Blockchain Based Secure, Efficient, and Scalable Platform for the Organ Donation Process of Healthcare Industry

Keyur Parmar, Vadlapudi Devanand Kumar, Neduri Leela Prasanth, Pranoppal, Kasa Charan Teja, Shriniwas Patil, and Kaushal A. Shah

Abstract Organ transplantation is one of the most effective medical procedures to save lives. An individual's organs can save up to nine lives. However, individuals refuse to donate organs because of lack of awareness and trust in the procedure, leading to the reduction in the number of organ donors. Individuals who wish to donate organs have to go through a complex administrative process, and sometimes these donated organs are managed by unauthorised individuals. To encourage individuals who wish to donate organs, we need a secure, efficient, and scalable platform. In this article, we present our perspective on the blockchain based organ donation management, in particular, for organ donation between organ donors and patients. The proposed platform uses the smart contract to automate the organ donation process and reduces the overall time of organ donation process. The proposed blockchain-based Organ Donation Platform (ODP) help patients in finding a matching donor efficiently. The ODP facilitates the process of organ donation by a decentralized network ensuring security, integrity, and transparency that eliminates the intermediaries. We comparatively evaluate the performance of the proposed ODP with the state-of-the-art literature. The proposed ODP is not only secure and scalable, but also efficient and reliable to find matching donor without revealing their identities.

Keywords Blockchain · Smart contract · Ethereum · Security · Public key cryptography · Organ donation · Healthcare · Transparency

1 Introduction

Organ transplantation is a medical process to remove a non-functional organ from the patient and then surgically replace it with a new organ taken from a healthy person.

K. Parmar (✉) · V. D. Kumar · N. L. Prasanth · Pranoppal · K. C. Teja · S. Patil
S. V. National Institute of Technology, Surat, India
e-mail: keyur@coed.svnit.ac.in

K. A. Shah
Pandit Deendayal Energy University, Gandhinagar, India

J. Hemanth et al. (eds.), *Intelligent Cyber Physical Systems and Internet of Things*,
Engineering Cyber-Physical Systems and Critical Infrastructures 3,
https://doi.org/10.1007/978-3-031-18497-0_13

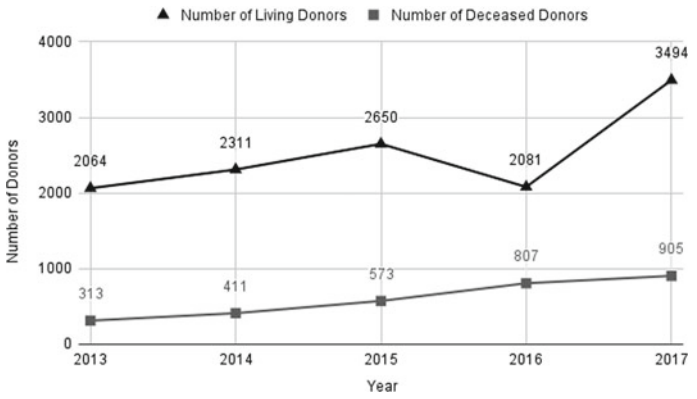

Fig. 1 Number of living and deceased organ donations from 2013–2017 [1]

Organ transplantation is one of the successful treatments for patients. Patients in need of organs often die due to a lack of information about donors in time.

Organ donation process is categorised into living organ donation and deceased organ donation. In living organ donation, organs are retrieved from a healthy living person and transplanted into patients. In deceased organ donation, the functioning organs are retrieved from a deceased person and transplanted into patients. The donation trend for living donors and deceased donors between the years 2013–2017 is shown in Fig. 1. The trend of donating organs is more in the case of living donors. Nevertheless, due to a lack of public awareness, organ donations in the case of deceased donors is less compared to living donors. The lack of public awareness results in the acute shortage of organs that otherwise can be used to save lives. Therefore, there is need to create awareness about the organ donation.

The Government of India organises organ donation programs such as National Organ Tissue Transplant Organization (NOTTO) [2] and Regional Organ Tissue Transplant Organization (ROTTO) [2]. Although the Government of India organises organ donation programs, individuals hesitate to donate organs due to the lack awareness about the of current organ donation programmes. Therefore, there is a need of transparent, secure, and a scalable platform for the organ donation process.

In organ donation, the challenge is to find a matching donor. The number of patients die because of an unavailability of a donor [1, 3]. Another challenge is the lengthy paperwork that delays the whole process of organ transplant. A non-relative organ donor has to go through a number of procedures, such as, getting consent from the state government or local hospital. Moreover, there is a lack of infrastructure for organ donation which makes the whole process complex even if the donors are available.

The above challenges are tackled by creating a decentralised system for the organ donation process. The proposed ODP will help individuals who wish to donate their organs and patients who are seeking organs.

In this article, we use the blockchain, a distributed ledger to store the data and to provide tamper resistance. Blockchain technology also guarantees security and transparency [4]. Therefore, a number of individuals will join the ODP who wish to donate organs. The proposed work uses the smart contract [5–7] with Ethereum Network [8, 9] to make the organ donation process automatic and fast. The smart contract reduces the time required to complete due formalities.

The proposed work ensures transparency between donors and recipients (patients) and helps patients in finding the vital organ. The proposed work solves the challenge of finding organ donors and provides a choice for patients to choose organ donors. The ODP is trustworthy because all records are maintained using blockchain. The ODP eliminates the illegal smuggling of organs by restricting illegal access to ODP. The ODP will help to save lives by connecting the suitable donor to the right patient at the right time.

In this article, our contributions are as follows:

1. We present a comprehensive literature review to identify the challenges in the conventional organ donation process.
2. We comparatively evaluate the strengths and weaknesses of the state-of-the-art proposals in the domain of organ donation.
3. We propose a blockchain based platform to facilitate patients to find a matching donor. The proposed blockchain based platform helps in mitigating the issues found in conventional organ donation process.
4. We implement the proposed blockchain based platform to demonstrate the working of the proposed ODP.
5. We evaluate the security and performance of the proposed blockchain based platform to highlight its strengths and weaknesses.

The rest of the article is organized as follows: In Sect. 2, we discuss the related work. In Sect. 3, we discuss the preliminaries related to the proposed system. Section 4 presents the proposed ODP. Section 5 presents the experimental implementation of the proposed ODP. In Sect. 6, we conclude the article by emphasizing our contribution.

2 Related Work

Organ donation is a well-researched topic that provides patients and organ donors a common platform. Chen et al. [10] identified an issue in a rule-based strategy of prioritising kidney donation in kidney donation programs where exchanges are initiated by Altruistic Donors (ADs). Authors developed a software-based decision support system. In addition, authors considered and compared two graph-based organ allocation algorithms, namely, MEU-Parallel and MEU-Sequential [10], to find the correct match. However, the authors work does not emphasize more on other kidney-allocation algorithms.

Prajapati et al. [11] implemented an online system to manage blood and organ transplant. The online system helps in searching for blood in case of emergency and in maintaining the records of blood and organ donors.

Kadam et al. [12] discuss the drawbacks of manual blood donation and the organ donation process. Authors proposed an electronic donation system that manages the records of blood and organ donors and enables patients to monitor and find the correct donor.

Rastogi and Tiwari [13] implemented an online web-based system for organ donation and management. An administrator manages the system. The administrator holds the rights and privileges to print the organs list. However, the system depends on the administrator which makes the system centralised and vulnerable to insider threats. Similarly, Ali et al. [14] implemented a web application with the support of a mobile application for a blood donation management system.

The existing systems manage organ donations, but these systems require a connection between organ donors, patients, and central trusted third-parties. The system that uses the central trusted third-party such as hospital agents or government agents is vulnerable to insider and outsider threats and discloses the organ donor's identity. If anonymity is not provided to organ donors and patients, the central third-party can contact patients to prioritise the patient to receive organs by asking for extra money.

Dajim et al. [15] implemented a decentralised organ donation application. Authors used blockchain technology [16, 17] to distribute the information. The use of blockchain makes the system secure and tamper-proof. However, anonymity is not provided for organ donors and patients. Rajan et al. [18] proposed a system for organ donation and transplantation using blockchain technology. Authors used smart contracts to reduce the cost of transactions. However, the system does not allow anyone to check the availability of organs. The existing systems fail to provide security, transparency, a tamper-resistance, and do not protect patients from insider and outsider adversaries.

Lakshminarayanan et al. [19] identified the dynamic update issue in blood management system. The authors proposed and implemented blockchain-based blood management system using hyperledger fabric framework to track the blood trail. The challenge of tracing thee blood trail is modelled as a supply-chain management issue. The proposed system provides transparency in blood donation process. However, the use of hyperledger fabric framework makes system permissioned. Therefore, no one can access system to get blood donation related information without getting permission from the network. Similarly, Quynh et al. [20] proposed blockchain-based innovative system to manage blood information. Authors proposed the system based on the architecture of hyperledger fabric with support of supply and demand of blood.

Hawashin et al. [21] proposed a private Ethereum blockchain-based solution to enable organ donation and transplantation management. The use of private blockchain makes system decentralized, secure, traceable, auditable, private, and trustworthy. However, the private blockchain makes the organ donation and transplantation not visible to people outside the organization.

3 Preliminaries

In this section, we briefly discuss the Blockchain [16, 17], Smart Contracts [5–7], and Ethereum [22].

3.1 Blockchain

"A blockchain is a continuously growing list of records called blocks, which are linked and secured using cryptography [23]." The idea to timestamp [24] all transactions is to maintain the order of transactions. In a blockchain, the new blocks are appended securely using cryptographic hash functions.

One of the fundamental features of the blockchain network is that it has no central authority. The blockchain network is shared among all the nodes and each node has a ledger or its own database, and the same copy is maintained by all nodes of the network. Therefore, any data present in the blockchain is secure, transparent, and tamper-proof [25].

3.2 Ethereum

Ethereum [22] is a stable platform that can be used to codify and exchanges based on contracts. Ethereum is an open-source, blockchain-based platform for creating and running safe smart contracts and distributed applications (DApps) [26].

3.2.1 Infura

Infura provides the tools and infrastructure with stable access to Ethere-um and InterPlanetary File System (IPFS). Infura enables developers to test and deploy its scaled blockchain applications.

3.2.2 Metamask

Metamask is a browser extension that enables users to create decentralised applications (DApps) [26] without using the Ethereum network as an Ethereum node. Metamask is also serves as wallet that stores the Ethers (cryptocurrency) and allows users to send and receive Ethers via a decentralised application (DApp) [26]. Metamask allows us to link Infura, another Ethereum node, and runs smart contracts on the node.

3.2.3 Web3.js

Web3.js is a collection of libraries that enables an HTTP or IPC connection to communicate with a local or remote Ethereum node. The Ethereum blockchain is accessed via the web3 JavaScript library. Web3.js can perform operations such as accessing user accounts, submitting transactions, and communicating with smart contracts. We use Web3 Truffle-HDWallet-provider. The Truffle-HDWallet-provider provides a convenient network to link Ethereum thro-ugh infura.io. For example, the HDWallet provider adds some truffle-required features like event filtering and transaction signing that are unavailable with Infura.

3.3 Smart Contracts

Smart contracts [5–7] are self-contained programmes that run on the blockchain network. Smart contracts are programmed to perform actions on blockchain as per the business logic and requirements [27]. The smart contract executes functions if certain code and business logic conditions are met or not met.

4 The Proposed Organ Donation Platform Using Blockchain Technology

We propose an efficient, secure and scalable platform to facilitate donors and patients to manage organ donation. The platform using which both donor and patient will be able to manage all the operations such as login and signup. Donors can provide the required information of the organs which he or she wish to donate, patients can also find the donors by searching for the required organ.

We present the whole process of the ODP as shown in Fig. 2. There are two entities in the system, namely, a donor and a recipient (patient). The entities are connected to

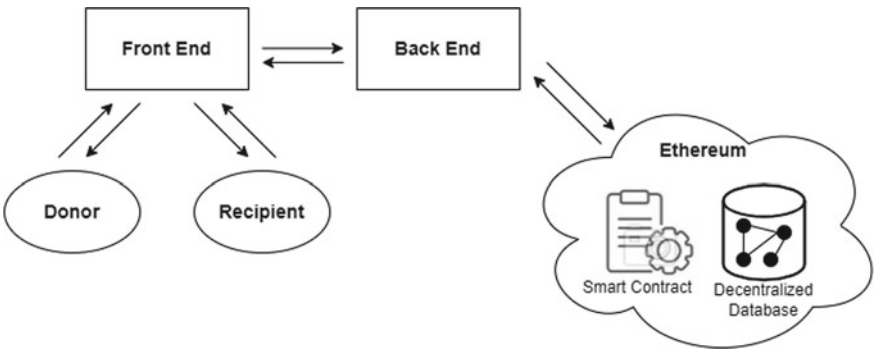

Fig. 2 Proposed organ donation platform using smart contracts with ethereum

the platform through front-end service where they can easily perform the operations such as login, signup, and search for organs. The back-end service executes the required operations requested through the front end, and all records are appended to the blockchain. The use of smart contracts [5–7] help in automating the organ donation process.

The algorithm is used to find the available donors for the required organs. The proposed algorithm to retrieve all donors with the same organ as recipient is as shown in Algorithm 1.

Algorithm 1 Algorithm to retrieve all donors with the same organ as recipient

```
Result: Donor details
Query database for all donors where recipient.organ= donor.organ;
if results.length >0 then
    Show available donors;
    From donors list select a donor based on city;
    View donor details to contact;
else
    Print("No donors available");
end
```

Next, we present another algorithm to find the correct donor for the patient to receive an organ and make the process more efficient so the patient can perform the transplantation in the available time. The algorithm to match donor and recipient based on location is presented in Algorithm 2.

Algorithm 2 Algorithm to match donor and recipient based on location

```
Result: Match donor and recipient so that they can contact each other
Function matchDonorRecipient(address donorId, address recipientId):
    public payable
    if match found for both donor and recipient then
        retrieve donor info using donor address;
        retrieve recipient info using recipient address;
    end
End Function
```

The proposed ODP provides transparency by adding donors on the blockchain that makes all the donors visible to anyone on the blockchain network with cryptoghraphically generated keys. The cryptographically generated keys are used to protect the privacy of the donors. The algorithm to add a donor to the blockchain is shown in Algorithm 3.

Algorithm 3 Algorithm to add donors to the blockchain

Result: Add Donor to the Blockchain
Each donor has the following attributes
$donorId, hash, organ, blood\_group, matchfound, exist$;
Validate donor credentials;
Call function Add_donor;
Function `Add_donor` $(donorID, memory\ hash, organ\_name, bgroup, factor)$ **:**
  public checkdonorexist(donorID):
    if $True$ **then**
      $Donors[donorID] \longleftarrow donor(donorID, hash, bgroup, organ\_name, false, true)\ donor\ array.push(donorID)$;
  end
End Function

5 Results and Analysis

In this section, we discuss the implementation of the proposed ODP. We also discuss each functionality implemented in detail. The ODP consist of three layers as follows:

1. HTML, CSS, Javascript is used as a front end user interface for the organ donor and recipient to provide all the functionalities.
2. A node.js server is used to interact with the Ethereum blockchain network and provides the required data to Javascript Frontend.
3. All the respective organ donor and recipient data are stored in a decentralised network using Ethereum.

The recipient logs in with the public key provided after registering. The credentials are to be provided by the user while signing up. The details of both donors and recipients are available in the blockchain ledger. Therefore, the proposed ODP can verify whether it is an existing user or not, if yes, then the system redirects the same to the login page otherwise, on the signup page.

There are two separate portals for both donors and patients while registering on the proposed platform. Organ donors will be asked for his or her basic information and also the list of organs donors wish to donate after filling out a consent form.

A patient will be able to register with his or her basic information and the organ that is required by the patient along with his contact information as a consent form.

Patients verifies the matched donor in the dashboard provided when patients log in, and when there are no matches, the dashboard shows the message, “no matches found” and suggests the active donor’s list as shown in Figs. 3 and 4, respectively.

In order to verify the security strength of the proposed platform, we compare the proposed platform with similar proposals in the domain of organ donation. The comparison is given in Table 1. The comparison is based on the well-known security services provided by existing proposals for organ donation. Based on the comparison of different organ donation proposals, in our opinion, the existing proposals only provides a few security services. However, in the proposed ODP, the confidentiality is achieved using PKC [28], the integrity of an information is verified by

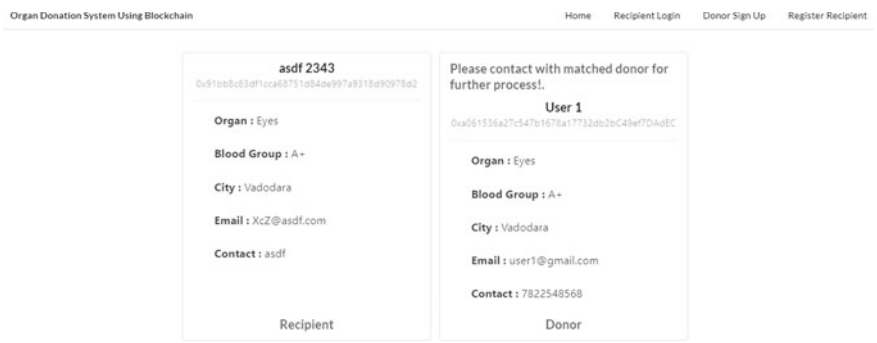

Fig. 3 Dashboard when donor is matched with recipient

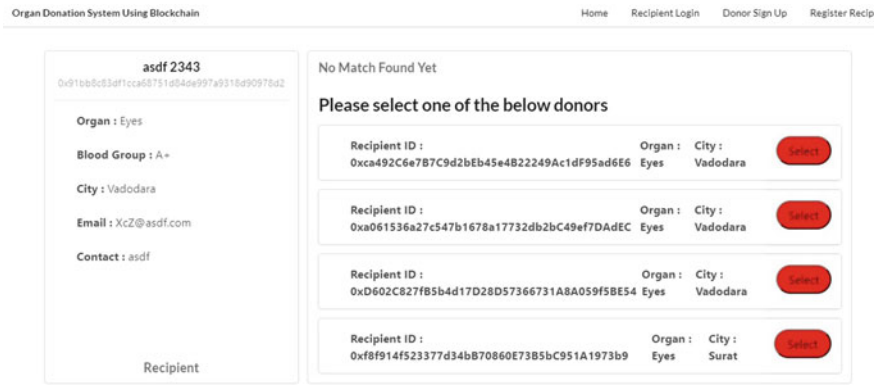

Fig. 4 Dashboard when no donor is matched with recipient

Table 1 Comparison of different organ donation systems

Authors	A	B	C	D	E	F	G	H
Chen et al. [10]	×	×	×	×	×	×	✓	✓
Prajapati et al. [11]	✓	×	×	×	×	×	×	×
Kadam et al. [12]	×	×	×	×	✓	×	×	✓
Rastogi and Tiwari [13]	×	×	×	×	✓	×	×	✓
Ali et al. [14]	×	×	×	×	✓	×	×	×
Dajim et al. [15]	×	×	✓	✓	×	×	×	✓
Ranjan et al. [18]	×	✓	✓	✓	×	✓	×	✓
Proposed Scheme	✓	✓	✓	✓	✓	✓	✓	✓

A awareness, *B* confidentiality and privacy, *C* decentralization, *D* tamper-resistance, *E* transparent, *F* automation, *G* algorithms to find match, *H* eliminate trusted third-party such as organ banks

comparing message digest of the information received along with encrypted information and with message digest of decrypted information. Privacy is achieved using an unique cryptographically generated key and it is unrelated to the identity of the users. Decentralization, tamper-resistance, and transparency are provided using blockchain technology [16, 17]. The protection from insider and outsider adversaries is achieved using timestamp. The platform is automated using smart contracts [5–7].

6 Conclusions and Future Works

In this article, we propose a platform for organ donation using blockchain technology. To protect organ donors and patients from adversaries, we need a platform that provides transparency in the organ donation system. The ODP uses blockchain technology to make the central trusted third-party, e.g. hospital agent or government agent, more transparent and accountable while managing organ donation. The ODP is trustworthy and significantly reliable. In addition, the ODP protects organ donors and patients from insider and outsider adversaries. As a future work, there is a possibility to use the optimised algorithm that supports multiple cities and hospitals as an authority to verify the donors and patients.

Acknowledgements This research was a part of the project "Design and Analysis of Secure and Efficient Smart Contracts Using Blockchain Technology". It was partially supported by the SEED Money/Research Grant of the author, Dr. Keyur Parmar, Department of Computer Science and Engineering, S. V. National Institute of Technology (NIT), Surat, India.

References

1. Ahammed Mekkodathil MA, Sathian B, Rajesh E, Kumar RN, Simkhada P, van Teijlingen E (2019) Current scenario of organ donation and transplantation in Kerala India. Nepal J Epidemiol 9(2):759. https://doi.org/10.3126/nje.v9i2.24679
2. National organ tissue transplant organization. https://notto.gov.in/download-forms.htm. Accessed 03 Apr 2022
3. Nallusamy S et al (2018) Organ donation-current Indian scenario. J Pract Cardiovasc Sci 4(3):177–177. https://doi.org/10.4103/jpcs.jpcs_59_18
4. Abhishek B, Panjanathan R, Sarobin VR, Raja BE, Narendra M (2022) Data security in e-health monitoring system. Mater Today Proc 62:4620–4628. http://orcid.org/10.1016/j.matpr.2022.03.079
5. Szabo N (1997) Formalizing and securing relationships on public networks. First Monday 2(9). https://doi.org/10.5210/fm.v2i9.548
6. Szabo N (1994) Smart contracts
7. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY (2019) Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst 49(11):2266–2277. https://doi.org/10.1109/TSMC.2019.2895123
8. Buterin V (2022) Ethereum: a next-generation smart contract and decentralized application platform. https://ethereum.github.io/yellowpaper/paper.pdf. Accessed 30 Apr 2022

9. Wood G et al (2014) Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap 151:1–34
10. Chen Y, Li Y, Kalbfleisch JD, Zhou Y, Leichtman A, Song PXK (2012) Graph-based optimization algorithm and software on kidney exchanges. Trans Biomed Eng 59(7):1985–1991. https://doi.org/10.1109/TBME.2012.2195663
11. Prajapati Mayur, Dungar Bhati YSHJ (2017) Online blood and organ transplant management system. Int J Eng Sci Res Technol 6(3):17–21. https://doi.org/10.5281/zenodo.266682
12. Nikhil Kadam N, Akshay Kaware VG (2020) Blood and organ donation system. Int J Sci Res Eng Dev 3(2):44–48
13. Rastogi S, Tiwari S (2019) Online organ donation management system. Int J Sci Res Eng Dev 5(10):445–448
14. Ali A, Jahan I, Islam A, Parvez S (2015) Blood donation management system. Am J Eng Res 4(6):123–136
15. Dajim LA, Al-Farras SA, Al-Shahrani BS, Al-Zuraib, AA, Merlin Mathew R (2019) Organ donation decentralized application using blockchain technology. In: Proceedings of the international conference on computer applications information security (ICCAIS), Riyadh, Saudi Arabia. IEEE, pp 1–4. https://doi.org/10.1109/CAIS.2019.8769459
16. Di Pierro M (2017) What is the blockchain? Comput Sci Eng 19(5):92–95. https://doi.org/10.1109/MCSE.2017.3421554
17. Nofer M, Gomber P, Hinz O, Schiereck D (2017) Blockchain. Bus Inf Syst Eng 59(3):183–187. https://doi.org/10.1007/s12599-017-0467-3
18. Ranjan P, Srivastava S, Gupta V, Tapaswi S, Kumar N (2019) Decentralised and distributed system for organ/tissue donation and transplantation. In: Proceedings of the conference on information and communication technology, Allahabad, India. IEEE, pp 1–6. https://doi.org/10.1109/CICT48419.2019.9066225
19. Lakshminarayanan S, Kumar P, Dhanya N (2020) Implementation of blockchain-based blood donation framework. In: Proceedings of ICCIDS: international conference on computational intelligence in data science, Chennai, India. Computational intelligence in data science. Springer, pp 276–290. https://doi.org/10.1007/978-3-030-63467-4_22
20. Quynh NTT, Son HX, Le TH, Huy HND, Vo KH, Luong HH, Tuan KNH, Anh TD, Duong-Trung N et al (2021) Toward a design of blood donation management by blockchain technologies. In: Proceedings of ICCSA: international conference on computational science and its applications. Lecture notes in computer science. Springer, Cagliari, Italy, pp 78–90. https://doi.org/10.1007/978-3-030-87010-2_6
21. Hawashin D, Jayaraman R, Salah K, Yaqoob I, Simsekler MCE, Ellahham S (2022) Blockchain-based management for organ donation and transplantation. IEEE Access 10:59013–59025. https://doi.org/10.1109/ACCESS.2022.3180008
22. Buterin V (2022) On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 28 Apr 2022
23. Vos J (2017) Blockchain and land administration: a happy marriage? Eur Property Law J 6(3):293–295. https://doi.org/10.1515/eplj-2017-0018
24. Haber S, Stornetta WS (1990) How to time-stamp a digital document. In: Proceedings of CRYPTO 90: advances in cryptology, conference on the theory and application of cryptography, Santa Barbara, USA. vol 537. Lecture notes in computer science. Springer, pp 437–455. https://doi.org/10.1007/3-540-38424-3_32
25. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decentralized Bus Rev
26. Metcalfe W et al (2020) Ethereum, smart contracts, dapps. Blockchain Crypt Currency 77. https://doi.org/10.1007/978-981-15-3376-1_5
27. Bashir I (2018) Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained, 2nd edn. Packt Publishing Ltd, ISBN: 978-1-78883-904-4
28. Al-Riyami SS, Paterson KG (2003) Certificateless public key cryptography. In: Proceddings of ASIACRYPT: advances in cryptology, international conference on the theory and application of cryptology and information security, Taipei, Taiwan. vol 2894. Springer, pp 452–473. https://doi.org/10.1007/978-3-540-40061-5_29