Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Analysis of Revocation Mechanisms for Blockchain Applications and a Proposed Model Based in Self-Sovereign Identity

Fernando Richter Vidal*

*Corresponding Author, MSc., Faculty of Science and Technology, University of Fernando Pessoa – Praça de 9 de Abril 349, 4249-004 Porto, Portugal. E-mail: 37705@ufp.edu.pt

Feliz Gouveia

Full Professor, Ph.D., Faculty of Science and Technology, University of Fernando Pessoa – Praça de 9 de Abril 349, 4249-004 Porto, Portugal. E-mail: fribeiro@ufp.edu.pt

Christophe Soares

Assistant Professor, Ph.D., Faculty of Science and Technology, University of Fernando Pessoa – Praça de 9 de Abril 349, 4249-004 Porto, Portugal. E-mail: csoares@ufp.edu.pt

Abstract

The blockchain's immutability has allowed previously centralized operations to operate in a new way. The possibility of applications having a new architecture is given thanks to the innovative properties of the technology, which brought alternative control designs for distributed systems and allowed applications to work without the need for a central controlling point. The expansion of blockchain to other areas beyond cryptocurrencies has shown the need for applications to implement solutions to deal with corrective operations. Blockchain 3.0 applications bring new solutions for business needs. However, as opposed to immutability, the revoking functionality is much more complex to be implemented in this type of architecture, but paramount to applications resilience, allowing faulty or invalid information to be revoked, ensuring thus that the blockchain can still be trusted. This work assesses and discusses revocation mechanisms to contribute to the technical feasibility of several applications, which require corrective operations. We present a model in the academic area, which can be replicated for other types of systems in other areas.

Keywords: Blockchain; Blockchain Revocation; Blockchain Applications; Self-Sovereign Identity; Decentralized Identifiers.

Journal of Information Technology Management, 2022, Special Issue, pp. 192-210.
Published by University of Tehran, Faculty of Management
doi: https://doi.org/10.22059/jitm.2022.87848
Article Type: Research Paper

Received: 30 July 2021
Received in revised form: 30 October 2021
Accepted: 30 November 2021
Published online: 26 June, 2022

Introduction

In 2009 with the emergence of the Bitcoin application (Nakamoto, 2008), the world became aware of the blockchain, a disruptive technology capable of offering several properties, such as immutability, privacy, reliability, and security. Although distributed systems are commonly used and well understood, the blockchain proposed mechanisms for applications to operate in a decentralized manner, without a single point of failure, forming a new type of application, the Decentralized Autonomous Organization (DAOs). Companies created under this new model have their business supported by algorithms, and often the code represents all the company's assets (Diedrich, 2016).

As Tapscott and Tapscott (2016) noted: "It is not the Bitcoin, and its speculative assets, that should interest you". The blockchain has been applied in several other areas (Drosatos & Kaldoudi, 2019) (Tse et al., 2017) (Goranovic et al., 2017), which confirms the technology's potential in applications beyond cryptocurrencies. However, the use of blockchain in different types of applications has shown that a revocation functionality needs to be worked on. Contrary to the main characteristic of the blockchain (e.g., immutability), a revocation operation can be a very complex and costly task in this type of system. Although some initiatives (Grigoriev & Shpilrain, 2021) (Ateniese et al., 2017)(Florian et al., 2019) allow blockchain redacting or erasing data, these solutions are not compatible with the current blockchain technology. We call the blockchain operation that cancels or reverses a transaction "revocation" because the blockchain data cannot be erased.

The Bitcoin and other cryptocurrencies were not based on the idea of canceling an operation, on the contrary, the idea was to offer a structure that would not allow changes that had already been confirmed by the network. In that way, the blockchain infrastructure is designed to not be modified. If a correction is to be made to previously stored information, it cannot be performed.

The figure 1 illustrates this statement. The image shows in a timeline changes that occurred in the Bitcoin and Ethereum networks. In the case of Bitcoin, the programmers attempt to increase the block size from 1MB to 8MB, resulted in the creation of a new network, Bitcoin Cash (Javarone & Wright, 2018). Another hard fork example occurred in October 2017, when Bitcoin Gold was created. The change consisted of modifying the current consensus mechanism Proof of Work (PoW), to work more lightly, with less processing needs (Hanke, 2016).

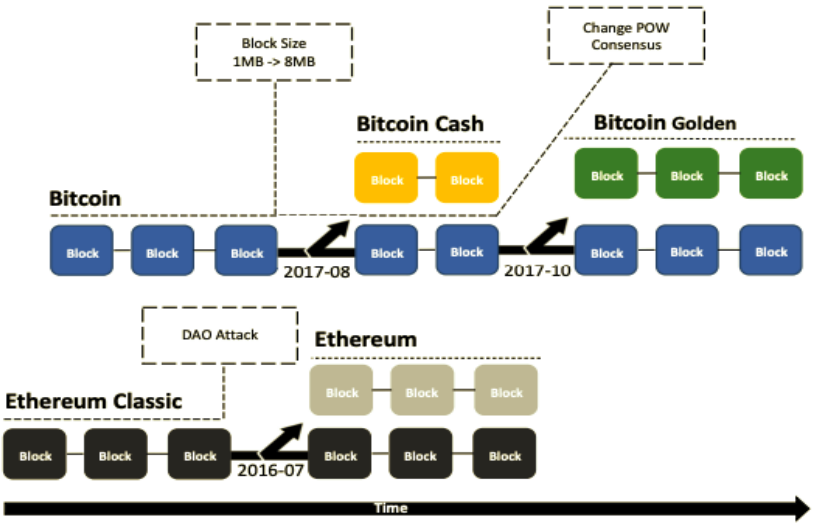

Figure 1 Blockchain Forks

As can also be seen in figure 1, a big change occurred on Ethereum. In 2016 the DAO application, which stored thousands of dollars worth of currency assets, suffered an attack and had about 50 million dollars stolen (Siegel, 2016). Faced with the impossibility of revoking such operations, even knowing they are fraudulent, the developers decided to fork the network, creating a new cryptocurrency, thus isolating the stolen operations on the old network.

These facts show the difficulty of building a solution capable of allowing revocation operations on an immutable and complex environment. Besides, not all blockchains work using the same resources, which makes the design of a compatible solution for all networks even a harder task. The community classifies blockchain applications into three categories, 1.0, 2.0, and 3.0. Categories 1.0 and 2.0 are related to cryptocurrencies or financial applications. The third classification is more extensive, being used in another kind of applications (di Francesco Maesa & Mori, 2020).

Although these examples show the big challenge to revoke credits in applications 1.0 and 2.0, in this paper we present a revocation model that supports several applications 3.0 that would benefit from the proposed functionality, without changing the existing blockchain system credit. The model we present approaches the revocation problem by creating a reverse link and a data revocation scheme.

Our experiments were related to the education area (i.e., issuing, sharing, and revoking academic certificates), however we observed similarities with other kinds of applications. These could benefit reusing the same model and approach. For instance, in the supply chain area, the contracts management can be improved, allowing the transfer of ownership safely. In healthcare area, families can take control of their records member, avoiding that sensitive

data being revealed. In the financial area, invoices could be revoked by a legal entity (i.e., in case it was the private key stolen).

This paper is organized as follows: the next section presents an overview of the concept of revocation; then, the existing approaches that address revocation are shown; after, we demonstrate our model; and finally, the conclusions of the paper are presented.

Revocation Background

Revocation is a term used in the legal field, which means ending the validity of a rule (Sgarbi, 2014). It is commonly used in digital certificates' life cycle. After all, it marks the end of life of the digital object because it expired or was compromised, and at the same time keeps the proof of its existence alive (Vigil et al., 2015). The same term is applied to the blockchain system due to the nature of these networks that consist of preserving records permanently.

As soon as the digital certificates based on Public Key Infrastructure (PKI) emerged, the need for dealing with the revocation issue was noticed, in a way that a good solution to the problem would be crucial for the widespread acceptance of the technology. The responsibility for this task was up to the Certificate Authorities (CA), which needed to provide a reliable revocation service, and to publish a suitable privacy policy (Jain, 2002).

Several mechanisms for revocation were proposed, such as Certificate Revocation List (CRL), Certificate Revocation System (CRS), Certificate Revocation Tree (CRT), On-line Certificate Status Protocol (OCSP) and Certificate Space Partitioning With Renewals (CSPR) (Walleck et al., 2008)(Goyal, 2007), in which the CRL and OCSP (Q. Wang et al., 2020) methods stood out. The CRL method consists of creating a kind of blacklist, built based on the scheme definition which is signed by a CA, and published periodically. In the list, the certificates are identified by their serial numbers and attached to a timestamp to control their validity. The OCSP method was developed by Internet Engineering Task Force (IETF) and consists of a protocol used to identify the validate status of a certificate. It is a client-server structure.

As in the PKI structure, the revocation is also an important matter which contributes to the expansion of the blockchain networks applications. However, the solution is much more difficult to be built because a CA that, for example, controls a list or defines a server similar to the OCSP format, can not be considered. This is because the most important benefits offered by the blockchain network would be lost (e.g., decentralization). The Massachusetts Institute of Technology (MIT) tried to implement in its Blockcert application a revocation approach based on CRL, but had, as a result, a centralized solution, which compromised one of the main benefits offered by the blockchain, self-sovereignty (Rujia & Galind, 2017) (Santos & Duffy, 2019) (F. Vidal et al., 2019) (F. R. Vidal et al., 2020b) (San et al., 2020). Because of that, the Blockcerts community has been discussing the matter in an attempt to find an alternative approach to the problem (Ronning & Chung, 2019).

Given this brief comparative analysis between the digital certificates revocation and blockchain registrations, it is clear that new approaches need to be explored since the revocation solutions offered by PKI do not meet the requirements of the blockchain. One approach to this revocation problem in blockchain systems, for example, could be the use of multi-signatures.

This technique is known in the world of public-key cryptography, which allows several parties to digitally sign a combined message, using their private keys (Gilboa, 1999). The concept is commonly used in cryptocurrencies (Zhou et al., 2016), using the expression M-to-N, where M represents the minimum number of signers and N the maximum number of keys involved. The blockchain application EduCTX uses this multi-signature feature to control an entire ecosystem of universities, which vote among themselves to revoke the participation of a member of the (Turkanović et al., 2018) network.

In the next section, some of the approaches to the revocation problem in blockchains are presented.

State of the art

The following describes some of the works that proposed specific revocation mechanisms for the blockchain technology in different applications. First, some works related to the secure communication area on the internet are presented, then approaches in Internet of Thing (IoT), and finally solutions for the academic area.

CertLedger

CertLedger (Kubilay et al., 2018) is a type of PKI solution which uses blockchain technology to remove the dependency of the CAs over the Transport Layer Security (TLS) certificates (Dierks & Rescorla, 2008) (A. Freier, P. Karlton, 2011), used to create a secure communication of a channel. Its functionality is inspired by the Google Certificate Transparency (CT) solution (Laurie et al., 2013), in which a log mechanism using Merkle Hash Tree (MHT) is implemented, allowing batch verification of certificates. The benefit of the Certledger approach in comparison to the Google solution is in the decentralized distribution of these logs. Taking as an example the Bitcoin, a 51% attack type, which would be able to give total control of the network, would be extremely expensive and could cost even 500K dollars per hour of processing (Saad et al., 2019).

The CertLedger publication also presents a systemic view of several mechanisms based on PKI, describing how each solution tries to decentralize the CA functions, such as the certificate revocation. Unlike the approaches evidenced by the works mentioned (Eckersley, 2012)(Laurie et al., 2013)(Ryan, 2014)(Kim et al., 2013), CertLedger applies the use of blockchain technology. As a result, there is the elimination of Man-in-The-Middle (MITM) attacks, and also the gain in transparency in the revocation processes.

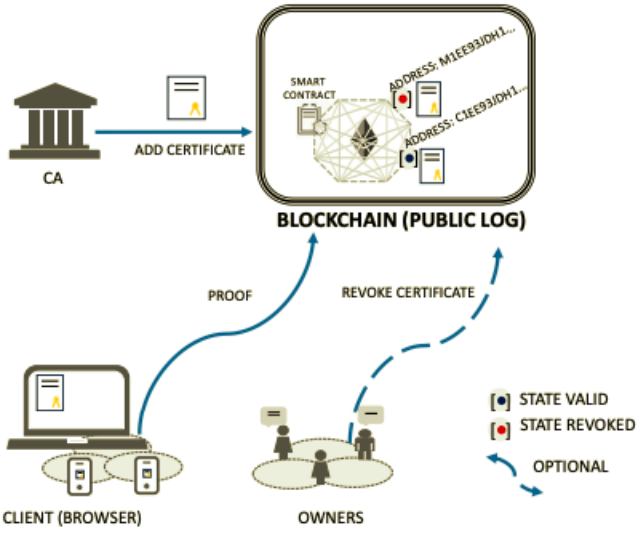

Figure 2 Certledger Architecture (Kubilay et al., 2018)

As shown in figure 2 digital certificates are represented by objects and their status. Each object has its unique blockchain address. The states of these objects are controlled by a smart contract and are stored on Ethereum, a blockchain network. Since TLS certificates are stored in the blockchain the browser verification can be executed independently. The query of the state in the object's address can return a status of valid or revoked. Certificate owners also gain autonomy because they can revoke the certificate without relying on CA.

Blockchain Revocation Transparency (RT)

The work proposed by Z. Wang et al. (2019) consists of a solution that uses blockchain technology, but keeps the compatibility with the X.509 standard for certificates. Its contribution is related to offering greater security for the Secure Sockets Layer (SSL)/TLS communication channels. The mechanism allows clients (e.g., browsers) to query public immutable logs, which contain status information from secure servers.

The idea is very similar to the Certledger solution, in which certificates are published on a global blockchain network. However, this model is more extensive because it includes both SSL and TLS protocols instead of only TLS. Besides, this proposal is backward compatible with the PKI scheme, such as the CRL and OCSP mechanism.

The provided immutable certificate database allows clients to monitor the status of a SSL/TLS server, checking whether the certificates used have been revoked, or are still valid. Although less usual, the CA itself can also be validated.

In comparison to Certledger and other works based on Ethereum (Matsumoto & Reischuk, 2017) this solution is not anchored to a specific blockchain and demonstrates the concern to provide a public log structure, which can be published on most types of

blockchain. The use of multi-signatures is also presented and applied to a set of web-services (called certifiers), which validate the entry of a new server on the network.

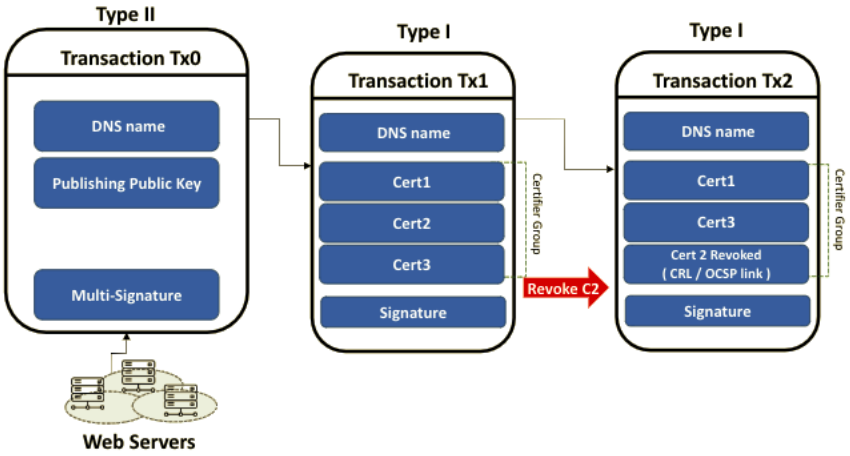

Figure 3 Certledger Architecture (Awaji, Solaiman, & Albshri, 2020)

As shown in figure 3, the model proposes the use of two types of transactions. Type II transactions act like a header that manages all other data. The name of the server is registered by its Domain Name System (DNS) name, and all of its certificates are included in type I transactions. If there is a need to revoke all certificates, all is necessary is to cancel the type II transaction. If it is necessary to cancel a single certificate linked to that server, a new type I transaction will be created, excluding the referred group certificate. Besides, a CRT list or a OCSP server will be updated, recording the fact that this last operation is only to maintain the system's compatibility.

To validate the model, the prototype was implemented on an Nginx web server, and a Firefox browser was used.

Certificate Revocation for 5G IoT

The work of Hewa et al. (2020) presents a revocation proposal in the context of 5G communications. The reduced storage space of IoT devices demands that each implemented resource be optimized about the storage space used. In this aspect, the blockchain contributes to the problem offering the asymmetric cryptographic algorithm of elliptic curves, which results in secure (Mahto & Yadav, 2017) (Gura et al., 2004) (Singh et al., 2016) (Mahto & Yadav, 2018) and smaller(Hankerson et al., 2004) keys. In this work, Elliptic Curve Qu Vanstone (ECQV) was used in the certificates that sign the operations.

The purpose of the work is to automatically revoke a certificate used to record operations of a IoT device on the blockchain using a smart contract. However, unlike the Certledger in which Ethereum was used, this solution uses the Hyperledger Fabric (Cachin & Vukolić, 2017) technology.

The software uses a smart contract to categorizes the threats, and create scores for them. If the score is greater than the predefined parameter, the certificate is automatically revoked. The reasons for revocation and the certificate history data are recorded and published on the blockchain for future investigations.

Revocations for academic certificates

As observes Schär and Fabian (2019), academic certificates are useful only if they can be verified. Blockchain has brought great innovation to diplomas (Awaji, Solaiman, & Albshri, 2020) (Iragorri, 2018)(Ocheja et al., 2019)(F. R. Vidal et al., 2020a)(F. Vidal et al., 2019), because besides offering a secure mechanism for verification it also ensures privacy. Also, there are benefits related to revoking certificates, because of the immutable timestamp. However, several issues about this operation have been raised (Hamilton Duffy, 2017)(Karasavvas, 2018)(F. R. Vidal et al., 2020b) (Santos & Duffy, 2019) (San et al., 2020), so that there is still no consensus on the best way to do it. This section mentions some of the approaches that have been taken to address the diploma's revocation problem.

San et al. (2020) presents a proposal to create a structured blockchain record, able to reference the revoked diplomas. One single transaction can keep several records, which are identified by a sequential integer number, called id. The number of the id by a transaction is limited to the size of 640 bits. The model suggests this size due to the limitation of the tested network, the Bitcoin, which only allows storing about 80 bytes in the OP_RETURN field (Bartoletti & Pompianu, 2017).

Blockcerts has tried two approaches for revocation. One approach to revoke certificates recorded control data in Bitcoin Unspent Transaction Output (UTXO) transactions. The other approach was developed using the Open Badge standard (IMS Global Learning Consortium, 2018), and for this reason, it operated in the form of CRL. There is a third approach planned (Ronning & Chung, 2019), where the use of Verifiable Credentials (VC) is discussed. In this approach, there is a discussion about how to use the available endpoints of the standard. For example, they can point either to a CRL or to a smart contract.

Santos and Duffy (2019) identified the opportunity to revoke certificates using Ethereum smart contracts. For this method to work, the issuance of the certificate must be prepared to instantiate a smart contract. The model deals with the revocation of records in two ways: revocation in batch batchRevocationStatus and individual revocation individualRevokedList. The operation is very similar to the other examples cited here in this work (which used smart contracts) and consists of modifying and checking the status of the digital object (i.e., revoked or not). Similarly, other studies also implement the issuance of certificates using smart contracts, for example, Palma et al. (2019).

F. R. Vidal et al. (2020b) presents and discusses some questions related to the blockchain storage limitation and the difficulty to create a revocation solution to academic diplomas, capable of working with most blockchains. The work proposes the use of a complimentary file to allow the storage of a large amount of data, which would be unfeasible to be stored in the blockchain. The model suggests using a Interplanetary File System (IPFS) network to distribute the complementary file as well as other approaches, that use blockchain and IPFS together (Kumar & Tripathi, 2019) (Yu et al., 2020) (Rajalakshmi et al., 2018).

After analyzing these solutions, we conclude that the revocation is applied in a very particular way by each application. In the next section, we present our solution which uses a scheme global identity, that can be applied in several kinds of applications.

Model Based Self-Sovereign Identity

The revocation models we have described imply that the functionality of the revoke operation is linked to a structural change in the asset's original record. This means that it would only be possible to revoke new records created from a newly defined structure. For example, the works (San et al., 2020) (Santos & Duffy, 2019) (Palma et al., 2019) present a solution for the revocation of academic certificates, but require a change in the process of issuing the certificates to ensure that functionality. Therefore, these approaches are not compatible with old records.

We suggest that the record of the revocation operation for blockchain applications references the original transaction, indicating that it has been revoked. However, storing assets in transactions that operate in a decentralized and sovereign manner is a recent challenge, which did not even exist four years ago (Avellaneda et al., 2019). Therefore, we propose a model using VC and Decentralized Identifier (DID), which, combined, provide a mechanism to store the revocation operation, and at the same time, keep the sovereignty of the asset's owner.

In our model, the application is the owner that has control over all blockchain data. The DID standard allows to delegate one identity, and this functionality is used by the application to expand the control.

Before the blockchain, digital identity solutions were based on federated identity protocols that worked on the Internet, such as OpenID. The goal was to centralize identity data, mainly on social networks.

With the use of the blockchain and the concept of decentralized sovereign identity, new protocols have been proposed. In this work, we combine the use of VC and DID standards that are being developed by World Wide Web Consortium (W3C) VC had its first version published in November 2019 (Reed et al., 2019) and consists of a new data model for

interoperability of self-sovereign identity technologies. A DID is a data structure containing the user's identifier (public key) and other metadata required to create transactions with that identifier.

The figure 4 shows a revocation operation triggered by a generic application, which is revoking three transactions, tx1,tx2 and tx3. The proposed model considers that there may be several public addresses being managed by a single system. That is because an owner may decide to have multiple keys to separate control from several different types of assets. For example, a university may have separate keys to managing the academic records for each of its colleges or schools.

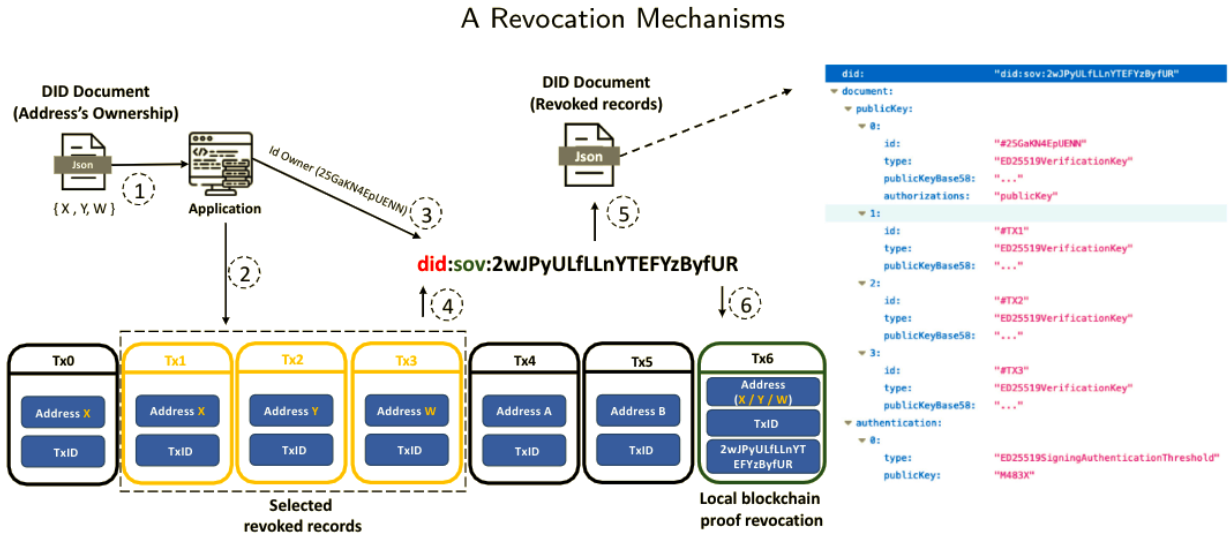

Figure 4 Revoking a group of transaction

To create a DID it is necessary to choose the method on which the model's operation will be based. There are different methods and those can be applied for different purposes1. For this model we used the did: sov method, a specification focused on addressing identity. In this type of method, the identifiers are published on a sovrin2 blockchain. As can be seen in figure 4, an identifier is generated, which has two functions: uniquely identifying the document, and providing mechanisms to the owner to prove his ownership, while keeping his privacy.

We are suggesting in this paper the Sovrin method for DID. However, the DID standard is compatible with several methods. In this case, the Sovrin had performance issues or was unavailable. Our model seeks to change DID method. There are alternative methods that can be implemented, such as DID: IPFS, which generates a link for an IPFS system.

The identifier's generation works in two steps: in the first step, all owner addresses are concatenated in a single address, applying a base58 function (the same as Bitcoin). The result

[1] https://w3c.github.io/did-spec-registries/\#did-document-metadata
[2] https://sovrin.org

of the expression Base58 (address x, address y, address w), generates the id owner, a 21 or 22 character string. The second step is to mark the transactions that will be revoked. Considering that each transaction on the blockchain is uniquely identified by its txid, this will be the information stored in DID to represent each revoked transaction. Several txids will form an owner revocation group. The identifier of this group is calculated by a base58 function, in which all txids of the group are concatenated, together with id owner previously calculated. In this example the generated identifier was: did: sov: 2wJPyULfLLnYTEFYzByfUR.

Also noted in figure 4, an area represented by the transaction tx6, which contains the content of the group identifier. The registration address is done with one of the owner's addresses. The goal is to have a simplified registration on the blockchain, so that the application, by consulting a DID, can verify its integrity in a "disconnected" way (Sovrin is a private blockchain network). Currently, Sovrin has few operators distributed geographically, which can impact unavailability or low-performance (Tissato Nakamura et al., 2019).

We use DID for two functions: identifying the owner and identifying revoked transactions.

Some operations can be performed, such as updating the revoked transaction group. To do this, simply register the DID again with an update operation. Note that the operation does not change the original identifier of DID, which makes it easier for tracking. In this case, the transaction tx6 remains valid to assert that the document exists on the local network.

In the example below, a new transaction is created for the revoked records.

```
{
  "submitterId": #2wJPyULfLLnYTEFYzByfUR,
  "signature": [...,]
  "reqId": 1,
  "operation": {
     "type": "NYM",
     "did": #25GaKN4EpUENN,
     "document": {
        "publicKey": [{
           "id": #TX1
           "type": ED25519VerificationKey
           "publicKeyBase58": ...
        },{
           "id": #TX2
           "type": ED25519VerificationKey
           "publicKeyBase58": ...
        },{
           "id": #TX3
           "type": ED25519VerificationKey
           "publicKeyBase58": ...
        },{
           "id": #TX0
           "type": ED25519VerificationKey
           "publicKeyBase58": ...
```

```
        }
        }],

        "authentication": [{
           "type": "ED25519SigningAuthenticationThreshold",
           "threshold": 1,
           "publicKey": [...]
        }],
        "service": [{
          "type":apiService,
          "serviceEndpoint": http:\\ufp.edu.pt\api
        }]
     }
   }
}
```

This update operation brings a lot of flexibility to the system, because it is possible, for example, to change a controlling public key (i.e., through the authorizations tag), in a scenario such as a stolen key or management change.

Thus far the model presented has shown how to reference existing records to a reversed state, however, there is still an important issue to be addressed. The complementary information in the registration of a revocation. As F. R. Vidal et al. (2020b) observe, due to its architecture, it is not practical to consider recording justifications and other data related to a revocation operation, using the blockchain as a database.

As an alternative to this problem, we propose the use of VC. Among the several meta-data offered by the standard, there is one called credential object, which contains statements on one or more subjects (Reed et al., 2019). At this point, we refer to the revocation DID created, thus relating the complementary file to the document that identifies the revoked data. We also use Extensibility, standard metadata that allows us to create custom fields (Reed et al., 2019). This information can be viewed through figure 5.

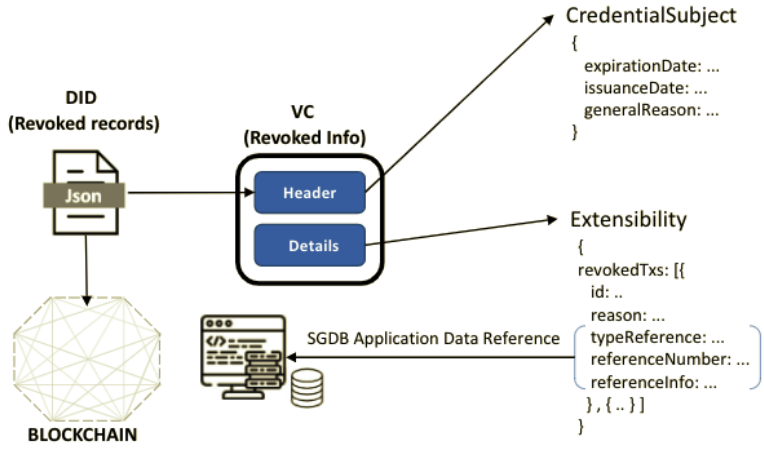

Figure 5 VC Information Revocation File Structure

The code below demonstrates an example of a complementary file in which detailed information regarding academic certificates that have been revoked is stored.

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://ufp.edu.pt/contexts/revokecompl.jsonld"
 ],
 "id": "http://ufp.edu.pt/credentials/4643",
 "type": ["VerifiableCredential", "CustomExt12"],
 "issuer": "https://ufp.edu.pt/issuers/14",
 "issuanceDate": "2020-10-24T05:28:04Z",
 "expirationDate:" "2025-10-24T05:28:04Z",
 "generalReason": "The diploma was revoked due an internal error"
 "credentialSubject": {
  "id": "did:sov:2wJPyULfLLnYTEFYzByfUR",
  "name": "Revoked records of UFP CertEdu System",
 },
 "revokedTxs:" [{
  "id":tx0,
  "reason:" "Wrong student's ID"
  "typeReference:" Integer
  "referenceNumber:" 37705
  "referenceInfo:" "ID number registred"
 },
 {
  "id":tx1,
  "reason:" "E-mail address doesn't exist "
  "typeReference:" Integer
  "referenceNumber:" 39901
  "referenceInfo:" "ID number registred"
 },
 {
  "id":tx2,
  "reason:" "Wrong student's name "
  "typeReference:" Integer
  "referenceNumber:" 40103
  "referenceInfo:" "ID number registred"
 }
 ]
 "proof": {  }
}
```

The fields generalReason and revokedTxs have been customized so that applications can record information about their revoked blockchain transactions. The generated file contains a digital signature (i.e., proof tag), which serves for third parties to verify its integrity.

Conclusion

The blockchain is a database that uses cryptographic mechanisms, however, it has low storage capacity when compared to traditional databases. For this reason, usually, applications write only surrogates to the blockchain, such as the hash of academic certificates or other documents, which are used for authenticity checks. Given this characteristic of blockchains, the revocation mechanism must operate in a similar way, recording only a reversal transaction reference.

Assets that are anchored in a blockchain are usually represented by digital files, structured as JavaScript Object Notation (JSON) or Extensible Markup Language (XML). We propose that the revocation operation should work in the same way, generating a related digital file. However, we propose to use VC to make such information available, mainly due to the flexibility the standard offers, in addition to offering embedded integrity mechanisms (e.g., digital signature). We developed CertEdu (F. R. Vidal et al., 2020a), a prototype for issuing academic certificates on Blockchain, which can distribute diplomas on Ethereum or Bitcoin chains. We adapted the original revocation mechanism (i.e., developed with OpenBadge standard) to work with the VC standard.

A generic solution for revoking records needs to consider that each application has its specific requirements. There is no way to define a static structure for all of them. That is why it is necessary to consider the most diverse types of fields required, to reference the information revoked in the blockchain. In the example shown, the revocation file links the student's registration number to the internal registration system and lists the reasons for which a diploma was revoked.

The proposed model differs from other approaches described in this paper. It does not constrain its operation to a re-engineering of the original application and can be used to revoke old records. Therefore, solutions such as redacting, erasing or pruning, demands new blockchain designs, thus they are not compatible with the current blockchain architecture.

The use of DID enabled the secure identification of owners and their transactions and offered autonomy to revoke their operations. To prevent the process from being centralized to a controller, the standard easily allows changing the composition of the authorizing keys. In addition, the update operation preserves the document's identifier, which allows increasing the number of revoked transactions without adding new transaction registration costs.

Some limitations have been identified. For example, within the model presented, it would not be possible to implement a mechanism similar to the work (Hewa et al., 2020), in which the revocation of an existing record is done automatically, as in the example mentioned by a score calculation. There is also no way to separate revocations from records that are represented in a grouped manner, within a single transaction.

In the current transaction blockchain model, there is no difference to register a "repeatable" transaction in the network. An interesting approach would be creating a mechanism for credit compensation, to applications create the corrective records with less charge. These issues will be addressed in future work, as the model is improved.

From a business perspective, there are benefits to the use of blockchain for academic certificates. According to European Commission/EACEA/Eurydice (2018) in Europe, there was an increase in the number of degrees from 23% (2012) to 39% (2016), with 4.5 million new diplomas per year. However, is quite common tampering on academic certificates. It can take a long time for verification on average 12 days to verify that a diploma is genuine (Awaji, Solaiman, & Marshall, 2020).

The use of blockchain in this type of application brings several benefits to the business, reducing this time and decentralizing the verification process. The use of sovereign identity demonstrated by this work improves the identity of students and universities.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

A. Freier, P. Karlton, P. K. (2011). The Secure Sockets Layer (SSL) Protocol Version 3.0. *RFC 6101*.

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017). Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, 111–126. https://doi.org/10.1109/EuroSP.2017.37

Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K. H., Maler, E., Reed, D., & Sporny, M. (2019). Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Communications Standards Magazine*, *3*(4), 10–13. https://doi.org/10.1109/MCOMSTD.2019.9031542

Awaji, B., Solaiman, E., & Albshri, A. (2020). Blockchain-Based Applications in Higher Education. *Proceedings of the 5th International Conference on Information and Education Innovations*, 96–104. https://doi.org/10.1145/3411681.3411688

Awaji, B., Solaiman, E., & Marshall, L. (2020). Investigating the Requirements for Building a Blockchain-Based Achievement Record System. *Proceedings of the 5th International Conference on Information and Education Innovations*, 56–60. https://doi.org/10.1145/3411681.3411691

Bartoletti, M., & Pompianu, L. (2017). An analysis of Bitcoin OP_RETURN metadata. *CoRR, abs/1702.0*. http://arxiv.org/abs/1702.01024

Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. In A. W. Richa (Ed.), *Leibniz International Proceedings in Informatics, LIPIcs* (pp. 1–16). Schloss Dagstuhl--Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.DISC.2017.1

di Francesco Maesa, D., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019

Diedrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. CreateSpace Independent Publishing.

Dierks, T., & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol*. IETF RFC 5246.

Drosatos, G., & Kaldoudi, E. (2019). Blockchain Applications in the Biomedical Domain: A Scoping Review. *Computational and Structural Biotechnology Journal*, *17*, 229–240. https://doi.org/10.1016/j.csbj.2019.01.010

Eckersley, P. (2012). *Sovereign key cryptography for internet domains*. Internet Draft. https://github.com/EFForg/sovereign-keys

European Commission/EACEA/Eurydice. (2018). The European Higher Education Area in 2018: Bologna Process Implementation Report. *European Education*, *35*(2), 9–15. https://doi.org/10.2753/EUE1056-493435029

Florian, M., Henningsen, S., Beaucamp, S., & Scheuermann, B. (2019). Erasing Data from Blockchain Nodes. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 367–376. https://doi.org/10.1109/EuroSPW.2019.00047

Gilboa, N. (1999). Two Party RSA Key Generation. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 116–129). https://doi.org/10.1007/3-540-48405-1_8

Goranovic, A., Meisel, M., Fotiadis, L., Wilker, S., Treytl, A., & Sauter, T. (2017). Blockchain applications in microgrids an overview of current projects and concepts. *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, 6153–6158. https://doi.org/10.1109/IECON.2017.8217069

Goyal, V. (2007). Certificate Revocation Using Fine Grained Certificate Space Partitioning. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 247–259). https://doi.org/10.1007/978-3-540-77366-5_24

Grigoriev, D., & Shpilrain, V. (2021). RSA and redactable blockchains. *International Journal of Computer Mathematics: Computer Systems Theory*, *6*(1), 1–6. https://doi.org/10.1080/23799927.2020.1842808

Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-Bit CPUs. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Hamilton Duffy, K. (2017). *Blockcerts Revocation*. Github. https://github.com/IMSGlobal/cert-schema/issues/24

Hanke, T. (2016). AsicBoost - {A} Speedup for Bitcoin Mining. *CoRR, abs/1604.0*. http://arxiv.org/abs/1604.00575

Hankerson, D., Vanstone, S., & Menezes, A. (2004). Guide to Elliptic Curve Cryptography. In *Guide to Elliptic Curve Cryptography*. Springer Publishing Company, Incorporated. https://doi.org/10.1007/b97644

Hewa, T., Bracken, A., Ylianttila, M., & Liyanage, M. (2020). Blockchain-based Automated Certificate Revocation for 5G IoT. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 1–7. https://doi.org/10.1109/ICC40277.2020.9148820

IMS Global Learning Consortium. (2018). *Open Badges v2.0 IMS Final Release*. http://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html

Iragorri, C. (2018). Academic certificates on Hyperledger. In *Hyperledger Global Forum*. Hyperledger Global Forum. https://bit.ly/2Ww116I

Jain, G. (2002). *Certificate Revocation: A Survey*. Computer Science Department, University of Pennsylvania. http://citeseer.ist.psu.edu/511985.html

Javarone, M. A., & Wright, C. S. (2018). From Bitcoin to Bitcoin Cash. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18*, 77–81. https://doi.org/10.1145/3211933.3211947

Karasavvas, K. (2018). Revoking Records in an Immutable Ledger: A Platform for Issuing and Revoking Official Documents on Public Blockchains. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 105–111. https://doi.org/10.1109/CVCBT.2018.00019

Kim, T. H.-J., Huang, L.-S., Perring, A., Jackson, C., & Gligor, V. (2013). Accountable key infrastructure (AKI). *Proceedings of the 22nd International Conference on World Wide Web - WWW '13*, 679–690. https://doi.org/10.1145/2488388.2488448

Kubilay, M. Y., Kiraz, M. S., & Mantar, H. A. (2018). CertLedger: {A} New {PKI} Model with Certificate Transparency Based on Blockchain. *CoRR*, *abs/1806.0*. http://arxiv.org/abs/1806.03914

Kumar, R., & Tripathi, R. (2019). Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain. *2019 Fifth International Conference on Image Information Processing (ICIIP)*, 246–251. https://doi.org/10.1109/ICIIP47207.2019.8985677

Laurie, B., Langley, A., & Kasper, E. (2013). RFC 6962: Certificate Transparency. *RFC*.

Mahto, D., & Yadav, D. K. (2017). RSA and ECC: A comparative analysis. *International Journal of Applied Engineering Research*.

Mahto, D., & Yadav, D. K. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. *International Journal of Network Security*, *20*(4), 625–635. https://doi.org/10.6633/IJNS.201807_20(4).04

Matsumoto, S., & Reischuk, R. M. (2017). IKP: Turning a PKI Around with Decentralized Automated Incentives. *2017 IEEE Symposium on Security and Privacy (SP)*, 410–426. https://doi.org/10.1109/SP.2017.57

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*. https://doi.org/10.1007/s10838-008-9062-0

Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*. https://doi.org/10.1186/s41039-019-0097-0

Palma, L. M., Vigil, M. A. G., Pereira, F. L., & Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in Brazil. *International Journal of Network Management*, *29*(3), e2061. https://doi.org/10.1002/nem.2061

Rajalakshmi, A., Lakshmy, K. V., Sindhu, M., & Amritha, P. (2018). A Blockchain and IPFS based framework for secure Research record keeping. *International Journal of Pure and Applied Mathematics*, *119*(15). https://acadpubl.eu/hub/2018-119-15/4/751.pdf

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2019). *Decentralized Identifiers (DIDs) v0.11*. W3C. https://w3c-ccg.github.io/did-spec/

Ronning, A., & Chung, W. W. (2019). *Blockcerts V3 Proposal*. https://nbviewer.jupyter.org/github/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/BlockcertsV3.pdf

Rujia, L., & Galind, D. (2017). *BTCert*. Universidade de Birmingham. https://github.com/BlockTechCert/BTCert

Ryan, M. D. (2014). Enhanced Certificate Transparency and End-to-End Encrypted Mail. *Proceedings 2014 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2014.23379

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the Attack Surface of Blockchain: {A} Systematic Overview. *CoRR*, *abs/1904.0*. http://arxiv.org/abs/1904.03487

San, A. M., Chotikakamthorn, N., & Sathitwiriyawong, C. (2020). Blockchain-based Learning Credential Revision and Revocation Method. *Proceedings of the 21st Annual Conference on Information Technology Education*, 42–45. https://doi.org/10.1145/3368308.3415456

Santos, J., & Duffy, K. H. (2019). *A Decentralized Approach to Blockcerts Credential Revocation*. https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/final-documents/blockcerts-revocation.md

Schär, F., & Fabian, M. (2019). Blockchain diplomas: Using smart contracts to secure academic credentials. *Beiträge Zur Hochschulforschung*, *48*.

Sgarbi, A. (2014). "Revogação": uma abordagem pragmática. *Revista Direito, Estado e Sociedade*, *29*. https://doi.org/10.17808/des.29.285

Siegel, D. (2016). *Understanding The DAO Attack*. https://www.coindesk.com/understanding-dao-hack-journalists

Singh, S. R., Khan, A. K., & Singh, S. R. (2016). Performance evaluation of RSA and Elliptic Curve Cryptography. *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, 302–306. https://doi.org/10.1109/IC3I.2016.7917979

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money ... *Sage Publications, Inc.*

Tissato Nakamura, E., Cezar Herédia Marino, F., Reynaldo FormigoniIlho Filho, J., Luís Ribeiro, S., & Padilha de Oliveira, V. (2019). Identidade Digital Descentralizada: Conceitos, aplicações, iniciativas, plataforma de desenvolvimento e implementação de caso de uso. In *XIX Simposio Brasileiro de Seguranca da Informacao e de Sistemas Computacionais - SBSeg 2019*. SBSeg. https://www.ic.unicamp.br/~bit/mo809/seminarios/07-out/Identidade Digital Descentralizada.pdf

Tse, D., Zhang, B., Yang, Y., Cheng, C., & Mu, H. (2017). Blockchain application in food supply information security. *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 1357–1361. https://doi.org/10.1109/IEEM.2017.8290114

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2789929

Vidal, F., Gouveia, F., & Soares, C. (2019). Analysis of Blockchain Technology for Higher Education. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 28–33. https://doi.org/10.1109/CyberC.2019.00015

Vidal, F. R., Gouveia, F., & Soares, C. (2020a). Blockchain Application in Higher Education Diploma Management and Results Analysis. *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 865--870. https://doi.org/10.25046/aj0506104

Vidal, F. R., Gouveia, F., & Soares, C. (2020b). Revocation Mechanisms for Academic Certificates Stored on a Blockchain. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI49556.2020.9141088

Vigil, M., Buchmann, J., Cabarcas, D., Weinert, C., & Wiesmaier, A. (2015). Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey. *Computers & Security*, *50*, 16–32. https://doi.org/10.1016/j.cose.2014.12.004

Walleck, D., Li, Y., & Xu, S. (2008). Empirical Analysis of Certificate Revocation Lists. In V. Atluri (Ed.), *Data and Applications Security XXII* (pp. 159–174). Springer Berlin Heidelberg.

Wang, Q., Gao, D., & Chen, D. (2020). Certificate Revocation Schemes in Vehicular Networks: A Survey. *IEEE Access*, *8*, 26223–26234. https://doi.org/10.1109/ACCESS.2020.2970460

Wang, Z., Lin, J., Cai, Q., Wang, Q., Jing, J., & Zha, D. (2019). Blockchain-Based Certificate Transparency and Revocation Transparency. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 144–162). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-58820-8_11

Yu, Y., Zhao, Y., Li, Y., Du, X., Wang, L., & Guizani, M. (2020). Blockchain-Based Anonymous Authentication With Selective Revocation for Smart Industrial Applications. *IEEE Transactions on Industrial Informatics*, *16*(5), 3290–3300. https://doi.org/10.1109/TII.2019.2944678

Zhou, X., Wu, Q., Qin, B., Huang, X., & Liu, J. (2016). Distributed Bitcoin Account Management. *2016 IEEE Trustcom/BigDataSE/ISPA*, 105–112. https://doi.org/10.1109/TrustCom.2016.0052

Bibliographic information of this paper for citing:

Richter Vidal, Fernando; Gouveia, Feliz & Soares, Christophe (2022). Analysis of Revocation Mechanisms for Blockchain Applications and a Proposed Model Based in Self-Sovereign Identity. *Journal of Information Technology Management*, Special Issue, 192-210. https://doi.org/10.22059/jitm.2022.87848