Future Generation Computer Systems 110 (2020) 675–685

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A blockchain-based eHealthcare system interoperating with WBANs☆

Junchao Wang [a], Kaining Han [a,*], Anastasios Alexandridis [b], Zhiyu Chen [b], Zeljko Zilic [b], Yu Pang [c], Gwanggil Jeon [d,e,*], Francesco Piccialli [f]

[a] Department of Biomedical Engineering, Shantou University, Shantou, Guandong, China
[b] Department of Electrical and Computer Engineering, McGill University, Montreal, Canada
[c] Chongqing University of Posts and Telecommunications, Chongqing, China
[d] School of Electronic Engineering, Xidian University, Xi'an, Shaanxi, China
[e] Department of Embedded Systems Engineering, Incheon National University, Incheon, Republic of Korea
[f] Department of Electrical Engineering and Information Technology, University of Naples Federico II Via Claudio, 21 - 80125 Napoli, Italy

ARTICLE INFO

Article history:
Received 9 August 2019
Received in revised form 20 September 2019
Accepted 27 September 2019
Available online 8 October 2019

Keywords:
Blockchain
eHealthcare
Wireless body area network

ABSTRACT

Due to the increasing population of the elderly and patients with chronic diseases, more and more individuals are suffering from the limited service capabilities of the traditional medical systems. Benefiting from the rapid development of biomedical sensors, Internet of Things, and modern communication and network technologies, eHealthcare systems start appearing in the medical services, especially for the remote physical condition monitoring which improves the efficiency of the traditional medical systems. To provide a secure and low power healthcare solution, a blockchain-based eHealthcare system interoperating with wireless body area networks (WBAN) has been proposed, which utilizes the WBAN to network the devices of the patients and the blockchain technology as the data transmitting and storage method. The evaluation results show that the proposed system has the advantages of low hardware resources utilization, high-security protection level, and stable performance.

1. Introduction

The number of patients with chronic diseases in the world has increased from 118 million to 149 million in the past 25 years, while the number will rise to 171 million in the next 10 years [1]. However, the low-efficient conventional medical and healthcare systems cannot provide timely and efficient medical services to the public. For instance, based on the report by the Fraser Institute [2], the average waiting time for consulting medical professionals was 21.2 weeks in 2017 in Canada. In other words, the current and future patients need to wait for around 5 months in the queues before consulting the medical doctors about their physical conditions. To shorten the waiting time for consulting medical professionals, some countries with a huge population such as China started to adopt the triage-type hierarchical diagnosis and treatment based on the conditions of the patients [3]. Even though it helped improve the efficiency of traditional medical systems, there is still a huge demand for efficient, economical, and secure 24/7 healthcare systems, which can not only monitor the physical conditions of the patients but also store the data and give feedback to the patients under protection if necessary. Fortunately, with the rapid development of modern technology, eHealthcare systems provide the possibility to address such a demand. The concept of eHealthcare system meets the goals of "Triple Aim" for improving conventional healthcare nicely: improving the individual experience of care; improving the health of populations; and reducing the per capita costs of care for populations [4]. Concretely, by utilizing modern biomedical sensors, various types of networks, and cloud storage, an eHealthcare system can support all stages of care for the patients including prevention, diagnosis, treatment, and follow up remotely [5,6] as it is illustrated in Fig. 1.

Generally, an eHealthcare system has two types of communication protocols. One is the network around the human skin surface which supports the communication between the biomedical sensors and the centralized devices, while the other one is the pervasive network that supports the communications between the other parts in the eHealthcare system, including the cloud storage. In term of the communication protocol around the human skin surface, even though Bluetooth and Zigbee have been widely utilized in eHealthcare systems, their drawbacks are obvious. Since neither Bluetooth nor Zigbee is dedicated to eHealthcare data transmission, the frequency, data rate, power consumption, and security schemes are not suitable for eHealthcare circumstances [7]. In 2012, a communication protocol standard of IEEE 802.15.6 Wireless Body Area Networks (WBAN) was

☆ This work is partially supported by the National Science Foundation of China (Grant no. 61471075, 61671091).

* Corresponding authors.
E-mail addresses: knhan@stu.edu.cn (K. Han), ggjeon@gmail.com (G. Jeon).

https://doi.org/10.1016/j.future.2019.09.049
0167-739X/

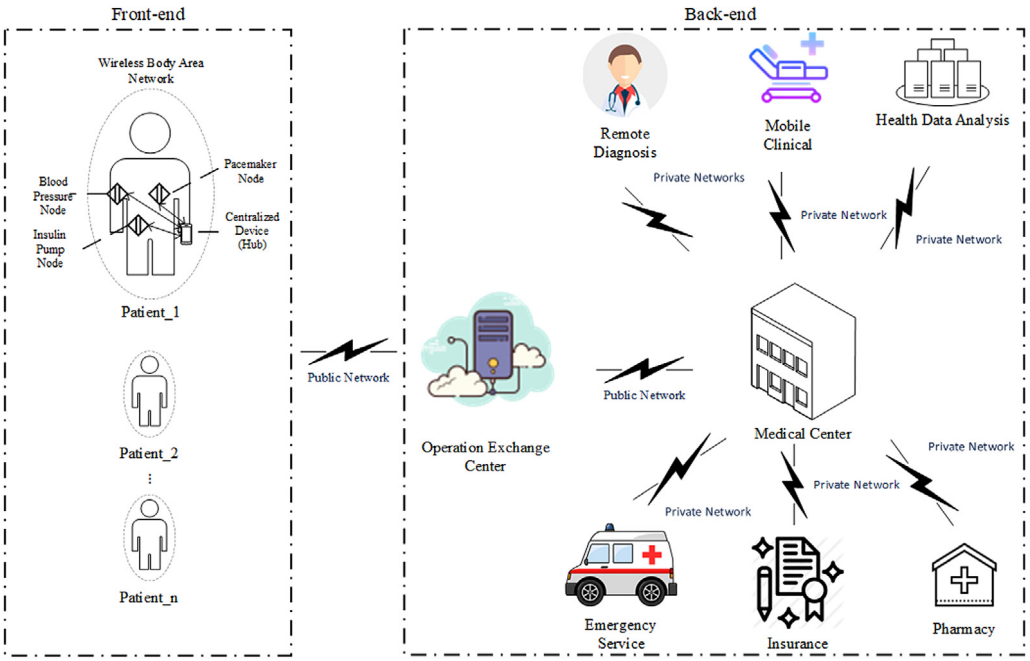


Fig. 1. Architecture of a typical eHealthcare system.

released. The standard specifies the details regarding the communication according to the characteristics of the data that needs to be transmitted between the biomedical sensors and centralized devices. To be more precise, compared to Bluetooth and Zigbee, WBAN is more sensitive to the power consumption due to the power supply constraints [8] while it has lower requirements for the frequency, data rate, and bandwidth since the data collected by the sensors is relatively simple and the transmission period could be much longer. As a theoretical analysis, article [6] compares the power consumption and usage of WBAN, Bluetooth, Zigbee, and WiFi protocols. It shows that the WBAN standards take 0.1 mW to less than 10 mW power consumption, which leads to weeks to months usage. While the Bluetooth and Zigbee protocols take 10 mW to 100 mW power consumption, which results in only days of usage. The IEEE 802.15.6 standard also specifies a lightweight security scheme consisting of authentication and encryption, which is dedicated to WBANs [9,10]. In addition, a novel data transmitting mechanism has been proposed for WBAN systems which improves the data transmission efficiency [11].

In recent years, the blockchain technology has attracted huge academic and industrial research attention due to its ability to provide trust in transactions and allow decentralized distributed systems for a wide range of activities [12–14]. By utilizing blockchains, different peers in the system can achieve the same functionality with the same amount of certainty without having a central authority [15–17].

eHealthcare systems are transmitting extremely private biomedical data which is directly related to the health condition of the patients, which will not be adopted if there are still security concerns. The interoperability and automation between medical services including medical professional, pharmacies, insurance companies, and emergency systems are relatively challenging for conventional medical systems.

The blockchain technology could be a solution for the urgent need of trust, security, and privacy for the healthcare system. It is possibly to use the blockchain to share data and provide smart contracts for healthcare. There are multiple potential use cases of blockchain-based medical data systems. Among the most significant cases are Electronic Health Records (EHRs) for personalized medicine. In personalized medicine, numerous sensors track various physiological state variables, such as blood sample data, exercise, nutrition, and various medicaments, and the collected data is used to infer the medicament dosing. The blockchain-based medical data system can resolve the challenges of providing the trusted prescriptions, medicaments, and sensor data in the exchange among medical practitioners, pharmacies, insurance companies and patients, such that no faulty data hinders the health/wellness regimen.

The blockchain can provide a distributed database where every change is strictly and permanently logged. Every change comes in the form of a transaction which is signed with a private key. Privacy is also mandated with access control rules so only those with the authority to view information or make changes can do so [18]. These properties are extremely useful in a healthcare system.

A blockchain-based eHealthcare system interoperating with WBAN is proposed in this paper. WBAN can be found in the front-end of the sensing subsystem, where it interconnects sensor nodes together, which in turn interact with a blockchain network found in the back-end. The front-end is also comprised of the users participating in the system. The WBAN handles communication between sensor nodes, and the blockchain handles secure storage of data. The blockchain does not exist to further secure the WBAN, which is already secure, and the WBAN also does not exist to provide communication between blockchain peers which maintain copies of the ledger, which are already communicating over encrypted internet channels. Both the WBAN and blockchain are orthogonal, and one does not address each other, but instead they interoperate to address challenges present in a eHealthcare system, by creating the proposed eHealthcare system. This is different from various eHealthcare solutions utilizing technologies such as Bluetooth Low Energy (BLE) and traditional databases.

Benefiting from the combination of WBAN and blockchain technologies, the advantages of the proposed system are as follows. First, the power consumption is relatively low in the local networks around the human skin surface of the patients. Secondly, data from different roles in the system are trustworthy. Thirdly, computation, analysis, and data storage are decentralized without having a central authority in the back-end. Further, the

immutability and non-repudiation properties of the blockchain back-end offer powerful anti-tampering logging and auditing. However, there are some disadvantages of blockchain technology. Due to the complexity of the algorithms, it requires high computing resources and power consumption at each node. Further, differences between blockchain platforms (such as Hyperledger, Ethereum, etc.) create incompatibilities, and make development a more difficult task.

These disadvantages were critical in the selection of the system architecture. The WBAN nodes could have theoretically also been blockchain network peers that each stores a copy of the ledger. This would have simplified the system architecture, by reducing the number of components. However, the interconnected sensor nodes are resource constrained, and cannot perform the complex computations required in the blockchain. For this reason, the system is separated into front and back ends, and the sensor nodes simply interact with a blockchain-based decentralized back-end. This is achieved by utilizing secured communication channels between the front-end and back-end. More precisely, data from the sensors is aggregated in a WBAN hub, or WBAN centralized device, from which it is transmitted to a back-end securely, through an exposed Representational State Transfer (REST) API secured with Transport Layer Security (TLS). All data transfers between REST clients and servers is encrypted. While there have been promising experimental evaluations of blockchain in low power nodes [19], they are unavailable to the public and relatively immature.

The motivation of the research is following. First, the blockchain technology can provide trusted networks when applying into finance, and insurance fields due to the features of decentralized storage and achieving consensus [20]. The security of eHealthcare system could also benefit from those features of the blockchain technology by including the technology in the implementation. Moreover, as the most fundamental element of the eHealthcare system, WBAN supports the communications between biomedical sensors attached or implanted in the human body with the centralized devices of the patients, which is protected by its own security scheme. The interoperation between the security scheme of WBAN and the security specifications of the blockchain-based eHealthcare system could be a challenge when they are working together with each other to ensure the security of the whole system. Few published works can be found regarding the security issues of interoperation between WBAN and eHealthcare systems [21,22], while all of them proposed the security scheme and privacy protection solution for non-blockchain eHealthcare systems. In this paper, a blockchain-based eHealthcare system interoperating with WBAN has been proposed, which is bringing together the advantages of both technologies in a compatible and meaningful way.

The paper is organized as follows. The preliminaries and related work are presented in Section 2. Afterward, in Section 3, the functionality description and system architecture of the proposed blockchain-based eHealthcare system interoperating with WBAN are demonstrated. Moreover, the implementation and evaluation of the proposed system are shown in Sections 4 and 5 respectively. Finally, Section 6 concludes the paper and lists potential ideas for future extensions of this work.

2. Preliminaries and related work

2.1. Wireless Body Area Network (WBAN)

In 2012, the IEEE 802.15.6 standard for WBAN was released, which specifies the communication parameters such as frequency, data rate, and so on based on the characteristics of the data transmission in WBAN. WBAN provides a communication protocol dedicated to the communications between the biomedical sensors and centralized devices around the human skin surface since it meets the requirements for efficient, economical, and uninterrupted health condition monitoring. Compared to conventional wireless communication protocols such as Bluetooth and Zigbee, the communication range, transmission speed, and bandwidth of WBAN are relatively small since the nodes in WBAN are extremely sensitive to the power consumption due to the battery supply constraints, which is especially true for implanted devices [7]. The IEEE 802.15.6 standard also specifies a unique lightweight security scheme consisting of authentication and encryption which provides enough data protection while the power consumption is also acceptable [23].

One of the most critical advantages that WBAN has compared to other wireless communication protocols is ultra-low power consumption at different data rates. For instance, when the data rate is 1 Mbps, the power consumption that WBAN can achieve is as low as 0.1 mW to 8 mW, while the power consumption of Bluetooth is between 8 mW to 100 mW. In addition, when the data rate is 100 kbps, the power consumption of WBAN is between 0.03 mW to 8 mW while it is 5 mW to 50 mW for ZigBee [7]. The wireless communication in WBAN has less interference, since it supports a large range of transmission frequencies from 400 MHz to 5 GHz, while ZigBee and Bluetooth are all working at 2.4 GHz [7]. Furthermore, the IEEE 802.15.6 standard specifies a unique security protocol to protect the communications in WBAN [22].

In terms of the security specifications of WBAN, there are three security levels specified in the communications of WBAN, which are level 0, level 1, and level 2 respectively [22]. The security level of the communications in WBAN is determined by the information contained in the communications. The communications identified as security level 0, which are unsecured communications, only contain non-confidential information such as timestamps. In these cases, neither authentication nor encryption is required. The communications specified as security level 1 contain private but not critical information such as name, age, gender, and locations, which shall not be accessed by someone does not has the authority. Therefore, authentication is necessary for these communications. In terms of the security level 2, the communications contain most confidential, as well as critical, information including biomedical data collected from the patients, the feedback from the hospitals and doctors, the parameters for the insulin pump, and so on. This data has a direct relationship with the physical conditions of the patients and intruding into these communications could cause fatal health issues. Therefore, for the communications specified as security level 2, both authentication and encryption are required. In terms of the methods used for authentication and encryption, the IEEE 802.15.6 standard has specified the validation of certificates as the method for authentication, and Elliptic-curve Cryptography (ECC) as the way to generate the key for Advanced Encryption Standard (AES), which is the encryption method to be used [24]. The standard also leaves some room for the engineers to improve the security performance of the WBAN systems regarding the detailed implementations of the security scheme of WBAN.

2.2. Blockchain basics

In 2008, blockchain was invented by Satoshi Nakamoto [25] to serve as the public transaction ledger of the bitcoin, which addressed the issue of double spending for digital currency without a trusted authority. Afterward, the blockchain technology has been applied to various areas such as finance, insurance, as well as healthcare systems [26]. Meanwhile, a lot of research attention has been given to various areas of blockchain in recent

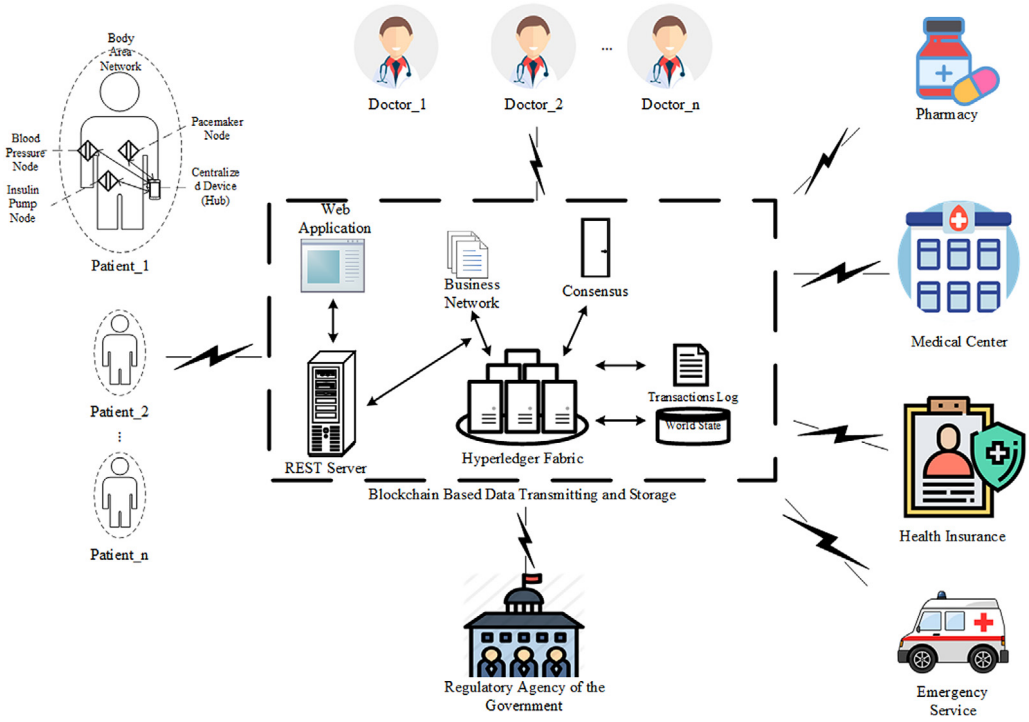


Fig. 2. Architecture of the proposed system.

years such as the blockchain platform with different features [27], application of blockchain in mobile devices [28], and processing methods for different data types in blockchain [29–31].

Generally speaking, blockchain is a technology which can build a distributed database consisting of a list of blocks. The blocks in the database are connected with each other, and every node in the blockchain can not only generate the blocks but also store them. In terms of the data structure of the block, it contains the timestamp of its generation, the hash of the previous block, and the transaction data [17]. Different nodes in the blockchain can achieve consensus without a trusted authority, which provides better privacy protection than conventional centralized network technologies [16,32].

2.3. Related work

The personal data collected by biomedical sensors in WBAN and other health-related data in the eHealthcare system (including blood pressure, glucose level, parameters for an insulin pump, parameters for pacemakers, and so on) are extremely critical and hacking into the eHealthcare system could cause fatal health issues [33]. The blockchain technology provides a potential solution of distributed data management for eHealthcare systems.

There are few publications discussing the possibility of applying the blockchain technology to healthcare applications. In 2016, [34] proposed a secure system for pervasive social network based healthcare, while the authors focused more on the network side instead of the realistic medical application circumstances. In the article [35], the authors discussed the utilization of blockchain distributed ledger technologies for biomedical and health care applications. The benefits of blockchain for biomedical and health care applications were illustrated in the paper, while the system architecture and detailed implementation were not given. A decentralized personal data management system using blockchain was proposed in 2015 [36]. This research focused on the privacy protection and data management of personal data, while the system architecture of the eHealthcare system was not given. Article [37] proposed a blockchain based medical data access and permission management system called MedRec. Benefiting from the decentralized feature of the blockchain, it manages authentication, confidentiality, accountability and data sharing — crucial considerations when handling electronic medical records (EMRs). Also, it discussed the cooperation between the proposed system and the Health Insurance Portability and Accountability Act (HIPAA) for continued health insurance coverage for patients having different medical services in different locations. In the paper [38], the authors implemented a healthcare industry application, Healthchain, using IBM Blockchain initiative, which illustrates multiple advantages than the conventional medical systems.

3. Proposed blockchain-based eHealthcare system interoperating with WBAN

3.1. System architecture

Fig. 2 illustrates the architecture of the proposed blockchain-based eHealthcare system. In terms of the roles in the proposed system, there are patients, medical doctors, medical center(s), insurance providers, medicament suppliers (including common pharmacies) and emergency services, all of which consist the users of the system. The detailed functionality and operations of each role are specified by smart contracts between the parties, and its overall operation is demonstrated in the following subsections. The data transmission between the sensors and centralized devices around the patients is supported by WBAN based on the IEEE 802.15.6 standard, while the data transmission and storage applies to all the roles in the proposed system.

3.2. Roles in the proposed blockchain-based eHealthcare system

As aforementioned, there are six roles in the proposed system which are patients, doctors, medical center(s), emergency services, insurance providers, and medicament suppliers, as shown in Fig. 2.

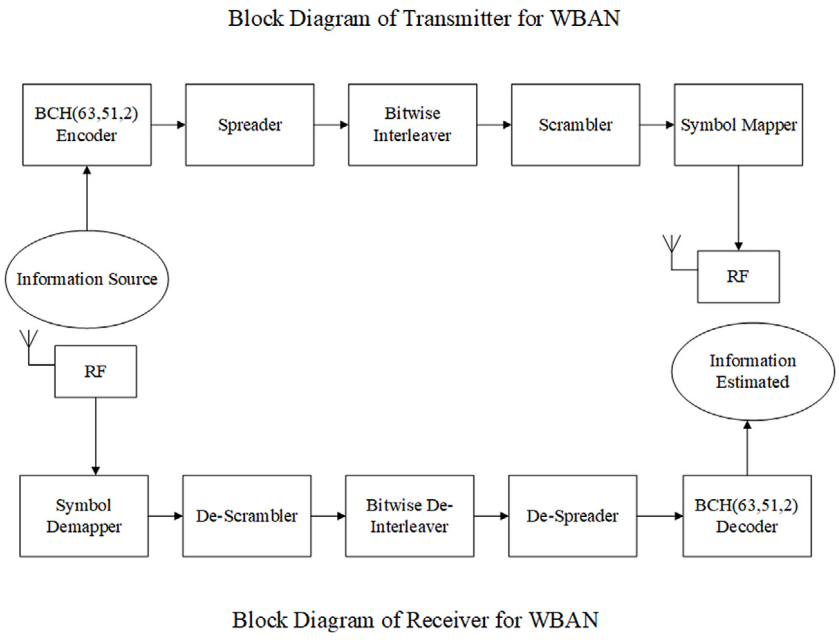


Fig. 3. Block diagram of transceiver for WBAN.

As the most fundamental part of the eHealthcare system, patients need to transmit the biomedical data collected from the sensors to the centralized devices for every period of time t which is specified by the stack of the centralized devices. The centralized devices give the latest instructions to the sensors. The communication protocol in this scenario is WBAN which is dedicated to the communications between the sensors and the centralized devices. Afterward, the centralized devices generate the information structure which contains the patients' ID, patients name, corresponding medical doctor, time, and location information, then submit a transaction to the blockchain network in order to update the physical data of the patients.

In terms of medical professionals, every individual physician only has access to the physical record of the patients who have been assigned to them. Doctors could also give medical instructions to the patients by submitting transactions to update the medical instructions. The structure, in this case, contains corresponding patient, the ID of the doctor, medical instructions, and time. The patients who are assigned to the specific doctor grant access to their own medical instructions.

Medical centers and emergency services are two parts that interoperate with each other closely in the proposed eHealthcare system. Medical centers have the highest authority to access all of the medical data in the blockchain. There are two functionalities for the medical centers, one is assigning different doctors to various patients, while the other is to assign the emergency services to specific patients based on the physical condition of the patients, which are collected by the WBAN around the patients. Once the emergency service has been assigned to a patient, the emergency service will grant access to all the medical and physical record related to the specific patient until the emergency service is terminated. For patients that need renewable supplies of medicament, the contract between the patient, insurance providers and medicament suppliers (both the original producers and distributors such as pharmacies) specify the exact condition under which the medicament renewal is safe to supply, as well as when all the payments are received. The feedback information on the quantities of medicament is also made available (under all privacy protection mechanisms) to physicians and medicament makers, such that the dosing of the medicament can be optimized and also personalized for a given patient.

The government is playing a more and more significant role in the modern healthcare systems in recent years especially for the quality monitoring of the medical services and infectious disease predictions based on the big data analysis [39]. In the proposed blockchain based eHealthcare system, the regulatory agency of the government is one of the roles. It has access to all of the transactions in the blockchain.

3.3. WBAN in the proposed eHealthcare system

In the scenarios of the proposed eHealthcare system, WBAN has been utilized as the communication solution for the data transmission between the sensors and centralized devices around the patients. As specified by the standard, the transceivers of WBAN consist of BCH encoder, spreader, bitwise interleaver, scrambler, symbol mapper, RF front end, and corresponding inverse operation modules [10] as illustrated in the Fig. 3. Benefitting from the nature of WBAN [7], the power consumption for the patient's side has been reduced dramatically compared to Bluetooth. The detailed implementation and evaluation of the WBAN in the proposed system are demonstrated in Sections 4 and 5.

3.4. Blockchain based data transmitting and storage in the proposed eHealthcare system

In a conventional medical system, all the data is stored in a central database. Based on the roles in the medical system, different users shall have various permissions to access different types of data. For instance, medical doctors shall have access to all the data belonging to their corresponding patients, while an ambulance shall have access to the location and the historical medical record of a patient who has been assigned to rescue. However, the drawbacks are obvious: once the central database has been attacked or the data in a central database has tampered, all the participants of the system will be impacted. In a blockchain-based system, the ledger is append-only and distributed. There is no single point of failure, and tampering is not feasible. Altering data requires submitting a correction transaction which is subject to the nonrepudiation properties of the blockchain, that is, every

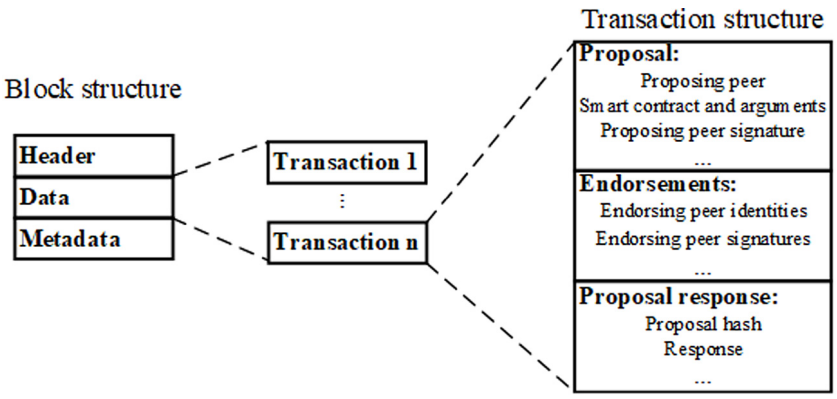


Fig. 4. Block and transaction structures.

transaction is cryptographically signed and secure. Further, the transaction needs to be endorsed by the relevant parties. The combination of an append-only ledger requiring cryptographically signed transactions achieves powerful, immutable logging and auditing. The endorsement also ensures the transactions will only be accepted if they meet the endorsement policies specified in the medical system. Last but not least, the privacy of data and access to it can be enforced through access control rules.

The blockchain-based data transmitting and storage module is composed of several sub-modules, each of which has a different function.

Hyperledger Fabric is the core of the blockchain module, it is a distributed ledger technology (DLT) platform designed for the enterprise. In an enterprise use case, several things need to be considered. For instance, the participants need to have identities, the networks need to be permissioned, and the transactions need to be private and confidential. Hyperledger Fabric was designed with these things in mind. It is configurable and supports modular consensus protocols, which need not require a cryptocurrency to incentivize mining or smart contract execution. This reduces the risk of attacks and makes the computational power required compared to that of any other distributed system.

Hyperledger Fabric relies on two components, the transaction log, and the world state, to make a ledger. Concisely, the world state is the current state of the ledger, that is, a key–value pair (kvp) database showing the state of the system at any given moment. The transaction log, on the other hand, also called blockchain, is the log of all transactions, consisting of all the changes that have been made to the world state that result in the current state of it. Following the transaction log can recreate the current world state. A good analogy for the world state and transaction log is the current balance and history of transactions in a banking account. It is easy to understand that following the history from the creation of the banking account will result in the current balance. The ledger is replicated on every peer.

As discussed, Hyperledger Fabric does not feature or incentivize mining. In fact, it does not use computationally expensive consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) varieties whatsoever. Instead, various consensus algorithms, for example, Byzantine or crash fault tolerant, can be implemented. The way this is achieved is by ensuring that the participants are identified and authenticated in order to submit transactions. In other words, the network is permissioned and participants trust each other, albeit not to an unconditional extent.

Hyperledger Fabric achieves consensus by ensuring that all transactions taking place are confirmed to be correct and happen in order. A transaction flow will be presented here. The transaction will be proposed at first by a peer, and then sent to endorsing peers as specified by the endorsement policies. The transaction will then be simulated by the endorsing peers that will validate and vote for the transaction. The results are then broadcast to the ordering service, which will order the transactions into lists of records called blocks, before sending them to the peers, where they are finalized in each peer's copy of the distributed ledger.

Blocks, responsible for the naming of the blockchain, are an integral part of any blockchain platform. In Hyperledger Fabric they are comprised of a header, a data section that contains one or more transactions which have been ordered, and a trailer that contains metadata. The blocks are connected together using cryptographic methods; more specifically, a block's header will contain a hash of the previous block.

Fig. 4 illustrates a diagram of a block and a transaction respectively, indicating what are the contents of the block, and transaction(s) found within the block, in more detail to aid with the visualization of the transaction flow and the ordering of transactions into blocks.

Using Hyperledger tools, a business network is deployed on Fabric, which implements the architecture of the system. The business network contains assets, participants, and transactions, the combination of which is called the model of the network, transaction functions, also called smart contracts, and access control rules. An example of a network asset is a patient's medical record, an example of a network participant is a user of the system, such as a patient, and an example of a network transaction is updating the patient's medical record using the immutability property found in blockchains. The participants are essentially images of the users within the network, and users can be associated with an identity. The identity is used to connect to the business network and is subject to the specified access control rules mentioned above. An example of access control would be that a patient identity may only view information related to itself, whereas a medical center would have access to all its patients.

Access to the business network needs to be available to the participants, and in order to do so, the network is exposed as a REST API. The REST servers are configured to be secured with TLS, and all communication between them and the clients is encrypted. The REST servers allow a web application to interface with the business network and Hyperledger Fabric. The web application is used by the users to access the blockchain-based data transmitting and storage system, where they sign in to the business network with their identity, through the REST servers. The REST servers can also be accessed by the WBAN front-end nodes that aggregate data.

4. Implementation of the proposed blockchain-based eHealthcare system interoperating with WBAN

To evaluate the proposed blockchain-based eHealthcare system, a miniBEE platform which contains a Xilinx Vertex

6 XC6VSX475T FPGA and runs CentOS, one smartphone with Android operating system, and two PCs have been utilized to simulate all the roles in the proposed system. The miniBEE platform is a high-performance BEEcube-based Software Defined Radio (SDR) platform with RF, FPGA, CPU, and network interfaces, fully programmable from Matlab/Simulink and proprietary software. The miniBEE was provided by CMC Microsystems. The miniBEE platform is running the WBAN transceiver specified by the IEEE 802.15.6 standard to simulate a patient in the WBAN environment in the proposed system, while the blockchain network is deployed on the Hyperledger Fabric platform.

4.1. Implementation of the blockchain in the proposed system

For the blockchain-based data transmitting and storage module evaluation, the Hyperledger Fabric platform version 1.0 is used. Additionally, the Hyperledger Fabric Composer framework is used to model and deploy the business network on Fabric, and Hyperledger Composer REST server is used to expose the business network as a REST API. For the web application, Node-RED is used.

For the implementation, Fabric is configured with simple parameters of one peer node belonging to one organization, one certificate authority (CA), and one orderer node. Fabric supports two ordering services, SOLO and Kafka. The orderer is running the SOLO ordering service, which is a simple non-production ordering service consisting of a single process. Kafka is based on the Apache Kafka and offers crash fault tolerance by supporting several nodes. In the system there is no real consensus taking place as there is a single orderer node, however, SOLO is considerably easier to set up, and is the preferred approach for development and testing. In a production environment this would not acceptable, and as such using Kafka would be mandatory.

All the Fabric processes (peers, certificate authority, and orderer) ran inside Docker containers, with them, as well as the Fabric Composer framework, and REST server running in an Ubuntu 16.04 LTS 64-bit virtual machine.

In the model of the business network deployed on Hyperledger Fabric describing the architecture of the blockchain-based data transmitting and storage system, six participants, one asset, and four transactions are defined. The transactions are implemented in javascript, as transaction functions, also called chaincode or smart contracts. Access control rules are also specified, allowing or denying access to resources depending on the identity of the user, which is tied to a specific participant.

The participants are doctors, patients, medical centers, or hospitals, emergency services, or ambulances, medicament suppliers, or pharmacies, insurance companies and last but not least, the regulatory agency of the government. The asset is the patient health records, which contain information on both the patients and their doctors. Last but not least, the transactions can update the health records by submitting health information from the patients' side, update the health records with medical instructions from the appropriate doctor, as well as assign and remove an emergency service participant to a patient. The insurance companies are aware of all medical instruction submitted. Any payments that may be required are automatically made when a medical instruction is submitted, as part of the same transaction. Medicaments are also supplied if necessary. The insurance companies can automatically pay when needed, but they also have access to a plethora of information which can be used to form statistics. Meaningful statistics are extremely powerful for insurance companies, as they can be used to accurately compute risks and premiums by actuarial principles.

The business network is defined in the Hyperledger Composer Modeling Language, which is used to describe the participants, assets, and transactions. A Unified Modeling Language (UML) class diagram of the business network model was created, using PlantUML, which is featured in Fig. 5. In the diagram, the network is modeled to clearly show participants, assets, and transactions. A participant (for instance patient) or asset (for instance the patient's health record) that is added to the network will implement an instance of the respective participant or asset (Patient or PatientHealthRecord) found in the model.

Access control rules are used to allow or deny access as needed. For example, patients may only view their own health record, whereas doctors may only view their patients' health records. A medical center may view the health records of all the patients that use it. The emergency services temporarily gain or lose access to patient health records, as necessary. Medicament suppliers may view health records of patients that require medicaments, however less personalized information such that they cannot, for instance, view the name of a patient. Insurance companies may access all the data of their customers should the latter party agrees, be it individuals like patients or organizations like medical centers. The above properties can be found described in the Hyperledger Composer Access Control Language and control the network by providing declarative access control over the modeled elements. They can be used to determine which users can read, create, update, or delete elements in the business network. Participant instances are associated with identities, which essentially are the users that can perform operations on the network, and are subject to the aforementioned access control rules.

4.2. Implementation of the WBAN in the proposed system

The WBAN in the proposed system is implemented by the MiniBEE4 software defined radio (SDR) platform for evaluation purposes. The Virtex-6 XC6VSX475T Xilinx FPGA embedded in the MiniBEE 4 platform runs a baseband transmitting module and a receiving module of WBAN, two Square-Root Raised Cosine (SRRC) filters, a digital down converter (DDC), and a low-pass filter. The FMC111 radio frequency (RF) front end is embedded in the platform, which consists of a digital–analog converter (DAC), a up converter, an amplifier, a low noise amplifier (LNA), a down converter, a band-pass filter, and a digital–analog converter, which are used to process the RF transmission. Two omnidirectional antennas have been utilized as the transmitting antenna and receiving antenna. Furthermore, a microcontroller unit (MCU) has been connected to the FPGA to generate and verify the source data. The architecture of the implementation of WBAN in the proposed system is demonstrated in Fig. 6.

5. Evaluation of the proposed system

The evaluation environment of the proposed blockchain-based eHealthcare system interoperating with WBAN is performed as shown in Table 1. A web application has been provided to every role in the system to have access to the blockchain-based data transmitting and storage system. Detailed evaluation has been separated into two parts, which are the evaluation of the blockchain-based data transmitting and storage system and WBAN respectively.

5.1. Blockchain-based data transmitting and storage in the proposed system

The average latency to process a transaction was measured to be approximately 2350 ms per transaction. This is the latency to submit a transaction, all the way from aggregating the data in a sensor node hub and sending it through the REST API to the blockchain back-end, to the proposal, endorsement, and ordering

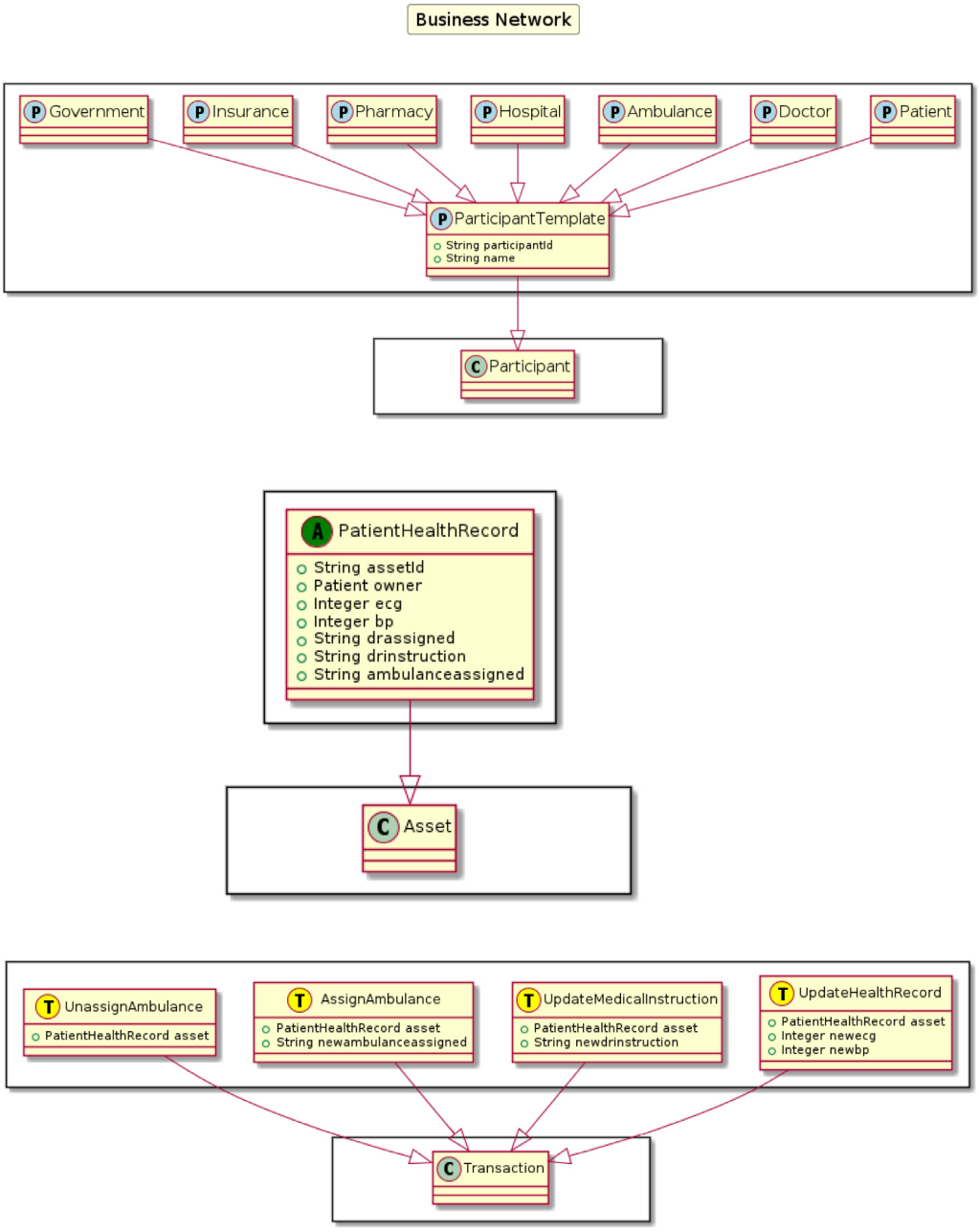


Fig. 5. UML class diagram showing the business network model.

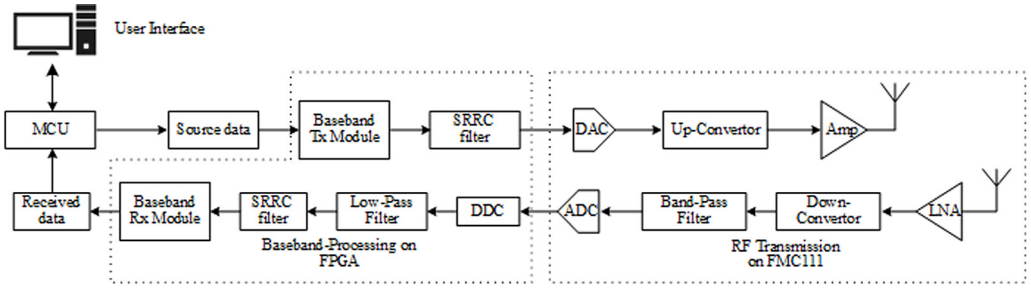


Fig. 6. Implementation of WBAN in the proposed system.

of the transaction into a block. This latency would theoretically allow up to 51 users to submit transactions to the system once every two minutes each, assuming no transactions ever overlap. This is also only taking into consideration biomedical data that updates patient health records, other transactions would need to execute too.

Table 1
Evaluation environment.

Roles	Evaluation environment
Patients and WBAN	BEECube MiniBEE4
Blockchain based data transmitting and storage	Hyperledger Fabric
Doctors	PC
Medical center(s)	PC
Emergency service	PC

Table 2
System parameters.

SDR evaluation platform	BEEcube miniBEE4
Radio frequency	915 MHz
Middle frequency	30.72 MHz
ADC sample rate	250 Msps
Modulation	$\pi/4$ DQPSK
Baseband symbol rate	31.25 Msps

Table 3
Hardware resource utilization of the baseband test demo module.

Hardware resources[a]	Specifications	Utilization ratio
LUTs	14,805/297,600	4%
Registers	11,707/595,200	1%
Memory	81/1,064	7%
DSPs	190/2,016	9%
Clock frequency	250 MHz	–

[a]FPGA platform: Virtex-6 XC6VSX475T Xilinx FPGA.

This number is influenced by various parameters such as the number of peers, the number of machines the peers are running on, as well as the computational power of the physical, or virtual, machines themselves, or even network latency in the case of multiple physical machines. The most important parameters, however, are the ordering service used in Hyperledger Fabric, and its configuration. As discussed above, the SOLO ordering service is centralized and consists of a single process running on a single node. SOLO is therefore acceptable for testing purposes, but not for a production environment.

Further, the achieved performance is insufficient to support a realistic situation of a regular sized medical center. Therefore optimizations in the blockchain would be necessary. Tweaking the blockchain ordering service to create blocks more frequently could improve performance for instance. Moreover, Hyperledger Fabric employs MultiVersion Concurrency Control (MVCC) to prevent the double spending problem. Therefore, overlapping transactions are not executed. Workarounds for this could be implementing a queue between the users and the blockchain back-end, which ensures that transactions will execute until they succeed. Another performance gain could be achieved by performing bulk reads/writes during MVCC validation and commit [40]. [40] showcases a more complete work regarding Hyperledger performance and optimizations.

5.2. WBAN in the proposed system

As aforementioned, the implementation of the WBAN part of the proposed system is performed on the BEEcube miniBEE4 platform. The setup of parameters for the FMC111 RF front end is demonstrated in Table 2, where the 915 MHz radio frequency and $\pi/4$-DQPSK modulation are defined in the IEEE 802.15.6 standard. Note that the 915 MHz frequency band is the free Industrial Scientific Medical Band (ISM) in North America. While the $\pi/4$-DQPSK modulation supports the highest transmission data rate in the mandatory feature in IEEE 802.15.6 standard. Meanwhile, the parameters, such as frequency band and modulation methods, could be easily reconfigured in the SDR platform. The other parameters are set up according to the practical system requirements. The detailed evaluation results regarding the utilization of Look Up Tables (LUTs), registers, memory, and Digital Signal Processing Units (DSPs) are illustrated in Table 3. Firstly, it can be found that the proposed design utilizes a quite low hardware resource, which means, on one hand, the SDR platform is quite extensive for further improvement. On the other hand, however, the proposed design could be implemented with low hardware cost in a future ASIC chip. An SDR platform based evaluation is presented in this work as an early functional verification prototype. The advantage of SDR platform lies on an easily re-configurable feature. Even though the power and energy efficiency of SDR platform outperforms CPU, GPU platforms, it is not comparable to ASIC implementation. In our previous work, we implemented a WBAN transmitter and receiver with ASIC as [9], which shows extremely low power and energy consumption.

The symbol rate of the WBAN implementation achieves 31.25 Msps, which means the data rate is up to 62.5 Mbps. As the centralized sensor hub has been set up to perform transactions in the blockchain every two minutes while the size of biomedical data in the eHealthcare system is between 10k bits to 1M bits as specified by the proposed implementation, the data rate that can be supported in WBAN is more than sufficient in order for it to interoperate with the blockchain-based system, and can even be extended in the future for larger transactions.

As can be seen from the evaluation results, the WBAN implementation of the proposed blockchain-based eHealthcare system has relatively low hardware resources utilization. The symbol rate and frequency of the WBAN implementation demonstrate that it could interoperate with the blockchain-based data transmission and storage system in the proposed system properly since the sensor hub has been set up to perform transactions every two minutes.

6. Conclusion and future work

In this paper, a blockchain-based eHealthcare system interoperating with WBAN, which follows the specifications in the IEEE 802.15.6 standard, has been proposed. The evaluation results demonstrate that the proposed system has the advantages of low hardware utilization, high-security protection level, and stable performance. Therefore, the proposed eHealthcare system has great potential to be applied in modern medical systems.

In the future, more research will follow in this project. First, research regarding improving the blockchain network of the system will be undertaken, since the blockchain network can only support a maximum of 51 users for now, which is not suitable for a medical center with a large number of patients and doctors. More practical evaluations in the medical institutions will also be investigated to explore the performance of the proposed system in practical medical circumstances. As such, the technology will potentially be more competitive against traditional large data processing systems and databases [41].

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] World Health Organization, WHO—Address to the Sixty-ninth World Health Assembly, Tech. Rep., World Health Organization, 2016, URL http://www.who.int/dg/speeches/2016/wha-69/en/.

[2] B. Barua, Waiting Your Turn: Wait Times for Health Care in Canada, 2017 Report, Tech. rep., Fraser Institute, 2018, URL https://www.fraserinstitute.org/sites/default/files/waiting-your-turn-2017.pdf.

[3] L.V. Jian, Improvement of hierarhical diagnosis and treatment system under deepening medical and health reform, Chin. Hosp. Manag. 34 (6) (2014) 1–3.

[4] D.M. Berwick, T.W. Nolan, J. Whittington, The triple aim: Care, health, and cost, Health Aff. 27 (3) (2008) 759–769, http://dx.doi.org/10.1377/hlthaff.27.3.759, URL http://www.healthaffairs.org/doi/10.1377/hlthaff.27.3.759.

[5] I. Iakovidis, Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe 1, Int. J. Med. Inf. 52 (1998) 105–115, URL https://ac.els-cdn.com/S1386505698001294/1-s2.0-S1386505698001294-main.pdf?_tid=004bb9d4-1cce-4d37-86ed-710d968a710e&acdnat=1530814922_030611789b16d0a2fec5fe31e754bfcf.

[6] G. Papanastasiou, A. Drigas, C. Skianis, M. Lytras, E. Papanastasiou, Patient-centric ICTs based healthcare for students with learning, physical and/or sensory disabilities, Telemat. Inform. 35 (4) (2018) 654–664, http://dx.doi.org/10.1016/j.tele.2017.09.002, URL https://linkinghub.elsevier.com/retrieve/pii/S0736585316304919.

[7] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour, Wireless body area networks: A survey, IEEE Commun. Surv. Tutor. (2014) http://dx.doi.org/10.1109/SURV.2013.121313.00064.

[8] K.S. Kwak, S. Ullah, N. Ullah, An overview of IEEE 802.15.6 standard, in: 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL 2010, IEEE, 2010, pp. 1–6, http://dx.doi.org/10.1109/ISABEL.2010.5702867, URL http://ieeexplore.ieee.org/document/5702867/.

[9] J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A lightweight multi-layer authentication protocol for wireless body area networks, Future Gener. Comput. Syst. 78 (2018) 956–963, http://dx.doi.org/10.1016/J.FUTURE.2016.11.033, URL https://www.sciencedirect.com/science/article/pii/S0167739X16306963.

[10] J. Wang, K. Han, A. Alexandridis, Z. Zilic, J. Lin, Y. Pang, X. Yang, A baseband processing ASIC for body area networks, J. Ambient Intell. Humaniz. Comput. 0 (2018) 3, http://dx.doi.org/10.1007/s12652-018-0870-8.

[11] M. Ambigavathi, D. Sridharan, Energy efficient and load balanced priority queue algorithm for Wireless Body Area Network, Future Gener. Comput. Syst. (2018) http://dx.doi.org/10.1016/J.FUTURE.2018.05.044, URL https://www.sciencedirect.com/science/article/pii/S0167739X18308458.

[12] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) http://dx.doi.org/10.1016/J.FUTURE.2017.08.020, URL https://www.sciencedirect.com/science/article/pii/S0167739X17318332.

[13] M. Swan, Blockchain : Blueprint for a New Economy, O'Reilly Media, Inc., 2015, URL https://books.google.ca/books?id=4vFiBgAAQBAJ&dq=blockchain&lr=.

[14] M.-A. Sicilia, A. Visvizi, Blockchain and OECD data repositories: opportunities and policymaking implications, Libr. Hi Tech 37 (1) (2019) 30–42, http://dx.doi.org/10.1108/LHT-12-2017-0276, URL https://www.emeraldinsight.com/doi/10.1108/LHT-12-2017-0276.

[15] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190, http://dx.doi.org/10.1016/J.FUTURE.2018.05.046, URL https://www.sciencedirect.com/science/article/pii/S0167739X17329205.

[16] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: Challenges and opportunities, Future Gener. Comput. Syst. 78 (2018) 544–546, http://dx.doi.org/10.1016/J.FUTURE.2017.07.060, URL https://www.sciencedirect.com/science/article/pii/S0167739X17316667.

[17] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access (2016) http://dx.doi.org/10.1109/ACCESS.2016.2566339.

[18] hyperledger-fabricdocs Documentation Release master hyperledger, 2019, URL https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/release-1.4/hyperledger-fabric.pdf.

[19] A. Dorri, S.S. Kanhere, R. Jurdak, Towards an optimized blockchain for IoT, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, IoTDI'17, ACM Press, New York, USA, 2017, pp. 173–178, http://dx.doi.org/10.1145/3054977.3055003, URL http://dl.acm.org/citation.cfm?doid=3054977.3055003.

[20] Z. Xie, S. Dai, H.-N. Chen, X. Wang, Blockchain challenges and opportunities: a survey, in: International Congress on Big Data, Vol. 14, (4) 2018, pp. 352–375, URL https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf.

[21] M. Barua, M.S. Alam, Xiaohui. Liang, Xuemin. Shen, Secure and quality of service assurance scheduling scheme for WBAN with application to eHealth, in: 2011 IEEE Wireless Communications and Networking Conference, IEEE, 2011, pp. 1102–1106, http://dx.doi.org/10.1109/WCNC.2011.5779285, URL http://ieeexplore.ieee.org/document/5779285/.

[22] A. Soceanu, M. Vasylenko, A. Egner, T. Muntean, Managing the privacy and security of eHealth data, in: 2015 20th International Conference on Control Systems and Computer Science, IEEE, 2015, pp. 439–446, http://dx.doi.org/10.1109/CSCS.2015.76, URL http://ieeexplore.ieee.org/document/7168466/.

[23] J. Wang, K. Han, A. Alexandridis, Z. Zilic, Y. Pang, J. Lin, An ASIC implementation of security scheme for body area networks, in: 2018 IEEE International Symposium on Circuits and Systems, ISCAS, IEEE, 2018, pp. 1–5, http://dx.doi.org/10.1109/ISCAS.2018.8351098, URL https://ieeexplore.ieee.org/document/8351098/.

[24] Institute of Electrical and Electronics Engineers, IEEE-SA Standards Board, IEEE standard for local and metropolitan area networks. Part 15.6, Wireless body area networks, Institute of Electrical and Electronics Engineers, 2012, p. 257, URL https://ieeexplore.ieee.org/document/6161600.

[25] E. Staff, Blockchains: The great chain of being sure about things, Econ. Retriev. 18 (2016).

[26] G. Osband, Blockchain: The Concept for Health Plan CMOs, Tech. Rep., EXL Digital Intelligence center, 2018, URL https://www.exlservice.com/resources/assets/library/documents/Blockchain_The_Concept_for_Health_Plan_CMOs.pdf.

[27] M. Muzammal, Q. Qu, B. Nasrulin, Renovating blockchain with distributed databases: An open source system, Future Gener. Comput. Syst. 90 (2019) 105–117, http://dx.doi.org/10.1016/J.FUTURE.2018.07.042, URL https://www.sciencedirect.com/science/article/pii/S0167739X18308732#!.

[28] B. Nasrulin, M. Muzammal, Q. Qu, ChainMOB: Mobility analytics on blockchain, in: 2018 19th IEEE International Conference on Mobile Data Management, MDM, IEEE, 2018, pp. 292–293, http://dx.doi.org/10.1109/MDM.2018.00056, URL https://ieeexplore.ieee.org/document/8411296/.

[29] I. Nurgaliev, M. Muzammal, Q. Qu, Enabling blockchain for efficient spatio-temporal query processing, in: International Conference on Web Information Systems Engineering, WISE 2018, Springer, Cham, 2018, pp. 36–51, http://dx.doi.org/10.1007/978-3-030-02922-7_3, URL http://link.springer.com/10.1007/978-3-030-02922-7_3.

[30] B. Nasrulin, M. Muzammal, Q. Qu, A robust spatio-temporal verification protocol for blockchain, in: International Conference on Web Information Systems Engineering, Springer, Cham, 2018, pp. 52–67, http://dx.doi.org/10.1007/978-3-030-02922-7_4, URL http://link.springer.com/10.1007/978-3-030-02922-7_4.

[31] Q. Qu, I. Nurgaliev, M. Muzammal, C.S. Jensen, J. Fan, On spatio-temporal blockchain query processing, Future Gener. Comput. Syst. 98 (2019) 208–218, http://dx.doi.org/10.1016/J.FUTURE.2019.03.038, URL https://www.sciencedirect.com/science/article/pii/S0167739X18314213#!.

[32] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660, http://dx.doi.org/10.1016/J.FUTURE.2013.01.010, URL https://www.sciencedirect.com/science/article/pii/S0167739X13000241.

[33] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. 28 (3) (2012) 583–592, http://dx.doi.org/10.1016/J.FUTURE.2010.12.006, URL https://www.sciencedirect.com/science/article/pii/S0167739X10002554.

[34] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, IEEE Access (2016) http://dx.doi.org/10.1109/ACCESS.2016.2645904.

[35] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inf. Assoc. 24 (6) (2017) 1211–1220, http://dx.doi.org/10.1093/jamia/ocx068, URL https://academic.oup.com/jamia/article/24/6/1211/4108087.

[36] G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184, http://dx.doi.org/10.1109/SPW.2015.27, URL http://ieeexplore.ieee.org/document/7163223/.

[37] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data, OBD, IEEE, 2016, pp. 25–30, http://dx.doi.org/10.1109/OBD.2016.11, URL http://ieeexplore.ieee.org/document/7573685/.

[38] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology & Engineering Management Conference, TEMSCON, IEEE, 2017, pp. 137–141, http://dx.doi.org/10.1109/TEMSCON.2017.7998367, URL http://ieeexplore.ieee.org/document/7998367/.

[39] J. Archenaa, E.A.M. Anita, A survey of big data analytics in healthcare and government, Procedia Comput. Sci. 50 (2015) 408–413, http://dx.doi.org/10.1016/J.PROCS.2015.04.021, URL https://www.sciencedirect.com/science/article/pii/S1877050915005220.

[40] P. Thakkar, S. Nathan, B. Viswanathan, Performance benchmarking and optimizing hyperledger fabric blockchain platform, in: 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, MASCOTS, IEEE, 2018, pp. 264–276, http://dx.doi.org/10.1109/MASCOTS.2018.00034, URL https://ieeexplore.ieee.org/document/8526892/.

[41] T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.-L. Tan, Blockbench, in: Proceedings of the 2017 ACM International Conference on Management of Data, SIGMOD'17, ACM Press, New York, USA, 2017, pp. 1085–1100, http://dx.doi.org/10.1145/3035918.3064033, URL http://dl.acm.org/citation.cfm?doid=3035918.3064033.

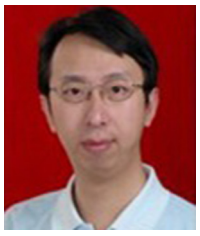
Junchao Wang was born in 1990. He received the B.E. degree in Microelectronics from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2013, the M.S. degree in Electrical Engineering from Illinois Institute of Technology, Chicago, US, in 2015, and the Ph.D. degree in Electrical Engineering from McGill University, Montreal, Canada, in 2019. Currently, he is an Assistant Professor with the Department of Biomedical Engineering, Shantou University. His current research interests include Body Area Network, stochastic computing, low power VLSI, and CNFET.

Kaining Han was born in 1991. He received the B.E. degree and Ph.D. degree in communication engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2014 and 2019. He was a Graduate Research Trainee with the Department of Electrical and Computer Engineering of McGill University, Montreal, Canada. Currently, he is an Assistant Professor with the Department of Biomedical Engineering, Shantou University. His research interests include high-speed low-power DSP technology with VLSI, wireless body area networks and stochastic computing based system designs.

Anastasios Alexandridis received the B.Sc. degree in Computer Engineering from Frederick University, Nicosia, Cyprus, in 2015, and his M.Sc. degree in Analog Electronics from the University of Edinburgh, Edinburgh, UK, in 2016. He is currently pursuing his Ph.D degree working together with the Integrated Microsystems Laboratory in McGill University, Montreal, Canada. His current research interests include but are not limited to Cloud, Internet of Things (IoT), Blockchains, and Body Area Networks.

Zhiyu Chen was born in 1997. He is currently pursuing the B.E. degree in Electrical Engineering in McGill University, Montreal, Canada, since 2015. His current research interest is Body Area Network.

Zeljko Zilic received the B.Eng. degree from the University of Zagreb, Zagreb, Croatia, and the M.Sc. and Ph.D. degrees from the University of Toronto, Toronto, ON, Canada, all in electrical and computer engineering. From 1996 to 1997, he was with Lucent Microelectronics, where he was involved in the design, test, and verification of Orca FPGAs. He joined McGill University, Montreal, QC, Canada, in 1998, where he is currently a Professor. He has published more than 250 papers, for which he received several awards. His current interests include the design of deeply embedded systems, most notably the systems that improve wellness and health. He has graduated over 50 M.Eng. and Ph.D. students, who have received numerous awards for their theses and have moved on to leading industrial and academic institutions upon their graduation. Dr. Zilic is the Senior Member of the ACM. He has been the Chercheur Strategique Research Chair from the Province of Quebec. He received the Wighton Fellowship for laboratory course teaching by Sandford Fleming Foundation and the National Council of Deans of Engineering and Applied Science.



Yu Pang received the Ph.D. degree from the Department of Electrical and Computer Engineering at McGill University in 2010. Now he is a professor at Chongqing University of Posts and Telecommunications. His current research interests include wireless communications, circuit design and parallel computing.

Gwanggil Jeon received the Ph.D. degree in Department of Electronics and Computer Engineering from Hanyang University, Seoul, Korea, in 2008. From 2008 to 2009, he was with the Department of Electronics and Computer Engineering, Hanyang University, from 2009 to 2011, he was with the School of Information Technology and Engineering (SITE), University of Ottawa, as a postdoctoral fellow, and from 2011 to 2012, he was with the Graduate School of Science & Technology, Niigata University, as an assistant professor. He is currently a professor at Xidian University and Incheon National University. His research interests fall under the umbrella of image processing, particularly image compression, motion estimation, demosaicking, and image enhancement as well as computational intelligence such as fuzzy and rough sets theories. He was the recipient of the IEEE Chester Sall Award in 2007 and the 2008 ETRI Journal Paper Award.

Francesco Piccialli is an Assistant Professor at the University of Naples FEDERICO II, Department of Electrical Engineering and Information Technology. His research interests are focused on the Internet of Things (IoT) and Internet of Everything (IoE) paradigms. He is also focusing my research on Data Mining and Data Analytics techniques applied on data coming from IoT world. Consequently, topics of his research are certainly that of the Smart environments, Location-Based and Context-Aware services and applications, which finalize their applications within the Smart City framework.