Utilizing blockchain technology for IoT-based healthcare systems

Raad Mohammed¹,*, Raaid Alubady¹, Ali Sherbaz²

¹College of Information Technology, University of Babylon, Iraq
²College of Faculty of Science University and Technology, of Northampton, UK

E-mail: raadmohammed797@gmail.com

Abstract. Recent years have witnessed a widespread interest in healthcare issues and the search for faster and safer service for patients. Electronic health record was established to provide advanced health services. Researchers seek to provide permanent and simplified ways to monitor patients remotely using remote patient monitors. One of these methods is the use of Internet of Things (IoT) devices, where the healthcare provider can monitor the patient remotely. However, with the current centralized electronic patient record system and increase in number of IoT devices, security and privacy issues have arisen, as some patients may not want to disclose their data, in addition to particular concerns or risks that affect the patient's life. To reduce these issues, several studies have presented the use of blockchain technology as a trustworthy network of solutions to ensure patient information security and secure the transfer of IoT devices' data. In this regard, this research is an attempt to present a new framework that facilitates the storage and transfer of patient data in the blockchain by merging the electronic health record and remote patient monitoring techniques into a single framework using Django. This framework allows the transfer of data from IoT devices to multiple peers, making use of the smart contract provided by the Ethereum platform.

1. Introduction

The healthcare system has undergone many changes within a short period of time. New technologies have changed the patterns of healthcare, as procedures that used to require weeks to be completed are now achieved within a day [1]. The Electronic Health Record (EHRs) is considered the cornerstone of providing a modern health service, as there is no loss of records, personal clinical diagnosis decisions, or anonymous people with no identities. EHR includes diagnoses, medications, patient medical histories, test and laboratory results, and all tools related to decision-making for patient care [2]. Another recent technology that has facilitated patient care is Remote Patient Monitoring (RPM). Whereby patients are monitored outside traditional clinical health contexts. The Internet of Things (IoT) devices are among the best applications for RPM. These devices (especially those which can easily be worn) improved the speed of caring for patients by continuously monitoring the events that take place on the patient, even if the patient is in a place far from the healthcare provider (for example at home) [3]. The EHR system contains sensitive information such as the patient’s name, age, sex, type of disease, condition and required treatments, and these factors are considered to be part of the patient's privacy. Since they may not want to disclose them, the data must therefore be stored in a safe manner that ensures the protection of the patient’s information and privacy [4]. Likewise, the transfer of data in RPM systems between the patient and the doctor must occur in a safe manner to ensure that not
penetration takes place and thus guarantees the privacy of patient data. Given the current centralized system that does not allow patients to control their records, many problems have arisen in terms of the patient’s safety and privacy. There are also concerns regarding penetration when transferring data between the patient and the healthcare providers [5]. Improving the safety of data transmission and storage forms the basis of the work presented in this paper. The reliable blockchain technology is the main axis used to store and transfer data in a secure and smart way, so as to provide a trusted, smart healthcare system.

This research is organized in the following manner: In Section 2, a brief review is provided on each of the healthcare system, the electronic health record, the Internet of Things environment and their uses in centralized, decentralized and distributed systems. In addition, reviews are presented on the blockchain technology, the Ethereum network, and the smart contract. Finally, this section ends by shedding light on the most prominent challenges facing the healthcare system, the Internet of Things, and the remote patient monitoring system, followed by summarizing some related works within the scope of this research. Section 3 explains the research problem and the challenges to be solved by the proposed system, thus presenting the desired objectives for this research. Section 4 explains the processing of the proposed system, as well as its requirements and implementation. This is followed by an evaluation of the most important security requirements that our proposed system addresses in comparison to alternative studies. Section 5 presents the evaluation of the system and draws a comparison with traditional systems and other related works. Finally, Section 6 presents a summary of the research and the solutions it provides within the field of research.

2. Background and Related Works

2.1. Healthcare Environment

Healthcare is of great importance to most countries. Beside economics, it is one of the major political issues. Therefore, most governments focus on how to support and improve this system [6]. There are many reasons why people use healthcare, including to treat diseases, examine their health condition, improve their lives, or obtain information about their health status [7]. The advancement of healthcare technologies over the past few years has reduced the cost of services provided by the health sector. The health system facilitated the possibility of storing patient data and accessing them faster by creating an electronic record for patients. In addition, modern technologies have provided more comfort for the patient by monitoring his health condition remotely through the establishment of a remote patient monitoring system that relies on Internet devices. However, with the availability of these technologies, many problems have arisen related to security and privacy that require searching for other techniques to solve these problems, the most important of which is the blockchain technology that has been proposed in the present system and will be discussed in later sections.

2.2. Internet of Things

The concept of the Internet of Things appeared in 1999, when Kevin Ashton referred to it as connected objects that can be identified using radio frequency identification technology (RFID). However, the precise definition of the Internet of Things remains subjected to different viewpoints. In the general sense, the Internet of Things (IoT) is a network of physical objects (computers, vehicles, smart phones, buildings, cameras ... etc.) integrated with electronic circuits, software and sensors, so that these devices can collect and exchange data and control remotely, thereby increasing its accuracy and efficiency [8]. Internet of Things devices have many characteristics that provide flexibility and accuracy [9], the most important of these characteristics are:

- **Heterogeneity**: IoT devices can communicate with each other even if they are heterogeneous and in different networks.
- **Interconnectivity**: Everything is interconnected with global information and communication structure.
- **Safety**: The use of IoT enables the addressing of most concerns, especially those related to human health, home and work monitoring.
• **Dynamic changes**: The devices' state changes dynamically according to their demands, such as movement and rest, speed and location.

In the centralized application environment, all the nodes are connected to a central node, so only the central node will be responsible for the data, transfer and storage. On this basis, the important question to be asked is: Can it be assured that this data is not tampered with? This is a difficult question to answer in the centralized environment, where data can be changed according to the interests of private entities, which implies that the information they provide may not be completely trusted.

The combined ability of blockchain and IoT devices to save or monitor data is desirable, since reaching a decentralized consensus is critical within a large network of devices. It ensures that all devices have the same state of data collected and outsource the computational power needed to implement specific IoT use cases on the blockchain. Currently, creating larger networks of sensors and serving them all with Smart Contract (SC) is a waste of time, which is why it is desirable to implement the SC Generator framework to simplify and speed up this process [10].

2.3. **Blockchain Technology**

A blockchain is a ledger completely distributed over a peer-to-peer network that uses encryption to securely host applications and store data. Each node in the blockchain network maintains a complete copy of the ledger and upon validation of the transaction, these ledgers update continuously. Initially, the blockchain was designed as a network for financial transactions using the Bitcoin digital currency, but given the encryption and decentralization features of the blockchain technology, it is suitable for cyber security systems. The ledger consists of a number of blocks chained together by a hash mechanism. Each block consists of two parts, the first includes the number of transactions that have been executed and verified. The second part is called the header of the block, where the header information such as the timestamp and the hash of that block and the previous one are stored. In this way, a group of existing blocks are joined together to form a chain of blocks, and the longer the chain is, the more secure it will be against counterfeiting. The following sub-sections discuss the Ethereum platform, as well as its most important characteristics and connection with blockchain technology.

2.3.1. **Ethereum**

The Ethereum network allows developers to create decentralized applications, as it is a software platform based on blockchain technology. In 2013, Ethereum was described by a white paper presented by Vitalik Buterin, where he and a group of other founders secured funding in an online public crowd sale during 2014, after which the blockchain was officially launched in the summer of 2015. Ethereum miners generate a cryptocurrency called (ETH) and it is associated with Ethereum. Table 1 below shows the currency of the ether currency.

| Table 1. Currency of the Ether Currency |
|----------------------------------------|
| 1 Eth is |  |
| wei | $10^{18}$ |
| Kwei | $10^{15}$ |
| Mwei | $10^{12}$ |
| Gwei | $10^9$ |
| szabo | $10^6$ |
| finney | $10^3$ |
| ether | 1 |
Ethereum provides users with the ability to save the entire Turing token called smart contracts (SCs) in the blockchain. These SCs are simultaneously evaluated by multiple blockchain users to ensure that everyone has the same contract status. As with the transactions being evaluated and executed, the SC costs a small amount of Ether to the owner of the SC [11].

2.3.2. Smart Contract
A smart contract is a package of software used to facilitate the process of exchanging money, property, or data. When it is linked to the blockchain, it becomes autonomous and cannot be stopped or tampered through the intervention of a third party. Figure 1 illustrates the example of smart contract architecture.

![Smart Contract Architecture](image)

**Figure 1.** Smart Contract Architecture

With regards to healthcare, blockchain technology and smart contracts are considered a safe way to share the patient’s record electronically, or to transfer data from remote patient monitoring devices, because smart contracts are distinguished by allowing only authorized persons or devices to access the patient’s record or its attachments. They also enable interoperability via collaborative version control in order to maintain the consistency of the record [12].

2.4. Related Work
The following review of related works will indicate the motive behind the present research. In [5], some examples are reviewed on the use of blockchain technology in preserving the privacy of patients. The authors of {Formatting Citation} present a survey of the amount of research concerned with healthcare and the apparent increase in recent years using blockchain technology in healthcare. In [14], the authors propose the use of blockchain technology based on Ethereum protocols to improve the security of a remote patient monitoring system, in addition to using cloud technology to store information and send alerts. In [15] the authors presented a new framework model for the blockchain, based on its distributed nature to address the computationally prohibitive costs of the blockchain. It requires a wide bandwidth, based on advanced cryptography.

As for [16], blockchain technology is used to create a decentralized records system (MedRec), which manages authentication, confidentiality, and data sharing. The researchers provided an insight into the potential of data economies to emerge, in order to enable researchers of engaging patients in obtaining metadata. The researchers in [17] offer a blockchain-layer model as well as a review of related research using the blockchain technology in the Internet of Things, and address the open and future problems of combining these two technologies.
The work in [18] also proposed to establish an electronic health record management system based on the use of blockchain technology. It has implemented a model for managing the electronic health record using the licensed blockchain platform. In [19], they present the most prominent challenges facing the use of blockchain technology with the Internet of Things, proposing the use of a secure and private structure for the Internet of things based on blockchain technology, while maintaining the same security and privacy characteristics of the blockchain. Finally, [20] tries to prove the effectiveness of blockchain technology in clinical trials and data protection by calculating the timestamp the transaction takes on the blockchain.

3. Challenges, Research Problem and Objectives

In the field of healthcare, the main challenges in 2020, as published by the Health Care Executive Group (HCEG), are:

i. **Costs and transparency**: medical and pharmaceutical costs, access to and quality of healthcare.

ii. **Data and Analytics**: Utilizing new technologies presented in data analysis, whether it involves internet devices, laboratories, or others, to improve health outcomes.

iii. **Interoperability / access to consumer data**: To add value to the collected data and systems, a mechanism is being sought to integrate and improve the exchange of member data (electronic patient record, financial statements).

iv. **Privacy**: To enhance the confidence of the consumer to share his data, search for a mechanism to ensure consumer privacy from cyber attacks.

For the Internet of Things, the main challenges include:

- **Authentication and Identity Management**: Authentication is very important for the Internet of Things, as without it, systems can be exposed to danger if the opponent is able to register as a legitimate user. He will be able to access user data and tamper or bargain with it. Currently, the username and password are used in the central system.

- **Authorization and Access Control**: It is important to know, after verifying, whether the user has permission to accessibility so that IoT devices can be controlled.

- **Security Issues in Healthcare**: There are a very large number of attacks on the joints of healthcare that have emerged recently, for example the attack that took place in (Storm 2015), which targeted blood gas analyzers, CT scanners and X-ray machines. It is clear that there are security issues in medical systems that may enable hackers to defraud or extort infected persons. As we noted in the above, there are many challenges and problems that accompany the traditional central system, the most important of which is related to costs, security and privacy, and through research these problems are difficult to solve within the centralize system environment, so the goal of this research is to find a way to solve these problems through the use of the system decentralization.

The objectives that will be studied in this research can be summarized in the following points:

i. **Reducing costs**: The use of a decentralized system will reduce costs by not needing a third party

ii. **Security and privacy**: Using smart contract technology and storing data in the blockchain network will provide confidence and security, and maintain privacy.

iii. **Facilitating the service**: Using the Django interface (programmed in Python) to integrate the EPR with the RPM technology will contribute to the process of delivering a comprehensive healthcare service to patients in a simpler manner.
4. The Proposed System

In our proposed system, the focus lies on the criteria that enable the system to cover healthcare requirements and be trustworthy, as well as to simplify the system and make it more useful to the user. A user interface has been designed, consisting of an electronic health record and a remote patient monitoring system to be comprehensive for the requirements of electronic healthcare, as shown in Figure 2. The system is protected by means of the blockchain technology, taking advantage of the characteristics and algorithms that this technology has. In order to protect the system and prevent unauthorized persons from entering the system, the algorithm (proof of authority) has been used, whereby addresses will be validated before they are allowed to enter the system by means of validators. After the user becomes authorized to access the system, he can be upgraded to be an auditor.

This method is applied to increase the number of miners. In order to increase immutability in the system, the block chain was increased by placing each user in a separate block, and adding a third peer to create a multi-peer system. This process made us of the distributed blockchain system. Instead of using a separate smart contract for each system, one smart contract was written for both, and provided the option for the patient to choose the system they would desired. Ethereum protocols were used to transfer information privately instead of transferring it on the public network.

Figure 2. User Interface for the Proposed System

4.1. System Requirements

4.1.1. Electronic Health Record (EHR)

The Electronic Health Record (EHR) is an electronic record of patient health information created by healthcare providers. This information includes patient demographics, progress notes, problems, and medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. EHRs automate and simplify the doctor's workflow. The electronic health record has the power to create a complete record of a patient's clinical encounter, as well as support other care-related activities directly or indirectly across the interface, including evidence-based decision support, quality management, and outcome reports. In the proposed system, the necessary information related to the
patient, the doctor and the healthcare center and their addresses are written on the blockchain network, so that the EHR data is linked and saved in the blockchain network by creating a smart contract for the EHR.

4.1.2. Remote Patient Monitoring
Remote patient monitoring (RPM) is a subclass of telehealth that allows patients to use portable medical devices to collect patient-generated health data (PGHD) and send it to healthcare providers. These devices include common physiological data such as weight, blood pressure and heart rate, which can be collected using a remote patient monitoring system. Once patient data is collected, it is sent to the doctor's office via a software application that can be installed on computers or smartphones [21].

4.1.3. Django Rest Framework
The Django Rest Framework, which is written in Python, is used to build a user interface that consists of an electronic patient record and a remote data monitoring system. This interface will be linked to the smart contract through web3.py

4.1.4. Web3.py
It is a package of libraries that enables the creation of transactions, as well as to read and write data to and from smart contracts. Web3.py is linked to Ethereum through JSON RPC. Since the Ethereum network is a peer-to-peer network, every node gets the data on the network, the Web3.py allows us to communicate to one node on the Ethereum network instead of communicating to all the nodes using JSON RPC [22]. Web3.py allows us to read and write data through a single node on Ethereum.

4.1.5. Data Set
- The dataset in [23] is used for creating electronic health record.
- The dataset in [24] is used as it contains information of IoT devices, in order to implement it into our system.

4.2. System Implementation
As a proof of concept, it is important to point out that we used the solidity language to write the smart contract. We took advantage of the Ethereum protocols to write and transfer data on the blockchain in a private, rather than public network. A user interface was created using the Django Rest Framework managed by a Decentralized Application (DApp). The user interface included two sections that are connected to same smart contract, the first for creating Electronic Health Record (EHR), while the second for the Patient Monitoring Remotely (PMR).

Each user firstly, we will implement a "proof of authority" algorithm. Each user will be validated by means of a validator before being allowed to access. The EHR contains all the information necessary explain in Section (4.1.1), as well as the addresses in a blockchain for patient, doctor and health center, were created by applying the dataset in [23]. It was assumed that each of (Patient, Doctor, and Health Center) has an Ethereum address in the blockchain. After filling in all the fields, they are formed and processed in the back-end of the user interface, after which the data is sent to the smart contract linked with the user interface through Web3.py. The smart contract analyzes the data and then sends it to the blockchain for the purpose of saving.

In the second section of the user interface, dataset [24] is applied to the remote patient monitoring system, after completing the authorize requirements to enter the remote patient monitoring system. The assumption is made that the data set represents the information that reached the smart contract via Web3.py. The data will be sent to the same smart contract associated with the patient's electronic...
record, this process is to reduce the costs. The smart contract will analyze the data and compare it with the threshold, if the data is abnormal, the smart contract will write it on the blockchain in the form of an event and send an alert to each of the doctor, the patient and the health center in a private way to maintain the security of the data.

![Image of proposed system](image)

**Figure 3.** Explanation of Proposed System.

The proposed system used the distributed blockchain technology for a healthcare application, as illustrated in Figure 4. A third peer is added to become multi-peer to peer, where the information will be shared between those peers who have the same hash. Whenever any change in the information occurs to any peer, it will be easy to detect and reject this action. This will, in turn, strengthen the chain against hacking.

![Image of blockchain distributed system](image)

**Figure 4.** Blockchain Distributed System Multi Peer-to-Peer

5. **System Evaluation**

In comparison with the rest of the research related to the use of blockchain technology in the field of healthcare, we have provided an integrated electronic healthcare system that is detailed in a single user interface, as it contains the electronic patient record and the remote patient monitoring system protected by blockchain technology. The other researches focused on one of the two systems, either
the electronic patient record or a remote patient monitoring system to be protected with blockchain technology. Unlike the central systems that depend on the username and password to authorize users for login into the system, we applied an algorithm (Proof Of Authority) that checks every address trying to enter the system by means of validators. The latter are selected after give authorization for the addresses. In this procedure, the number of miners is increased, as this will benefit us to increasing the immutability of the system [25]. Table 2 presents a comparison between our system vs. related work and traditional systems.

| Matrix             | Traditional System                                                                 | Proposed System                                                                 |
|--------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Comprehensiveness  | Related work and traditional system focus either to the electronic health record or the remote patient monitoring system. | Merging the two systems into one user interface and one smart contract.          |
| Confidentiality    | Encryption technology in traditional system.                                       | Proof Of Authority (Each address must be validated before it is allowed into the system). |
| Integrity          | Databases can be manipulated in the traditional system. Hash of blocks in the general concept of blockchain technology in related works. | High immutability by increasing the number of blocks and miners and adding a third peer. |
| Storage            | Cloud storage.                                                                     | Blockchain storage With a high speed of processing the transaction (POA).       |

The (Proof of Authority) algorithm saves time in processing data and completing the registration transaction, as compared to the rest of the algorithms used by Blockchain technology, which are shown in Figure 5.

![Figure 5. POA Blockchain Comparison](image-url)
To compare the immutability of the system, and to ensure that no tampering or alteration occurs to the information, our system ensures a high immutability by increasing the number of blocks and miners, using smart contract, and adding a third peer to become a multi-peer system. Hyong S. Kim and Ke Wang [25] proved that the immutability in blockchain technology depends on the number of blocks and miners through their testing of a different set of blockchain structures. It is difficult for the attacker to calculate the hash and access to the data, whereas the databases in traditional systems are more vulnerable to hacking. Table 2 shows a simple comparison between the traditional systems that depend on the centralized architecture and related work that use blockchain technology as compared with our proposed system.

6. Conclusion
The privacy and security of healthcare data is one of the most important academic issues at present, and due to limitations in the central system, current security solutions are inadequate. In this paper we presented a model for building a comprehensive health system that integrates the electronic health record and remote patient monitoring system into one interface. Using Django, we used blockchain technology to maintain the security and privacy of patient data. Our system contributes to reducing costs by eliminating the third-party concept as well as by building a lightweight smart contract that reduces the cost of conducting a transaction in the blockchain. Our proposed system ensures that no manipulation and alteration of data is allowed through the high immutability that we have provided by increasing the number of blocks, miners and adding a third peer.

7. References
[1] Vatandoost M, Litkouhi S. 2019. The Future of Healthcare Facilities: How Technology and Medical Advances May Shape Hospitals of the Future. Hosp Pract Res.4(1):1–11.
[2] Ehrenstein V, Kharrazi H, Lehmann H, Taylor CO. 2019. Obtaining Data From Electronic Health Records. Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User’s Guide. p. 1–92. Available from: https://www.ncbi.nlm.nih.gov/books/NBK551878/
[3] Real-time and Remote Patient Monitoring Trends How Sensors and Devices Are Forever Changing the Face of Healthcare 2017. TE Connectivity. Available from: http://content.healthaffairs.org/content/32/11/2013.full.
[4] Keshta I, Odeh A. 2020. Security and Privacy of Electronic Health Records: Concerns and Challenges. Egypt Informatics J. pp. 1–7.
[5] Engelhardt MA. 2017. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol Innov Manag Rev. 7(10):22–34.
[6] Okuonzi SA. 2004. Political Economy of Health with Reference to Primary Health. Heal Policy Dev.2(1):1–5.
[7] Bernstein A, Hing E, Moss A, Allen K, Siller A, Tiggle R. 2003. Health care in America: Trends in Utilization. National Center for Health Statistics. Available from: https://www.cdc.gov/nchs/data/misc/healthcare.pdf.
[8] Kalla A, Prombage P, Liyanage M., 2020. Introduction to IoT. In: IoT Security. pp. 1–25.
[9] Patel K, Patel S. 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. Int J Eng Sci Comput.6(5):6122-6131.
[10] Khan MA, Algarini F, Quasim MT. 2020. Decentralised Internet of Things. (January):3–20.
[11] Luck S. 2017. Design and Implementation of a Smart Contract Creator Framework for IoT Devices. University of Zurich. Available from: https://www.csg.uzh.ch/csg/en/.
[12] Sofia B. 2016. Blockchain-Enabled Smart Contracts : Applications and Challenges. arXiv Prepr arXiv181004699v2.1–3.
[13] Agbo C, Mahmoud Q, Eklund J. 2019. Blockchain Technology in Healthcare: A Systematic Review. Healthcare.7(2):56.
[14] Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. 2018. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst. 42(7):8.
[15] Dwivedi AD, Srivastava G, Dhar S, Singh R. 2019. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors (Switzerland).19(2):1–17.
[16] Azaria A, Ekbлав A, Vieira T, Lippman A. 2016. MedRec: Using Blockchain for Medical Data Access
and Permission Management. Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016. p. 25–30.

[17] Zorzo AF, Nunes HC, Lunardi RC, Michelin RA, Kanhere SS. 2018. Dependable IoT Using Blockchain-Based Technology. In: Proceedings - 8th Latin-American Symposium on Dependable Computing, LADC. p. 1–19.

[18] Usmana M, Usman Q. 2019. Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. In: 2019 International Conference on Identification, Information and Knowledge in the Internet of 2019 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2019). p. 321–327.

[19] Dorri A, Kanhere SS, Jurdak R. 2016. Blockchain in Internet of Things: Challenges and Solutions. arXiv Prepr arXiv160805187.129–37.

[20] Irving G, Holden J. 2016. How Blockchain-timestamped Protocols Could Improve the Trustworthiness of Medical Science. F1000Research.5(May):1-5.

[21] Malasinghe LP, Ramzan N, Dahal K. 2019. Remote Patient Monitoring: A Comprehensive Study. J Ambient Intell Humaniz Comput.10(1):57–76.

[22] McCubbin G. 2020. Intro to Web3.py - Ethereum For Python Developers. Dapp University. [cited 2020 Aug 25]. Available from: https://www.dappuniversity.com/articles/web3-py-intro.

[23] Malamud N. 2020. nyc-reach-members-1.csv. data.world.

[24] Shi K, Schellenberger S, Will C, Steigleder T, Michler F, Fuchs J, et al. 2020. A Dataset Of Radar-Recorded Heart Sounds And Vital Signs Including Synchronised Reference Sensor Signals. Sci Data.7(1):1–12.

[25] Kim HS, Wang K. 2018. Immutability Measure for Different Blockchain Structures. In: 2018 IEEE 39th Sarnoff Symposium, Sarnoff. p. 1--5.