Towards an Optimized Blockchain-Based Secure Medical Prescription-Management System

Imen Ahmed 1, Mariem Turki 1, Mouna Baklouti 1, Bouthaina Dammak 2,* and Amnah Alshahrani 2

1 CES Lab, ENIS, University of Sfax, Sfax 3038, Tunisia; imen.ahmed@enis.tn (I.A.); mariem.turki@isimg.tn (M.T.); mouna.baklouti@enis.tn (M.B.)
2 Department of Computer Science, Applied College, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; aalshahrani@pnu.edu.sa

* Correspondence: bdammak@pnu.edu.sa

Abstract: This work introduces a blockchain-based secure medical prescription-management system seamlessly integrated with a dynamic Internet of Things (IoT) framework. Notably, this integration constitutes a pivotal challenge in the arena of resource-constrained IoT devices: energy consumption. The choice of a suitable blockchain consensus mechanism emerges as the linchpin in surmounting this hurdle. Thus, this paper conducts a comprehensive comparison of energy consumption between two distinct consensus mechanisms: Proof of Work (PoW) and Quorum-based Byzantine fault tolerance (QBFT). Furthermore, an assessment of the most energy-efficient algorithm is performed across multiple networks and various parameters. This approach ensures the acquisition of reliable and statistically significant data, enabling meaningful conclusions to be drawn about the system’s performance in real-world scenarios. The experimental results show that, compared to the PoW, the QBFT consensus mechanism reduced the energy consumption by an average of 5%. This finding underscores the significant advantage of QBFT in addressing the energy consumption challenges posed by resource-constrained IoT devices. In addition to its inherent benefits of privacy and block time efficiency, the Quorum blockchain emerges as a more sustainable choice for IoT applications due to its lower power consumption.

Keywords: blockchain; healthcare; IoT; energy consumption; consensus mechanism

1. Introduction

Just as the Internet has revolutionized the way we interact, the emerging blockchain technology, one of the major tools of digital transformation, has led to a complete overhaul of transaction management and verification. This technology, broadly speaking, is a secure and distributed database that is shared among all participants in the network, without a central body of control, and that makes it possible to store and transmit information in a transparent and secure way [1,2]. One of the key features of this technology is its ability to create a secure and tamper-proof record of transactions. Once a block has been added to the blockchain, it cannot be altered without invalidating the entire chain. This makes it very difficult for anyone to manipulate or tamper with the data recorded on the blockchain [3].

This has led to a complete overhaul of transaction management and verification in several industries, ranging from the financial sector to healthcare and supply chain management. Particularly in the pharmaceutical sector, where one of the most challenging issues is balancing the security of medical data with the ease of traceability [4–6], blockchain has already demonstrated its reliability by establishing trust and collaboration in multiple projects such as drug traceability systems and prescription-management systems [7,8]. In order to reduce drug fraud by prescription tampering, in this work, we are interested in using blockchain technology in a pharmacy-management system, in particular a medical prescription-management system, to ensure the security of the recorded data and the traceability of each prescribed medication. Additionally, we harnessed the inherent strengths of
IoT technology, capitalizing on its rapidity and precision [9]. Given its widespread acclaim and significant contributions across various domains, the IoT stands as a technological asset augmenting our approach.

1.1. Motivation

Certain drugs are especially susceptible to illicit practices, including the black market and drug trafficking. These drugs are frequently obtained illegally from pharmacies, either through the repeated use of the same prescription or the use of falsified sequences [10,11]. Indeed, prescription tampering is a widespread drug fraud in the world, which is constantly developing. Recently, the results of a European Suspicious Orders Abuse Indicator Possible (OSIAP) [12] survey carried out in six European countries (France, Belgium, Spain, Italy, Sweden, and the Netherlands) have shown that prescription falsification is highly dependent on the organization of drug distribution, that is the medical prescription-management system. In fact, traditional prescription-management systems are unsatisfactory in fighting against fraud and falsification of prescriptions either for a weakness in the system itself or for its inability to be generalized such as for e-prescriptions or pharmaceutical record databases.

Recently, thanks to its transparency and its unalterability, blockchain has been used as a perfect, traceability tool and for verifying authenticity, in the process of prescribing and dispensing medication. Indeed, one potential use case for blockchain in prescription management is to create a tamper-proof record of prescription orders and medication dispensation. With blockchain, every transaction is recorded in a decentralized, secure, and immutable ledger, making it extremely difficult to alter or delete data without detection. This can help highly prevent prescription fraud. Another potential benefit of using blockchain in prescription management is the ability to provide patients with more control over their medical data. With blockchain, patients can securely access their medication history and share it with healthcare providers as needed, without the need for a centralized database.

Therefore, we propose in this work a blockchain-based prescription-management system, where all transactions made on medical prescriptions are recorded in chronological order and there will be no possibility of a transaction being modified or deleted. Hence, transparency and traceability, as well as the confidentiality of personal patient information are guaranteed.

1.2. Related Work

Several studies have indicated that the transition to electronic prescription (e-prescription) systems has a positive impact on the overall healthcare experience. Alqattan and Mirzal [13] proposed a comprehensive framework for implementing e-prescription systems within healthcare information systems, leveraging cloud computing infrastructure. They designed a cloud computing architecture that accommodates the scalability demands of e-prescription systems, ensuring seamless expansion to meet the evolving needs of healthcare providers. The authors asserted that their solution enhances the security of e-prescription systems; however, no development efforts related to the security objective are addressed nor implemented. Additionally, their framework emphasizes scalability, but lacks a detailed discussion or implementation strategies for addressing security concerns. Similar to the work presented in [13], different papers [14,15] leverage cloud computing to design e-prescription systems. Recently, a traceable medical prescription framework was proposed as a reliable tool that must be integrated into any strategy for the fight against drug fraud. In addition, since blockchain technology has proven to have incomparable features of traceability and transparency, several researchers have proposed to use it in drug prescription-management systems, to guarantee traceable transactions in a safe and fast way [16,17]. Cilli, Magnanini, Siliipigni, and Venettoni [1] exposed the problems of medical prescriptions, mainly related to patient data security and privacy, information authenticity, and service availability. To overcome these concerns, they proposed to rely on
the distributed ledger technology (DLT) by the use of specific cryptographic mechanisms on data in transmission and at rest on the platform. Their solution is based on a permissioned blockchain architecture [18], under the governance of the National Health Services (NHS), in which medical prescriptions are represented as non-fungible tokens (NFTs) managed by specific smart contracts, based on the Ethereum standard called ERC-721 [19]. Through specific decentralized applications (DApps), a doctor who has been granted a minter’s permission by the NHS creates the NFT, which ensures compliance with the roles of each of the actors.

Thatcher and Acharya [3] proposed RxBlock, a private decentralized application for digitized prescriptions that use Ethereum as the blockchain technology and enable the immutability principle to protect information exchange across users. The electronic prescription process, including mainly prescribing and filling medicines, is illustrated through the use of Ethereum smart contracts. Through smart contracts, each actor is allowed to apply for specific transactions that are recorded and serve as Prescription Drug Monitoring Programs (PDMPs), which are used for state-run databases. However, it is worth noting that the fully electronic prescription process outlined in these studies necessitates that all actors—doctors, pharmacists, and patients—are registered in the same system. This requirement may limit the system’s ability to serve prescriptions originating from doctors who are not registered in the platform, reducing the ease and flexibility of prescription management for both healthcare providers and patients. Alnafrani and Acharya [20] proposed SecureRx, a web-based application developed based on the Ethereum blockchain and RxCheck hub. An actor can grant a request through a web application, and a data request is initiated and recorded on the Ethereum blockchain with a timestamp; the same thing happens with all transactions. Garcia, Ramachandran, and Ueyama [12] explored smart contracts in two BFT-based blockchain platforms, namely Endermint and Hyperledger Besu, to build a decentralized e-prescription system. In this work, an empirical performance evaluation and comparison between Endermint, Hyperledger Besu, and Ethereum, a PoW blockchain, was presented. They demonstrated that, although the BFT-based blockchain solution is little used in the healthcare literature, Endermint and Hyperledger Besu are efficient solutions for the proposed e-prescription system and can be adopted for multi-stakeholder systems and frameworks. Azaria, Ekblaw, Vieira, and Lippman [21] focused on an Electronic Health Record (EHR) solution for e-prescriptions. They used smart contracts on an Ethereum blockchain to automate and track patient/provider transactions that associate electronic data stored in external databases. VigilRx [22] is proposed as a patient-centric prescription management system, in which storage management is provided through blockchain technology. The Ethereum blockchain is used as a public and distributed ledger and includes smart contracts that manage the storage and access to on-chain data. To store on-chain data, they rely on National Drug Codes (NDC), whose are managed by the U.S. Food and Drug Administration. One notable limitation of VigilRx, as detailed in the study, is its reliance on a public blockchain infrastructure for managing sensitive patient data within the healthcare domain. Unlike private or permissioned blockchains, which restrict access to authorized participants, the use of a public ledger raises concerns regarding data privacy and confidentiality.

Based on this study, and in terms of contributions to the research, we propose a blockchain-based prescription-management system that fosters a secure and collaborative environment between pharmacists and patients.

The key contributions of this paper can be summarized as follows:

1. A blockchain-based prescription-management system, which improves the traceability and transparency of medical prescriptions, as well as privacy and energy efficiency, in order to reduce fraud drug and counterfeiting, is proposed.
2. A smart contract is developed to manage various transactions between different actors in an efficient way.
3. Two types of blockchain, the Ethereum and Quorum blockchain, are explored in terms of energy consumption and performance evaluation.
4. A web application is designed and implemented, integrating IoT technology and using the Quorum blockchain to provide a more energy-efficient system.

This paper is structured as follows:

Section 2 presents an overview of blockchain technology. Section 3 describes our proposed blockchain-based prescription management DApp, while Section 4 introduces the design and implementation details. Section 5 provides a discussion and evaluation of the proposed approach, and Section 6 concludes the paper and outlines future work.

2. Blockchain Technology

This section introduces the basic concepts of blockchain technology, its components and its different types and features.

2.1. Definition and Main Components

Blockchain technology, known as a kind of fraud-resistant system, is a distributed ledger technology that allows for secure and transparent transactions to be recorded and verified without the need for a centralized authority [23,24]. Each transaction is recorded in a block, which is then added to a chain of previous blocks, using a cryptographic hash function, hence the name “blockchain”. This chain comprises multiple interconnected files, with each file containing vital data such as a timestamp indicating the data’s creation time and the historical data of the blockchain’s blocks [25]. This chain of blocks is secured using complex algorithms called consensus mechanisms. The nodes, individual devices or computers in the blockchain network, participate in the consensus process by validating transactions and blocks, and then voting on the validity of these transactions and blocks. Different consensus mechanisms have different requirements and criteria for nodes to participate in the consensus process. The blockchain’s encrypted nature and distributed ledger format make the data stored on it highly secure and virtually unhackable. This unparalleled level of security instills a great deal of trust and confidence [25].

2.2. Smart Contract

Smart contracts, another part of the blockchain that creates trust and accuracy, operate based on a set of rules encoded in computer code that govern the execution of the contract. One of the key benefits of smart contracts is that they eliminate the need for intermediaries and reduce transaction costs. They also provide greater efficiency, accuracy, and transparency compared to traditional contract-execution methods. Additionally, smart contracts are nonrepudiatable, meaning that, once a contract is executed, it cannot be reversed or altered, which provides greater security and trust in the contract’s execution [26].

2.3. Types and Features of Blockchain Technology

There are mainly four kinds of blockchain network: public, private, consortium, and hybrid [27]:

• Public blockchain, in which all the participated users can join the network and can perform read and write transactions, without verifying the transacting parties’ identities, such as the Bitcoin blockchain.
• Private blockchain: Private blockchains are permissioned networks where prior authorization is required to join. Only trusted and pre-authorized participants can join the network and perform write transactions, such as the Quorum and Hyperledger blockchain.
• Hybrid combines elements of both public and private blockchains. It enables a network to be decentralized and transparent, while also providing secure and private transactions for certain participants.
• Consortium blockchain: Also known as Federated blockchain, is a subtype of permissioned blockchains, in which a group of entities or organizations jointly manage the network.
Among the key features of blockchain technology that make it a revolutionary technology in the digital world, we can mention the following:

- **Decentralization**: One of the most prominent features of blockchain technology is its decentralized nature, which eliminates the need for intermediaries or third-party entities to validate transactions. Transactions are validated and recorded on a distributed network of computers or nodes, allowing for greater security and transparency.

- **Immutability and data integrity**: Once a new transaction has been added to the blockchain database, it cannot be modified directly, and it can only be deleted after consensus has been reached. The blockchain’s participants can utilize this feature to enhance regulatory compliance and minimize fraudulent activities.

- **Transparency**: All transactions on the blockchain network are visible to all network participants, providing a transparent and auditable record of every transaction. This enables greater accountability and trust among network participants.

- **Efficiency**: Blockchain technology enables fast and efficient transactions, eliminating the need for intermediaries and reducing transaction costs. However, it is important to note that scalability issues can pose challenges to the speed and efficiency of certain blockchains. Despite this, blockchain technology remains a popular choice for applications that prioritize fast and secure transactions, such as financial services and supply chain management.

- **Security**: Blockchain technology employs advanced cryptographic algorithms and protocols to secure transactions and protect the network from malicious attacks. Public blockchains, with their decentralized structure, typically exhibit greater resilience to cyberattacks. However, private and permissioned blockchains, due to their limited number of nodes, may face vulnerabilities. Additional security measures are crucial for these networks. Overall, while blockchain offers inherent security features, the implementation strategies must adapt to address specific vulnerabilities.

### 3. Blockchain-Based Prescription Management DApp Overview

This section presents an overview of our DApp, describing the participating actors and the possible interactions among them, as well as the system architecture.

#### 3.1. System Presentation and Architecture

This DApp serves as a comprehensive blockchain-based management system, facilitating seamless collaboration and efficient management for pharmacists, patients, and administrators. Our solution does not require doctors who prescribe medications to be registered in the system in order to serve the patient, providing a reliable solution for handling prescriptions regardless of their source. This feature enhances accessibility, flexibility, and convenience, facilitating seamless prescription management for both healthcare providers and patients. The principal roles of the actors involved in the system are detailed as follows:

- **The admin**, who represents a national agency, plays a crucial role in overseeing all actors and their activities within the platform. Among the main responsibilities of the admin, he/she is able to perform the following:
  - Handle the registration process for pharmacists. Upon receiving a registration request, he/she meticulously reviews the information provided by the initiator pharmacists. Once he/she completes the registration process and approves a pharmacist’s request, the DApp automatically generates a registration confirmation email containing essential details, including the login credentials.
  - Register and manage the list of market-approved drugs, ensuring that only safe, effective, and compliant medications are available within the platform.

- **Pharmacist**: As key stakeholders within the blockchain-based management system, pharmacists play a vital role in ensuring seamless pharmacy operations and providing
optimal patient care according to multiple essential features and functionalities, such as the following:

- **Register and manage prescriptions**: securely record prescription details, including drug information, dosage instructions, and patient data.
- **Register patients and generate Quick Response (QR) code**: Pharmacists have the authority to register patients within the platform. Upon registration, the DApp generates a unique QR code for each patient. These QR codes serve as a secure and convenient way for patients to access their accounts, enabling them to view their prescription history, medication details, and other relevant healthcare information.
- **Access market-approved drug list**: This comprehensive and up-to-date catalog of medications enables pharmacists to make informed decisions while dispensing prescriptions. Access to detailed drug information, such as contraindications and potential interactions, enhances patient safety and ensures compliance with prescribed treatments.
- **Access registered pharmacists list**: This feature fosters communication and knowledge sharing among professionals, promoting best practices and continuous learning within the pharmaceutical community.

- **Patient**: As active participants in the blockchain-based management system, patients are at the heart of the healthcare ecosystem. The DApp offers a patient-centric approach, empowering them with convenient and secure access to vital healthcare information.
  - **QR code account access**: Upon registration, the DApp provides patients with a unique QR code linked to their accounts. By scanning this QR code, patients can conveniently access their personalized healthcare information, including medication history and relevant prescription details.
  - **Access medication history**: Patients can easily access their comprehensive medication history through the DApp. The platform maintains a secure and up-to-date record of all prescriptions, dosages, and corresponding healthcare providers.
  - **Access registered pharmacists list**: This directory enables them to connect with trusted and qualified healthcare providers for consultations and personalized medication-related advice.

By harnessing the power of blockchain technology, this medical prescription-management system DApp enriches the pharmaceutical landscape, fostering a collaborative environment that benefits both pharmacists and their patients.

When treating a prescription, the pharmacist has two possibilities: either the prescription is being processed for the first time and has not been registered in the platform or it is already recorded in the platform:

- **Prescription processed for the first time**: In the case of a prescription processed for the first time, the prescription does not have a QR code. Therefore, the pharmacist needs to manually register the prescription details within the platform. This involves entering all relevant information regarding the prescription, such as the medication name, dosage, treatment duration, the prescribing doctor’s name, and patient information, into the computer system or dedicated electronic platform. Without a QR code, manual registration is necessary to ensure that the prescription is processed correctly and that all required information is available for the patient’s future follow-up. Upon inputting the prescription details, the DApp generates a unique QR code specific to that particular prescription. This QR code becomes an integral part of the prescription document, enabling quick access to critical information, simplifying medication management, and promoting patient safety.

- **Prescription already registered**: In this case, the pharmacist scans the QR code and gains access to the prescription history, which allows him/her to verify the relevant
data of the prescription and complete the purchase procedures with complete safety and transparency.

In instances where the patient is not yet registered within the DApp, pharmacists have the authority to create an account on the patient’s behalf. As part of the registration process, a personalized QR code is provided to the patient. This unique QR code serves as a secure identifier, linking the patient to his/her healthcare information within the platform.

The architecture of the proposed prescription-management system is composed of 3 layers, as described in Figure 1.

![Figure 1. Blockchain-based prescription-management architecture.](image)

We developed a web application (web layer) that enables seamless interaction with the blockchain platform (blockchain layer). This interface is integrated with an advanced IoT system (sensing layer) that utilizes a camera and a Raspberry board with a QR code reader and scanner application to accurately identify medical prescriptions.

3.2. Main Process of Blockchain-Based Prescription-Management System

The sequence diagram presented in Figure 2 depicts the main process of our proposed system with its different steps, clarifying the interactions between different actors.

This prescription-management system operates on a permissioned blockchain platform, using smart contracts to manage the prescription life-cycle and user transactions. To become a member of the proposed system’s blockchain network, pharmacists are required to submit a request to the National Health Services. Upon identity verification, the administrator will register the pharmacists and send a confirmation email, including their password. Once registered, pharmacists can access the platform using their wallet address and password. This access allows them to efficiently consult and manage registered prescriptions, register patients, access the list of registered pharmacists, and check the approved drugs list.

When a pharmacist receives a patient, the first step is to verify whether the prescription is already registered using the QR code reader and scanner:

- If the prescription is being served for the first time, the pharmacist will proceed to register it in the system.
• If it is already registered, he/she will check the remaining quantity of the requested drugs and the expiration date. Subsequently, the pharmacist will update the prescription information accordingly.

In case the patient is not registered yet, the pharmacist can create an account for him/her, and the system will generate a unique QR code. This QR code grants the patients access to their medication history, which remains confidential and can only be consulted by the patients. Registered patients, in addition to managing their prescriptions, have the ability to access the pharmacist users list and view the list of approved drugs.

Figure 2. Sequence diagram of the proposed system.

Regarding the system’s level of authorization, it is important to note that the system utilizes an authoritative model that relies on users’ mutual recognition and their affected roles.

The smart contract, designed for this proposed system, incorporates all necessary functions to manage and modify the entire life-cycle of medical prescriptions while ensuring proper separation and management of actors’ roles. Each transaction is securely published on the blockchain platform and recorded, ensuring traceability and transparency throughout the process. Table 1 presents some examples of functions used in the smart contract.

For a clearer understanding of the smart contract’s functionalities, we outline several algorithms employed within our proposed solution.

Algorithm 1 explains the steps in registering a new pharmacist. The inputs to the smart contract, needed by the functions, are shown with their descriptions. The function addPharmacist() executes exclusively when the caller’s address aligns with that of the admin. Once registered, the pharmacist will receive an email confirming that the registration was successful, along with his/her encrypted password.

Algorithm 2 outlines the process of registering a new patient. The function appPatient() only executes when accessed by a registered pharmacist. Upon successful registration, the patient will receive an email confirming the process, accompanied by a QR code. This QR code grants the patient access to his/her profile and medical history.
In Algorithm 3, we introduce a series of functions related to the registration and updating of prescriptions. These functions play a crucial role in the management of prescriptions within the system.

**Table 1.** Examples of functions in the smart contract.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addPharmacist()</td>
<td>register pharmacist in the platform</td>
</tr>
<tr>
<td>addPatient()</td>
<td>register patient in the platform</td>
</tr>
<tr>
<td>addMADrug()</td>
<td>register approved drug in the market-authorized drug list</td>
</tr>
<tr>
<td>addPresc()</td>
<td>register new prescription</td>
</tr>
<tr>
<td>updatePresc()</td>
<td>update an already registered prescription</td>
</tr>
<tr>
<td>getPresc()</td>
<td>check if a prescription is already registered and retrieve its details</td>
</tr>
<tr>
<td>getUser()</td>
<td>obtain user information</td>
</tr>
<tr>
<td>getPresc()</td>
<td>consult specific prescription information if registered</td>
</tr>
</tbody>
</table>

**Algorithm 1: addPharmacist**

**Input:** walletAddr, name, email, phone, city;

**Output:** Emit an event declaring that the new pharmacist has been registered newUserId;

**Data:**
- walletAddr: the Ethereum address of the pharmacist
- name: the name of the pharmacist
- email: the email of the pharmacist
- phone: the phone number of the pharmacist
- city: the city where the pharmacy is located
- newUserId: a new ID for the new registered pharmacist

**Initialization:**
- userIds: a map that associates Ethereum addresses with integers (userIds)
- users: table of all registered pharmacists

```plaintext
if admin == msg.sender then
  if walletAddr does not exist then
    Associate the user wallet address with a new ID
    Store the new pharmacist details
    Generate a password, and send it to the pharmacist’s email
  end
  else
    Revert contract state, and show an error (the pharmacist is not registered yet)
  end
else
  error: Only admin can initialize
end
```
Algorithm 2: addPatient

**Input**: patientWalletAddr, patientName, patientAge, patientCity, patientMail, patientPhone;

**Output**: Emit an event declaring that the new patient has been registered;

if patientWalletAddr does not exist then
    Store the new patient details
    Generate QR code, and send it to patient’s email
else
    Revert contract state, and show an error;

Algorithm 3: Implemented functionalities

1. addPresc()

**Input**: prescRef, PatientName, DrName, DrCity, TotalDrugs, drugsDetails[drugRef, totalQuantity, servedQuantity], issueDate

**Output**: Emit an event declaring that a new prescription has been registered

Specific QR code generated

Store prescription’s details

if totalQuantity = servedQuantity or it has been 3 months since the issueDate then
    Lock the prescription;

2. getPresc()

**Input**: prescRef

**Output**: Return details of prescription

Calculate remaining quantity

remainingQuantity ← totalQuantity - servedQuantity;

3. getDrug()

**Input**: prescRef, drugRef

**Output**: Return details of drug

4. updatePresc()

**Input**: prescRef, drugRef, newServedQuantity

if Prescription is unlocked, and newServedQuantity ≤ remainingQuantity then
    Store the new served quantity;
    Update remaining quantity;
    if remainingQuantity = 0 or it has been 3 months since the issueDate then
        Lock the prescription;
    end
else
    Revert contract state, and show an error;
end

4. Implementation and Test of Blockchain-Based Prescription Management System

As previously discussed in the preceding sections, the prescription blockchain management system in this work comprises three layers: a blockchain platform, a web application, and an IoT system. In this section, we offer a comprehensive overview and delve into the implementation details of each of these subsystems.

4.1. Blockchain Platform

In order to develop our blockchain-based system and compile, deploy, and interact with the designed smart contract, we used multiple environments. Thus, in Figure 3, we illustrate the essential components in the software architecture of our system.

The initial stage in implementing our decentralized application involved identifying a blockchain network that best suited our use case: a pharmaceutical application requiring robust security and data authenticity for sensitive information, while also demanding energy efficiency to accommodate the inclusion of IoT devices. Given that sensitive personal
data in prescriptions are being examined, privacy is of paramount importance. Utilizing a private blockchain offers greater control over data access and dissemination, mitigating the risks associated with publishing sensitive information on a public network, thus the decision to opt for a private blockchain solution. We propose to explore two types of blockchains: **Ethereum** and **Quorum**. Ethereum is renowned for being a popular platform for building and deploying decentralized applications (DApps). It is important to note that, in our research, we used an older version of Ethereum, which operated on a PoW consensus mechanism. However, it is necessary to acknowledge that Ethereum has been undergoing a transition to a Proof of Stake (PoS) consensus mechanism, as part of the Ethereum 2.0 upgrades. On the other hand, Quorum, based on Ethereum, retains the fundamental Ethereum features, including smart contract functionality, while incorporating additional privacy and permissioning features. To determine the most suitable blockchain for our application—Ethereum or Quorum—we conducted an energy consumption comparison experiment between the two. In the next section, we will present the detailed methodology of the experiment along with its results.

![Diagram](image)

**Figure 3.** Implementation environment.

The smart contract created for this proposed system has been written in the **Solidity** programming language, compiled and deployed with **Truffle**. In this phase of the project, another essential component employed is **Metamask**. It serves as a user-friendly and lightweight client, which, when added as a Google Chrome extension, functions as a digital wallet. This wallet allows users to effectively manage their ether’s across multiple accounts and execute transactions on the blockchain. The interaction with the blockchain is performed with a JavaScript library called **Web3**.

### 4.2. Web Application

The web application, or the front-end of our system, is the interface through which users can conveniently interact with smart contracts. The proposed system aims to ensure the principle of least privilege for all participants in the system. As already seen in the previous sections, three actors are involved in the system, namely admin, pharmacist, and patient.

We have adopted the **Vue.js** framework for crafting our user interface. Vue.js stands as a versatile JavaScript framework known for its user-friendly nature, facilitating the creation of code that is both straightforward to learn and amenable to testing and upkeep. Within the Vue.js environment, the necessary libraries and ecosystems are readily available for constructing client-side business logic. The development process involves segmenting
a web page into modular components, each encapsulating its own set of HTML, CSS, and JavaScript code.

Figure 4b provides an example of the authentication interface within our DApp. Serving as the initial interface, this page promptly materializes when a pre-registered user connects to the blockchain platform. To unlock access to the array of interfaces within the platform, the user is required to accurately input his/her wallet address along with the password dispatched to his/her designated email address.

The “add prescription” function, illustrated in Figure 4a, initiates the prescription’s life cycle. It is important to note that only the pharmacist within the system has the authorization to create and update prescriptions.

The web application offers comprehensive functionality across all of the platform’s interfaces. Notably, these interfaces enable the administrator to register pharmacists and oversee the roster of authorized pharmaceuticals. Pharmacists are empowered to generate and revise prescriptions, as well as to enroll patients. Furthermore, patients gain the ability to access their medical prescriptions at any given moment and maintain a record of their medical history. The DApp adheres to robust security measures to safeguard patient and prescription data. Patient confidentiality and data protection are prioritized, instilling trust among all stakeholders. Through its innovative approach, this DApp contributes to an efficient and patient-centric healthcare ecosystem, benefiting pharmacists, patients, and healthcare providers alike.

4.3. IoT System

Expanding on the prior sections, once the prescription details are registered, the DApp generates an exclusive QR code tailored to that specific prescription. This QR code acts as a repository for the prescription’s information, encapsulated in the form of black and white squares. For the implementation of this data-encoding mechanism, we have opted for an IoT system, consisting of a Raspberry Pi board and a Pi camera, presented in Figure 5, specifically designed for QR code scanning.
This setup enables pharmacists to swiftly scan and authenticate the pertinent prescription data, thereby facilitating seamless purchase procedures.

Using a QR code with a Raspberry Pi-based IoT system offers several benefits:

- **Real-time processing:** Raspberry Pi’s processing power enables real-time QR code scanning and information extraction. This responsiveness is critical for applications that require immediate access to data.
- **Ease of programming:** Raspberry Pi supports various programming languages, simplifying the development of QR code-scanning applications. This versatility accommodates developers with different coding backgrounds.
- **Camera module compatibility:** Raspberry Pi camera modules are well suited for capturing images, including QR codes. Their compatibility ensures optimal image quality and reliable QR code recognition.
- **Scalability:** Raspberry Pi-based solutions are scalable, making them suitable for environments with varying scanning demands. Adding more units to the setup can accommodate increased QR code scanning requirements.
- **Low energy consumption:** Raspberry Pi boards are energy-efficient, making them suitable for continuous operations without significant power consumption.

We chose to utilize a Raspberry Pi equipped with a camera and QR code reader due to its potential to establish a robust connection between the physical world and blockchain technology. The Raspberry Pi is adept at efficiently capturing, processing, and performing real-time transmission of information encoded within QR codes. This capability enables not only the extraction of essential data, but also seamless interaction with a blockchain platform.

5. **Experimental Results**

In this section, we conduct a comprehensive analysis using carefully selected evaluation metrics and methodologies to evaluate the performance of the entire system. The evaluation process encompassed diverse experiments, representing various scenarios and use cases, to ensure a robust assessment:

1. Firstly, we undertook a series of experiments to evaluate the energy consumption of two consensus algorithms, namely the PoW and the QBFT. The objective was to compare and contrast the energy efficiency of the two protocols when invoking the functions of the smart contract of the proposed system.

2. In the second part, we evaluated the most energy efficient algorithm under multiple networks and various parameters to obtain reliable and statistically significant data, allowing us to draw meaningful conclusions about the system while running in the real world.

5.1. **Energy Consumption Comparison**

Choosing the appropriate consensus algorithm to achieve efficient energy consumption in IoT devices is crucial for several reasons such as the energy constraint, the scalability, the resource constraints, and the latency consideration.

As mentioned in Section 4.1, both Quorum and Ethereum are based on the Ethereum blockchain, but there are several key differences between them. Ethereum is a more general-purpose blockchain platform with a larger developer community and more established ecosystem and currently uses a Proof of Work (PoW) consensus mechanism. In comparison, Quorum is a specialized platform with enhanced privacy features and a modified version of the practical Byzantine fault tolerance (PBFT) consensus mechanism. The difference in the network architectures between these two blockchains can lead to differences in energy consumption.

However, the energy consumption of a blockchain network depends on many factors, including the number of nodes in the network, the computing power of each node, and especially, the specific implementation of the consensus algorithm. It is important to mention here that, in a blockchain network, a node refers to any device or computer that is...
connected to the network and participates in the validation and propagation of transactions and blocks.

In this paper, the energy consumption measurement of a node implemented in the IoT system (Raspberry Pi) is addressed for two different types of consensus mechanisms, namely the PoW and QBFT, to decide which one is more appropriate for IoT applications. Hence, this comparison test consisted of three phases:

1. Measuring the Raspberry Pi power while the DApp is implemented with the Ethereum blockchain based on PoW consensus.
2. Measuring the Raspberry Pi power while the DApp is implemented with the Quorum blockchain based on QBFT consensus.
3. Comparing the power consumption between both cases.

The energy consumption of a transaction in a blockchain network can vary based on a number of factors such as the complexity of the transaction, the gas price, the network congestion, and the network size. The scale of deployment used for this comparison test was 3 nodes for the Ethereum network, as well as for Quorum, since QBFT consensus requires a threshold of 2/3 of the total validator nodes to reach consensus. So, the minimum scale was used here; it is important to mention that having more nodes in the Quorum network increases fault tolerance and makes the network more resistant to attacks or failures. For the Ethereum network, we conducted experiments using a mining difficulty set to 0x2000, representing a moderately challenging level for miners in the network. Figure 6 presents the nodes’ implementation in each case. The distribution of the nodes is as follows:

- Two nodes were implemented on a PC, with the processor features of an Intel(R) Core(TM) i5-7200U CPU @ 2.50 GHz 2.70 GHz with 8 GB of RAM;
- The third, which is the node dedicated to testing, was implemented on a Raspberry Pi 3 model B+ with a 64-bit OS and 1 GB of RAM.

To measure energy consumption in IoT devices, which is the Raspberry Pi in this DApp, a USB voltage- and current-detection module was used, as presented in Figure 7. It is a simple tester displaying the voltage present on the USB connector and showing the current consumption of the attached USB devices. The voltage measured by the USB power detector can be in the range of 3–9 V, while the intensity is measured in the range of 0–5 A. In this experiment, the Raspberry Pi is powered by 5.21 V/2.5 A, and its consumption is estimated to be 500 mA on average.

After implementing the three nodes, each scenario begins with the first transaction, which involves deploying the smart contract. Subsequently, the different functions presented in Table 2 are executed while measuring the power consumption of the Raspberry Pi for each operation. The procedure was repeated 10 times for each transaction to ensure
obtaining results as precise as possible, and the deviation between executed transactions was about 3 min.

Figure 7. Energy consumption measurement using USB voltage- and current-detection module.

Table 2. Energy consumption measurement for Ethereum and Quorum implemented on Raspberry Pi.

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Power Consumption (Watts)</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ethereum</td>
<td>Quorum</td>
</tr>
<tr>
<td>Contract deployment</td>
<td>2.71</td>
<td>2.50</td>
</tr>
<tr>
<td>addPharmacist()</td>
<td>3.03</td>
<td>2.92</td>
</tr>
<tr>
<td>addPresc()</td>
<td>2.92</td>
<td>2.81</td>
</tr>
<tr>
<td>updatePresc()</td>
<td>2.92</td>
<td>2.71</td>
</tr>
<tr>
<td>addDrugMA()</td>
<td>2.71</td>
<td>2.61</td>
</tr>
<tr>
<td>newServedQ()</td>
<td>2.82</td>
<td>2.71</td>
</tr>
<tr>
<td>getPresc()</td>
<td>2.29</td>
<td>2.29</td>
</tr>
<tr>
<td>fakeBlock</td>
<td>2.71</td>
<td>2.61</td>
</tr>
</tbody>
</table>

The power measured in watts is calculated using Equation (1).

\[ W = A \times V \]  

(1)

where \( W \) represents power, \( A \) represents current intensity, and \( V \) represents voltage (\( V = 5.21 \) v in this case).

Table 2 includes the acquired readings and calculations of Raspberry Pi power consumption (measured in watts) obtained from the experiments. Figure 8 illustrates also a comparison of both results.

Figure 8. Energy consumption (measured in watts) comparison between Ethereum and Quorum.
As shown in Table 2, the improvement of Quorum reached 8%, which is an important value considering that the number of transactions is over a hundred per second for the Quorum blockchain. This experiment validated our expectations that the Quorum blockchain is more energy efficient in IoT devices than Ethereum with a remarkable difference. Quorum consensus eliminates the energy-intensive mining process associated with PoW algorithms, thereby significantly reducing the energy consumption, and consequently, the costs will be reduced. This contribution demonstrates that the energy consumption of blockchain technology varies and depends on the consensus mechanism used and that using blockchain technology with non-PoW consensus, such as QBFT consensus, may substantially mitigate sustainability issues in IoT systems.

However, the use of the Quorum blockchain, particularly PBFT consensus, showed better energy efficiency and performance. In addition, PBFT creates a new node faster than PoW consensus, which may indicate that it is more viable for the IoT environment. The outcomes of this experiment also reveal that both the type and number of parameters in a smart contract function have an impact on energy consumption. Indeed, as is shown in Table 2, for example, the energy consumption of the transaction addPrec(), which has nine parameters, was approximately 2.71 w, whereas the addDrugMA() function with only four parameters consumed 2.61 w. A difference of 0.1 w becomes significant when considering the entire blockchain network, particularly in scenarios involving approximately 1000 transactions per second (tps). We can also notice that, the more parameters a function has, the more computational power is required to execute it, and thus, the more energy is consumed, as presented in Figure 9.

![Energy consumption according to the number of function parameters in Quorum blockchain](chart)

Figure 9. Energy consumption (measured in watts) according to the number of function parameters in Quorum blockchain.

Furthermore, the number of parameters can also affect the size of the data that need to be stored on the blockchain, which can in turn affect the energy consumption. When data are stored on a blockchain, they need to be replicated across all nodes in the network, which, in turn, can increase the energy consumption of the system. Consequently, optimizing the implemented smart contract, particularly in terms of the parameters, can improve the energy consumption in the Quorum network more and more.

5.2. Performance Analysis

After studying the energy consumption and obtaining better results with the QBFT consensus algorithm, one other crucial aspect that warrants further investigation is the scalability issue. Specifically, it is imperative to study the impact of scaling up the system and increasing the number of nodes on the DApp performances. Accurately assessing and evaluating the performance of a blockchain network relies heavily on the utilization of specific metrics [28,29]. In this paper, our focus lies in evaluating the Quorum blockchain network operating under the QBFT consensus mechanism focusing on the following metrics:
• Transaction throughput: This metric measures the number of transactions the blockchain can process per second (tps). Higher throughput indicates better performance and scalability.
• Latency: This refers to the time it takes for a transaction to be propagated across the network and confirmed. Lower latency is desirable for time-sensitive applications.

To achieve this, we utilized the Hyperledger Caliper tool [30]. Specifically, we made use of a customized version of the Caliper tool, designed to be compatible with the Quorum blockchain since Quorum is not yet supported as a System Under Test [31].

On the other side, we opted for the most commonly used functions in the system to execute the experiments. Table 3 shows the details of the selected functions.

Table 3. Details of the studied functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>addPresc()</td>
<td>uint256 prescRef, string memory PatientName,</td>
</tr>
<tr>
<td></td>
<td>string memory DrName, string memory DrCity, uint TotDrugs,</td>
</tr>
<tr>
<td></td>
<td>uint[] memory drugsRef, uint[] memory Qtt, uint[] memory Qts,</td>
</tr>
<tr>
<td></td>
<td>issueDate</td>
</tr>
<tr>
<td>updatePresc()</td>
<td>uint256 prescRef, uint256 drugRef, uint256 newServedQ,</td>
</tr>
<tr>
<td>getPresc()</td>
<td>uint256 prescRef</td>
</tr>
</tbody>
</table>

The addPresc() and updatePresc() functions are the most invoked by the blockchain network in real-word applications. We conducted a comprehensive evaluation of these selected functions by performing a series of experiments within Quorum networks of varying sizes. The experimentation involved three distinct network configurations, specifically 5 nodes, 10 nodes, and 20 nodes, each utilizing the Quorum Byzantine fault tolerance (QBFT) consensus algorithm. To carry out the experiments, we executed the chosen functions under different send rates (25, 50, 75, 100, and 200), ensuring a wide range of data points to assess system performance comprehensively.

All the experiments were conducted on the same machine with 16 CPUs (two sockets with 8 CPUs per socket running one thread each) and 32 GB of RAM. Finally, a Ubuntu 20.04.4 LTS was installed on this machine.

Throughout the experiments, we recorded the throughput results of the selected functions within the 5-node, 10-node, and 20-node networks. These results are shown in Figure 10. The throughput results of the functions addPresc() and updatePresc() are depicted in Figure 10a and 10b, respectively. The curves of the studied functions exhibit a comparable pattern and network behavior with better results for the function updatePresc(). This can be explained by the fact that the function addPresc() has more string parameters, which might require additional processing and a longer computation time.

On the other side, both functions demonstrate that the throughput is higher in blockchain networks with fewer nodes due to the smaller number of voters compared to larger networks. This can be attributed to the reduced complexity and overhead in
blockchain networks with fewer nodes. Since the number of voters, which participate in the QBFT consensus process (2/3 of the total voters), is smaller in these networks, the coordination and agreement among nodes are achieved more swiftly. As a result, the throughput, representing the rate of successful transactions processed, tends to be higher in such scenarios. In contrast, larger networks with a greater number of voters can experience relatively more intricate consensus negotiations, potentially leading to a slightly lower throughput due to the increased coordination efforts required among a larger set of nodes.

Finally, notice that, as the send rate increases, the throughput also experiences a corresponding rise. This trend can be linked to the network’s capacity to manage a higher influx of transactions, allowing for faster processing and validation.

However, beyond a certain threshold specific to each network size, a noteworthy transition occurs. The throughput, after initially rising, reaches a ceiling and becomes relatively constant despite further increases in the send rate. This phenomenon can be explained by the inherent limitations of the network’s capacity, resource allocation, and processing capabilities. As the network becomes saturated with a high volume of incoming transactions, it reaches a point where additional transaction submissions do not significantly enhance the overall throughput. Instead, the network operates at its peak processing capacity, and any subsequent increase in the send rate has a limited effect on throughput improvement.

Investigating the latency variations, Figure 11 illustrates the results of the studied functions within networks of 5 nodes, 10 nodes, and 20 nodes with various send rates. Actually, these results are correlated with the throughput ones. Indeed, as the size of the blockchain network grows larger, the latency tends to increase. This increase can be attributed to the larger number of nodes and the complexity involved in reaching consensus across a larger distributed network. Furthermore, the latency experiences an upward shift as the send rate increases. This happens because more transactions competing for network resources and processing capacity result in increased latency.

![Figure 11](image1.png)

Finally, the latency and throughput results of the getPresc() function are reported in Figure 12. Experiments on read-only transactions showed that the process of reading data from the blockchain incurred minimal latency, meaning the time delay between initiating the request and receiving the data was negligible (ranging from 0.01 s to 0.04 s). This is due to the inherent design of blockchain systems, where data retrieval operations primarily involve accessing already stored information from the local data of the node receiving the request, without performing any complex computational tasks. As a result, the time taken to retrieve data during read operations is typically quite low. Moreover, notice that the latency outcomes remain consistently comparable across the networks with 5 nodes, 10 nodes, and 20 nodes.

Furthermore, the throughput of the getPresc() function within all the tested blockchain networks exhibits a linear relationship with the number of transactions or requests being processed concurrently (send rate). This means that, as the number of simultaneous read requests increases, the system’s capacity to handle these requests scales proportionally. The linear relationship between throughput and concurrent read requests underscores the
decentralized nature of blockchain networks and their ability to efficiently serve multiple pharmacists accessing data in parallel.

![Figure 12](image1.png)  ![Figure 12](image2.png)

(a) Latency of the function getPresc.  (b) Latency of the function getPresc.

Figure 12. Throughput and latency of the function getPresc.

To summarize, we provide a comparative analysis of our proposed solution for an optimized blockchain-based secure medical prescription management system with existing solutions. A condensed overview of this analysis is provided in Table 4.

Table 4. Comparison between our proposed solution and existing solutions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Decentralization</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>BC platform</td>
<td>Ethereum</td>
<td>Ethereum</td>
<td>----</td>
<td>----</td>
<td>Quorum</td>
</tr>
<tr>
<td>Mode of Operation</td>
<td>public</td>
<td>private</td>
<td>----</td>
<td>----</td>
<td>private</td>
</tr>
<tr>
<td>Transparency</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Traceability</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Privacy</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Throughput Evaluation</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>IoT integration</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Energy consumption measurement</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

6. Conclusions

In conclusion, this paper introduces a distributed application tailored for the pharmaceutical domain, revolutionizing medical prescription management through the integration of a blockchain-based web application. The framework incorporates an IoT system adept at QR code reading, enhancing security and transparency in the pharmaceutical landscape. By meticulously assessing the energy consumption, our study highlights the advantages of utilizing the Quorum blockchain platform, employing its QBFT consensus mechanism. Notably, this approach demonstrates a 5% increase in efficiency compared to Ethereum’s PoW protocol.

In the pursuit of in-depth insights, a comprehensive performance evaluation was conducted on the Quorum blockchain with the QBFT consensus mechanism. Utilizing network configurations encompassing 5, 10, and 20 nodes, alongside varying send rates, our analysis delved into the nuanced interplay between network size, transaction velocity, and system performance. Through the interpretation of the throughput and latency results, we shed light on the scalability and responsiveness of the Quorum blockchain in managing medical prescriptions, thereby providing valuable guidance for the integration of blockchain technology within the pharmaceutical sector.
Author Contributions: Methodology, M.T. and M.B.; Software, I.A. and M.T.; Validation, M.B., B.D. and A.A.; Formal analysis, I.A. and M.T.; Investigation, M.T.; Resources, I.A. and A.A.; Data curation, I.A.; Writing—original draft, I.A. and M.T.; Writing—review & editing, M.B. and B.D.; Visualization, B.D. and A.A.; Supervision, M.B.; Project administration, M.B.; Funding acquisition, B.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No. (44- PRFA-P- 137)

Data Availability Statement: The data presented in this study are available in this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.