BLOCKCHAIN BASED DIGITAL IDENTITY MANAGEMENT

Çağatay KÖLÜŞ
Selçuk University, Department of Information Technologies

Fatih BAŞÇİFTÇİ
Selçuk University, Faculty of Technology, Department of Computer Engineering

ABSTRACT

Identity is a tool that identifies a person or group and ensures that they are recognized by others. Personal identification cards issued by the states to people contain specific information about the person given. Identity systems used for centuries are now digitalized, ID cards with chips and passports with chips have entered our lives. In the past, only information such as name, surname and place of birth were included in ID cards with chips and passports. But today, in addition to our personal information, it includes our biometric information such as fingerprints, iris, digital signatures. Blockchain technology, which has entered our lives with the financial sector, offers application areas in different sectors and subjects. Some of these are IoT (internet of things), security and reliability systems, copyrights, public and health sectors. In this study, it has been mentioned about the advantages and the features obtained by using blockchain technology in identity management. The purpose of this study; It is to ensure the safe use of identity information thanks to the features provided by the block chain such as distributed database called DLT (distributed ledger technology), peer-to-peer transmission, transparency and irreversible records. Also in this study, a software that can simulate blockchain technology was created and an Android application that reads data with NFC (Near Field Communication) technology was developed. Thus, the process of adding the data in the ID card or passport to the block chain by reading the data from NFC with the Android application can be performed.

Keywords: Blockchain, identity, Android

1. INTRODUCTION

Identity indicates who people are, what type of person they are, or how they relate to others [1]. Today, identity is a tool that introduces a person or a group and makes it known by others. Countries have developed various systems to determine who their citizens are and ID cards are one of these Technologies [2]. States give their citizens personal identity cards in order to identify their own citizens. The identity cards provided contain data that identifies the person. Information such as the name, surname and date of birth of the person can be given as an example. In addition to being biometric identifiers, identities also have usage purposes such as access to public services and security. Identity systems were first used in Europe between the 15th and 17th centuries [3].

Today's ID cards contain chips in addition to the old ID cards. Identity systems used for centuries are now digitalized, chip ID cards and chip passports have entered our lives. The chip contains the user's personal information. In figure 1, there is an image that includes the front and back sides of the passport with chip and ID card with chip.

Figure 1. Turkish Passport and Turkish ID Card

Digital identity cards have fields of application that are actively used in public services, the healthcare industry, and the financial industry, thereby facilitating people's lives. Examples include changing the residence address in the public service, obtaining a health certificate in the health sector, and using it in the credit sector in the financial sector.

Before digitizing passports and identity cards, only information such as name, surname, birthplace are available today; It includes our biometric information such as fingerprint, iris, digital signature.

Authentication systems include methods called factors. The most known authentication factors are:

- Something you know (Username, password, etc.)
- Something you have (Access card, password generation device, etc.)
- Something about yourself (Fingerprint, iris, retina etc.)

Blockchain is a series of blocks that keep a list of transaction records [4]. Blockchain consists of cryptographic data blocks, and this concept was introduced in 2008 with a Bitcoin article that introduced itself as Satoshi Nakamoto and published by an unknown person [5]. The true identity of this person or persons remains a mystery even though there are various claims.

Blockchain has four main features. These features are; distributed database, peer-to-peer transmission, transparency and irreversible records. There are many advantages of blockchain technology. Some of these are those;

- A third party agents are not needed for transactions between people.
- Transactions are public and visible.
- The realized transactions cannot be changed and have a transparent structure.

Blockchain technology, which has entered our lives with the financial sector, offers application areas in different sectors and subjects. Some of these are IoT (internet of things), security and reliability systems, copyrights, public and health sectors.

Blockchain technology has entered our lives with Bitcoin, one of the digital currencies, and is still used today due to its advantages. In addition, new application areas are emerging day by day. Although this technology is mostly known for its use in the financial sector, it can also be used in areas such as IoT (Internet of Things), security and reliability systems, authentication, copyrights, the public sector and health.

The working principle of blockchain technology is given in the image in Figure 2 prepared by Financial Times.

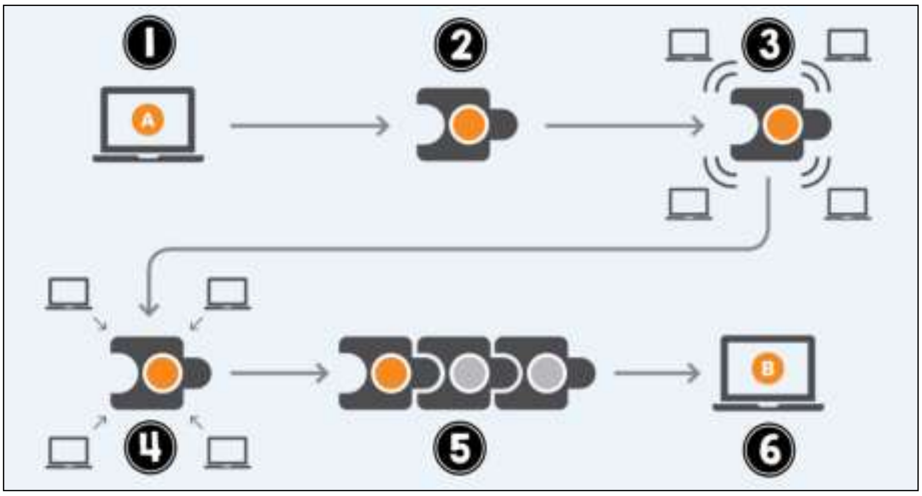


Figure 2. Working Principle of Blockchain

If we explain the working principle of blockchain through the figure:

1. Person A wants to send money to Person B
2. This process is created as a block
3. The created block is included in the network and everyone is aware of this block
4. Those on the network approve of this block
5. The approved block is added to the chain
6. Transfer of money from person A to person B is complete

Block chain technology offers a very suitable use for identity systems. By using these two technologies together, it is possible to store and use credentials securely. In a system where data is managed by technology companies (3rd party), the security of identity data is always in danger. Identity data security can be ensured thanks to features such as distributed database of blockchain, peer-to-peer transmission, transparency and irreversible records.

DLT - (Distributed Ledger Technology) is the foundation of the blockchain. DLT does not need a center and verifies transactions between people through computer networks. [6] DLT offers a solution to the Byzantine Generals Problem defined by Leslie Lamport et al. In 1982. This problem involves that the generals surrounding a fortress can be difficult and erroneous to communicate with each other and to achieve mutual agreement [7].

In this study, the advantages and the features provided by using blockchain technology in identity management are mentioned. The purpose of this study; It is to ensure that the credentials are used safely thanks to the features such as distributed database called DLT provided by the block chain, peer-to-peer transmission, transparency and irreversible records. In addition, in this study, a software that can simulate blockchain technology was created and an Android application that reads data with NFC technology was developed.

2. METHOD

There are many ways to use blockchain technology with identity systems. The technologies and requirements to be used in this study are as follows:

- Blockchain technology
- NFC technology
- ID card with chip or passport with chip
- NFC supporting smart phone
- An application that reads data on the ID card or passport using NFC technology

The realization of the above-mentioned technologies and requirements was carried out by the following method:

1. Creating a software that can simulate block chain technology,
2. Development of an Android application that reads data from NFC,
3. Reading the data in the ID card or passport using NFC technology and Android application and adding it to the block chain

3. APPLICATION

In this section, an Android application has been developed in Android Studio. This application performs:

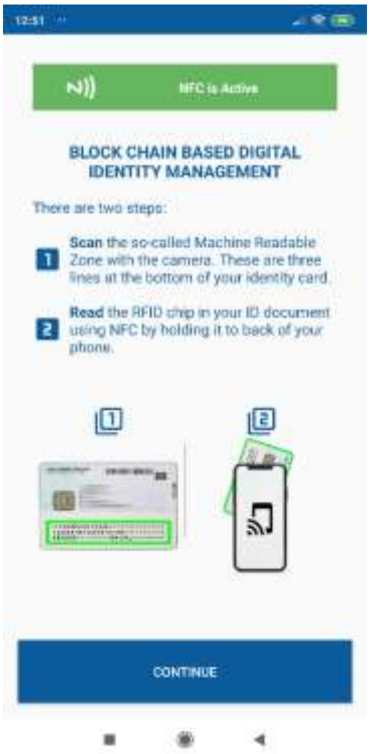
- Receipt of data on chip ID or passport with NFC technology
- Adding the received data to the blockchain

The working principle of the application is stated below:

1. The user will scan the MRZ section on the ID card or passport with the camera.
2. Serial number, date of birth and validity period information in MRZ section are obtained with OCR technology.
3. In order to receive data using NFC technology, the user is asked to bring the ID card or passport closer to the mobile phone.
4. Information on the ID card or passport is obtained and this information is displayed to the user.

5. The information obtained is added to the blockchain.

The opening screen of the application is given in figure 3. On this screen, there is an indicator that indicates the NFC status. There are also texts and images that contain the instructions for use of the application.



NFC is Active

BLOCK CHAIN BASED DIGITAL IDENTITY MANAGEMENT

There are two steps:

1 **Scan** the so-called Machine Readable Zone with the camera. These are three lines at the bottom of your identity card.

2 **Read** the RFID chip in your ID document using NFC by holding it to back of your phone.

Figure 3. Application Opening Screen

The scanning of the MRZ section on the back of the ID card is carried out by the camera. After selecting the continue button, the camera screen opens. This screen is shown in figure 4. Reading the MRZ section with the camera takes less than 1 second when performed with the right angle and light.

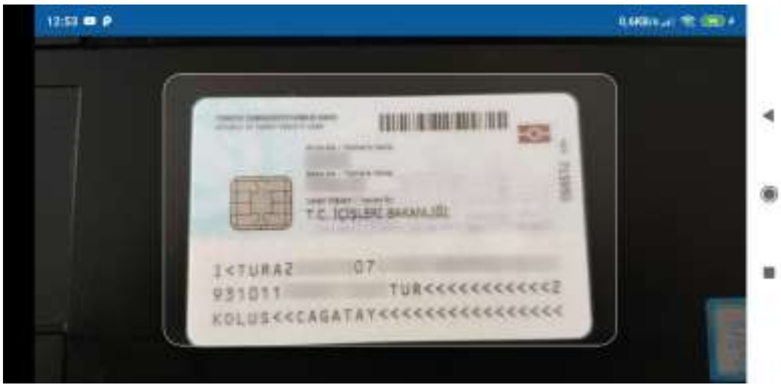
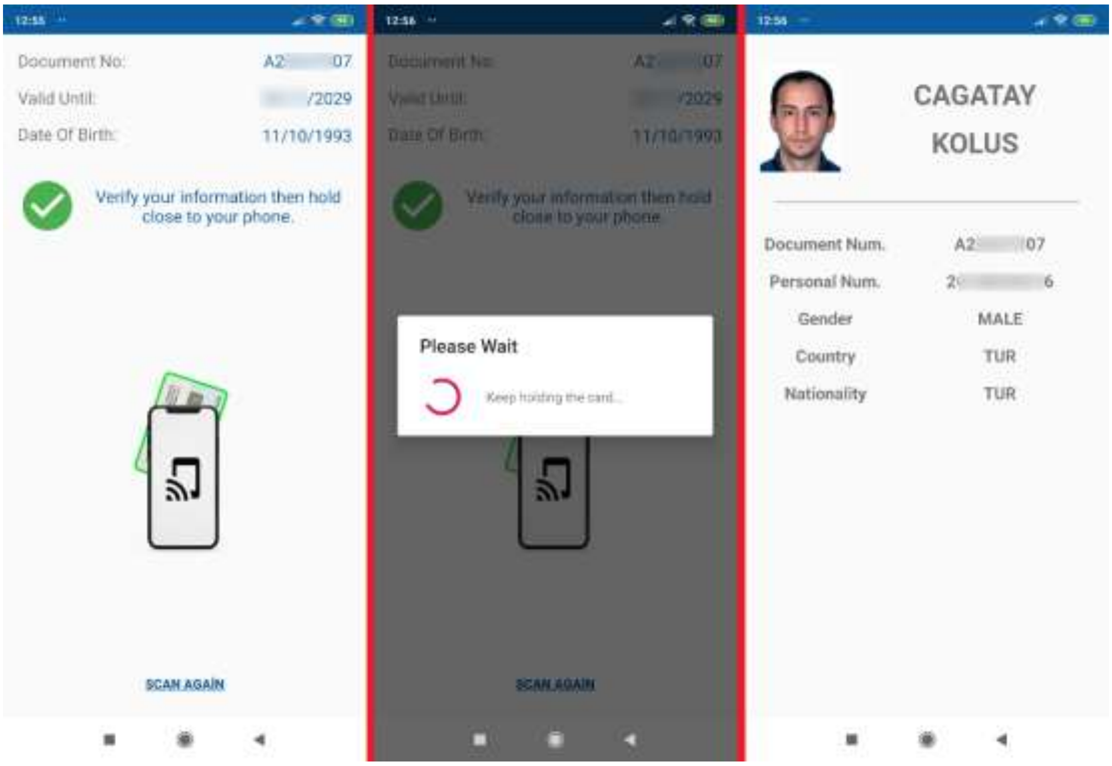


Figure 4. ID Card Scan Screen

After the serial number, date of birth and expire date information in the MRZ section of the ID card are successfully read, this information is displayed to the user on a screen. The user is asked to verify this information and, if correct, bring the card closer to the back of the device. Keeping the card steady, obtaining information with NFC technology is done in this step. After the information is received, some information on the card is reported to the user on the summary page. The images related to this narrative are given in figure 5.



Document No: A2[redacted]07
Valid Until: [redacted]/2029
Date Of Birth: 11/10/1993

Verify your information then hold close to your phone.

SCAN AGAIN

Please Wait
Keep holding the card...

CAGATAY KOLUS

Document Num. A2[redacted]07
Personal Num. 2[redacted]6
Gender MALE
Country TUR
Nationality TUR

Figure 5. Reading the Data in the ID Card with NFC

The operations for the ID card can also be carried out for the passport. The screen shot of the 2-line MRZ field on the passport with the camera is given in figure 6.

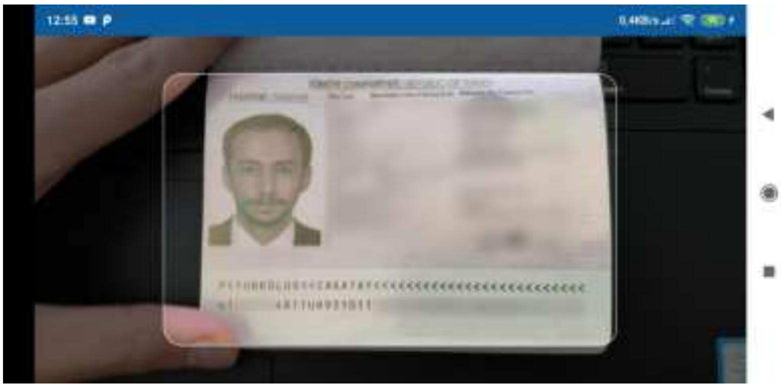
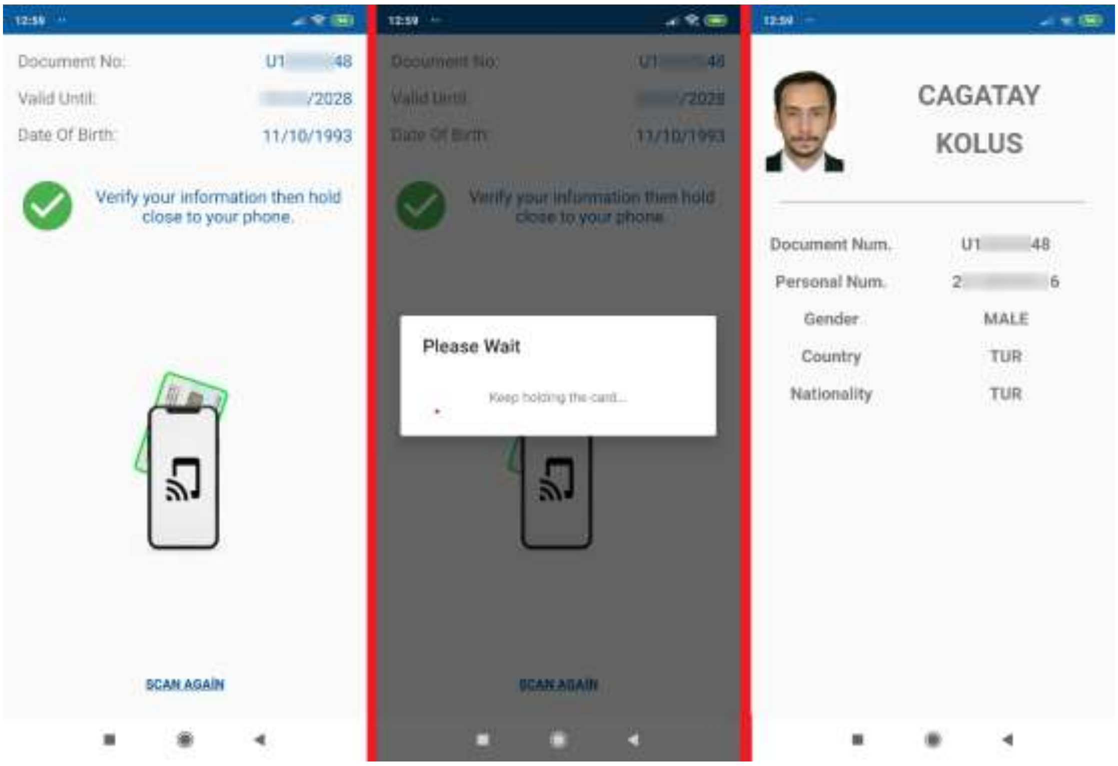


Figure 6. Passport Scan Screen

After the serial number, date of birth and expire date information in the MRZ section of the passport are read successfully, this information is displayed to the user on a screen. The user is asked to verify this information and, if correct, bring the passport closer to the back of the device. Keeping the passport steady, obtaining information with NFC technology is done in this step. After the information is received, some information in the passport is reported to the user on the summary page. Images related to this narrative are given in figure 7.



Document No: U1[redacted]48
Valid Until: [redacted]/2028
Date Of Birth: 11/10/1993

Verify your information then hold close to your phone.

SCAN AGAIN

Document No: U1[redacted]48
Valid Until: [redacted]/2028
Date Of Birth: 11/10/1993

Verify your information then hold close to your phone.

Please Wait

Keep holding the card...

SCAN AGAIN

CAGATAY
KOLUS

Document Num.	U1[redacted]48
Personal Num.	2[redacted]6
Gender	MALE
Country	TUR
Nationality	TUR

Figure 7. Reading the Data in the Passport with NFC

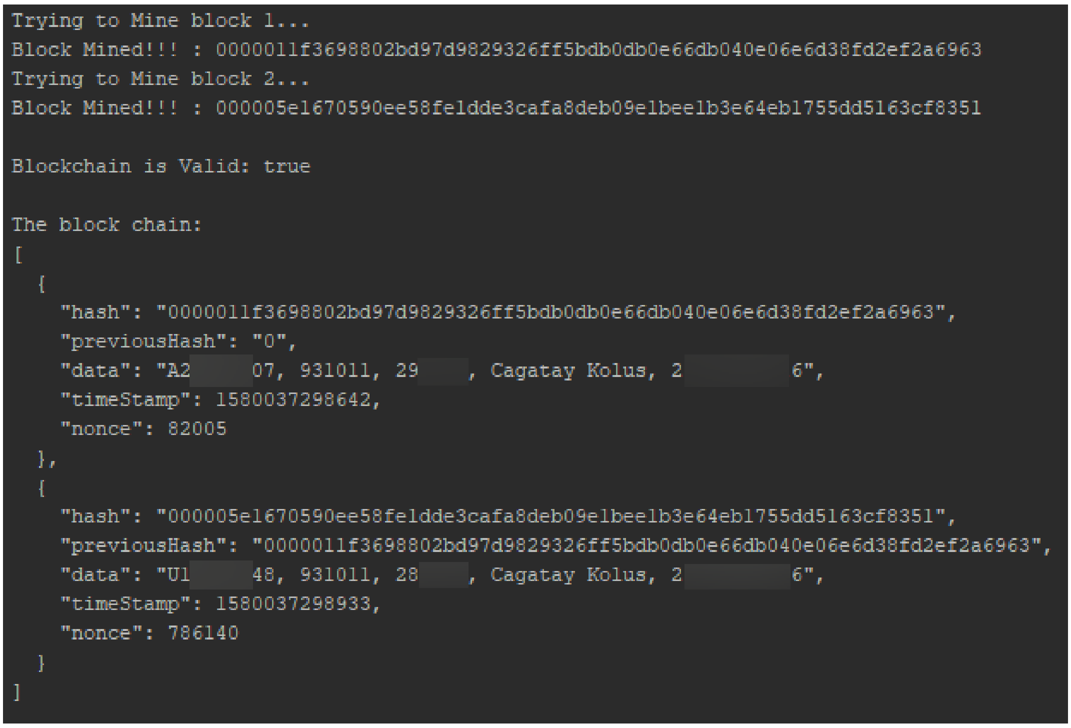
As a result of the above operations, 1 identity card and 1 passport were transferred to digital environment. Although the owners of the two identities are the same person, there is no negative situation in adding the identities to the blockchain. The data added to the blockchain are as follows:

Data in block 1: Located on the identity card; serial number, date of birth, expire date, name, surname and identification number

Data in block 2: Located in the passport; serial number, date of birth, expire date, name, surname and identification number

Each block was added to the chain and a block chain of 2 blocks was obtained. Each block has its own hash value. The subsequent blocks also contain the hash value of the previous block. In this way, the change in any block in the block chain is not accepted because it disrupts the whole chain. Even when a single letter of data in a block changes, the hash value that will be created next is changing.

In figure 8, an image showing 2 blocks added to the block chain is given. In this image, the hash value of each block, the verification of the block chain and the data in each block are given. The data added as a block includes the serial number, date of birth, expire date, name, surname and identity number of the user on the identity card or passport.



```
Trying to Mine block 1...
Block Mined!!! : 0000011f3698802bd97d9829326ff5bdb0db0e66db040e06e6d38fd2ef2a6963
Trying to Mine block 2...
Block Mined!!! : 000005e1670590ee58fe1dde3cafa8deb09e1bee1b3e64eb1755dd5163cf8351

Blockchain is Valid: true

The block chain:
[
  {
    "hash": "0000011f3698802bd97d9829326ff5bdb0db0e66db040e06e6d38fd2ef2a6963",
    "previousHash": "0",
    "data": "A2[redacted]07, 931011, 29[redacted], Cagatay Kolus, 2[redacted]6",
    "timeStamp": 1580037298642,
    "nonce": 82005
  },
  {
    "hash": "000005e1670590ee58fe1dde3cafa8deb09e1bee1b3e64eb1755dd5163cf8351",
    "previousHash": "0000011f3698802bd97d9829326ff5bdb0db0e66db040e06e6d38fd2ef2a6963",
    "data": "U1[redacted]48, 931011, 28[redacted], Cagatay Kolus, 2[redacted]6",
    "timeStamp": 1580037298933,
    "nonce": 786140
  }
]
```

Figure 8. Adding Identities to Blockchain

4. ANALYSIS AND INTERPRETATION OF RESULTS

Thanks to the developed Android application, the identity of the user has been transferred to the digital environment and added as a block to the blockchain. Apart from the sample in practice, the process of transferring the identity information of 10 people to digital media and adding it to the block chain was carried out. After adding to the block chain, hash value is obtained for each block. In order to test the blockchain, a single letter change was made in the identity information of the third person and the addition to the blockchain was performed. As can be seen in table 1, the hash values of the changed blocks are calculated differently for the 3rd and later blocks. Thus, the verification process of the blockchain cannot be performed, since there will be a calculation error in the third and other identities of the blockchain.

Table 1. Comparison of Hash Values of Changed and Unchanged Blockchains

Block No	Normal Block Chain Hash Values	Block Chain Hash Values Changed From the Third Block
1	0000077af07e0bda54efbabba183924c1 b30ca6ee6f72d97701434631ca7e124	0000077af07e0bda54efbabba183924c1 b30ca6ee6f72d97701434631ca7e124
2	00000c81dc0495cfcc1691cd31a7aab06c b45c3aa66c478e9d72890e0c594553	00000c81dc0495cfcc1691cd31a7aab06c b45c3aa66c478e9d72890e0c594553
3	0000083733fe16eb623866ca9c2d34104 a6d5716c1d6c96cfef0b7f208f41722	0000010531512d2eeebabb8399dddaf99d acf8e00d7af1d391be614cb3b3c158
4	0000016ecc95ffbb6a4fb4663ab98841a5 aab3afb6a4fa09d30517f843937563	00000e391ae8758d09cfe4c446c01b455ac c0cdbc3dbb6432ca7ff6d3a417c46
5	00000cff350470ded60d17a699e7b022d a3e1323a07588684735bb38f255b29d	00000cdae6e456e9bd43aecc43949abcaf0 e17281a2e983adc18f7e6c234b5d7
6	000008507881138595f39f8add8cdf0e656 4e6acc8e37bdab443ab5855dfbbd04	00000c051132350fe4c84c99b34dea5286c 35c5c5bff88585e31539859e2510b
7	00000da807c07688ee90a2b742b818c66 84c7702eddae3935b40d1d9c4752a79	00000cda6581c4345be14756257d6acad73 ec6a39cff770c92b4cab45e9af45c
8	00000431b25f44b24c0c2d4dc67ec33112 491d17e989f2ec8abc07fb09a5608b	00000f8d8805c5883f28e150f1c8afe200eb 80344f4f56296db98c2583c91cbc
9	00000fa2e3dcb4e27438b7d8bc5b26ec8c 7620aa8c9ee32c8183a9caa5ecc778	0000011dbc1c4749afa60d3f5d12e0dd358a 0a534fdc494c6963caf707645e9a
10	00000ccd87b6238b9075edf59833360ada 7ec05026097f460d718c7212f09d0f	00000e169e4539ad17dd2d1821c99da1ce3 27723801f7c6efa4b1b37454119a9

5. RESULT

In this study; An Android application that reads data from NFC has been developed and software that can simulate blockchain technology has been created. Thus, the process of adding the data in the ID card or passport to the block chain by reading the data with the help of the Android application using NFC technology.

In addition, the identity information of 10 people was transferred to digital media and the information of each person was added to the block chain as blocks. The effects of a change made in the 3rd block of the block chain on the block chain were tried to be tested. Since it affects the hash values of the blockchain in the 3rd block and the block that will be produced later, it has broken the accuracy of the blockchain.

As a result, digital identity management can be performed securely thanks to the features provided by the blockchain such as distributed database called DLT, peer-to-peer transmission, transparency and irreversible records.

6. REFERENCES

[1] Fearon, J. D., 1999, What is identity (as we now use the word). *Unpublished manuscript, Stanford University, Stanford, Calif*.

[2] Bennett, C. J., and Lyon, D., 2013, *Playing the identity card: surveillance, security and identification in global perspective*, Routledge.

[3] Lyon, D., 2009, *Identifying citizens: ID cards as surveillance*, Polity.

[4] Zheng, Z., Xie, S., Dai, H. N. and Wang, H., 2016, Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 1, 1-25.

[5] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system [online], *www.bitcoin.org*, 1-9 [Visit Date: 01 January 2020].

[6] Michael, J., Cohn, A. and Butcher, J. R., 2018, Blockchain Technology, *www.steptoe.com*, 1-11.

[7] Lamport, L., Shostak, R. and Pease, M., 1982, The Byzantine generals problem, *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382-401.