International Journal of Medical Informatics 148 (2021) 104399

Contents lists available at ScienceDirect

International Journal of Medical Informatics

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

Review article

The role of blockchain technology in telehealth and telemedicine

Raja Wasim Ahmad [a], Khaled Salah [a], Raja Jayaraman [a], Ibrar Yaqoob [a,*], Samer Ellahham [b], Mohammed Omar [a]

[a] Research Center on Digital Supply Chain and Operations Management (DSO), Khalifa University of Science and Technology, Abu Dhabi 127788, United Arab Emirates
[b] Heart & Vascular Institute, Cleveland Clinic Abu Dhabi, United Arab Emirates

ARTICLE INFO

Keywords:
Blockchain
COVID-19
Telemedicine
Telehealth
Smart contracts
Security

ABSTRACT

Objective. Telehealth and telemedicine systems aim to deliver remote healthcare services to mitigate the spread of COVID-9. Also, they can help to manage scarce healthcare resources to control the massive burden of COVID-19 patients in hospitals. However, a large portion of today's telehealth and telemedicine systems are centralized and fall short of providing necessary information security and privacy, operational transparency, health records immutability, and traceability to detect frauds related to patients' insurance claims and physician credentials. **Methods**. The current study has explored the potential opportunities and adaptability challenges for blockchain technology in telehealth and telemedicine sector. It has explored the key role that blockchain technology can play to provide necessary information security and privacy, operational transparency, health records immutability, and traceability to detect frauds related to patients' insurance claims and physician credentials. **Results**. Blockchain technology can improve telehealth and telemedicine services by offering remote healthcare services in a manner that is decentralized, tamper-proof, transparent, traceable, reliable, trustful, and secure. It enables health professionals to accurately identify frauds related to physician educational credentials and medical testing kits commonly used for home-based diagnosis. **Conclusions**. Wide deployment of blockchain in telehealth and telemedicine technology is still in its infancy. Several challenges and research problems need to be resolved to enable the widespread adoption of blockchain technology in telehealth and telemedicine systems.

1. Introduction

The recent challenges and globalized transmission of Coronavirus (COVID-19) present important needs to establish reliable, resilient, and robust patient care and health services [1,2]. The COVID-19 pandemic boosts the uptake of telehealth and telemedicine technology as it can safely enable communication with physicians and health specialists through virtual channels to minimize the spread of infection. Several companies and platforms, such as Teladoc Health, JD Health, and Rush University Medical Center (RUMC) have recently witnessed a rapid increase in demand for telehealth and telemedicine services to combat the spread of the COVID-19 virus [3–6]. Telehealth and remote consultations enable efficient healthcare access and offer better care coordination and treatment outcomes. Centralization is a key impediment in existing telehealth and telemedicine systems that poses the risk of single point of failure. In addition, data in current telehealth and telemedicine systems are prone to a variety of external and internal data breaches compromising the reliability and availability of systems [1,7,8]. Blockchain technology can help to address such crucial problems. The emerging blockchain technology follows a distributed architecture to manage a shared ledger of health records among diverse participants, wherein all ledger copies are kept verified and synced with every node affiliated with the blockchain [9,10]. Tracking the locations visited by infected patients, protecting remote patient-doctor consultation records, tracing medications and medical test kits across the supply chain, verifying the credentials of physicians, and proving the provenance of malfunction medical test kits, are among the key challenges that can be addressed through blockchain technology.

Telemedicine enables healthcare professionals to remotely monitor, diagnose, and treat patients by offering cost-efficient services, thereby minimizing patient access and workforce limitations, expanding technology capabilities, and mitigating the risk of exposure of physicians, staff, or patients to the COVID-19 virus. Similarly, telehealth employs digital information and communication technologies to help the patients to manage their illness through improved self-care and access to education and support systems [11,3,12]. The major benefits of existing telehealth and telemedicine systems are highlighted in Fig. 1 that reveal virtual healthcare systems have the potential to successfully mitigate the

* Corresponding author.

https://doi.org/10.1016/j.ijmedinf.2021.104399
Received 22 June 2020; Received in revised form 27 November 2020; Accepted 19 January 2021
Available online 28 January 2021
1386-5056/

spread of airborne infections to handle COVID-19 pandemic. Moreover, the adoption of blockchain technology into existing telehealth and telemedicine systems can bring numerous opportunities for secure digitization of healthcare, such as successfully establish the provenance of clinical data, legitimacy of users seeking patient data, manage identities of devices used for remote patient monitoring, preserve patient anonymity, and automate the payments settlement. Fig. 2 highlights the intrinsic features of blockchain technology, such as transparency, immutability, auditability, and anonymity of users and data.

The decentralization feature increases the overall robustness of existing healthcare systems, and thus Electronic Health Records (EHRs) of the patient are preserved against adversarial attacks or accidental data loss [2,13–15]. Moreover, the consensus protocols ensure the agreement on the current state of the blockchain ledger to establish trust among telehealth and telemedicine participants [10]. The immutability of health records is assured due to public-key cryptography which makes every transaction to be digitally signed first before it can be verified and written onto the ledger. The distinguishing features and benefits of employing blockchain technology to digitize telehealth and telemedicine services are highlighted in Table 1. The unique requirements of the healthcare industry, such as fast and real-time EHR sharing [16], patient-centered health data management [17], low cost, high performance, data security, privacy, availability, and transparent establishment of the provenance of health records [18], can be satisfied through blockchain technology. Besides, leveraging blockchain for interactive medical approaches including "doctor in the loop" can lead to enhance their protection against possible database manipulation threats through tamper-proof log data [19]. Blockchain technology paired with smart contracts automates operations and services of telehealth and telemedicine in an efficient and trustful way. A smart contract is a self-executing program that runs on the blockchain platform. It automates the business processes and supersedes the role of intermediaries in current healthcare systems. The predefined rules among the participating organizations are translated into smart contract functions to establish trust [20].

Smart contracts have been extensively practiced in existing systems that are proposed to digitize healthcare services [21]. More specifically, the existing studies have mainly focused on securing patients' EHR [16,10,22], traceability of COVID-19 outbreak [23–25], drugs supply chain management [26,18,27,28], and digitization of telemedicine industry [29,30,14]. An Ethereum-based telemedicine solution presented in [31] has preserved the integrity of EHR by storing IPFS hashes of EHR in the decentralized network. Another system proposed in [32] has combined artificial intelligence (AI) and blockchain technology for securing and monetizing the patient's health data. The multi-access Edge computing (MEC) and blockchain-based system presented in [33] has employed various smart contracts to swiftly and securely transfer the cryptocurrency to the wallet of patients as an incentive for sharing their health data. The Etherum-based system presented in [34] enables real-time patient's health monitoring and successfully maintains a timestamped log of medication taken by the patients. In [30], the authors presented a dynamic and flexible multi-authority-based telemedicine system that stores EHR on the chain to assure that data cannot be modified or deleted by the network users. It also allows patients to enroll and leave the network freely. Table 2 outlines and compares several studies that have reviewed the role of blockchain-based systems in different healthcare areas. As can be seen in Table 2, none of the existing studies have explored the role of blockchain technology in telehealth and telemedicine systems, unlike our study. The key contributions of this paper are summarized below:

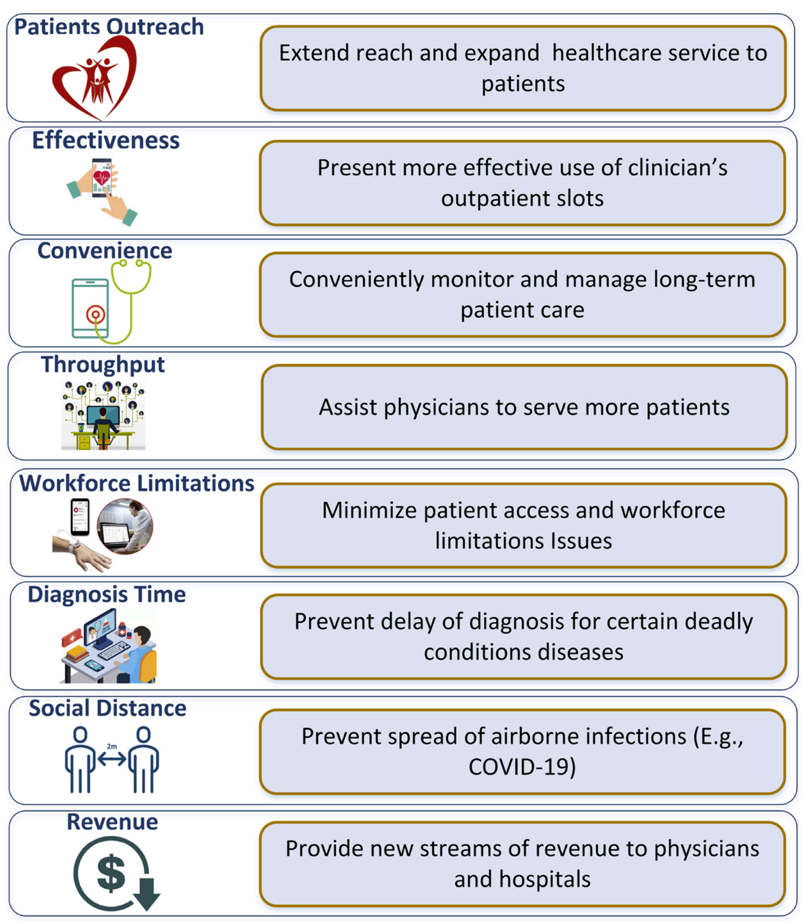

Fig. 1. Benefits of telehealth and telemedicine services.

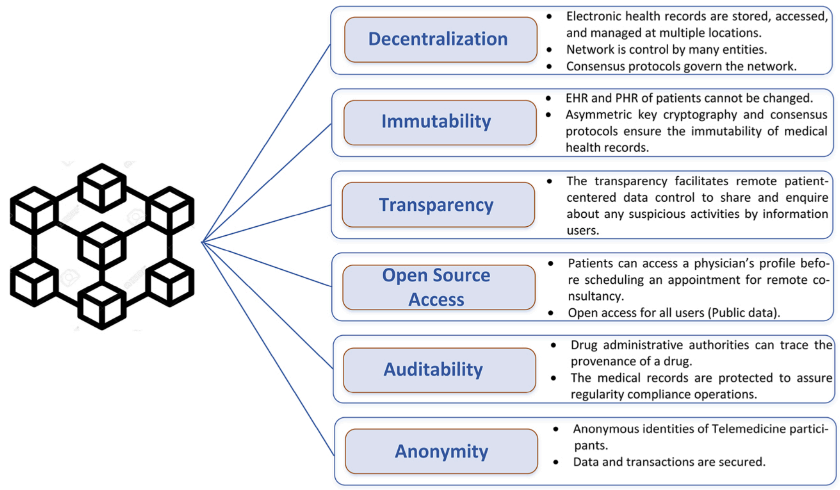

Fig. 2. An overview of key elements and features of blockchain technology for telehealth and telemedicine.

Table 1
Comparison of traditional, centralized, and blockchain supported telehealth and telemedicine systems.

	Traditional Healthcare System	Centralized Telemedicine System	Blockchain Supported Telemedicine
Cost	High	Low	Low
Patient Waiting Time	Very High	Low	Low
Fault Tolerance	NO	NO	YES
Requirement for In-Person Visit	YES	NO	NO
Data Provenance	NO	NO	YES
Health Record Manipulation	YES	YES	NO
Documentation	YES	YES	NO
System Administration	Centralized	Centralized	Decentralized
Audit Trials	NO	NO	YES
Data Privacy &Security	Hard	Hard	Easy
Transparency	NO	NO	YES
Reliability &Integrity	Low	Low	High

- We discuss the potential opportunities that blockchain technology can offer to telehealth and telemedicine systems by alleviating their key limitations in terms of reliability, traceability, immutability, transparency, data provenance, audit, trust, and security.
- We present recent case studies to demonstrate the practicality of blockchain technology in telehealth and telemedicine domain.
- We discuss several open research challenges that prevent existing telehealth and telemedicine systems to fully exploit the benefits of blockchain technology.

The remainder of the paper is organized as follows. Section 2 presents potential opportunities for blockchain technology in telehealth and telemedicine. Section 3 reviews recently reported blockchain-based projects for telehealth and telemedicine services. Section 4 presents a discussion on research challenges. Section 5 discusses the conclusions and opportunities for future research.

2. Blockchain opportunities in telehealth and telemedicine

In this section, we briefly discuss the key opportunities brought about by blockchain technology for telehealth and telemedicine to ensure trust among healthcare participants, as shown in Fig. 3.

2.1. Patient consent management

The effectiveness of virtual care and health monitoring depends on

Table 2
Comparison of existing surveys on blockchian-based healthcare studies.

Article	EHR/PHR Management	Health Insurance	Telehealth Use Cases	Telemedicine Use Cases	Patients Health Follow-Up	Drugs/Pharmaceutical Management	Industry- based Research-projects
[35]	✓	✓	×	×	×	✓	×
[36]	✓	✓	×	×	×	×	×
[37]	✓	✓	×	×	×	×	×
[27]	✓	✓	×	×	×	✓	✓
[38]	✓	✓	×	×	×	✓	×
[28]	✓	×	×	×	×	✓	✓
[39]	✓	✓	×	×	×	✓	×
[40]	✓	✓	×	×	×	✓	×
[41]	✓	✓	×	×	×	✓	×
[42]	✓	✓	×	×	×	✓	✓
[22]	✓	✓	×	×	×	×	×
Our Study	✓	✓	✓	✓	✓	✓	✓

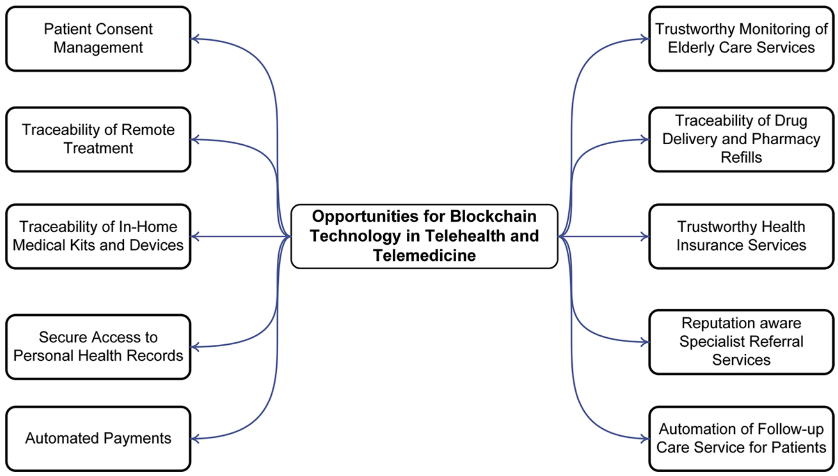

Fig. 3. Potential opportunities for blockchain technology in telehealth and telemedicine.

the integrity of the EHRs that include a patient's medical history, diagnosis, medication, and treatment plans. The EHRs are highly sensitive and private information, which needs to be securely shared among peers, such as hospitals, pharmacies, and health regularity authorities to maintain a patient's medical data up to date [10,43]. The health legislation for telemedicine has empowered patients to control and manage their clinical data by setting data access and usage rules. The traditional consent management systems face several challenges, such as high convergence time in sharing EHR with the specialist, limited trust on the third-party servers that implement patient consent management services, and the inability to conduct fair audit trials. Blockchain technology can help to enforce trust as no intermediaries are involved. Through blockchain, the consent management is assured and protected through several peers belonging to different participating organizations [44–46]. Moreover, the intrinsic immutability, traceability, and transparency features of blockchain can assist to conduct audit trials to verify compliance with consent management policies. Fig. 4 highlights various participants that trigger telemedicine services to store health data on blockchain and local storage systems.

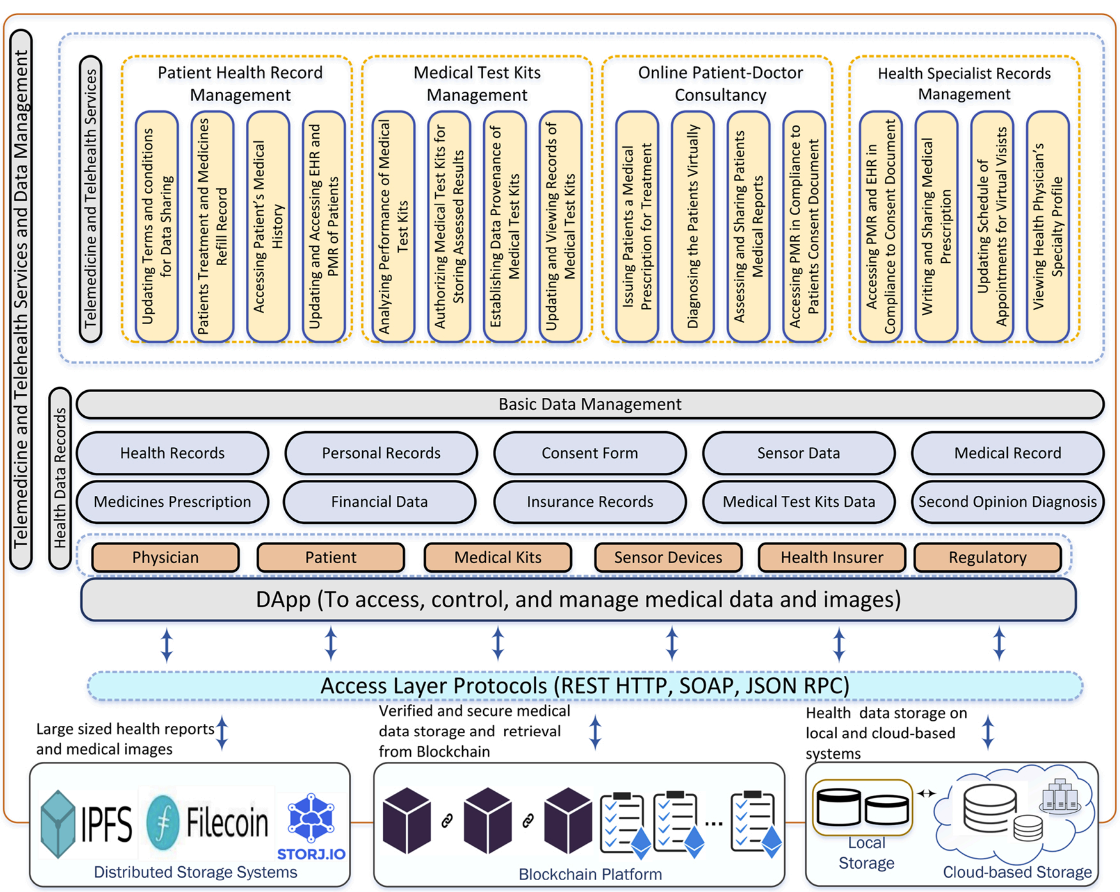

Fig. 4. Blockchain-based health data storage, access, and management in telehealth and telemedicine services.

2.2. Traceability of remote treatment

Practicing telehealth and telemedicine requires an electronic face-to-face encounter of patients and specialists for effective health assessment of the remote patient. The telehealth service provisioning follows direct-to-consumer (D2C) and business-to-business (B2B) models. In the former model, patients can electronically communicate to doctors to discuss their health conditions; whereas, in the latter model, the caregivers can remotely participate in the consultation and medical education services (e.g., patient surgery) through tools that support audio and video conferencing. In the electronic face-to-face consultation, asynchronous transfer of videos and images (that might include x-rays or other diagnostic test results) can assist caregivers to accurately diagnose the health condition of the patients [5,47]. In existing telemedicine systems, health organizations are unable to manage the silos of patient health records due to limited data sharing among each other. To overcome this issue, blockchain technology provides a single and coherent view of the EHR of patients for all participating stakeholders. The visibility and transparency of health records enable the related participating organizations to trace the medical history of a patient to propose suitable treatment. For instance, through blockchain technology, audits can be carried out to find who accessed and exactly what transactions were performed on electronic records.

2.3. Traceability of in-home medical kits and devices

In-home medical kits and devices can assist patients to perform self-diagnosis in a nonclinical environment. The adoption of off-the-shelf test kits and devices to assess specific biochemical responses for the self-checkup and early disease detection can minimize overall healthcare costs [48,49]. In the traditional centralized telehealth-based systems, the lack of transparency, visibility, and data provenance about the medical kits hinders physicians and patients to procure trustworthy medical kits from reputed manufacturers. For such a situation, blockchain technology can be used to immutably and transparently record transactions related to ownership and performance of testing kits on the distributed ledger. The smart contracts can be used to record reputation scores for all medical test kits and devices that are used for home care services based on their performance reviews. As a result, the immutable data provenance records about the in-home medical test kits and their reputation scores can be helpful for the patients, physicians, and laboratory engineers to procure highly accurate and trustworthy medical kits from the reputed manufactures.

2.4. Secure access to personal health records

A Personal Health Record (PHR) is an individual's health data, personal, and other information related to the care of the patient. The records of the PHR are created, maintained, and managed by the owner of the data [50]. However, the EHR contains more extensive health records as they are created, maintained, and managed by the healthcare providers. The traditional systems used to offer virtual healthcare services are mostly based on cloud platforms that are less trustworthy as they are managed by a single entity. Also, the integrity of PHRs in traditional cloud-based systems is compromised. The intrinsic features of decentralized blockchain technology enables the owner of the medical data to maintain the privacy of the data. The smart contracts can register and authorize the users to access the patient data in compliance with the patient consent policy. Also, the flexibility feature of blockchain technology assists the data owner to share and control data with legitimate users while complying with terms and conditions set by the data owner [9,16,30].

2.5. Automated payments

The current healthcare systems often employ centralized third-party services to settle payments among patients, caregiver, and insurance companies for using services. However, the centralized payment settlement methodologies are relatively slow, potentially vulnerable to hacking, and nontransparent. Moreover, the centralized payment settlement systems either do not support micropayments or they present extremely expensive micropayments. To support micropayments in the telehealth sector, the blockchain platform offers cryptocurrency tokens based payment. Hence, the direct transfer of cryptocurrency tokens to the wallet of the service provider presents a fast, secure, transparent, and auditable system that does not need a central mediation service to resolve the payment settlement disputes [51–53]. Moreover, the digitally signed payment-settlement transactions can assure the health service providers and consumers cannot repudiate transactions in the future. Blockchain technology can support implementing cash on delivery service to minimize the chances of payment related frauds. For instance, when implementing remote drug delivery service for telepharmacy, smart contracts can be programmed to hold and transfer the cryptocurrency tokens to the wallet of pharmacists only when the drugs are successfully received by the remote patient.

2.6. Trustworthy monitoring of elderly care services

The technological advancements in the Internet of things (IoT) can assist the telehealth sector to monitor a patient's health remotely through precise biomedical sensors [54–58]. The biomedical sensors can continuously monitor and store health data on a high-performance edge server that helps to analyze the health condition of a patient. The health data can be related to vital indicators, such as blood pressure and body temperature. However, the inaccurate data captured through a malfunctioning device can lead to medical errors. To satisfactorily resolve this issue, the decentralized blockchain technology employs smart contracts to register and verify the access rights of biomedical sensors to store the EHR on the ledger [34]. In order to respond to an unforeseen emergency, smart contracts can timely trigger alerts to doctors and health centers. For in-home care service, the IoT-assisted blockchain systems can proactively trigger a medication refill notification for the patient. Fig. 5 presents a system that leverages blockchain-based smart contracts for monitoring a remote patient's health. It assures that only authorized users having compliance with the patient consent form can access to the EHR of a patient.

2.7. Traceability of drug delivery and pharmacy refills

The virtual online consultancy based healthcare systems require the physician to transact on the blockchain to share medication prescription with the local pharmacy. Through the hash functions, blockchain technology can assist to eliminate the potential prescription errors and record alteration [59,60]. The registered pharmacists can access the drugs prescription stored on the blockchain to verify, prepare, and send the drugs to the patients. In return, the shipper can record its current location on the blockchain to assist pharmacists and patients to track and trace the shipment. Moreover, the transparency and traceability of blockchain transactions can enable the patients and doctors to verify the legitimacy of the medicine through its data provenance [61]. Through automation, a smart contract can automatically place a (periodic) prescription refill order for the medicine to the pharmacists once a predefined criterion is met. In response, the pharmacy can authenticate and validate the prescription to refill it. After the successful prescription refill, it is shipped to the patient, and records are updated accordingly.

2.8. Trustworthy health insurance services

A large number of patients are usually least interested to disclose their medical details to the insurance companies due to limited incentives and strict privacy-preserving policies. Consequently, the patients often opt for an inappropriate insurance policy that can lead to the

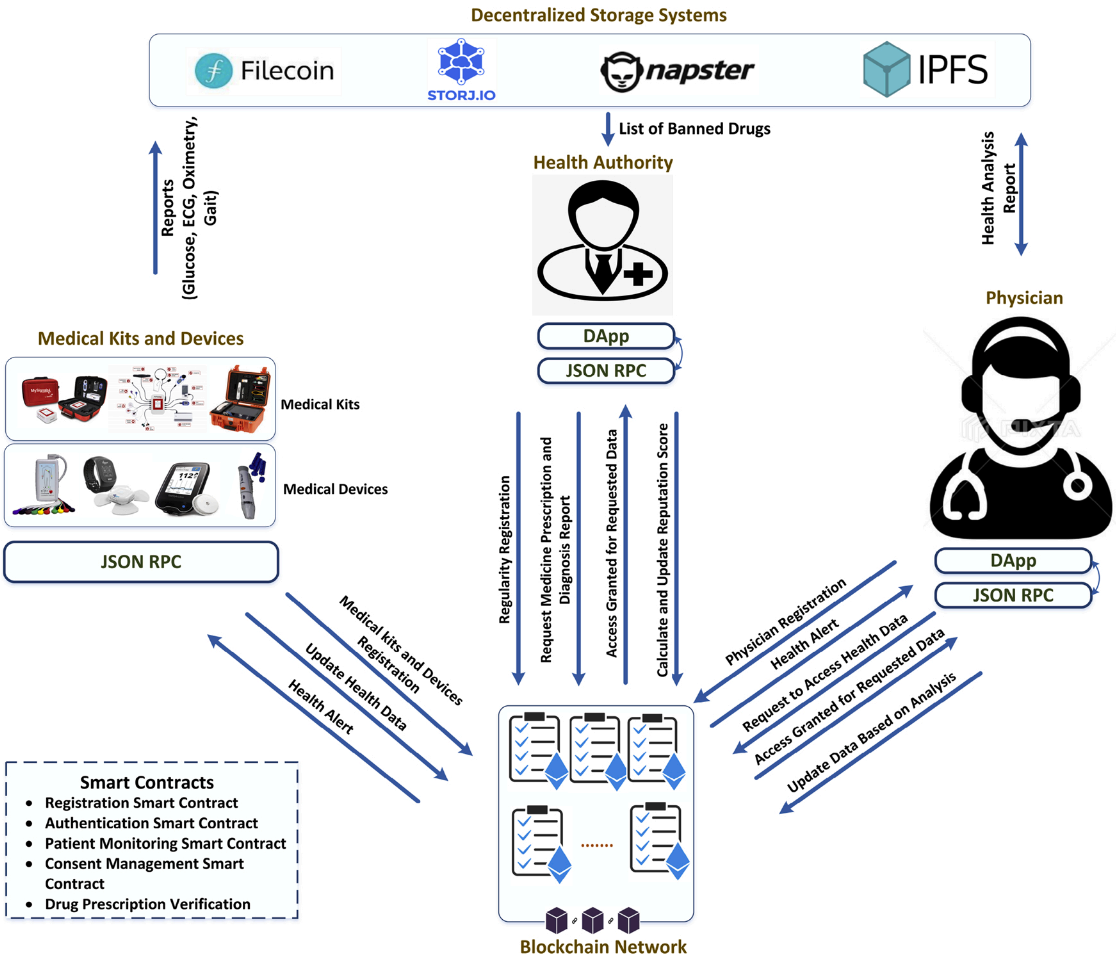

Fig. 5. Remote patient monitoring using blockchain-based smart contracts.

rejection of genuine insurance claims. The virtual health-based legislation protects the patient's rights to reimburse at the same rate as in the case of physical healthcare systems. The insurance-related frauds (e.g., the presentation of a wrong medical claim to an insurance company) require many days to establish the truth from the given information. Blockchain technology can assist the insurance providers to minimize the insurance frauds by granting them access to the medical record of a patient (consent-based). The patients can be incentivized for allowing the insurance providers to use the medical data of the patients. Also, numerous insurance companies offer incentives in terms of cryptocurrency tokens to the premium holders for maintaining their healthy lifestyle, such as tracking the visits to Gym [53,62]. For establishing trust, the smart devices attached to the patient can transact on the blockchain.

2.9. Reputation aware specialist referral services

The telemedicine participants, such as patients, referring healthcare providers, and consulting healthcare specialists are the vital entities involved in telemedicine-based cross-regional and cross-disciplinary diagnosis and treatment [63,64]. Through medical alliances and smart contracts, medical referrals and experts opinions are sought during remote patient treatment. In a blockchain-based solution, the referring healthcare provider can store the referral documents on the IPFS server that returns IPFS hash of the document for storing it on the blockchain to authorize consulting healthcare specialists to access it. Through IPFS hash stored on the blockchain, it can be identified that whether or not the stored document on the IPFS server is altered. The consulting healthcare specialist can examine the health report of the patient for examination, and subsequently health specialists can store such a diagnosis report on to the blockchain ledger. Based on the total service time and satisfaction score of the consulting health specialist, the referring healthcare provider can update the reputation score on the blockchain.

2.10. Automation of follow-up care service for patients

Follow-up care service enables health professionals to closely monitor the health of a patient after completing treatment. In certain cases, the follow-up service requires the patient to share reports of blood and urine tests with the practitioners before registering for a virtual meeting [65]. Blockchain technology can automate the patient's follow-up service through smart contracts. The smart contracts can automatically trigger a notification to remind the patient, physician, and nursing staff about the upcoming follow-up schedule [66,67]. The physician can access the transparent and immutable EHR of the patient to verify the health condition of a patient that was recorded during the last follow-up meeting (virtual). Moreover, by using IPFS servers that can host medical test reports, the patient can use a smart contract to register and share the IPFS hash with the physician for accessing health reports.

3. Blockchain-based projects and synergies for telehealth and telemedicine

Several organizations, such as CallHealth, Medildger, and Embleema have developed blockchain-based systems to offer trust and operational transparency in healthcare systems. The blockchain-based systems; namely, SMEAD, WellLinc, MedBlock, and MedRec have improved healthcare industry services by enabling healthcare professionals to perform business operations in a reliable, trusted, transparent, auditable, trackable, and secure way [68]. This section presents the five most recent and prominent start-ups and projects focused on the integration of blockchain technology with telehealth and telemedicine systems.

3.1. MedCredits

MedCredits is an Ethereum-based system that assists physicians in diagnosing dermatology patients using telemedicine service. It is a secure system that protects users from malicious entities by implementing reputation-based systems to incentivize and penalize honest and dishonest behaviors, respectively [47]. Moreover, it has implemented a Token-Curated Registry (TCR) service that enables experts in the network by validating the licenses of physicians to permit only high-quality physicians to join the platform [69]. Two of the Ethereum-based smart contracts implemented in Medcredits help to automate the payments based on escrow protocol and validate medical cases. The protocol requires patients to deposit escrow in the wallet of a smart contract before uploading the description of health issues and supporting images. The physician can access a patient's health symptoms to diagnose and prescribe treatments using the blockchain. In response, the patient can apply for a second health opinion (through the case validation contract, if required). The case validation smart contract sends the case to another physician for seeking a second opinion [47,69,70].

3.2. Medicalchain

Medicalchain has leveraged Ethereum and Hyperledger Fabric platforms for implementing services related to remote patient-to-doctor consultancy and health data marketplace applications. It facilitates the patients to securely share health data with healthcare professionals under specified terms and conditions. The EHR marketplace feature in the Medicalchain platform allows authorized patients to privately negotiate the terms and conditions for EHR data usage by the third-party healthcare professionals [53,71]. The premissioned Hyperledger Fabric features enable Medicalchain to implement the access control policies that support access control for varying levels. The MedicalChain has employed an external registration service named 'Civic's registration service' to manage the keys [53]. The ERC20 token was used for the Ethereum platform to assist the participants to transparently use the platform services to settle payments and identify insurance frauds [53,71,72].

3.3. HealPoint

HealPoint has employed the Ethereum platform to implement on-demand telemedicine services. It assists patients to use virtual health consultation services for sharing patient's symptoms, medical history and vital signs with the physician. Moreover, the Ethereum-based smart contracts implemented by the HealPoint can enable patients to get the second opinion (using schelling-coin algorithm [73]) from several medical experts globally. An AI-based system is integrated with HealPoint to match and recommend the appropriate physicians that match to the patient's health symptoms. Before providing a health service, experts in the network verifies the identity and license of the physician to either allow or reject the request to join the network. Also, to handle frauds, the physicians are required to deposit their stake in the wallet of a smart contract [74]. In the end, all the interactions with the patients are digitally signed before recording them on the ledger for audit purposes [74,75].

3.4. MyHealthMyData (MHMD)

MHMD [76] is an open biomedical information network that helps to establish a connection between individuals and organizations by empowering them to manage and control their data by themselves. It aims to reshape and transform the way sensitive data is stored. This initiative also encourages hospitals to anonymously make data available for open research. Key elements and technologies that are involved in this project include blockchain, dynamic consent, personal data account, smart contracts, multilevel de-identification and encryption technologies, and big data analytics. From the data security point of view, it employs a public blockchain platform that stores information into hash language-based codes. More specifically, smart contracts are used to automate the execution of all transactions under certain user-defined conditions. The blockchain-based solution helps to distribute the control among multiple stakeholders that lead to provide stringent protection against fraudulent activities. It also provides transparency, traceability, trackability, audit, security, and data provenance support by storing all the data in a fully tamper-proof and decentralized manner. The blockchain-based approach endorses the vision of MHMD by making it a secure and trustworthy information marketplace that helps to create valuable relations between EU citizens, hospitals, research centers, and businesses [76].

3.5. ROBOMED

Robomed is a network of clinical organizations that is controlled and administered by the Ethereum blockchain-based smart contracts. It aims to provide effective medical services to the patients (Value-based care). Robomed EHR, a medical information system, allows healthcare organizations to register, connect, and manage themselves within the Robomed network using Ethereum smart contracts. The basic functionalities of the Robomed EHR module include real-time monitoring of all interactions with the patient, decision-making for medical personnel, the establishment of personnel access rights, displaying the schedule of health specialists, analyzing the health condition of patients via charts, and health consultancy services via telemedicine. The Robomed mobile module enables patients to receive telemedicine consultations, postponed or cancel their visits, and comply with the rules defined in the consent contract during EHR sharing to the clinic. By using smart contracts, the organizations of Robomed can monitor and verify the health outcomes of the patient and comply with the clinical guideline for value-based health services. RBM (an Ethereum token) is acceptable to all Robomed organizations to use it as a method of payment. RBM token complies with the ERC-20 standard of the Ethereum platform [77,78].

4. Open research challenges

This section presents several open research challenges related to the adaptability of blockchain in telehealth and telemedicine.

4.1. Organizational challenges to the adoption of blockchain

The traditional telemedicine systems mostly rely on outdated methods to store, maintain, and protect patients' data which can limit the collaboration opportunities among the healthcare participants and providers. This increases the system cost that can profoundly influence the effectiveness of a patient's treatment. Blockchain technology assures that the complete and trustworthy medical history of a patient can be maintained and tracked by the authorized users through immutable records of transactions and medical records [79–81,14]. However, the lack of awareness, immaturity of the technology, and unavailability of security and privacy standards prevent telehealth participants to unlock the full potential of blockchain technology [82]. Therefore, blockchain technology needs further research to develop standards and regulations for the widespread adoption of blockchain in telehealth and telemedicine. Moreover, the monetary incentives for participating organizations to make a shift towards blockchain technology should be researched.

4.2. Security vulnerabilities of smart contracts

Vulnerabilities and bugs in the smart contracts can significantly affect its normal behavior, resulting in tampering and disrupting the medical history of a patient [83,84]. For instance, through a reentrancy vulnerability attack [85], a smart contract that has exclusive privileges to communicate with another contract can either alter the EHR of a patient or it can retrieve funds from the wallet of a legitimate user [86]. The researchers have proposed several diagnostic tools, such as ZeppelinOS, SolCover, and Oyente. Such tools help to identify the vulnerable features of smart contracts to assist the developers to propose countermeasures against external threats [83,17]. However, the proposed solutions are inadequate to identify all types of vulnerabilities and bugs in a smart contract. Therefore, preventive measures should be taken to rigorously test smart contracts for potential vulnerabilities through diverse test cases using multiple tools prior to their deployment.

4.3. Large-sized health data and escalating transaction rate

Blockchain-enabled telemedicine and telehealth services require close coordination and collaboration among healthcare participants to maintain a consistent and up-to-date medical history of a patient to minimize medical diagnosis errors. Thus, telehealth services can generate an enormous amount of data that requires fast data processing to obtain insights from the health data [87]. However, in the current blockchain platforms, the large amount of healthcare data affects transaction fees and total waiting time of a transaction to be confirmed [88,89]. The Ethereum platform can handle up to twenty transactions per second [90]. Moreover, considering the high volume of transactions for telehealth services, the storage requirements of distributed ledger technology also increases. The incorporation of an additional edge or fog-based layer [91] in the existing frameworks for data preprocessing can help to minimize the transaction rate.

4.4. Interoperability support for cross-platform transactions

The patient health referral services demand to securely transact across the blockchain platforms from the health participants, such as physicians and patients. The interoperability support of blockchain platforms facilitates users to seamlessly communicate with each other without requiring intermediaries for transaction translation and forwarding [26]. For instance, an interoperability supported platform can assist the health practitioners to use Bitcoin tokens for business transactions on the Ethereum blockchain network. However, architecting interoperable blockchain platforms is challenging due to various issues, such as differences in supported languages and consensus protocols of the blockchain platforms [92,93]. Ideally, the interoperable platforms should be fast, secure, and fault-tolerant to shield the privacy of telehealth users.

5. Concluding remarks and recommendations

In this paper, we focused on leveraging blockchain technology for telehealth and telemedicine systems by discussing its key features to provide remote healthcare services in a manner that is decentralized, tamper-proof, traceable, immutable, auditable, and secure. We have explored and discussed the potential opportunities offered by blockchain technology for telehealth and telemedicine systems. We presented recent blockchain-based projects that have successfully assisted physicians to deliver healthcare services remotely. Finally, we identified and discussed several challenges that need further research to extend the capabilities of the existing blockchain-based systems to improve telehealth and telemedicine services. Our key findings followed by concluding remarks are stated below:

- Blockchain technology can play a vital role to successfully secure health data from adversaries using smart contracts by assuring strict compliance with the rules specified in patient consent forms.
- The continuous remote monitoring of patients requires an early settlement of healthcare transactions to minimize medical errors. Therefore, stimulating innovation in the existing blockchain technologies to minimize transaction processing time can greatly increase its suitability for the healthcare sector.
- The inherited provenance feature of blockchain technology can enable health professionals to accurately identify frauds related to physician educational credentials and medical testing kits commonly used for home-based diagnosis.
- The high data security and privacy make private and consortium blockchain-based systems highly suitable for digitization and automation of telehealth and telemedicine services.

6. Summary points

What was already known on the topic?

- Blockchain technology has become prevalent in financial industries.
- The COVID-19 pandemic has boosted the uptake of telehealth and telemedicine technology.
- Centralization is a key impediment in existing telehealth and telemedicine systems that poses the risk of single point of failure. Also, data in current telehealth and telemedicine systems are prone to a variety of external and internal data breaches compromising the reliability and availability of systems.

What did this study add?

- Blockchain-based solutions can bring major improvements in telehealth and telemedicine systems by alleviating their key limitations in terms of reliability, traceability, immutability, transparency, data provenance, audit, trust, and security.
- Several challenges are preventing existing telehealth and telemedicine systems to fully exploit the benefits of blockchain technology.

Conflict of interest

None.

Acknowledgments

This work was supported by the Khalifa University of Science and Technology under Award CIRA-2019-001 and RCII-2019-002- Research Center for Digital Supply Chain and Operations Management.

References

[1] A. Azim, M.N. Islam, P.E. Spranger, Blockchain and novel coronavirus: towards preventing Ltdc:COVID-19:rtdc and future pandemics, Iberoamerican J. Med. (2020) (Epub ahead of print).
[2] D. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey, TechRxiv (2020).
[3] V. Chamola, V. Hassija, V. Gupta, M. Guizani, A comprehensive review of the COVID-19 pandemic and the role of IoT, Drones, AI, Blockchain, and 5G in managing its impact, IEEE Access 8 (2020) 90225–90265.
[4] B. Siwicki, Telemedicine During COVID-19: Benefits, Limitations, Burdens, Adaptation. Available online at: https://www.healthcareitnews.com/news/telemedicine-during-covid-19-benefits-limitations-burdens-adaptation, May 2020 (accessed 16.05.20).
[5] J. Gorke, Telehealth Continues To Change The Face Of Healthcare Delivery – For The Better. Available online at: https://www.forbes.com/sites/jeffgorke/2019/09/24/telehealth-continues-to-change-the-face-of-healthcare-delivery-for-the-better/#58669cbf565f, April 2020 (accessed 27.04.20).

[6] J.E. Hollander, B.G. Carr, Virtually perfect? Telemedicine for COVID-19, N. Engl. J. Med. 382 (18) (2020) 1679–1681.
[7] Z. Jin, Y. Chen, Telemedicine in the cloud era: prospects and challenges, IEEE Pervas. Comput. 14 (1) (2015) 54–61.
[8] A.G. Ekeland, A. Bowes, S. Flottorp, Effectiveness of telemedicine: a systematic review of reviews, Int. J. Med. Inform. 79 (11) (2010) 736–771.
[9] A.F. da Conceição, F.S.C. da Silva, V. Rocha, A. Locoro, J.M. Barguil, Eletronic Health Records Using Blockchain Technology, arXiv preprint arXiv:1804.10078, 2018.
[10] Dubovitskaya A., Xu Z., Ryu S., Schumacher M., Wang F., Secure and trustable electronic medical records sharing using blockchain, 2017, American Medical Informatics Association, AMIA annual symposium proceedings, vol. 2017, 650.
[11] S. Chughtai, S. Ellahham, Telemedicine to revolutionize outpatient based healthcare. Available online at: http://thearabhospital.com/articles-eng/telemedicine-revolutionize-outpatient-based-healthcare/, May 2020 (accessed 31.05.20).
[12] S. Stowe, S. Harding, Telecare, telehealth and telemedicine, Eur. Geriatr. Med. 1 (3) (2010) 193–197.
[13] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics 9 (1) (2020) 94.
[14] B. Bennett, Using telehealth as a model for blockchain HIT adoption, Telehealth Med. Today 2 (4) (2017).
[15] A. Margheri, M. Masi, A. Miladi, V. Sassone, J. Rosenzweig, Decentralised provenance for healthcare data, Int. J. Med. Inform. (2020) 104197.
[16] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustain. Cities Soc. 39 (2018) 283–297.
[17] Y.-C. Hu, T.-T. Lee, D. Chatzopoulos, P. Hui, Analyzing smart contract interactions and contract level state consensus, Concurr. Comput. Pract. Exp. 32 (12) (2020) e5228.
[18] R. Kumar, R. Tripathi, Traceability of counterfeit medicine supply chain through blockchain. 11th International Conference on Communication Systems & Networks (COMSNETS), IEEE, Bengaluru, India, 2019, pp. 568–570.
[19] P. Kieseberg, J. Schantl, P. Frühwirt, E. Weippl, A. Holzinger, Witnesses for the doctor in the loop. International Conference on Brain Informatics and Health, Springer, Cham, 2015, pp. 369–378.
[20] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: challenges, advances and platforms, Fut. Gen. Comput. Syst. 105 (2020) 475–491.
[21] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences – a scoping review, Int. J. Med. Inform. 134 (2020) 104040.
[22] E. Chukwu, L. Garg, A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations, IEEE Access 8 (2020) 21196–21214.
[23] D.S.W. Ting, L. Carin, V. Dzau, T.Y. Wong, Digital technology and COVID-19, Nat. Med. 26 (4) (2020) 459–461.
[24] R. Vaishya, A. Haleem, A. Vaish, M. Javaid, Emerging technologies to combat COVID-19 pandemic, J. Clin. Exp. Hepatol. (2020).
[25] R.W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, M. Omar, Blockchain and COVID-19 pandemic: applications and challenges, TechRxiv (2020).
[26] K. Rabah, Challenges & opportunities for blockchain powered healthcare systems: a review, Mara Res. J. Med. Health Sci. 1 (1) (2017) 45–52.
[27] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.
[28] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surveys 53 (2) (2020) 1–27.
[29] S. Shubbar, Ultrasound Medical Imaging Systems Using Telemedicine and Blockchain for Remote Monitoring of Responses to Neoadjuvant Chemotherapy in Women's Breast Cancer: Concept and Implementation, Kent State University, 2017 (Ph.D. dissertation).
[30] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, Z. Wang, Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system, IEEE Access 7 (2019) 88012–88025.
[31] A. Abugabah, N. Nizam, A.A. Alzubi, Decentralized telemedicine framework for a smart healthcare ecosystem, IEEE Access 8 (2020) 166575–166588.
[32] K.A. Colón, Creating a patient-centered, global, decentralized health system: combining new payment and care delivery models with telemedicine, AI, and Blockchain technology, Blockchain in Healthcare Today 1 (2018), pp. 10-30953.
[33] T. Hewa, A. Braeken, M. Ylianttila, M. Liyanage, Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT, The 8th IEEE International Conference on Communications and Networking (IEEE ComNet') (2020).
[34] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018) 130.
[35] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: a systematic review, Healthcare 7 (2) (2019) 56. Multidisciplinary Digital Publishing Institute.
[36] T. McGhin, K.-K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: research challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 62–75.
[37] H.M. Hussien, S.M. Yasin, S. Udzir, A.A. Zaidan, B.B. Zaidan, A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction, J. Med. Syst. 43 (10) (2019) 320.
[38] I. Radanović, R. Likić, Opportunities for use of blockchain technology in medicine, Appl. Health Econ. Health Policy 16 (5) (2018) 583–590.
[39] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.
[40] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, A. Abd-Alrazaq, The benefits and threats of blockchain technology in healthcare: a scoping review, Int. J. Med. Inform. (2020) 104246.
[41] A. Tandon, A. Dhir, N. Islam, M. Mäntymäki, Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda, Comput. Ind. 122 (2020) 103290.
[42] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural. Comput. Appl. (2021), https://doi.org/10.1007/s00521-020-05519-w.
[43] E. Saweros, Y.-T. Song, Connecting heterogeneous electronic health record systems using tangle. International Conference on Ubiquitous Information Management and Communication, Springer, Phuket, Thailand, 2019, pp. 858–869.
[44] P. Genestier, S. Zouarhi, P. Limeux, D. Excoffier, A. Prola, S. Sandon, J.-M. Temerson, Blockchain for consent management in the ehealth environment: a nugget for privacy and security challenges, J. Int. Soc. Telemed. eHealth 5 (2017). GKR-e24.
[45] X. Zhang, S. Poslad, Z. Ma, Block-based access control for blockchain-based electronic medical records (EMRs) query in ehealth. IEEE Global Communications Conference (GLOBECOM), IEEE, Abu Dhabi, United Arab Emirates, 2018, pp. 1–7.
[46] X. Zhang, S. Poslad, Blockchain support for flexible queries with granular access control to electronic medical records (EMR). IEEE International Conference on Communications (ICC), IEEE, Kansas City, MO, USA, 2018, pp. 1–6.
[47] K. Mannaro, G. Baralla, A. Pinna, S. Ibba, A blockchain approach applied to a teledermatology platform in the Sardinian region (Italy), Information 9 (2) (2018) 44.
[48] R. Li, Multifunctional self-diagnostic device for in-home health-checkup, US Patent App. 10/904,818, June 2005.
[49] S.M. Weissman, K. Zellmer, N. Gill, D. Wham, Implementing a virtual health telemedicine program in a community setting, J. Genet. Counsel. 27 (2) (2018) 323–325.
[50] U.D. of Health, H. Services, et al., Personal Health Records and the HIPAA Privacy Rule, Washington, DC., 2008.
[51] M. Prokofieva, S.J. Miah, Blockchain in healthcare, Australas. J. Inf. Syst. 23 (2019).
[52] J.D. Halamka, G. Alterovitz, W.J. Buchanan, T. Cenaj, K.A. Clauson, V. Dhillon, F. D. Hudson, M.M. Mokhtari, D.A. Porto, A. Rutschman, et al., Top 10 blockchain predictions for the (near) future of healthcare, Blockchain Healthc. Today (2019).
[53] Medicalchain, White Paper, Medicalchain, 2018.
[54] H.S.Z. Kazmi, F. Nazeer, S. Mubarak, S. Hameed, A. Basharat, N. Javaid, Trusted remote patient monitoring using blockchain-based smart contracts. International Conference on Broadband and Wireless Computing, Communication and Applications, Springer, Antwerp, Belgium, 2019, pp. 765–776.
[55] M. Rehman, P.P. Jayaraman, C. Perera, The emergence of edge-centric distributed IoT analytics platforms. Internet of Things, Chapman and Hall/CRC, 2017, pp. 213–228.
[56] M.H. ur Rehman, E. Ahmed, I. Yaqoob, I.A.T. Hashem, M. Imran, S. Ahmad, Big data analytics in industrial IoT using a concentric computing model, IEEE Commun. Mag. 56 (2) (2018) 37–43.
[57] K. Salah, A. Alfalasi, M. Alfalasi, M. Alharmoudi, M. Alzaabi, A. Alzyeodi, R. Ahmad, IoT-enabled shipping container with environmental monitoring and location tracking, 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC) (2020) 1–6.
[58] M. Alblooshi, K. Salah, Y. Alhammadi, Blockchain-based ownership management for medical IoT (MIoT) devices. International Conference on Innovations in Information Technology (IIT), IEEE, Al Ain, United Arab Emirates, 2018, pp. 151–156.
[59] IHS, Telehealth and Pharma: Creating Opportunities for Remote Drug Delivery and Clinical Trials. Available online at: https://ihsmarkit.com/research-analysis/telehealth-pharma-creating-opportunities-for-remote-drug-delivery-and-clinical-trials.html, April 2020 (accessed 29.04.20).
[60] Y. El-Miedany, Telehealth and telemedicine: how the digital era is changing standard health care, Smart Homecare Technol. Telehealth 4 (2017) 43–51.
[61] M. Thakore, Transforming Healthcare: Blockchain Based Medical Prescription Tracking. Available online at: https://hackernoon.com/transforming-healthcare-blockchain-based-medical-prescription-tracking-58e7c4b59227, April 2020 (accessed 28.04.20).
[62] M. Raikwar, S. Mazumdar, S. Ruj, S.S. Gupta, A. Chattopadhyay, K.-Y. Lam, A blockchain framework for insurance processes. 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, Paris, France, 2018, pp. 1–4.
[63] C.K. Lee, Blockchain application with health token in medical & health industrials. 2nd International Conference on Social Science, Public Health and Education (SSPHE 2018), Atlantis Press, Sanya, China, 2019.
[64] P. Webster, The Telemedicine Referral Case Process. Available online at: https://telemedicine.arizona.edu/sites/, April 2020 (accessed 25.04.20).
[65] S. Heath, Patient Engagement Strategies for Post-Discharge Follow-Up Care. Available online at: https://patientengagementhit.com/features/, May 2020 (accessed 05.05.20).
[66] D. Srinivasan, Integrating Blockchain and Healthcare Through Patient Portals. Available online at: https://espeoblockchain.com/integrating-blockchain-and-healthcare-through-patient-portals/, May 2020 (accessed 05.05.20).

[67] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: challenges and future perspectives, Cryptography 3 (1) (2019) 3.
[68] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, E. Hossain, A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes, IEEE Access 8 (2020) 118433–118471.
[69] Medcredits: The Fastest Way to a Diagnosis, Anytime, Anywhere, White Paper, MedCredits, Inc., USA, 2018.
[70] J.M. Todaro, Overview of MedCredits. Available online at: http://medcredits.io/team/, May 2020 (accessed 06.05.20).
[71] L. Fuentes, Clinicappchain: a low-cost blockchain Hyperledger solution for healthcare, Blockchain and Applications: International Congress, vol. 1010 (2019) 36.
[72] R.M. Aileni, G. Suciu, IoMT: a blockchain perspective. Decentralised Internet of Things, Springer, 2020, pp. 199–215.
[73] V. Buterin, SchellingCoin: A Minimal-Trust Universal Data Feed. Available online at: https://blog.ethereum.org/, March 2014 (accessed 02.06.20).
[74] Healpoint, White Paper, Laboratory Information Systems, Los Angeles, 2018.
[75] B. Poly, HealPoint: Blockchain Based Platform for Healthcare Second Opinion. Available online at: https://angel.co/company/healpoint, May 2020 (accessed 12.05.20).
[76] My Health My Data, A New Paradigm In Healthcare Data Privacy And Security. Available online at: http://www.myhealthmydata.eu/, November 2020 (accessed 22.11.20).
[77] Robomed Network: Initial Coin Offering, White Paper, Robomed Network, Inc., Rusia, 2017.
[78] L. Hang, E. Choi, D.-H. Kim, A novel EMR integrity management based on a medical blockchain platform in hospital, Electronics 8 (4) (2019) 467.
[79] B. Bennett, Blockchain HIE overview: a framework for healthcare interoperability, Telehealth Med. Today 2 (3) (2017).
[80] M. Raskin, The Law and Legality of Smart Contracts, 2016.
[81] D. Hurley, Blockchain for patient and HCP data rights management: lessons from an enterprise install, Telehealth Med. Today (2018).
[82] A. Kolan, S. Tjoa, P. Kieseberg, Medical blockchains and privacy in Austria – technical and legal aspects, International Conference on Software Security and Assurance (ICSSA), Vienna, Austria (2020) 1–7.
[83] A. Mense, M. Flatscher, Security vulnerabilities in Ethereum smart contracts, Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services, Halifax, NS, Canada (2018) 375–380.
[84] u. Rehman, K. Salah, E. Damiani, D. Svetinovic, Trust in blockchain cryptocurrency ecosystem, IEEE Trans. Eng. Manage. 67 (4) (2020) 1196–1212.
[85] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, B. Roscoe, Reguard: finding reentrancy bugs in smart contracts. 40th International Conference on Software Engineering: Companion (ICSE-Companion), IEEE, Gothenburg, Sweden, 2018, pp. 65–68.
[86] H. Chen, M. Pendleton, L. Njilla, S. Xu, A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses, arXiv preprint arXiv:1908.04507, 2019.
[87] A.A. Mazlan, S.M. Daud, S.M. Sam, H. Abas, S.Z.A. Rasid, M.F. Yusof, Scalability challenges in healthcare blockchain system-a systematic review, IEEE Access 8 (2020) 23663–23673.
[88] R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: economics, technology, and governance, J. Econ. Perspect. 29 (2) (2015) 213–238.
[89] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, M. Maffei, Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability, NDSS, 2019.
[90] G. Wood, et al., Ethereum: a secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper 151 (2014) (2014) 1–32.
[91] M. Debe, K. Salah, M.H.U. Rehman, D. Svetinovic, IoT public Fog nodes reputation system: a decentralized solution using Ethereum blockchain, IEEE Access 7 (2019) 178082–178093.
[92] M. Herlihy, Atomic cross-chain Swaps, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing (2018) 245–254.
[93] M.H. Miraz, D.C. Donald, Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities, Ann. Emerg. Technol. Comput. 3 (2019).