Creating a Private University Blockchain for More Secure Data Storage

Krisztián Bálint

Óbuda University Keleti Károly Faculty of Business and Management, Budapest, balint.krisztian1@kgk.uni-obuda.hu

Abstract: Secure data storage is becoming more and more important these days. Theadvantage of databases is that the data is saved in an organized manner, so it is easyto review. Their disadvantage is greater vulnerability, as these data are recorded inan organized and structured manner so that in the event of a database being hacked,an attacker can easily see the information obtained without authorization.University databases often store sensitive student data that must be protected incyberspace. My research goal is to investigate whether it is possible to create a private university blockchain where data can be stored securely, even in the longterm. As part of the practical implementation, my goal is to create a blockchainbased database with the genesis block and determine its block sizes. This isnecessary because with the appearance of large amounts of data (Big Data),blockchain networks often become overloaded and this problem can be solved bylimiting the block size. After creating the blockchain, I define its data storageconditions, as this can only be ordered by the owner of the blockchain, in this case,the university.

Keywords: Blockchain, database, security, policy

1 Introduction

Blockchain is a distributed database technology that prevents falsification and modification of data. It was first published in October 2008 by a certain person or group named Satoshi Nakamotoon page the sketch of the Bitcoin blockchain technology. Marc Andersen, who created the first popular browser program, Netscape, said that whoever created blockchain deserves a Nobel Prize. With this, one of the biggest problems of the Internet, the trust issue, was solved in one fell swoop by creating a distributed trust network (Puskás, 2018). The use of blockchain systems can create new value in many areas, from government and administrative functions to scientific collaboration. Due to the nature of the area, it is often visibly restrained in public, but the mapping and implementation of the use of blockchains in security areas has also begun. Such areas:

- Cyber protection and data security,
- Protection of critical infrastructures,
- Disaster prevention and prevention,
- Law enforcement,
- The national defense and
- The intelligence (Kocsis, 2020).

The use of blockchain technology makes it possible to store data securely also in the education system.

2 Modern Storage Solutions

The essence of blockchain-based data management is an encryption (cryptographic) procedure where each party has at least one public and one private key pair (so-called asymmetric encryption), which are sequences of digital signals and characters. Using the public key algorithm, any user can perform data management operations on the network, during which the information and data involved in the process (e.g. sharing, "moving" data) is encrypted with its private key. The data encrypted in this way, as well as the public keys of the parties involved in the operation (e.g. sender and recipient), can be seen by any other user on the network. Still, only the parties can interpret and decode it using their private keys. The party initiating the data management operation encrypts the information with the encryption algorithm running on the network and its own unique secret key. Then it assigns the recipient party's public key to the encrypted data it determines, thus creating the coded form of the original data. From now on, only the coded data created in this way will be visible to all users in the blockchain system (Eszteri, 2020).

Before creating a blockchain, it is necessary to examine what blockchain solutions are available today. Such is the public and private blockchain.

- Public blockchain: a typical example is the Bitcoin or Ethereum network. Anyone can join the chain, start and validate a transaction. Miners are often rewarded with a in exchange for their work for validation. Its advantages include transparency and accessibility, however, we can count on the high computational demand as a disadvantage or, depending on the use, we can easily list transparency here again. The calculation operations which are necessary for the validation of the blocks are basically a significant item on the cost side, and transparency in a large company environment is not considered ideal, where the leakage of business secrets is not allowed. Proof of Work (PoW) is a widespread

mechanism, but this may soon be replaced by Proof of Stake (PoS) due to its huge energy requirements.

- Private blockchain: Basically, the idea of the blockchain was based on public access, but over time, the need for private implementation also developed. In this type, it is created by the owner of the blockchain the rules, as a result of which he determines the remuneration for mining or who is entitled to access the network. It is also known as a permission-based network. Area of use where sensitive data is handled, e.g. financial or insurance sector, healthcare (Sipos 2020).

  In order to safely store sensitive university data, I therefore choose to create a private blockchain in practice.

3 The creation of a private UDSC (Universities Data Storage Chain) blockchain

As part of the practical implementation, I created a private university blockchain called UDSC. Only the administrator I defined in advance had access to this blockchain. For the sake of the speed of the blockchain, I set the size of the blocks to 1 MB, so that the data stored in the blocks can be accessed quickly enough in practice. The first diagram shows the steps involved in creating the UDSC blockchain.

University chain-util generate UDSC
the default settings would be used:
/default ~ university chain/UDSC/chainsettings.dat chainsettings.dat include:
Database addresses [receiver (cloud storage) IP address, sender (university) IP address],
Terms of GDPR database.
Next, the UDSC blockchain would be initialized, and the genesis block would be created
university chain UDSC
The server will be started in those few seconds after the genesis block has been found, then the node address needs to be connected:
UDSC@192.168.0.1:8008
After these steps, the connection can be attempted from a second server:
university chain UDSC@192.168.0.1:8008
After the message confirming the chain has been initialized, the permission is not given for connection to the database. The address would be copied and pasted: 192.168.0.2

Figure 1 The creation of a private UDSC (Universities Data Storage Chain) blockchain (Bálint, 2021)

In the case of the constitution of an independent, university-based blockchain, the educational institution could define the favorable data storage conditions itself. These may be the following:

- Wider based access to the given blockchain,
- The definition of the blocks' size,
- The definition of the terms of use,
- The genesis block, to which all the other blocks are connected, stays in the property of the university,
- The limiting of the access to the blockchain (only the entitled should use it),
- The definition of data protection policy,
- For increased security, the blockchain may be started on multiple servers,
- The nodes are more easily supervised,
- The system becomes more transparent,
- The eventual attacks are more easily reconnaissance.
- It provides a possibility for rapid reaction, in case of a hacker attack,
- The conditions contained within the smart contract are primarily defined by the faculty (Bálint, 2021).

4 Creating a smart contract for automated data transmission

A smart contract is one based on blockchain technology a solution that automatically executes the conditions defined therein by bypassing an external third party as an enforcer. In such a case, there is no need for a lawyer neither when the contract is concluded nor when it is enforced. It only executes instructions that are predetermined in the terms of the contract. These conditions are called triggers. The following 4 conditions are required when concluding a smart contract:

- For the subject of the contract, which is actually the subject of the contract,
- To define conditions precisely. Only if they are met can the contained in the contract,
- For authentication. The subject of the contract must be authenticated with the digital signature, as well as its conditions,

- Last but not least, a blockchain is also needed where the contract can be created (Budai, 2018).

Features of the smart contract:

- He constantly checks himself,
- It runs itself on the nodes of the blockchain, so it is available at all hours of the day. The users only need an Internet connection.
- It cannot be manipulated, as the code cannot be modified afterwards. The entered data is foreign cannot overwrite (Virtuális, 2020).
- The lifecycle of the smart contract cannot be modified, its content is implemented (Környei, 2018).

The advantages of a smart contract are as follows:

- Constancy. The conditions specified in the contract are automatically implemented, if they are fulfilled.
- Transparency. The conditions recorded in the smart contract are public to other participants.
- Speed. Since there is no need for human intervention, it is stipulated in the contract conditions are automatically executed within a short time (Stefán, 2021).

Disadvantages of a smart contract:

- Human errors. Since the code of the smart contract is written by humans, errors may occur. If the programmer does not notice this in time, the faulty smart contract can enter the blockchain, where it performs a task that is not suitable for the parties.
- The code of a faulty smart contract in the blockchain cannot be modified afterwards.
- Legal issues. The vision of smart contracts in the absence of state legislation uncertain. It is not known what will happen when state bodies start regulating contracts.
- A negative arising from the decentralization structure. In case of infringement, there is no central body that can compensate the user (Honti, 2020).

As part of the practical implementation, I connected the smart contract with the university database, like this I was able to manage data access effectively. In this way, I performed the query and the access control using the algorithm of the contract. These settings are illustrated in the second second figure below.

```
function access (Obudai University database)
Input: query (Obudai University database)
Output: permission granted; permission denied
  if message (Obudai University database) exists & query (Obudai University database) valid then
   security camera enabled/disabled
      if the University of Obudai database is registered in the given list then
        admin verification
         if admin available = access is adequate then
           return allowed
         else
         return denied
        end if
       else
       return denied
      end if
else
  return denied
end if
end function
```

Figure 2 The Definition of the Smart Contract, Linked to the UDSC

(Bálint, 2021)

When writing the smart contract, I paid special attention to sending the data to the blockchain using the smart contract, and to the cloud-based database, which is less secure. This is presented in the third figure below.

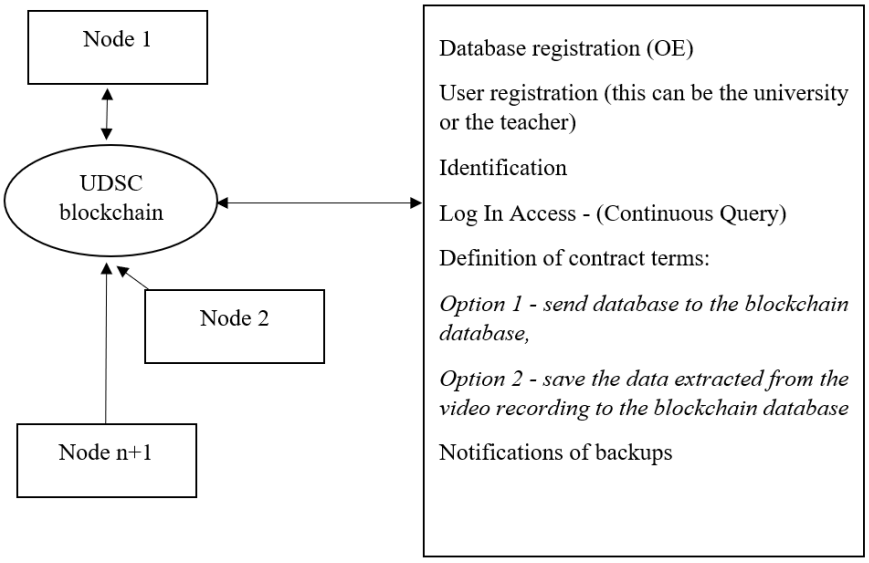

Figure 3 The Scheme of the Smart Contract and the Operation of the UDSC Blockchain

Conclusions

Nowadays, there are many data storage solutions to choose from. In addition to the traditional cloud-based data storage solution, blockchain-based data storage has also appeared. Thanks to its decentralized solution, greater database security can be achieved through its application. The potential of the blockchain has not yet been fully exploited, as the scientific world is also constantly learning about it. Storing university data is an important aspect, so after examining the possibilities of public and private blockchains, I created a private UDSC blockchain. In order to manage data more efficiently, I wrote a smart contract, which I linked to the blockchain, so that the data was sent in an automated way. In summary, I could conclude that the joint application of blockchain and smart contract means greater database security for universities than its centralized counterparts.

References

[1] Bálint K. (2021): Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a Universities' Modern Security Cameras. *Acta Polytechnica Hungarica*, DOI: 10.12700/APH.18.2.2021.2.7, Volume 18, Issue Number 2, pp.127-142.

[2] Bálint K. (2021): The connection of a Blockchain with Students' Attendance Register based on Security Cameras. *IEEE 19th International Symposium on Intelligent Systems and Informatics,* SISY*,* Subotica, Serbia, 191 p. pp. 67-70.

[3] BUDAI G. (2018): Blockchain a kriptovaluták és az okos szerződések világa. *Gazdasági Egyetem, Gazdálkodási Kar*, Zalaegerszeg, https://bit.ly/3vw0TDP (downloaded: 2022.12.08.) pp. 1-67.

[4] Eszteri D. (2020): A blokklánc mint személyes adatkezelési technológia GDPR-megfelelőségéről. Állam és Jogtudomány Kar, Budapest, 61.4 pp. 24-51.

[5] Honti R. (2020): Mi is az az okos szerződés, avagy smart contract. Crypto Falka, https://bit.ly/2OGFMv0 (downloaded: 2022.12.08.)

[6] Kocsis I. (2020): Blokklánc alkalmazási lehetőségek a biztonság területén és bevezetés-tervezésük. *Scientia et Securitas*, Budapesti Műszaki és Gazdaságtudományi Egyetem, Méréstechnika és Információs Rendszerek Tanszék, Budapest, pp. 12-20.

[7] Környei M. (2018): Programozott kollektív bölcsesség – Az okos szerződések alapkérdései. 2018. https://bit.ly/2CxR1n3 (downloaded: 2022.12.08.)

[8] Puskás G. (2018): Kriptovaluta bányászat a gyakorlatban. *Finance Computer science, Information Economy*, Budapesti Corvinus Egyetem Gazdálkodástudományi Kar Infokommunikációs Tanszék, pp. 57-78.

[9] Sipos D. (2020): Blokklánc-technológia alkalmazása az ellátási láncokban. *Multidiszciplináris Tudományok - Fiatal Kutatók különszám*, Miskolci Egyetem, Informatikai Intézet, Alkalmazott Informatikai Intézeti Tanszék, Tudományok 10.2, pp. 525-531.

[10] Stefán I. (2021): Az okos szerződések létrejöttének és érvénytelenségének kérdései. *Miskolci Jogi Szemle* 16.3, https://bit.ly/3v4Q9yd (downloaded: 2022.12.08.), pp. 298-312.

[11] Virtuális C. (2020): Mi az okos szerződés. *Blog Kripto Okos szerződés,* https://bit.ly/2BgOUn5 (downloaded: 2022.12.08.)