MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange

Alaa Awad Abdellatif*†, Lutfi Samara‡, Amr Mohamed*, Aiman Erbad*, Carla Fabiana Chiasserini†, Mohsen Guizani*, Mark Dennis O'Connor+, and James Laughton+
*Department of Computer Science and Engineering, Qatar University
†Department of Electronics and Telecommunications, Politecnico di Torino
‡Department of Electrical Engineering, Qatar University
+Mobile Healthcare Service, Hamad Medical Corporation, Qatar

***Abstract*—Medical data exchange between diverse e-health entities can lead to a better healthcare quality, improving the response time in emergency conditions, and a more accurate control of critical medical events (e.g., national health threats or epidemics). However, exchanging large amount of information between different e-health entities is challenging in terms of security, privacy, and network loads, especially for large-scale healthcare systems. Indeed, recent solutions suffer from poor scalability, computational cost, and slow response. Thus, this paper proposes Medical-Edge-Blockchain (MEdge-Chain), a holistic framework that exploits the integration of edge computing and blockchain based technologies to process large amounts of medical data. Specifically, the proposed framework describes a healthcare system that aims to aggregate diverse health entities in a unique national healthcare system by enabling swift, secure exchange and storage of medical data. Moreover, we design an automated patients monitoring scheme, at the edge, which enables the remote monitoring and efficient discovery of critical medical events. Then, we integrate this scheme with a blockchain architecture to optimize medical data exchanging between diverse entities. Furthermore, we develop a blockchain-based optimization model that aims to optimize the latency and computational cost of medical data exchange between different health entities, hence providing effective and secure healthcare services. Finally, we show the effectiveness of our system in adapting to different critical events, while highlighting the benefits of the proposed intelligent health system.**

***Index Terms*—Blockchain, edge computing, Internet of Medical Things (IoMT), priority assignment, remote health monitoring.**

I. Introduction

Advances in e-health and Internet of Medical Things (IoMT) technologies can play an integral, crucial, and evolving role in providing swift responses to outbreaks and health crises. The intensive and easy deployment of IoMT devices enable intelligent health systems to acquire massive amounts of data that require efficient processing and transferring [1]. In light of the recent pandemic, the development of smart and secure health system with efficient medical data exchange capabilities across diverse entities becomes a worldwide interest. A pivotal contribution towards the development of intelligent health system can be achieved by automating most of the healthcare functions to provide efficient healthcare services. Emerging technologies, such as Artificial Intelligence (AI), Edge Computing, and Blockchain, can turn this vision into reality. Such technologies can transform the traditional health system into an intelligent health system that enables effective collection, processing, and exchange of medical data. Indeed, intelligent health system can support diverse functions, including event detection and characterization, real-time remote monitoring, and speeding up clinical trials of new treatments.

In the era of smart health, all health-related services should be executed in an efficient and distributed way. Thus, this paper proposes a secure intelligent health system that enables efficient medical data exchange and real-time remote monitoring of the patients' status outside health entities. Such a system is of extreme importance, especially during pandemics, since it allows for minimizing the patients' visits to the health entities, and hence it minimizes the loads on these entities and the risks of physical contact with the patients. However, remote accessibility of medical data by different entities comes with processing, communications, and security challenges [2], [3]. Typically, traditional healthcare systems implement weak security measures which could jeopardize the security of the overall system. For instance, from 2016 to 2017, the number of reported health-related attacks increased by 89% as reported in [4]. Also, several reports have shown that hospitals are facing a surge of cyberattacks during the recent COVID-19 pandemic [5]. These attacks can shut down services and impede healthcare [6].

In this paper, we propose Medical-Edge-Blockchain (MEdge-Chain), a framework that integrates *edge computing* and *blockchain* technologies to process the exchange of *medical* data, and thus address the design of an efficient, secure, and decentralized health system to fulfil the aforementioned challenges. We envision that bringing the intelligence close to the users/patients, using edge computing, along with exchanging the important data over a blockchain network is a key for optimizing medical data delivery. On one hand, blockchain is a decentralized ledger of transactions that are shared among multiple entities while preserving the integrity and consistency of the data through smart contracts [7], [8]. Hence, it effectively supports data processing and storage at different entities as well as their interconnections. Blockchain also provides traceability and audibility of transactions from multiple organizations, for instance, this can play a crucial role

in tracking the supply chain of certain drugs/vaccine during clinical trials. On the other hand, being decentralized allows for the potential application of edge computing, which enables a swift and portable detection of adverse events at the edge, and providing an immediate response from healthcare entities even when hospitals are overcrowded. We therefore aim at paving the way to design an efficient intelligent health system that addresses the above aspects through:

1) Designing a secure and decentralized health system that relies on blockchain and edge computing technologies to provide intelligent and optimized medical data exchange between diverse entities, e.g., hospitals, health insurance companies, etc.
2) Developing an automated patients monitoring scheme at the edge. The proposed scheme allows for an accurate detection of the changes in the patients' records, hence ensures a fast notification about the patient's state, at the edge-level, while allowing for exchanging only important information with the different participating entities in the intelligent health system.
3) Integrating the proposed edge scheme in a multi-channel blockchain architecture with a flexible, optimized configuration model, which allows for: (i) assigning different priorities for the acquired transactions based on their urgency level and importance; (ii) optimizing blockchain channels configuration to adapt to diverse types of applications/data with different characteristics.
4) Demonstrating the effectiveness of the proposed system in improving the performance of healthcare systems using a real-world dataset.

The rest of the paper is organized as follows: Section II presents the related work. Then, we introduce the main challenges that will be tackled in this paper, and the proposed system architecture and framework in Section III. After that, Section IV presents our patients monitoring scheme, while Section V introduces our blockchain optimization model with the priority assignment task. Performance evaluation of our system is then discussed in Section VI. Finally, the paper is concluded in Section VII.

II. Related work

This section discusses the related work which we have divided into two folds, medical data exchange solutions, and data exchange solutions addressing the security and scalability issues leveraging blockchain within healthcare systems.

A. Medical data exchange

Medical data exchange has attracted major attention with several works focusing on monitoring new virus outbreaks, such as the COVID-19 pandemic [9] and west Africa Ebola epidemic [10]. It is crucial to acquire medical information scattered across distributed healthcare entities to support in-depth data analysis and maintain personalized healthcare. However, large-scale data collection and processing while considering security and public trust is challenging [11]. The Cyberattacks on healthcare entities and privacy leakage threats put serious obstacles on exchanging private medical data. Moreover, relying on a centralized entity or web resources [7] for storing the data will not be adequate in case of epidemics.

Traditionally, public health systems deploy personnel in areas where the epidemic is centered to collect relevant information. This usually results in physically contacting infected individuals [12]. Then, data processing and analysis are performed in a central entity using the received periodic information from the infested areas. For instance, during the severe acute respiratory syndrome (SARS) outbreak in Toronto, an important step to perform seamless outbreak management was building an outbreak management database platform. This platform enables the exchange of public health information, gathering clinical information from hospitals, and integrating them into an interoperable database [13]. With the help of IoT and recent technologies, medical data exchange during epidemics can be run more smoothly. Thanks to the advances of edge computing and blockchain technologies, designing a secure, collaborative health model to implement the integration of multiple national and international entities is now more realizable than ever before.

B. Blockchain for medical data exchange

The power of security in blockchain comes from the collective resources of the crowd since most of the entities have to verify each block of data using a consensus algorithm, e.g. DPoS [14], [15]. Thus, the correctness of the acquired data can be guaranteed as long as the majority of the entities are honest. Also, any cyberattack has to beat the resources of the whole crowd collectively to be able to hack the integrity of the data, which makes attacks on the blockchain impractical [7], [16]. Blockchain can also serve as data centers since the functions of data storage and data search can be implemented in the blockchain using the indexed encrypted data, i.e., stored in the blockchain [17].

Recently, blockchain has been widely used as an appropriate infrastructure for healthcare data sharing due to its transparency, tamper-evidence, decentralization, and powerful security features [18], [19]. Different types of blockchain have been envisioned for the healthcare sector, including permissioned and permissionless blockchains [20]. Permissionless blockchains offer decentralized and secure data sharing, however, when advanced control and privacy are required, private or permissioned models turn out to be more efficient. Several blockchain frameworks (e.g., Ethereum and Hyper ledger Fabric), smart contracts[1], and consensus algorithms have been investigated in the literature [21]–[23].

The blockchain architectures that have been proposed so far in the literature can be broadly classified into two categories: patient-based and entity-based. In patient-based architectures, patients participate in the blockchain [24], [25]; in entity-based architectures, instead, health organizations, hospitals,

[1] A smart contract is a software that contains all instructions and rules agreed upon by all the entities to be applied on the blockchain: all the transactions need to be consistent with the smart contract before being added to the blockchain.

research institutes, and alike are the main actors, while patients only interact with the health organizations to acquire the service they need [26]. For instance, [14] exploits blockchain to link patients, hospitals, health bureaus, and diverse healthcare communities for enabling comprehensive medical records sharing and review. [27] presents a user-centric medical data exchange solution, where a mobile application is used to gather the data from wearable devices, then sharing the data with healthcare providers and insurance companies using permissioned blockchain. [28] introduces a blockchain-based system that enables data provenance, auditing, and control over shared medical data between different entities. This system utilizes smart contracts and an access control scheme to detect malicious activities on the shared data and deny access to offending entities. [29] proposes to use two blockchains to store electronic medical records (EMRs) and personal healthcare data (PHD) separately. Indeed, [29] aims to address the challenges of system throughput and fairness, due to the significant difference between storing and exchanging the PHD and EMRs, by leveraging two blockchains. However, most of the aforementioned approaches suffer from poor scalability, computational cost, and slow response. We therefore envision a solution that combines the blockchain-enabled architecture with intelligent processing at the edge so as to support secure exchange and processing of medical data. A preliminary version of our study has been presented in [30], where only a single-channel blockchain architecture is considered without edge functionality and priority assignment.

III. Challenges, Architecture, and Framework

In this section, we first highlight the key challenges of medical data processing/exchange, then we present our MEdge-Chain architecture and framework to address these challenges.

A. Challenges for efficient medical data exchange

For providing efficient healthcare services, piles of information from diverse locations (e.g., hospitals, clinics, etc) should be collected, processed, and analyzed. However, acquiring and exchanging such amount of information between different e-health entities at different geographical locations is challenging. Thus, the following issues have to be adequately addressed using the proposed MEdge-Chain architecture.

Limited resources: Given the increasing load on the hospitals, especially during the spread of infectious diseases (such as the recent COVID-19 outbreak), it is always recommended to move the patients with mild conditions into home care. However, remote monitoring of a large number of patients from different locations puts a significant load on wireless network. For instance, high-quality Electroencephalography (EEG) monitoring application can generate sample rate 250 sample/sec for each patient. Hence, for monitoring only the EEG signals of 30 patients, we need to transfer a data size of length 10.5 Gbps per day (assuming that each sample is represented in 2 bytes).

Secure connectivity: Medical data exchange across multiple organizations imposes major challenges on the system design in terms of network load and security. Indeed, the dramatic increase in the number of cyberattacks, directed to healthcare entities, has set a severe pressure on the healthcare system to securely collect, process, and share private medical data from different locations [6]. Thus, innovative methods for secure data access, processing, and analysis are needed to handle the enormous amounts of data from different locations.

Monitoring large number of patients: One major aspect for remote monitoring or home care is the precise monitoring of large number of patients at the same time. Healthcare systems must support efficient monitoring for the patients' state, in a timely manner, inside and outside the hospitals.

B. MEdge-Chain architecture

To address the above challenges, we propose the following MEdge-Chain system architecture, which is comprised of diverse e-health entities whose fundamental role is to monitor, promote, and maintain people's health. The proposed MEdge-Chain architecture, shown in Figure 1, is divided to two main networks: (a) a Local network, and (b) a blockchain network. For the sake of scalability, we consider that the intended e-health entities gather health-related data from the local network, process these data, and share important information through the blockchain network. The shared data are validated and stored locally by the various entities in the blockchain, which are trusted entities with large storage and computational capabilities [31].

The local network stretches from the data sources located on or around patients to the Local Healthcare Service Provider (LHSP), like e.g., a hospital. It contains the following major components:

a.1) Internet of Medical Things (IoMT): A combination of Internet of Things (IoT) devices attached/near to the patients to be leveraged for monitoring health conditions and activities within the smart assisted environment. Examples include: body area sensor networks (i.e., implantable or wearable sensors that measure different biosignals and vital signs), smartphones, IP cameras, and external medical and non-medical devices.

a.2) Local Healthcare Service Provider (LHSP): An LHSP is a medical facility which monitors and provides the required healthcare services for the local patients, records the patients' state, and provides prompt emergency services if needed. Most importantly, the LHSP plays a significant role in monitoring the patients' state not only inside the medical facility (intra-medical-facility patient care), but also outside such facilities, as e.g. home patient care related services. Also, it can be connected with the private clinics that may transfer patients to it for more advanced care, or even with the patient's close circle to follow up on the patient's conditions.

As far as the blockchain network is concerned (see Figure 1), the core is the multi-channel blockchain-based data sharing architecture that enables secure access, processing, and sharing of medical data among diverse e-health entities. Blockchain is indeed particularly suitable for secure medical data exchange because of its immutability and decentralization features, which are perfectly consistent with our proposed

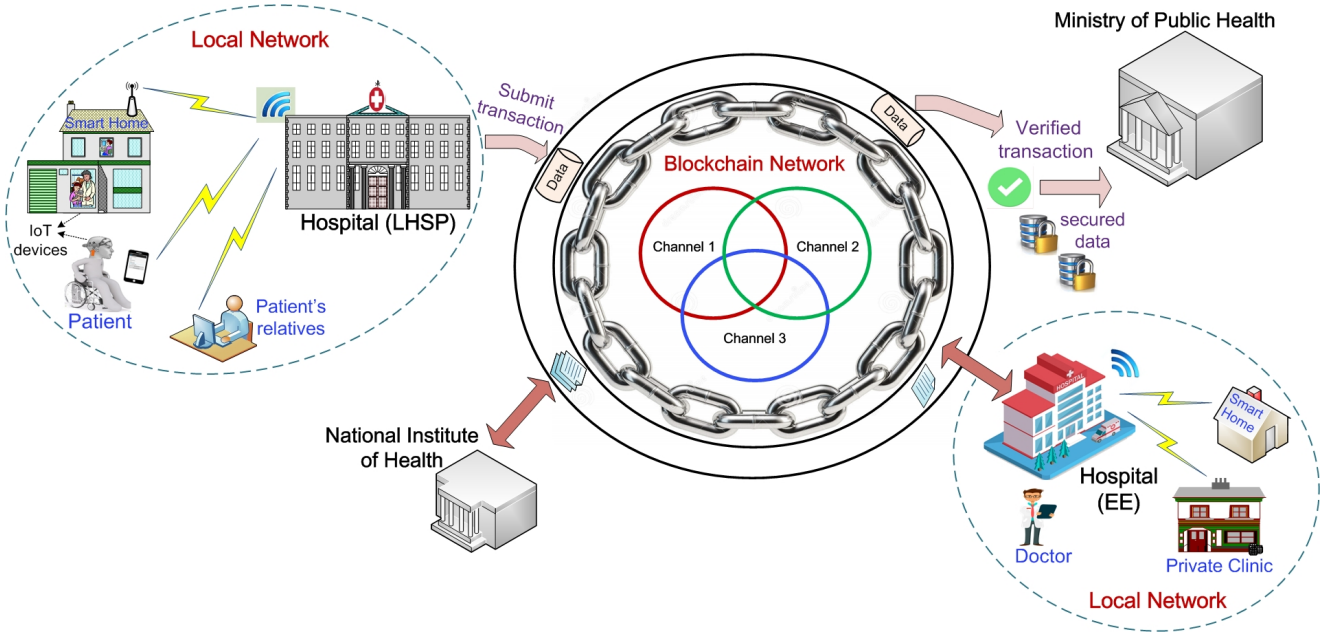


Fig. 1. The proposed MEdge-Chain system architecture.

MEdge-Chain architecture. Using blockchain, all transaction blocks (i.e., containing health-related information) can be securely shared, accessed, and stored by physicians, decision makers, and other healthcare entities. The latter include, but are not limited to:

b.1) External Edge (EE): In the proposed architecture, a hospital or a LHSP have more advanced tasks than the ones mentioned above: it can act also as an EE that is responsible for data storage, applying sophisticated data analysis techniques, and sharing important health-related information with public health entities. Hence, leveraging the power of edge computing, each entity can verify the authenticity and integrity of the medical data at the EE before sharing it within the blockchain.

b.2) Ministry of Public Health (MOPH): The main role of MOPH is monitoring the quality and effectiveness of healthcare services through coordination with different health entities. MOPH waives the responsibility of healthcare services to the hands of public and private health sectors while regulating, monitoring, and evaluating their healthcare services to guarantee an acceptable quality of care.

b.3) Other entities: Different entities can be also part of our MEdge-Chain system, such as National Institutes of Health (NIH), insurance companies, and pharmacies. For instance, NIH are major players in clinical research and health education.

C. The proposed MEdge-Chain framework

The ultimate goal of our MEdge-Chain system is to fulfill diverse challenges of medical data exchange mentioned above through implementing the following main functionality at the edge and blockchain (see Figure 2): (i) data collection, feature extraction, and patients' state monitoring, in order to ensure high-reliability and fast response time in detection of critical medical events; (ii) secure data accessibility anytime and anywhere to different entities.

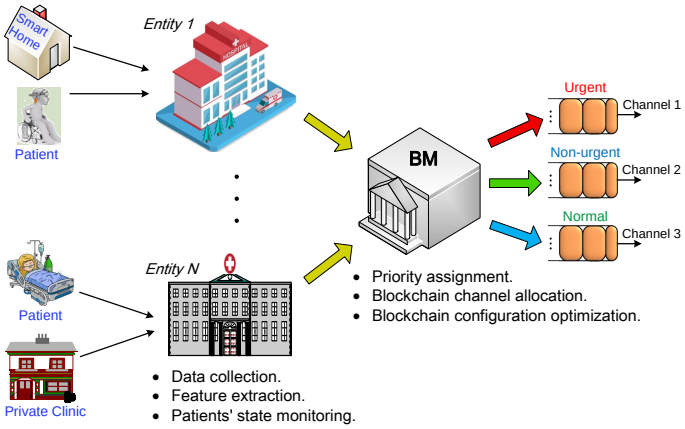


Fig. 2. Diagram representing the proposed MEdge-Chain framework, highlighting the different tasks performed by the edge and BM, as well as the corresponding data flow.

We envision that integrating edge computing with blockchain in our MEdge-Chain framework provides a potential solution to all of the aforementioned challenges. Indeed, leveraging edge computing allows for defining when and what data to share through the MEdge-Chain system. This is essential for ensuring that the most important and up-to-date information is available for investigation. In this context, we propose an automated patients' state monitoring scheme at the edge, which enables:

1) collecting the data of different patients (inside or outside the hospital);
2) identifying specific features from the acquired data that

TABLE I
LIST OF SYMBOLS USED THROUGHOUT THE PAPER.

Symbol	Meaning	Symbol	Meaning
$y(k)$	Discretized EEG Signal	S	Average Sojourn Time (Different Priorities)
$\mathfrak{N}$	Number of Samples	n	Number of Transactions per Block
$\mathcal{M}$	Mean	χ and t	Maximum and Minimum of n
σ^2	Variance	L, l_m	Block Variation Latency, Normalized Latency Metric
R	Root Mean Square	η, η_m	Security Metric, Normalized Security Metric
ν‘	Kurtosis	C, c_m	Cost Metric, Normalized Cost Metric
y^{min}	Minimum of y	α, β, γ	Weighting Parameters
y^{max}	Maximum of y	m	Number of Selected Validators
δ	Statistical Indicator	m^*, n^*	Optimal m, n
$\bar{\delta}$	Mean of δ	M and v	Maximum and Minimum of m
$\mathcal{C}$	Number of Channels	U	Utility Function
P	Number of Patients	ρ	Validator Payment
$\mathcal{K}$	change indicator vector	B	Transaction Size
ω	Status of Patient	q	Indicator factor representing the network scale
S^e	Average Sojourn Time (Equal Priorities)	K	Computational Resources
λ	Arrival Rate	O	Verification Feedback Size
μ	Service Rate	r_d and r_u	Downlink and Uplink Transmission Rates
S^g	Sojourn Time (Different Priorities)	ψ	Statistical parameter belonging to the block verification process

are informative and pertinent to the patients' state;
3) detecting major changes in the patients' state leveraging the identified features.

After processing the acquired information at the edge, we define the critical events that should be shared with other entities through permissioned blockchain. A general blockchain architecture mainly consists of: data sender, Blockchain Manager (BM), and validators. First, the data senders upload their data, in a form of "transactions", to the nearby BM. Then, the BM acts as a validators' manager: it distributes unverified blocks to the validators for verification, triggers the consensus process among the validators, and inserts the verified block in the blockchain [14]. Hence, the BM acts as the leader, while the validators are the followers that cooperate to complete the block verification task.

In our framework, we consider a multi-channel blockchain, where each channel corresponds to a separate chain of transactions that can be used for enabling data access and private communications among the channel users. Leveraging such architecture allows for treating different health-related events effectively. In particular, we consider three channels in our blockchain, channel 1 for urgent data (such as emergency notifications), channel 2 for non-urgent data but requiring a high security level (such as confidential legal messages), and channel 3 for normal data. The aim of proposing a multi-channel blockchain architecture, in our work, is motivated by the fact that when there is a minimal trust amongst participating entities (or when the transactions generated are not urgent) spending more time to verify and secure the transactions would be highly desirable. On the other hand, when the participating entities share high level of trust or when the nature of the transactions generated is urgent, enforcing high security will slow down the transaction throughput unnecessarily. This is particularly evident for the case of healthcare applications, where supporting swift response, in case of emergency, is a major goal for emergency care. Hence, urgent data (i.e., require minimum latency) should be given the highest priority and will deal with a less-restricted Blockchain, i.e., with minimum number of validators.

Accordingly, we propose three new tasks at the BM:

1) priority assignment, which aims to assign different priority levels for the received transactions from diverse entities based on their urgency level and arriving time;
2) blockchain channel allocation, which allocates the received transactions to the appropriate channel based on their urgency and security levels;
3) blockchain configuration optimization, where different blockchain configuration parameters are optimized based on diverse application requirements and data types.

We remark that the BM has a logical role that any entity in the proposed architecture can take on, possibly by taking turns, or that can be taken by the leading organization that wants to share its data [32].

In what follows, we present how the above functionality can be implemented at the edge and BM. Table I presents the main symbols used in the following sections.

IV. IMPLEMENTING THE EDGE FUNCTIONS

This section presents the first stage in our framework, which focuses on the edge functionality that aims at: (i) detecting the critical events at the edge level, and (ii) obtaining when and what data to share through the MEdge-Chain system, leveraging diverse blockchain channels. In particular, we consider as a case study how to increase the security and efficiency of clinical trials[2] for experimental medications and vaccines. Indeed, during epidemics, it is crucial to test new/different medications and vaccines on large number of patients with

[2]Clinical trials or clinical studies test potential medications/vaccines in larger number of volunteers/people with the disease to investigate whether they should be approved for wider use in the general population [33].

different circumstances and from different locations. Hence, if our MEdge-Chain system can adequately monitor this large number of patients, from different locations, before, during, and after taking a medication, it can speed up the testing process, which may help save more lives during epidemics. Moreover, it allows for conserving hospitals' facilities to absorb critical cases by enabling remote monitoring outside the hospitals. Thus, we propose an efficient, low-complexity and automated patients monitoring scheme at the edge.

Our scheme was designed leveraging real-world biological data that has been collected from patients undergoing routine planned treatment. The acquired data includes 14-channel EEG signals and routine observational data, such as temperature, blood pressure, and so on. Monitoring EEG signals provides an additional source of information to help in detecting changes of the patients' state, and to monitor the dosage of hypnotic drugs. The choice of considering EEG data in our work is motivated by the fact that EEG data is the main source of information depicting brain activities and disorders, which makes it the essential data for diagnosis of several brain disorders (such as Alzheimer's disease, Parkinson's, Epilepsy, and other seizure disorders) and brain-computer interface (BCI) applications.

Our data has been collected from 30 patients taking a specific medication during three different sessions. The three sessions represent the data of a patient *before*, *during*, and *after* taking the medication. More description about the data collection is presented in Section VI. However, without loss of generality, the proposed scheme and methodology can be easily applied to different types of data. The proposed scheme comprises the following main steps.

A. Feature extraction

The first step in our edge scheme is identifying the main statistical features that are informative, representative, and pertinent to our data changes detection. As shown by the signal behavior in Figure 3, it is difficult for the doctors to differentiate and detect the changes. However, after analyzing these signals, we found that they exhibit different mean, variance, and amplitude variations. Moreover, it is crucial to consider as relevant features the Root Mean Square (RMS), i.e., a good signal strength estimator, and kurtosis, i.e., a measure of the tailedness of the probability distribution. We therefore select the following four features, in addition to the minimum y_{ij}^{min} and maximum y_{ij}^{max} values of the acquired data:

Mean

$$\mathcal{M}_{ij} = \frac{1}{\mathfrak{N}} \sum_{k=1}^{\mathfrak{N}} y_{ij}(k), \tag{1}$$

Variance

$$\sigma_{ij}^2 = \frac{1}{\mathfrak{N}} \sum_{k=1}^{\mathfrak{N}} |y_{ij}(k) - \mathcal{M}_{ij}|^2, \tag{2}$$

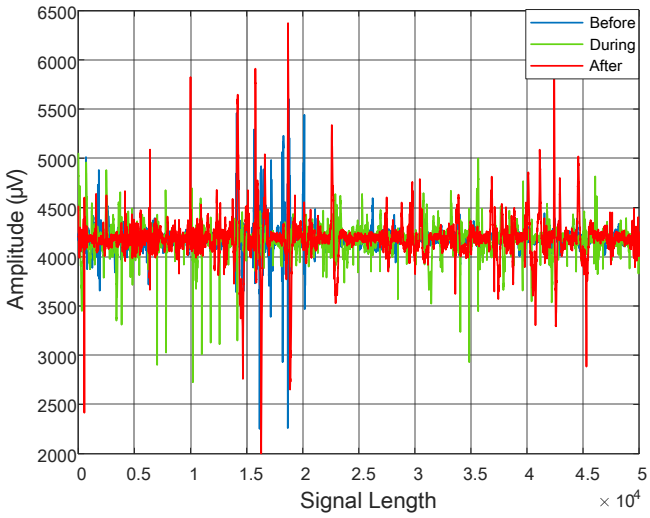


Fig. 3. An example of the acquired EEG signals, from one channel, in time domain: before, during, and after given the medication to a patient.

Root mean square

$$R_{ij} = \sqrt{\frac{1}{\mathfrak{N}} \sum_{k=1}^{\mathfrak{N}} |y_{ij}(k)|^2}, \tag{3}$$

Kurtosis

$$\nu_{ij} = \frac{\frac{1}{\mathfrak{N}} \sum_{k=1}^{\mathfrak{N}} (y_{ij}(k) - \mathcal{M}_{ij})^4}{\left(\frac{1}{\mathfrak{N}} \sum_{k=1}^{\mathfrak{N}} (y_{ij}(k) - \mathcal{M}_{ij})^2\right)^2}, \tag{4}$$

where $y_{ij}(k)$ is the values of input EEG signal for channel i and patient j, and $\mathfrak{N}$ is the number of samples. Accordingly, for a given patient j, the above features will be calculated, for each EEG channel i, to represent the patient's state over a time window of $\mathfrak{N}$ samples.

B. Changes detection and sharing

The second step in our edge scheme is detecting the major changes in the patient's state. Hence, based on the detected changes, the edge node (i.e., a hospital) can optimize what to share on the blochchain, as follows:

- in case of detecting major changes (i.e., of an emergency), it will share through blockchain an emergency notification, along with the raw data that may require further investigation;
- in case of detecting minor/no changes, it will share only the obtained features;
- in case of detecting major changes in one or two channels only, it means that the measurements may be inaccurate due to some errors in the experiment. Thus, it is recommended to notify the responsible physician to repeat the measurements.

We exploit the extracted features to perform an initial detection to the major changes in the acquired data at the edge. The advantages of our scheme is two-fold. First, by detecting the changes in the acquired data, at the edge, we can

significantly decrease the amount of information to be shared on the blockchain. Second, in case of emergency, a quick alert and notification can be initiated based on our scheme, hence facilitating effective analysis without wasting the physician's time.

The fundamental question now is: How can we obtain a simple yet accurate classification rule using the generated features to reveal the major changes in the acquired data? First, we define a statistical indicator δ_{ij}, for an EEG channel i and patient j, that integrates generated features as follows:

$$\delta_{ij} = \mathcal{M}_{ij} + \sigma_{ij}^2 + R_{ij} + \nu_{ij} + y_{ij}^{min} + y_{ij}^{max}. \quad (5)$$

Using (5), we define a change indicator vector $\mathcal{K}_j = [\kappa_{1j} \cdots \kappa_{Cj}]$ for a patient j, where κ_{ij} is defined as

$$\kappa_{ij} = \left[\frac{\left|\delta_{ij}^b - \delta_{ij}^d\right|}{\bar{\delta}} + \frac{\left|\delta_{ij}^d - \delta_{ij}^a\right|}{\bar{\delta}} \right] \times 100, \quad (6)$$

where

$$\bar{\delta} = \frac{\sum_{j=1}^{P} \sum_{i=1}^{\mathcal{C}} \delta_{ij}^b + \delta_{ij}^d + \delta_{ij}^a}{3\mathcal{C}P}. \quad (7)$$

In (6), $\bar{\delta}$ is the statistical mean of δ, acquired during offline training, for all channels $i \in \{1, \cdots, \mathcal{C}\}$ over all patients $j \in \{1, \cdots, P\}$.

Second, we define a classification rule using the obtained $\mathcal{K}_j$ to detect the major changes/errors of the acquired EEG data, where $\mathcal{K}_j$ will represent the condition part of the rule, while the status of the patient ω_j will represent its consequent part. Accordingly, we obtain through our experiments the following classification rule

$$\omega_j = \begin{cases} \text{Major}, & \text{if } |||[\mathcal{K}_j - \zeta]^+||_0 > 2 \\ \text{Minor}, & \text{if } |||[\mathcal{K}_j - \zeta]^+||_0 = 0 \\ \text{Repeat}, & \text{if } 0 < |||[\mathcal{K}_j - \zeta]^+||_0 \leq 2, \end{cases} \quad (8)$$

where $[\mathbf{a}]^+ = \max(0, \mathbf{a})$ provides a vector of either positive or 0 elements in a vector $\mathbf{a}$, $||.||_0$ is the zeroth norm operator, and ζ is a threshold that assesses the major changes in the EEG signal (e.g., we consider $\zeta = 30\%$).

We remark that this scheme will be exploited to obtain the status of the patient at the edge, hence optimizing what to share through blockchain. Moreover, it provides a quick detection for the major changes in the patient's state, while keeping the complexity low, hence it is amenable for implementation at any mobile edge.

V. Blockchain Optimization: Priority assignment and Solution

The second stage in our framework is developing an optimized blockchain configuration model that enables sharing of different health-related events and information among diverse healthcare entities. We envision that for designing an efficient health system, the acquired data from various entities should be treated in different ways, based on their urgency and security levels. For example, urgent data (i.e., require minimum latency) should be given highest priority and dealt with a less-restricted blockchain, i.e., with minimum number of validators. On the contrary, for low priority types of data but requiring a high security level, fully-restricted blockchain should be used (see Figure 4). In case of normal data, i.e., that has requirements on both latency and security, an optimized blockchain configuration is used. We remark that data types and emergency levels are defined at the edge by applying different data classification, event detection, and summarization techniques, as shown in Section III-C. In general, the more validators participate in the block verification stage, the higher the security level is, but also the larger the latency (due to the verification delay) and the higher the cost (due to verification fees) that are experienced [34], [35]. Instead, as the number of transactions per block grows, the latency increases, while the cost per transaction decreases [35], [36]. Accordingly, the proposed blockchain optimization addresses the aforementioned challenges by designing an event-driven secure data exchange scheme, as detailed below.

The proposed scheme draws on the BM concept [34], which acts as a validators' manager, that is responsible for:

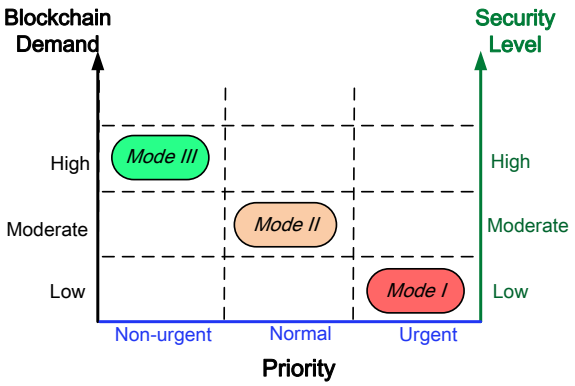
1) gathering the transactions from different entities,
2) assigning different priorities to the gathered transactions based on their urgency level,
3) updating the blockchain configuration considering urgency and security level of the gathered transactions,
4) preparing and distributing unverified blocks to the selected validators (e.g., hospitals, NIH, and MOPH, which have sufficient computation and storage resources),
5) interacting with the validators to complete block verification tasks.

Thus, the BM is a critical component in our scheme, which dynamically updates the blockchain configuration's parameters, based on the diverse applications' requirements and data types, such that the optimal trade-off among security, latency, and cost is obtained. Also, we remark that, in line with the traditional consensus scheme, the validators take turns in working as BM for a given time period [34].

A. Priority assignment

Before optimizing the blockchain configuration's parameters, we highlight the role of priority assignment task at the BM. This task aims to minimize the sojourn time of the received transactions from different entities based on their urgency level. Herein, the sojourn time refers to the total amount of time a transaction is expected to wait before being added to the blockchain. This sojourn time will be controlled by identifying different urgency levels, namely urgent, normal and non-urgent. Then, we adopt the use of queuing models to calculate the sojourn time based on the urgency levels of different received transactions. In particular, we define the sojourn time based on the preemptive-resume priority concept [37], i.e., the transactions with a higher priority interrupts the processing of transactions with lower priorities.

It is assumed that N entities (e.g., hospitals) are sending their transactions to the BM, each with an arrival rate λ_i, for $i \in \{1, \cdots, N\}$. All received transactions from different



Priority	Data type	Security Level
Urgent	Emergency data	Low
Normal	Biosignals' features	Moderate
Non-urgent	Confidential messages	High

Fig. 4. Blockchain modes based on the data priority and required security level.

entities are temporarily stored in the BM's buffers. In this paper, buffer overflows are negligible since it is assumed that $\sum_{i=1}^{N} \lambda_i < \mu$, where μ is the service rate at the BM. By adopting the well-established M/M/1 queuing model [38] (and the references therein) for the received transactions with equal priorities, the average sojourn time of entity i is defined as

$$S_i^e = \frac{1}{\mu - \sum_{i=1}^{N} \lambda_i}. \tag{9}$$

However, to handle the received transactions efficiently, the BM assigns different priorities for them based on their urgency levels and corresponding entity weight[3]. Hence, transactions with high urgency and coming from high impact entities will be assigned the highest priority. To derive the average sojourn time for transactions with different priorities, we start from the general expression of the sojourn time which we denote by S_i^g, that can be calculated by applying [37, Sec. 9.2]

$$S_i^g = \frac{\sum_{n=1}^{i} \lambda_i R_i}{(1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_i}{\mu}))(1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_{i-1}}{\mu}))} + \frac{B_i}{1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_{i-1}}{\mu})}, \tag{10}$$

where R_i and B_i are the mean service and mean residual service times of the i^{th} entity, respectively. The adopted M/M/1 queuing model implies that we have exponential service times with mean $B_i = 1/\mu$ and $R_i = 1/\mu$ [37]. Hence, substituting the aforementioned results in (10) yields the following average sojourn time expression

$$S_i = \frac{\frac{1}{\mu}\sum_{n=1}^{i} \lambda_i}{(1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_i}{\mu}))(1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_{i-1}}{\mu}))} + \frac{\frac{1}{\mu}}{1-(\frac{\lambda_1}{\mu}+\ldots+\frac{\lambda_{i-1}}{\mu})}. \tag{11}$$

To assess the benefits of the proposed urgency priority assignment compared to conventional techniques that utilize equal priority assignment, we present Figure 5. This figure depicts the average sojourn time versus the entity index. In this figure, we simulate the arrival rate of 21 different entities, where each entity is assigned a different priority based on the urgency level of its data. In particular, it is assumed that entities 1 through 8 have urgent data, entities 9 through 12 have normal data, and entities 13 through 21 have non-urgent data. Moreover, the packet arrival rate per entity is assumed to be constant and is equal to 2 transactions/s. The obtained results show that unlike the equal priority assignment, which obtains the same sojourn time for all entities, the proposed urgency priority assignment yields a significant reduction in sojourn time, especially for entities with an "urgent" status. We also observe that for the transactions belonging to low priority entities, the sojourn time is increased, when compared to that of the equal priority, which makes sense since it is tagged with low urgency (non-urgent). The figure also shows the effect of varying the average service rate on the obtained sojourn time. It is clear that the sojourn time increases when the service rate decreases, however, using our urgency priority assignment allows for decreasing the sojourn time of most of the entities (only three entities will have higher sojourn times than that of the equal priority assignment).

We remark that service rate $\mu = n/L$, where n is the number of transaction per block, and L is the block verification latency inside the blockchain. Thus, optimizing blockchain configuration will have direct impact on the obtained sojourn time, as will be shown later.

B. Optimal blockchain configuration

Given the received transactions with different priorities, the BM aims at mapping these transactions into different configurations of the blockchain. The proposed blockchain optimization model considers permissioned blockchain with Delegated Proof-of Stake (DPoS) consensus algorithm[4], which performs the consensus process using pre-selected validators [34]. Our model focuses on three main metrics at the BM, namely, latency (L), security (η), and cost (C). However, these metrics have different values and units, which must be first normalized with respect to their maximum values (denoted by l_m, η_m, and c_m, respectively) to make them comparable. Then, to deal with such conflicting metrics, we define an aggregate utility U, which combines them into a single function:

$$U = \alpha \cdot \frac{L}{l_m} + \beta \cdot \frac{\eta_m}{\eta} + \gamma \cdot \frac{C}{c_m}, \tag{12}$$

[3]Entity weight can represent the degree of influence that an entity has on the national health system

[4]Consensus algorithm is a process of ensuring the integrity and consistency of the blockchain across all participating entities [14].

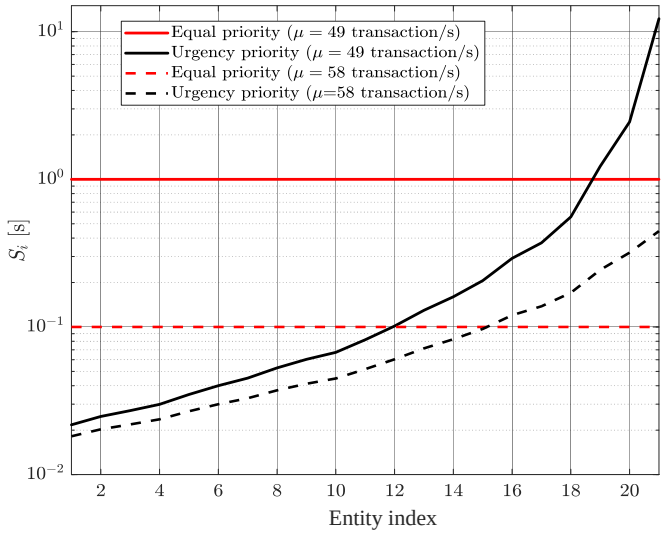


Fig. 5. The obtained average sojourn time for different entities using equal priority and urgency priority assignments, while varying service rate μ.

where α, β, and γ are weighting parameters representing the relative importance of the considered metrics, such that $\alpha + \beta + \gamma = 1$. Also, m is the number of selected validators, with maximum and minimum values equal to M and v, respectively, and n is the number of transactions per block, with maximum and minimum values equal to χ and t, respectively. Accordingly, the BM can obtain the best blockchain configuration, by solving the following optimization problem:

$$\textbf{P:} \ \min_{m,n} (U) \tag{13}$$

$$\text{s.t.} \ \ c_i \geq \rho_i \cdot x_i, \quad \forall i \in \{1, \cdots, m\} \tag{14}$$

$$v \leq m \leq M, \tag{15}$$

$$t \leq n \leq \chi. \tag{16}$$

In (13), the cost function is defined as $C = \frac{\sum_{i=1}^{m} c_i}{n}$, where c_i is the computational cost of validator i to finish the verification task, while the security level is defined as $\eta = \theta \cdot m^q$, where θ is a coefficient given by the system, and $q \geq 2$ is an indicator factor representing the network scale. L refers to the latency of the block verification process, which includes: (i) unverified block transmission from the BM to validators, (ii) block verification time, (iii) verification result broadcasting and comparison between validators, and (iv) verification feedback transmission from the validators to BM [34]. Hence, the latency is defined as

$$L = \frac{n \cdot B}{r_d} + \max_{i \in \{v, \cdots, M\}} \left(\frac{K}{x_i} \right) + \psi(n \cdot B)m + \frac{O}{r_u}, \tag{17}$$

where B is the transaction size, K is the required computational resources for block verification task, x_i is the available computational resources at validator i, O is the verification feedback size, r_d and r_u are, respectively, the downlink and uplink transmission rates from the BM to the validators and vice versa. In (17), ψ is a predefined parameter that can be obtained using the statistics belonging to the previous processes of block verification (as detailed in [34]). Finally, in our architecture, it is assumed that the validators are offloading their computational load of the verification process to the cloud/fog providers (CFPs). Hence, validator i should buy the required computing resources x_i from a CFP in order to access these resources from the remote cloud or the nearby fog computing unit [39]. Thus, for validator i to participate in the verification process, it should receive a cost c_i that at least covers its payment to the CFP. This condition is represented in constraint (14), where ρ_i represents the payment from validator i to the CFP, in order to acquire the needed resources for the verification process.

According to the acquired data types and application's requirements, the weighting coefficients α, β, and γ are defined. Hence, the optimal number of validators m^* and transactions per block n^* can be obtained by solving the proposed optimization problem. However, the above optimization problem is an integer programming optimization, which is an NP-complete problem [40]. In light of the problem complexity, we propose below a light-weight iterative approach for obtaining an efficient solution of the formulated problem.

In order to efficiently solve the formulated problem in (13), we look at the problem as a block size optimization, as a function of n, and a block verification optimization, as a function of m. The block verification variable can be considered as a global variable that is relevant to the overall blockchain process, while the block size variable is a local variable at the block preparation phase. We therefore decompose the problem into the block size and block verification sub-problems, such that each of them is a function of one decision variable only and, hence, can be solved independently of the other. Then, an efficient-iterative algorithm is proposed for obtaining the optimal solution of (13) by leveraging the proposed problem decomposition.

Starting by the block size problem, a closed-form expression for the solution can be obtained by imposing that the derivative with respect to n of the objective function is equal to 0, while considering m as a constant. I.e.,

$$\begin{aligned} \partial/\partial n \left[\alpha \cdot L + \beta \cdot \eta^{-1} + \gamma \cdot C \right] &= 0 \\ \alpha \left(\frac{B}{r_d} + \psi \cdot B \cdot m \right) - \gamma \frac{\sum_{i=1}^{m} \rho_i \cdot x_i}{n^2} &= 0 \\ \frac{\gamma \sum_{i=1}^{m} \rho_i \cdot x_i}{\alpha(\frac{B}{r_d} + \psi \cdot B \cdot m)} &= n^2. \end{aligned} \tag{18}$$

Thus, the optimal n is given by:

$$n = \sqrt{\frac{\gamma \sum_{i=1}^{m} \rho_i \cdot x_i}{\alpha(\frac{B}{r_d} + \psi \cdot B \cdot m)}}. \tag{19}$$

Considering block verification optimization, an efficient Blockchain Configuration Optimization (BCO) algorithm is proposed (see Algorithm 1). BCO algorithm leverages the idea of problem decomposition to find the optimal solution of (13) in practical scenarios, where different validators have different verification response time. The main steps of BCO algorithm can be summarized as follows:

1) BM distributes unverified blocks to the validators.
2) Validators that finish block verification faster are selected one by one.
3) Given the selected validators (m), n is calculated, using (19), and approximated to the nearest integer. Then, n^* is obtained, such that the constraint in (16) is satisfied.
4) After adding a new validator, we check the "*gain*" condition, i.e., the obtained reduction in the security term (i.e., $\beta \cdot \eta^{-1}$) is greater than the obtained increase in the latency and cost terms (resulting from adding the new validator). If the "*gain*" condition is satisfied, this validator is added to the selected validators, otherwise it is discarded and m^* is obtained.

We remark that the maximum number of iterations for the BCO algorithm to converge to the optimal solution is M, thanks to the derived closed-form solution for n^*.

Algorithm 1 Blockchain Configuration Optimization (BCO) algorithm

Input: x_i, ρ_i, v, M, t, χ.
for $m = v + 1 : M$ **do**
  Calculate n using (19).
  if $\lfloor n \rceil < t$. **then**
    $n^* = t$.
  else if $\lfloor n \rceil > \chi$. **then**
    $n^* = \chi$.
  else
    $n^* = \lfloor n \rceil$.
  end if
  if $\beta \cdot \eta^{-1}(m-1) - \beta \cdot \eta^{-1}(m) < (\alpha \cdot L(m) + \gamma \cdot C(m)) - (\alpha \cdot L(m-1) + \gamma \cdot C(m-1))$ **then**
    $m^* = m - 1$.
    Break % m^* is obtained
  end if
end for
Output: m^*, n^*.

VI. Simulation Results

For our performance evaluation, we use the data in [41] that has been collected from patients undergoing routine planned treatment. The data collection process has been carried out by our collaborators in the patient recovery center of Hamad Medical Corporation. The acquired data has been collected using EMOTIV EPOC+, which comprises 14 EEG channels (i.e., electrodes)[5] for whole brain sensing [42], in addition to the routine observational data such as temperature and blood pressure. This data has been collected from 30 patients receiving intravenous antibiotic medication. Each patient has been monitored for 30 minutes: before, during, and after taking the medication. Moreover, our results were generated considering 21 entities, where the packet arrival rate per entity is assumed to be uniformly distributed with mean equals to 1 transactions/s. Other simulation parameters are set as follows: $q = 4$, $O = 0.5$ Mb, $\theta = 1$, $r_d = 1.2$ Mbps, $r_u = 1.3$ Mbps, $K = 100$, and $B = 0.5$ Kilobits.

The first aspect we are interested in is identifying the changes in the acquired patients' records at the edge using the proposed patients monitoring scheme. To this end, Figure 6 demonstrates the variations in the defined change indicator δ over different EEG channels for six patients. This figure highlights that using the defined change indicator, a physician can easily interpret the EEG behavior of a patient before, during, and after taking a certain medication. For instance, patients 1, 4, and 5 have a clear increase in their EEG records after taking the medications, while patients 2 and 3 having almost the same behavior before, during, and after taking the medication. Interestingly, our scheme can also detect the errors in collecting the data. For instance, patient 6 has a very large value of δ for channel 14 only, which indicates that there is a problem in this channel during data collection. Hence, the physician should repeat this experiment for this patient before conducting further data analysis.

The second aspect we are interested in is the impact of blockchain configuration optimization on the different performance metrics. First, Figure 7 depicts the effect of changing the blockchain configuration parameters (i.e., number of validators m and number of transactions per block n) on the obtained utility function in (12), for applications with similar requirements in terms of security, latency, and cost ($\alpha = \beta = \gamma$). It is clear how changing the configuration parameters always corresponds to a significant change in the utility. Thus, it is important to optimize these parameters considering diverse applications' requirements and system performance.

As far as the blockchain configuration optimization is concerned, Figure 8 shows the convergence behavior of the proposed BCO algorithm to the optimal solution obtained by exhaustive search, given $M = 21$ and $N = 20$. We observe that our algorithm requires only 7 iterations to reach the optimal solution compared to exhaustive search that still does not converge after 420 iterations.

We now study, in Figure 9 and Figure 10, how changing blockchain configuration on different channels influences the performance. The plots in Figure 9 represent the main performance metrics considered in our framework (i.e., latency, security, and cost) as a function of the number of iterations until reaching to the convergence. Each curve therein corresponds to a channel configuration, and each plot corresponds to a performance metric. The configuration of the channels from 1 to 3 has been optimized using the proposed BCO scheme, while the configuration of channels 4 is assumed to be fixed, considering a fixed number of validators (i.e., $m = 8$) and a fixed number of transactions per block (i.e., $n = 80$). Herein, it is assumed that channel 1 is used for urgent data, channel 2 for normal data, and channel 3 for non-urgent data. Comparing the individual curves within each plot, we

[5]EEG monitoring are conducted using EEG electrodes, which gather and record the electrical activity of the brain. The acquired EEG signals are amplified, digitized, and then sent to a computer for processing and storage [42].

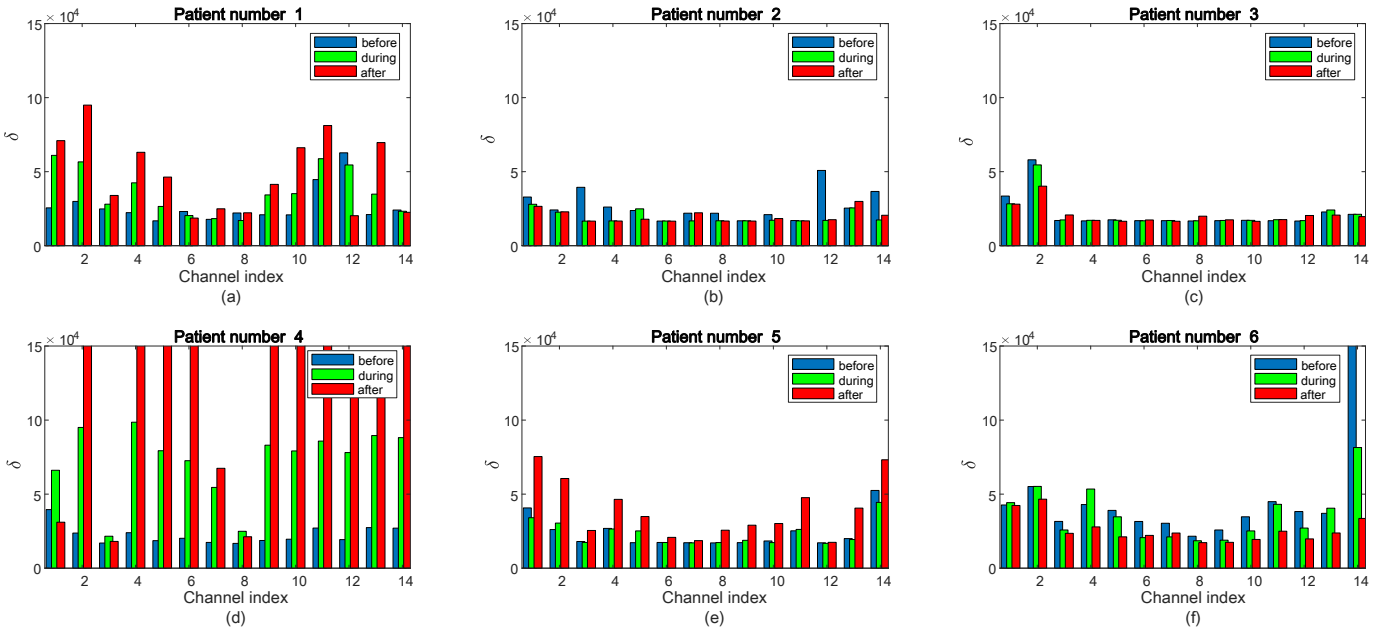


Fig. 6. The variations of change indicator δ, over different channels, for six patients: before, during, and after taking a medication.

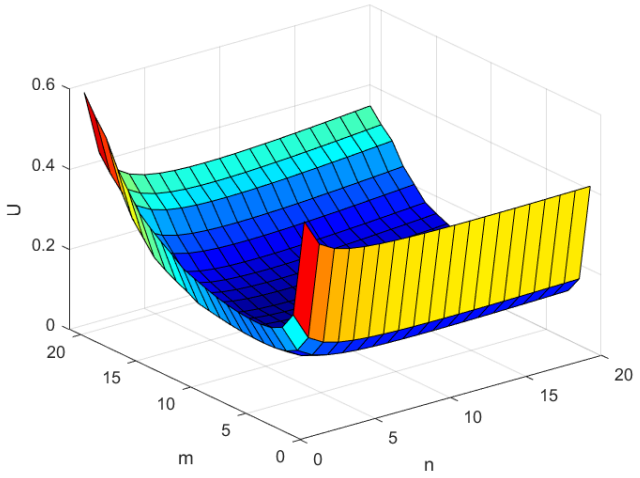


Fig. 7. The proposed objective function as the number of validators (m) and the number of transactions per block (n) vary, for a one blockchain channel.

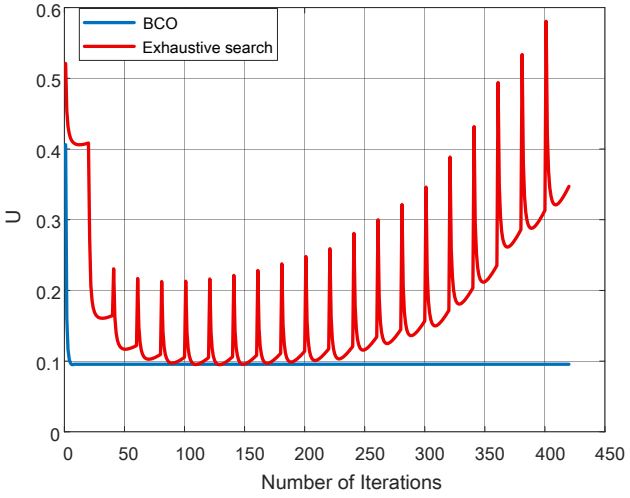


Fig. 8. Convergence behavior of the proposed algorithm compared to the solution obtained through exhaustive search.

can observe how our BCO algorithm efficiently adjusts different channels configurations according to the acquired data characteristics, such that the urgent data are sent by the lowest latency and computational cost, while the non-urgent data (i.e., require high security without latency constraint) are sent with the highest security level. Moreover, it clearly illustrates the tradeoff between increasing the security level and decreasing the latency. Thus, this result shows that it is important to have multiple channels with different configurations within the same blockchain to be able to adapt to diverse types of applications/data with different characteristics.

Finally, we assess how much, and for whom, our priority assignment scheme is beneficial. Figure 10 depicts how, for different channels configurations, priority assignment influences the obtained sojourn time. In this figure, different curves correspond to different channels with and without considering our priority assignment scheme. This figure highlights that assigning different priorities for different entities in the system (based on the urgency levels or the entity weight) yields a substantial decrease in sojourn time for high-priority entities, hence they can share their transactions with a substantially smaller delay.

VII. Conclusion

Next-generation healthcare systems are being shaped by incorporating emerging technologies to provide radical improvements in healthcare services. Thus, this paper proposes a novel, collaborative health system for enabling effective

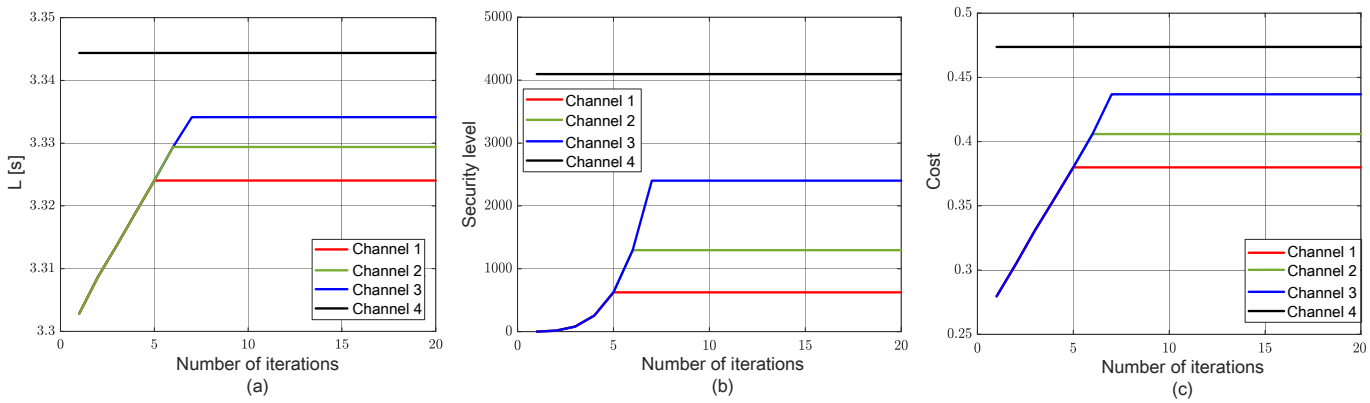


Fig. 9. A comparison of diverse blockchain performance metrics: (a) latency, (b) security, and (c) cost, for various blockchain channels with different configurations.

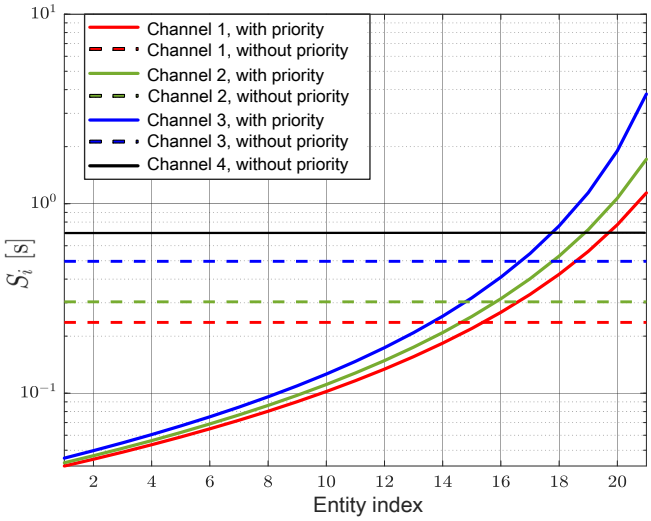


Fig. 10. The obtained average sojourn time for different blockchain channels with and without priority assignments.

and large-scale medical data exchange. The proposed MEdge-Chain system leverages edge computing and blockchain to provide secure transfer of large amount of medical data generated by various health entities. In particular, we propose an effective scheme for monitoring the patients, at the edge, to ensure early detection, scalability, and fast response for urgent events. Based on this scheme, we also develop an optimized blockchain configuration model with a queuing-based priority assignment method to optimally manage the received transactions from diverse entities. Our results show that mapping the characteristics of the gathered data into adequate configurations of the blockchain can significantly improve the performance of the overall MEdge-Chain system, while fulfilling different health entities' requirements.

Acknowledgement

This work was made possible by NPRP grant # NPRP12S-0305-190231 from the Qatar National Research Fund (a member of Qatar Foundation). The work of Mark Dennis O'Connor and James Laughton was supported by Abhath Project # MRC 01-17-091 from Hamad Medical Corporation. The findings achieved herein are solely the responsibility of the authors.

References

[1] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili, and A. Erbad, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

[2] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4101–4112, 2018.

[3] A. Emam, A. A. Abdellatif, A. Mohamed, and K. A. Harras, "Edge-Health: An energy-efficient edge-based remote mHealth monitoring system," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–7.

[4] "Healthcare report for 1st half of 2018," https://www.cryptonitenxt.com/resources, Accessed: 2020-12-5.

[5] "Hospitals face a surge of cyberattacks during the novel coronavirus pandemic," https://www.sfgate.com/news/article/Hospitals-face-a-surge-of-cyberattacks-during-the-15201802.php, Accessed: 2020-12-5.

[6] "Note to nations: Stop hacking hospitals," https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms, Accessed: 2020-12-5.

[7] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[8] O. Bouachir, M. Aloqaily, L. Tseng, and A. Boukerche, "Blockchain and fog computing for cyberphysical systems: The case of smart industry," *Computer*, vol. 53, no. 9, pp. 36–45, 2020.

[9] Marcello Ienca and Effy Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic," *Nature Medicine*, March 2020.

[10] Ilana J Schafer, Erik Knudsen, Lucy A McNamara, Sachin Agnihotri, Pierre E Rollin, and Asad Islam, "The epi info viral hemorrhagic fever (vhf) application: a resource for outbreak data management and contact tracing in the 2014–2016 west africa ebola epidemic," *The Journal of infectious diseases*, vol. 214, no. suppl_3, pp. S122–S136, 2016.

[11] Y. Xiao, Y. Jia, X. Cheng, J. Yu, Z. Liang, and Z. Tian, "I can see your brain: Investigating home-use electroencephalography system security," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6681–6691, 2019.

[12] SA Rasmussen and RA Goodman, "The cdc field epidemiology manual.," *New York: Oxford University Press*, 2019.

[13] Public Health Agency of Canada, "Learning from SARS: Renewal of public health in canada," http://www.phac-aspc.gc.ca/publicat/sars-sras/naylor, Accessed: 2020-12-5.

[14] Shuai Wang, Jing Wang, Xiao Wang, Tianyu Qiu, Yong Yuan, Liwei Ouyang, Yuanyuan Guo, and Fei-Yue Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, vol. 99, pp. 1–9, 2018.

[15] David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh, "A survey on blockchain for information systems management and security," *Information Processing Management*, vol. 58, no. 1, 2021.

[16] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[17] S. Jiang, J. Cao, J. A. McCann, Y. Yang, Y. Liu, X. Wang, and Y. Deng, "Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 405–410.

[18] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[19] I. A. Ridhawi, M. Aloqaily, A. Boukerche, and Y. Jaraweh, "A blockchain-based decentralized composition solution for iot services," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[20] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[21] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, vol. 42, no. 7, 2018.

[22] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *Journal of medical systems*, vol. 43, no. 2, 2019.

[23] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[24] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.

[25] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, 2019.

[26] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems*, vol. 42, no. 8, 2018.

[27] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–5.

[28] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[29] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A blockchain-based platform for healthcare information exchange," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2018, pp. 49–56.

[30] Alaa Awad Abdellatif, Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, and Ahmed Refaey, "SSHealth: Toward secure, blockchain-enabled healthcare systems," *accepted in IEEE Network*, 2020.

[31] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, June 2019.

[32] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 157–160, 2019.

[33] "Inside clinical trials: Testing medical products in people," https://www.fda.gov/drugs/drug-information-consumers/inside-clinical-trials-testing-medical-products-people, Accessed: 2020-07-2.

[34] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, March 2019.

[35] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, Sep. 2013, pp. 1–10.

[36] S. Shalaby, A. A. Abdellatif, A. Al-Ali, A. Mohamed, A. Erbad, and M. Guizani, "Performance evaluation of hyperledger fabric," in *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 608–613.

[37] I. Adan and J. Resing, *Queueing theory*, Eindhoven University of Technology, Eindhoven, 2002.

[38] F. Malandrino, C-F. Chiasserini, G. Einziger, and G. Scalosub, "Reducing service deployment cost through vnf sharing," *IEEE/ACM Transactions on Networking*, vol. 27, no. 6, pp. 2363–2376, 2019.

[39] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4585–4600, June 2019.

[40] Hemmecke R., Köppe M., Lee J., and Weismantel R., *Nonlinear Integer Programming*, Springer, Berlin, Heidelberg, 2010.

[41] Alaa Awad Abdellatif, Zina Chkirbene, Abeer Al-Marridi, Amr Mohamed, Aiman Erbad, Mark Dennis O'Connor, James Laughton, Anthony Villacorte, and Johansen Menez, "EEG data for patients receiving intravenous antibiotic medication," 2020.

[42] "Emotiv epoc+," 2020, Accessed: 2020-04-10.