in the main Blockchain database conducts the data access management. During the execution of the smart contract the patient loads the access profile and the recipient address as input parameters for the smart contract and the smart contract conducts the procedure for data selection, encryption and transfer to the requestor in a secured channel.

The public Blockchain-based healthcare system is usually a public permissioned type of Blockchain technology, where the patients provide unique identifier to access the network. The patient initiates the process of creation a personal and unique wallet address, conducted at the healthcare practitioner's premises. The healthcare practitioner forwards the request for wallet address creation to the governmental institution in order to match the patient's identity and the created wallet. The wallet creation finalizes at the patient's agent.

The distinct agents receive a wallet address from a dedicated address pool in order to improve the address space scalability. For example, the healthcare practitioners get a wallet address from the address pool dedicated to them, while the procedure of the wallet creation includes the information for the license number or work permit number provided by the governmental institution. The same person gets a separate wallet address from the patient's pool of addresses when acting as a patient.

Personal data access management procedure

The authors in [20] propose patient-centric procedures for *data access management* to the personal information in a healthcare application based on Blockchain technology. There are four protocols for data exchange: healthcare practitioner–patient, patient–healthcare practitioner, healthcare practitioner–healthcare practitioner and healthcare practitioner–third party. The first two procedures are patient–centric procedures, where the request for data access is routed directly to the patient. Contrary, the latter two procedures are pseudopatient–centric procedures due to interaction between the healthcare practitioner and the third parties without direct patient consent. These procedures assume indirect authorization for the healthcare practitioner for managing the patient's data. This approach is potentially unsafe and may cause leakage of personal data from the healthcare practitioner's agent.

The BloHeS architecture implements completely patient-centric data access management. The procedure for the data access management considers only one relation: patient–third party. The access management is easier due to the usage of the *access profiles*. Within these profiles, the patient can selects which fields from the medical records will be visible to the requestor.

The healthcare provider is the third party in the established communication with reading and writing privileges. The personal device has reading and writing privileges, while the insurance and pharmaceutical companies have only reading privileges. Practically, the data access is managed with only one procedure with multiple access profiles that is easily feasible with a smart contract. It allows the patient to have better control over the privacy of personal data. Figure 6 presents the procedure (protocol) for data access management.

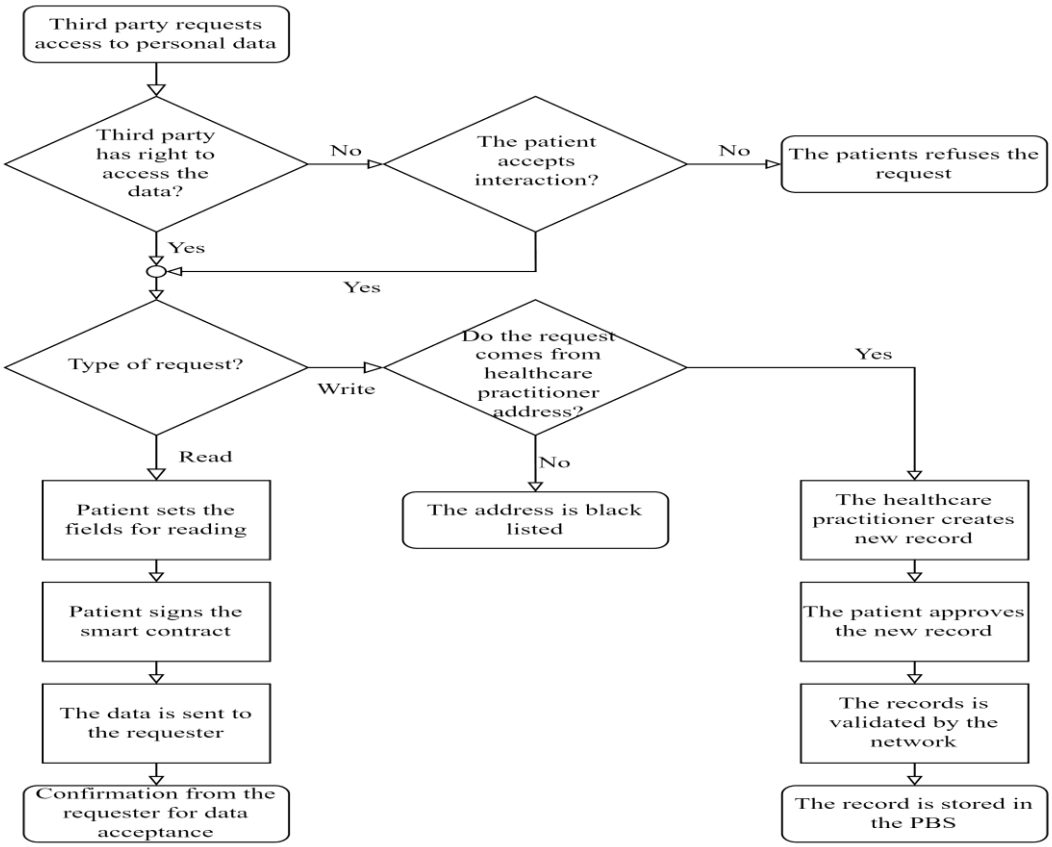

Fig. 6. Personal data access management protocol

GDPR and HIPAA compliance

The strongest characteristic of Blockchain technology is the ability to connect two blocks of data and make them *immutable*. The current position of the *GDPR regulation* and the "right to be forgotten" is a burden for the implementation of the Blockchain technologies for storing personal data due to the fact that the current Blockchain technologies do not have any procedures for modifying past records from the Blockchain database. The modification of any segment of the Blockchain database requires recalculation of the hash value that represents the links between the blocks. Contrary to the traditional Blockchain technologies, the data organization of the BloHeS system offers patient-centric control of personal data. It means that the patient can request data modification or deletion from the third parties that possess his personal data. The implementation of the Personal vault allows patient to trace who has access to his medical records. The signed agreement from the requestor is present in the PBS. The deletion of the personal data in the domain of third parties is conducted through the implementation of a smart contract signed by the third party. Moreover, the output of the signed smart contract is stored in the PBS. Adding information in the PBS for a given access to personal data or deletion of the personal data from the domain of the third parties protect the patient from potential misuse of his personal data.

The implementation of the "right to be forgotten" in the BloHeS system is simple, thanks to the segmented organization and independent PBSs of the patients. If the patient asks the third party to delete its personal data from its domain, the third party will only delete the data from the patient. This action will not affect the main Blockchain content.

The *HIPAA regulations* related to data privacy require the system that is using personal medical data to provide protection mechanisms for identifiable private data. To provide a high level of protection the private data has to be encrypted when the data traverse through the public network, but also when the data is stored in the database. This means that the HIPAA regulation requires the system to provide end-to-end privacy protection. The users of the BloHeS system establish encrypted tunnels for data exchange and use the Personal vault to keep the personal data securely encrypted.

Advantages and disadvantages of the BloHeS system

The proposed BloHeS system has advantage compared to the traditional healthcare systems. The most important advantage is the *enhanced privacy* of the medical records. The main enablers for the enhanced privacy are the Personal Blockchain Stream and the procedure for personal data access management. Both mechanisms contribute to definition of patient-centric approach for privacy protection and to compliance with GDPR and HIPAA regulations. Moreover, the storing of personal data in encrypted Personal vault ensures end-to-end privacy protection.

Furthermore, the patient-centric data access management allows definition of new business paradigm where the insurance companies and the pharmaceutical companies can improve their products. The Artificial Intelligence agents can be implemented for better diagnostics.

The BloHeS system also provides improved scalability compared to the healthcare applications built on top of the available Blockchain technologies. The improved scalability is a product of the introduced new scaling dimension. The hierarchical organization and clustering, implemented in the network organization and the consensus mechanism, provide decreased communication complexity that enables the increase in transaction throughput. The network organization and the segmentation of the consensus mechanism improve the scalability regarding the number of validators. These allow design and implementation of the BloHeS as a global healthcare system.

The implementation of the self-organization protocols for cluster management improves the cluster and network performances enabling the validators to be attached to the most optimal cluster, while managing low congestion cluster networks and keeping the cluster protected from at least one malicious validator.

The clustering approach for segmenting the network and the directional message forwarding between the clusters, makes the self-organization of the validators and the consensus mechanism susceptible to new types of attacks. Due to tight connection of the system with the Governmental agent and the legal system, the potential attacks can be suppressed with appropriate legal regulation.

The two-stage consensus achievement will slightly increase the time for transaction finalization due to the transaction requirement to go through two independent consensus cycles (Island consensus mechanism and Archiving consensus mechanism). Also, the self-organization protocols for cluster management may lead to scenarios where the validators are organized in large clusters, contributing to longer consensus achievement intervals. These will make the patients to experience extended waiting time for transaction finalization.

CONCLUSION

The new BloHeS system provides a promising scalable solution for global healthcare system based on Blockchain technology. It uses new approach for organization of the participants, introduces new consensus mechanism, and implements new organization of storage system. Several new protocols support optimal operation of the system.

This paper provides recapitulation of the new optimal consensus mechanism that will obtain better performance regarding the message count parameter, compared to the Tendermint consensus mechanism for same-sized networks of validators. The new consensus mechanism manages the consensus achievement in clustered and hierarchically organized Blockchain network. Additionally, it gives a short description of protocols for Island management providing, definition of the procedure for personal data access management and layout of the new block structure. The Island management protocols support the validators to be self-organized in clusters. The multilayered hierarchical structure requires a new block structure in order to reflect the new approach of consensus achievement.

This paper also defines the Personal Blockchain Stream and the organization of the Personal vault and wallet. The Personal vault enables the enhanced privacy of personal data through storing the private data in an encapsulated container-like structure. Moreover, the implementation of the Personal Blockchain Stream and the procedure for data access management achieves compliance with the GDPR and HIPAA regulations.

REFERENCES

[1] Karamachoski, J., Gavrilovska, L.: Framework for next generation of digital healthcare systems, *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures* (FABULOUS), 2019, pp. 12–24.

[2] Ismail, L., Materwala, H., Khan, M. A.: Performance evaluation of a patient-centric Blockchain-based healthcare records management framework, *Proceedings of the 2nd International Electronics Communication Conference*, 2020, pp. 39–50.

[3] Ethereum website. [Online]. Available: https://ethereum.org/en/. [Accessed: 02-2022]

[4] McFarlane, C., Beer, M., Brown, J., Prendergast, N.: Patientory: A healthcare peer-to-peer EMR storage network, **1**. 1, 2017. [Online]. Available: https://www.colleaga.org/sites/default/files/attachments/patientory_whitepaper.pdf. [Accessed: 06-2020]

[5] Ekblaw, A. C.: MedRec: Bblockchain for medical data access, permission management and trend analysis, 2017 [Online]. Available: https://dspace.mit.edu/handle/1721.1/109658. [Accessed: 03-2022]

[6] Zhang, P., White, J., Schmidt, D. C., Lenz, G., Rosenbloom, S. T.: FHIRChain: applying blockchain to securely and scalably share clinical data, *Computational and Structural Biotechnology Journal*, Vol. **16**, pp. 267–278 (2018).

[7] Hyperledger website. [Online]. Available: https://www.hyperledger.org/. [Accessed: 02-2022]

[8] Tanwar, S., Parekh, K., Evans, R.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications, *Journal of Information Security and Applications*, Vol. **50**, p. 102407 (2020).

[9] *Medicalchain Whitepaper 2.1*. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf. [Accessed: 06-2020]

[10] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain, *AMIA Annual Symposium Proceedings*, 2017, Vol. **2017**, p. 650.

[11] MyClinic website. [Online]. Available: https://myclinic.com/. [Accessed: 04-2022]

[12] J. Karamachoski and L. Gavrilovska: An optimal storage organization for Blockchain-based Public Healthcare System, *Journal of Electrical Engineering and Information Technologies*, Vol. **5**, no. 2, pp. 143–152 (2020).

[13] Karamachoski, J., Gavrilovska, L.: BloHeS Consensus Mechanism – Introduction and Performance Evaluation, *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures* (FABULOUS), 2022.

[14] Kwon, J.: *Tendermint: Consensus without mining*, *Draft v. 0.6*, 2014 [Online]. Available: https://tendermint.com/static/docs/tendermint.pdf. [Accessed: 03-2022]

[15] Miletić, L.: *Formal and simulation analysis of data dissemination algorithms in a blockchain network*, Senior thesis, University of Belgrade, 2018.

[16] Karamachoski, J., Gavrilovska, L.: BloHeS Island management protocols, *International Conference on Information Society and Technology*, 2022.

[17] Kwon, J., Buchman, E.: C*osmos – A Network of Distributed Ledgers*, 2018 [Online]. Available: https://v1.cosmos.network/resources/whitepaper. [Accessed: 03-2022]

[18] Arora, S. K., Kumar, G., Kim, T.: Blockchain based trust model using tendermint in vehicular adhoc networks, *Applied Sciences*, Vol. **11**, no. 5, p. 1998 (2021).

[19] Karamachoski, J., Gavrilovska, L.: Toward scalable architecture for the next generation Blockchain-based healthcare systems, *Proceedings of the Conference Balkancom 2019, Skopje, North Macedonia*, 2019, pp. 1–5.

[20] Ito, K., Tago, K., Jin, Q.: i-Blockchain: a Blockchain-empowered individual-centric framework for privacy-preserved use of personal health data, *9th International Conference on Information Technology in Medicine and Education* (*ITME*), 2018, pp. 829–833.