SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 3, NO. 3, DECEMBER 2020
DOI: 10.35377/saucis.03.03.757459

Design and Implementation of Blockchain Based Single Sign-On Authentication System for Web Applications

Mustafa Tanrıverdi[1]
[1]Gazi University; mustafatanriverdi@gazi.edu.tr; +90 312 2022200

Received 24 June 2020; Revised 9 December 2020; Accepted 12 December 2020; Published online 30 December 2020

Abstract

Today, many services are provided through web applications and the number of these applications is increasing rapidly. Nowadays, most users use their username and password to login to web applications. Many of these users also use the same login information in different applications. This causes a major security vulnerability for applications and users. As a solution to these weaknesses in the field of authentication, there have been many developments in recent years. Some of these studies have been third party identity authentication systems like Google and Facebook. Since this method also contains potential risks, studies have been conducted on the Two-Factor Authentication (2FA) method for more security. In parallel with the innovations that emerge every day, methods should be used in the field of authentication. In these times, blockchain technology offers solutions that make life easier in many areas thanks to its distributed, transparent, secure and immutable structure. In this study, blockchain based single sign-on (SSO) authentication system was developed and implemented for web applications. In this system, a public address and a private key are defined on the private blockchain network for users and this information is used for the 2FA method through the developed mobile application. Detailed information was given about the proposed system and technologies used in the study.

Keywords: blockchain, identity authentication, two-factor authentication (2FA), single sign-on (SSO), software development

1. Introduction

With the rapid development of internet technologies, many applications and services have started to serve on the web platform. Users can sign up for many applications and login to them with their own username and password. Users usually reuse the same credentials in order to login different applications and two-thirds of them since it is easy to memorize [1]. Although this situation provides great convenience to users, it poses a potential security risk for them and web applications as well. If an identity authentication mechanism can be implemented to be used by different applications together rather than being used by each application separately, each application does not need to manage own authentication task. This provides great convenience for both applications and users [2].

Identity authentication, which refers to authenticating user's real identity on the internet, plays an important role in protecting information security [3]. Thanks to recent advances, users can access to applications through third party identity authentication systems such as Google and Facebook. These centralized solutions have serious problems such as security challenges, single point of failure and poor transparency. Moreover, traditional authentication applications, like ones in which only username and password are used, have become open to threats today. One of the most appropriate solutions may be applied against to these threats is to use 2FA methods. To overcome these challenges, a blockchain-based SSO authentication system has been developed for web applications. Distributed, transparent, secure and immutable network of the blockchain has been utilized to effectively manage technologies such as SSO and 2FA.

In this study, a private blockchain system was established with the MultiChain [4] and a node was defined for each web application. It was aimed for users to be able to securely login to applications in the blockchain network with a single account without need for any third party verifier. Since each node in private blockchain is considered reliable, one node can safely access the data of the other nodes. Thanks to this feature of the blockchain, it was possible to provide SSO authentication for users for multiple applications.

In the private blockchain network, each user can create a public address and private key. At the time of creation, the private key is displayed to the user as QR code. At this stage, users can pair their private keys with the developed mobile application and then use these keys for 2FA through the mobile application. Considering the combination of these new and popular technologies and the shortcomings of similar studies in the literature, it can be said that this study is unique.

The remaining sections of this paper explain the following. Section II summarizes research related to the blockchain technology, identity authentication, MultiChain and 2FA. Section III describes the proposed blockchain based SSO authentication system for web applications.

2. Background and Related Works

2.1 Blockchain

For the first time, blockchain technology, which has become known and popular thanks to cyrpto currencies, has recently received great attention from various international organizations, industries and institutions. The number of blockchain-based solutions has increased rapidly in many different domains in recent years. Thanks to its solutions and features, blockchain has even been expressed by some researchers as more powerful technology than the Internet [5]. In the report published by Allied Market Research, it was stated that the blockchain market was $228 million in 2016 and could reach $5.4 billion by 2023 [6]. According to Nakamoto, the blockchain is a distributed data structure in which each transaction information is recorded and shared by the participants in the network [7]. Reyna et al. defined the blockchain as a distributed, transparent, unchangeable and secure data structure where the stakeholders in the network verify the reliability of transactions [8]. There are many similar blockchain definitions in the literature, from a technical point of view, it would be correct to define blockchain as a combination of decentralization mechanism and also a combination of cryptographic algorithms and distributed databases [9]. According to Zhao et al, the most important feature of Blockchain is the support of reliable and transparent operations through network-based calculations rather than people's monitoring or controlling [10]. The advantages of the blockchain can be listed as follows [11].

- A copy of the data is recorded by all stakeholders and everyone can access the data transactions. Data loss and destruction are prevented by this way.
- Thanks to digital signatures and verifications, it is ensured that the stakeholders can trust each other without any need for third party agents.
- Everyone is able to see the status of its transactions as well as the details of all transactions in the blockchain which ensures transparency.
- The data on the blockchain cannot be changed or deleted.
- It can work without a central authority and it cannot be controlled, canceled or closed by its distributed structure.

The existing blockchain systems are classified into three categories as public, private and consortium blockchain. Public blockchain offers an open platform that allows everyone to participate, write and mine. These blockchain systems do not have any restrictions and also referred as unauthorized blockchain. Private blockchain, which is managed by a person or a group, provides sharing and data exchange between one or several organizations. Consortium blockchain can be defined as a partially private and permissible blockchain where a predetermined set of nodes take the place of a single organization in verification and consensus processes [9].

2.2 MultiChain

Because of the advantages of the support of such an API for many programming languages, ease of use, performance and documentation, it has been influential in our choice of MultiChain as a blockchain application. MultiChain is a private blockchain protocol that manages the access to data using a list of registered participants [4]. Only registered participants have access to read and write blocks in the chain. The consensus method used by MultiChain is the Round Robin (RR) scheduling algorithm. The RR algorithm states that each block must have a signature from the participant who intends to create it. Adding multiple assets issuance and data streams (key-value databases) are provided by MultiChain. Data streams can be considered as a database like NoSQL with separate permissions isolated from the entire blockchain. A small piece of text or 64 MB binary data can be stored on the data stream [12].

2.3 Two Factor Authentication

Traditional single-factor authentication such as ‘‘username + password’’ has been used widely because it is easy to deploy without additional devices. However, this method is vulnerable to dictionary, snooping and brute force attacks [13]. This traditional method was effective when the internet and web applications were not widespread as current. Nowadays, it is possible to access passwords of users with the help of trojans' ability to monitor the keyboard or network attacks. As a solution, 2FA methods have been widely used with high security requirements in recent years [14]. In addition to text data such as password or code, 2FA also uses encrypted data created instantly via smart cards or mobile phones. Users need to verify this code or encrypted information in a very short time with hardware support. Google Authenticator [15] and LastPass [16] are examples of commonly used 2FA applications.

2.4 Blockchain Based Identity Authentication

Today, many services are provided via the internet and identity authentication is very important for service providers. As known, there are many problems in the current identity management systems. For example, many service providers are dependent on third party authentication providers that have been used in recent years and these providers can access user information and services. However, it may be exposed to various network attacks regardless of being a third-party authorized login or a traditional login with username and password, [17]. To overcome these problems, if blockchain is used for identity authentication, the following facilities can be provided.

- Thanks to the decentralized feature of the blockchain, service providers do not require any trusted central authority.
- The data on the blockchain is tamper-proof, which also prevents some illegal activities.
- If the service providers are allowed to participate in a private blockchain with permissions, users can access these services with a single account. This makes account management easier and more effective for users.
- Thanks to the public - private key features in the blockchain, users can send their identity information by encrypting it with their own private key instead of sending it directly to service providers.

The authentication technology based on blockchain has been a topic that has been studied by researchers in recent years [1], [18]. For the first time in 2014, Conner et al. proposed a blockchain public key infrastructure (PKI) system called Certcoin to solve some security problems [19]. Due to the transparent structure of blockchain, there were problems with user privacy in this solution. Then a privacy-awareness blockchain PKI, which achieve user anonymity through short term online public keys, was designed by Axon and Goldsmith [20]. In this study, storage and efficiency were neglected while user privacy was ensured. In the following years, the development of blockchain technology, improvements in performance and storage problems and the use of smart contracts made a significant contribution to the authentication process.

When the literature is analyzed, many blockchain-based authentication and authorization studies for Internet of Things(IoT) devices can be seen. The studies conducted by Jiang et al. [18] and Khalid et al. [21] can be given as an example to these studies. The number of studies conducted for web applications in this field is limited. One of the few current studies in this area was presented by Ezawa et al. in 2019. In this study, it is ensured that identity authentication is performed more securely using blockchain-based PKI structure and smart contracts through a verification and authorization server [2]. In this study, the web user needs to enter information such as public key certificate, random number and signature on the login screen, which can be considered extremely inappropriate for data security and ease of use.

Xiong et al. proposed a privacy-awareness authentication system for the multi-server environment in order to prevent single-point failure problem due to the centralized architecture [1]. The offered system provides a defence against various kinds of malicious attacks besides multiple security requirements like mutual authentication and user anonymity. The solution proposed in this study is a theoretical framework without applying to any specific scenario. An Ethereum-Based Cloud User Identity Management Protocol has been developed by Wang et al. [17]. In this study, the web user must write key data and encrypted hash values on the login screen, which is also followed in the study conducted by Xiong et al [1]. Patel et al. also designed a decentralized web authentication system using Ethereum based blockchain system prototype called DAuth [22]. In this study, users' private keys and smart contracts were used to ensure security and confidentiality. This study also has limitations in terms of usage for web users in daily life.

As mentioned in the introduction section, web users generally use many differnet applications today. It may cause problems for users to use separate accounts for each application or to login via third-party systems. To overcome this problem, researchers and companies have conducted studies involving different SSO solutions. Within the scope of the proposed system, an effective SSO can be presented by using the private blockchain created for the applications of an organization. A limited number of studies on blockchain-based SSO were found when the literature was scanned [23], [24]. These are also theoretical studies with suggestions.

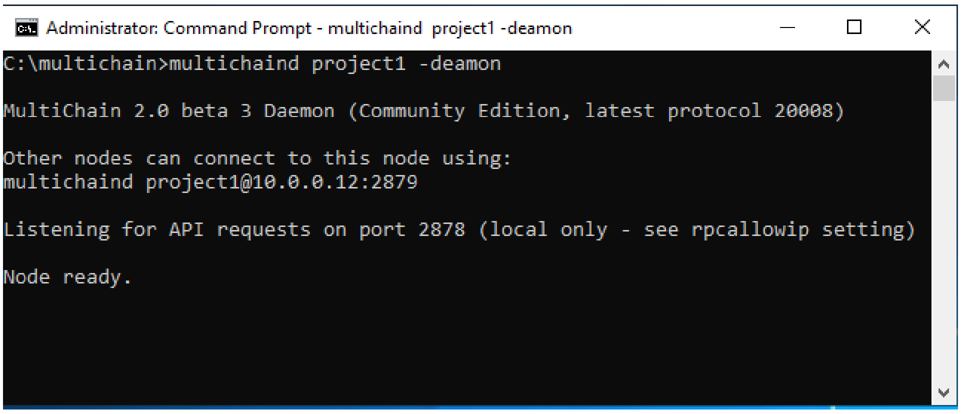
3. Implementation of Proposed System

This section provides detailed information about the developed blockchain based SSO authentication system for web applications. New and popular internet technologies such as blockchain, 2FA and SSO have been used in this system. In the design phase of the proposed system, these technologies were considered as modules and developed step by step. This progressive method has also been applied in the processes of the system's implementation. Therefore, it will be more understandable to give detailed information about the modules during the implementation stages. Information about these stages is given below.

3.1 Installation of Private Blockchain

One authenticator server named S0 and three web servers named S1, S2, S3 were used in the experimental environment. These servers running Windows 10 as the operating system have Intel Xeon 2.00 GHz processor and 8 GB memory. Food Ordering System, Student Information System and Online Petshop System were established on web servers. these applications were selected from the projects offered by Itsourcecode as open source [25].

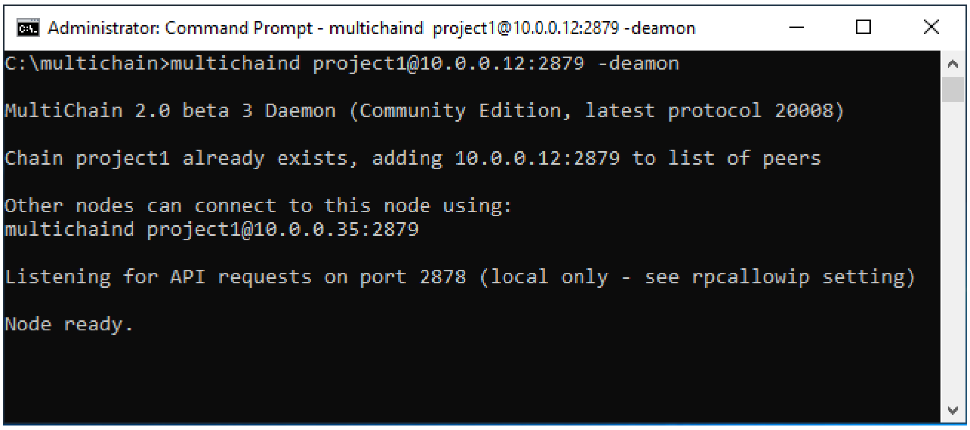
At first, as shown in Figure 1, a chain named project1 was created and published on the S0 server. As shown in the figure, the chain named project1 runs on port 2879 on server S0 with ip address 10.0.0.12.


Administrator: Command Prompt - multichaind project1 -deamon

```
C:\multichain>multichaind project1 -deamon

MultiChain 2.0 beta 3 Daemon (Community Edition, latest protocol 20008)

Other nodes can connect to this node using:
multichaind project1@10.0.0.12:2879

Listening for API requests on port 2878 (local only - see rpcallowip setting)

Node ready.
```

Figure1 Creating a chain with MultiChain

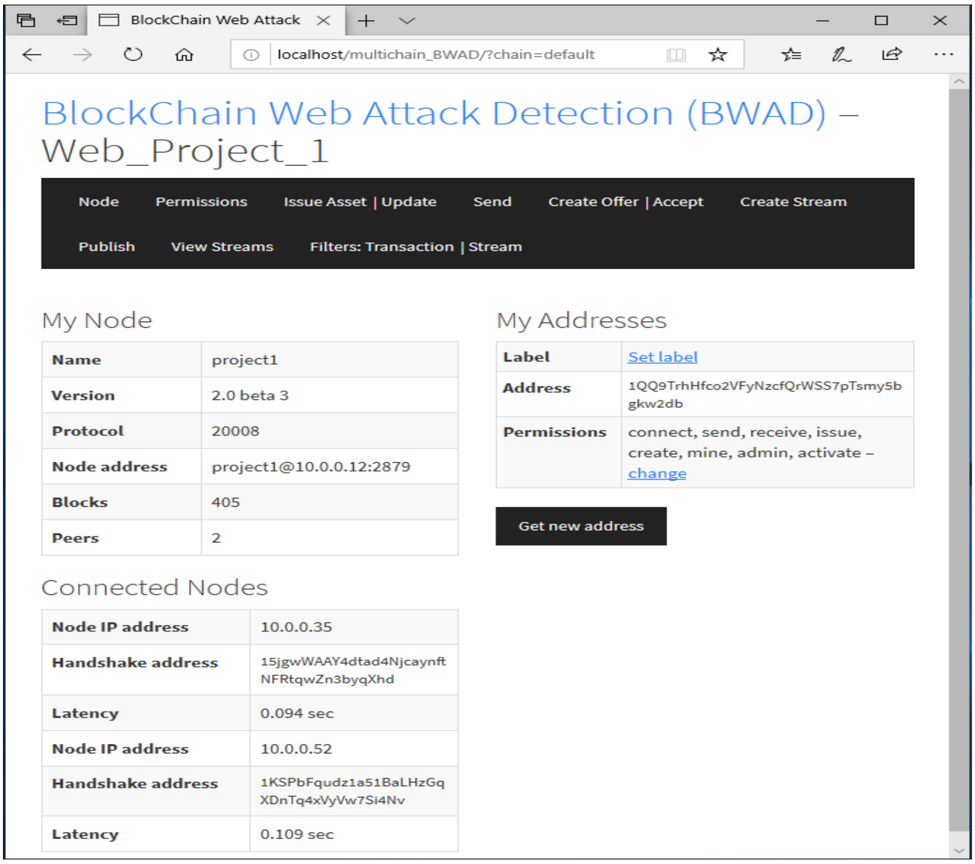
In the structure of MultiChain, it is necessary to authorize other nodes to connect, read and write in the chain. After the necessary permissions are granted in MultiChain and the firewall definitions are set for the IP addresses and port numbers are defined, nodes can connect to the chain. Figure 2 shows the connection status of the S1 server with the 10.0.0.35 ip address to the MultiChain created in S0 server with 10.0.0.12:2879 ip address and port. S2 and S3 servers are also connected in a similar way to the project1 chain.


Administrator: Command Prompt - multichaind project1@10.0.0.12:2879 -deamon

```
C:\multichain>multichaind project1@10.0.0.12:2879 -deamon

MultiChain 2.0 beta 3 Daemon (Community Edition, latest protocol 20008)

Chain project1 already exists, adding 10.0.0.12:2879 to list of peers

Other nodes can connect to this node using:
multichaind project1@10.0.0.35:2879

Listening for API requests on port 2878 (local only - see rpcallowip setting)

Node ready.
```

Figure 2 Connection the node to chain

The MultiChain Explorer application, which enables web-based browsing of blockchain activities, is presented to the developers by MultiChain. MultiChain Explorer application was installed on the servers and blockchain activities could be monitored instantly. Figure 3 shows a screenshot of the MultiChain Explorer web page, which indicates that the three nodes are participating in the chain named project1. As seen in the figüre 3, the chain named project1 was started by the S0 with the ip address 10.0.0.12 and port 2879. Then the nodes with the IP addresses 10.0.0.35 and 10.0.0.52 are connected to this chain.



BlockChain Web Attack Detection (BWAD) – Web_Project_1

My Node

Name	project1
Version	2.0 beta 3
Protocol	20008
Node address	project1@10.0.0.12:2879
Blocks	405
Peers	2

My Addresses

Label	Set label
Address	1QQ9TrhHfco2VFyNzcfQrWSS7pTsmy5bgkw2db
Permissions	connect, send, receive, issue, create, mine, admin, activate – change

Connected Nodes

Node IP address	10.0.0.35
Handshake address	15jgwWAAY4dtad4NjcaynftNFRtqwZn3byqXhd
Latency	0.094 sec
Node IP address	10.0.0.52
Handshake address	1KSPbFqudz1a51BaLHzGqXDnTq4xVyVw7Si4Nv
Latency	0.109 sec

Figure 3 Screenshot of the MultiChain Explorer application

Thanks to the private blockchain established through MultiChain, a distributed data sharing environment has been established for one authenticator server and three web servers. The block diagram of this private blockchain is presented in Figure 4.

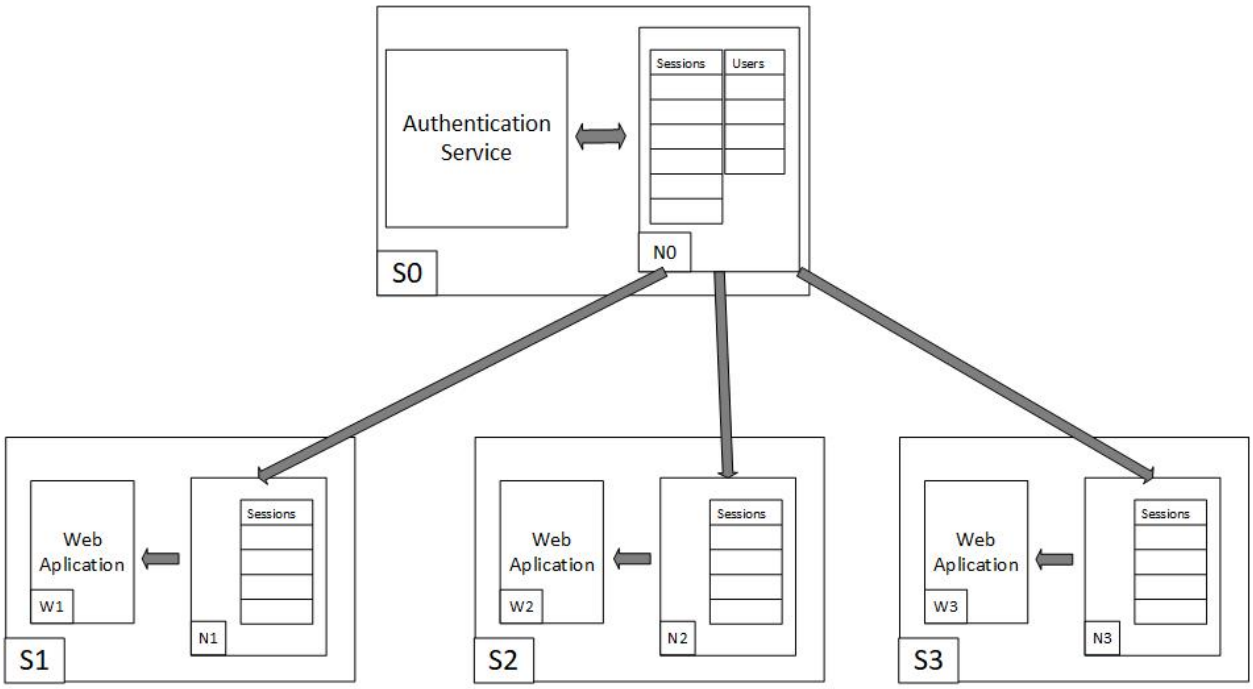


Figure 4 Block diagram of the private chain

S1, S2 and S3 servers have W1, W2 and W3 web applications and N1, N2, N3 nodes. The S0 server has a N0 node and authentication service.

3.2 Setting Up Data Streams, Permissions and Connections on Blockchain

In this system, json or text data is stored in different streams on the blockchain. It should be possible to define which servers can access to this data with which permissions (read or write). The data stream feature of the MultiChain is suitable for this purpose in terms of performance and data storage structure. As seen in figure 4, there are two data streams called sessions and users in the node of the authentication server S0. The web servers S1, S2 and S3 have only sessions data stream in their nodes. Username, password, and public key data of users are stored in the data streamwhich is called users. Username, generated encrypted value and time data of users who complete the authentication process are stored in sessions data stream. With this structure, it is aimed that the users can authenticate only through the authentication service in S0. Then, the data of the user whose authentication process is completed is recorded in the data stream called session. For this, users data stream is only available on the N0 node. For session data stream, N0 node is allowed to read and write while N1, N2 and N3 nodes are only allowed to read. In previous sections, the use of central solutions such as Google and Facebook for authentication has been noted to risk of single point of failure. In this system, S0_2 server, which is an exact copy of S0 server is created and included in the chain in order to avoid single point error. In this way, the authentication service will be ready to be activated and a copy of the data streams will be created.

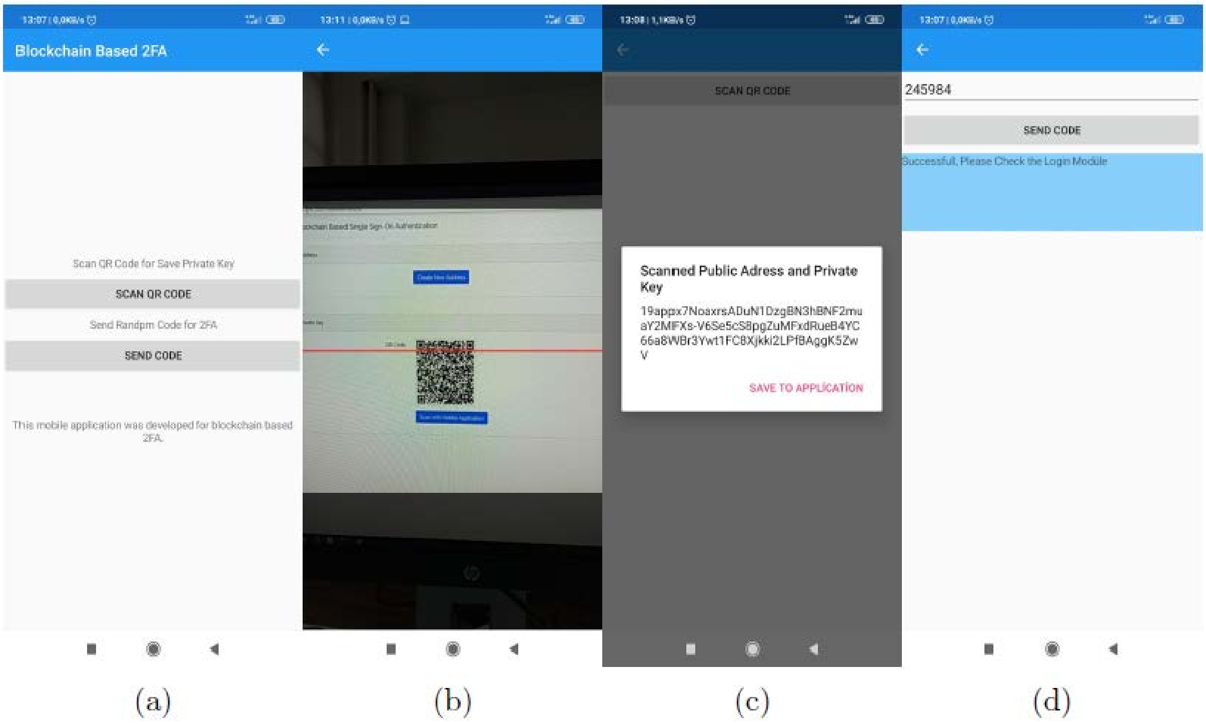
The authenticator service in S0 and W1, W2 and W3 web applications have been developed with PHP programming language. These applications can access the nodes on their servers through the PHP APIs provided by MultiChain. Through this API, applications can handle operations such as adding data to the data stream, reading data from the data stream, creating a public address and accessing the private key of a public address.

3.3 Mobile Application

Due to the security vulnerabilities of the traditional authentication method with username and password, a mobile application has been developed to provide users with 2FA possibilities. This mobile application has been developed with the Xamarin framework [26], which offers advanced features such as base libraries and multi-platform application development. The purpose of this application is to ensure that the user can safely store his private key and use it in the authentication process.

After the user logs in to the authentication service with the user name and password, he is be able to define a public address and access the QR code containing this address and private key data generated by the blockchain. The user is be able to match the public address and private key data to the mobile application by scanning the QR code seen on the screen into the mobile application. The user may renew his public address and private key data for reasons such as phone change or security concerns. To do so, the user must click on the "Create new address" via the mobile app and delete the old key data and define new the key and address data to the mobile application via the QR code generated by the authentication service.

In order to provide 2FA, a randomly generated code is displayed on the screen to the web user who entered his username and password correctly at the authentication stage. Then, the user is expected to encrypt this code with the private key via the mobile application and send it to the authentication service. If the encrypted data sent and the data created in the service match, the user is allowed to login the system. Figure 5a shows a screenshot of mainpage of mobile application. Figure 5b and 5c show screenshots of the mobile application for matching address and private key information. Figure 5d shows the use of the mobile application in 2FA.



This mobile application was developed for blockchain based 2FA.

Scanned Public Adress and Private Key

19appx7NoaxrsADuN1DzgBN3hBNF2muaY2MFXs-V6Se5cS8pgZuMFxdRueB4YC66a8WBr3Ywt1FC8XjkkI2LPfBAggK5ZwV

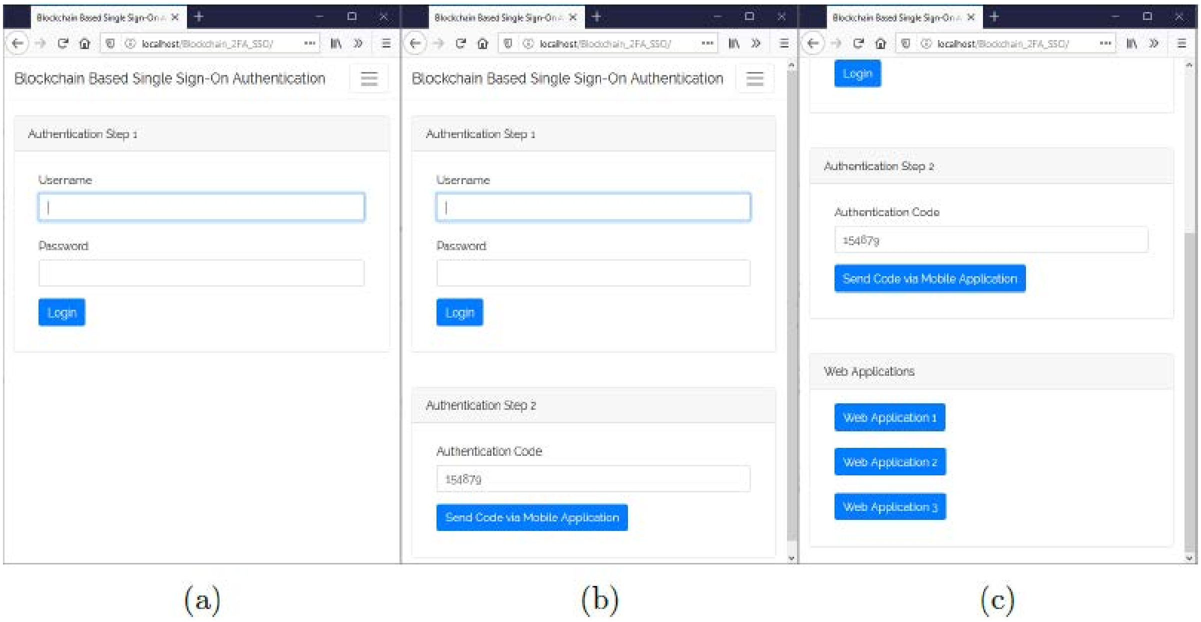
245984

Successful, Please Check the Login Module

Figure 5 Screenshots of mobile application

3.4 Identity Authentication

The login module has been developed to provide users with ease of SSO and security through 2FA. Web users use this login module and mobile application together for identity authentication. The screenshots of the login module are given in Figure 6.



(a)

Blockchain Based Single Sign-On Authentication

Authentication Step 1

Username

Password

(b)

Blockchain Based Single Sign-On Authentication

Authentication Step 1

Username

Password

Authentication Step 2

Authentication Code

154879

(c)

Authentication Step 2

Authentication Code

154879

Web Applications

Blockchain Based Single Sign-On A
localhost/Blockchain_2FA_SSO/
Login
Send Code via Mobile Application
Web Application 1
Web Application 2
Web Application 3

Figure 6 Screenshots of login module

This section provides information about a blockchain-based identity authentication that includes 2FA and SSO technologies. While developing this system, the data streams defined in blockchain, APIs of the MultiChain, login module and the mobile application developed were used. Figure 7 shows the general structure of the proposed system.

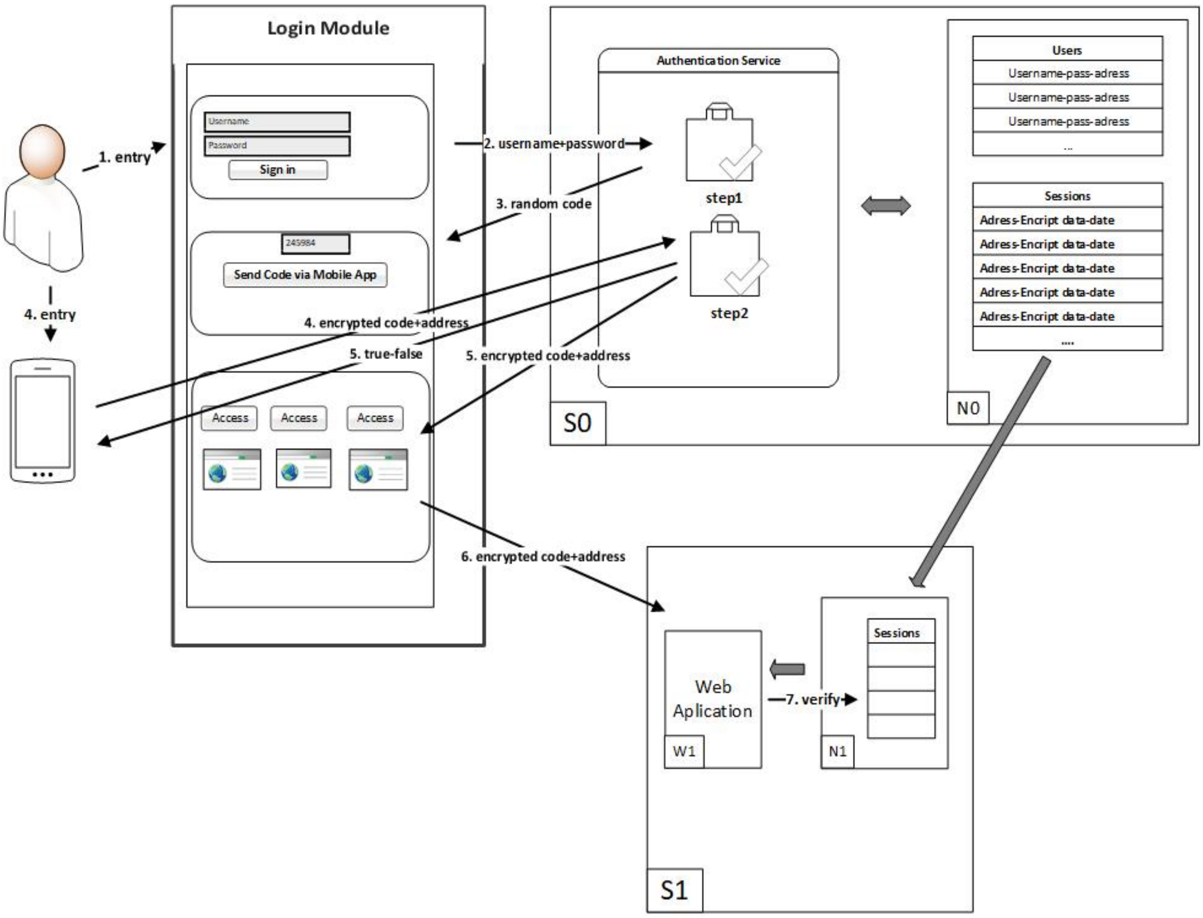


Figure 7 Blockchain-based identity authentication

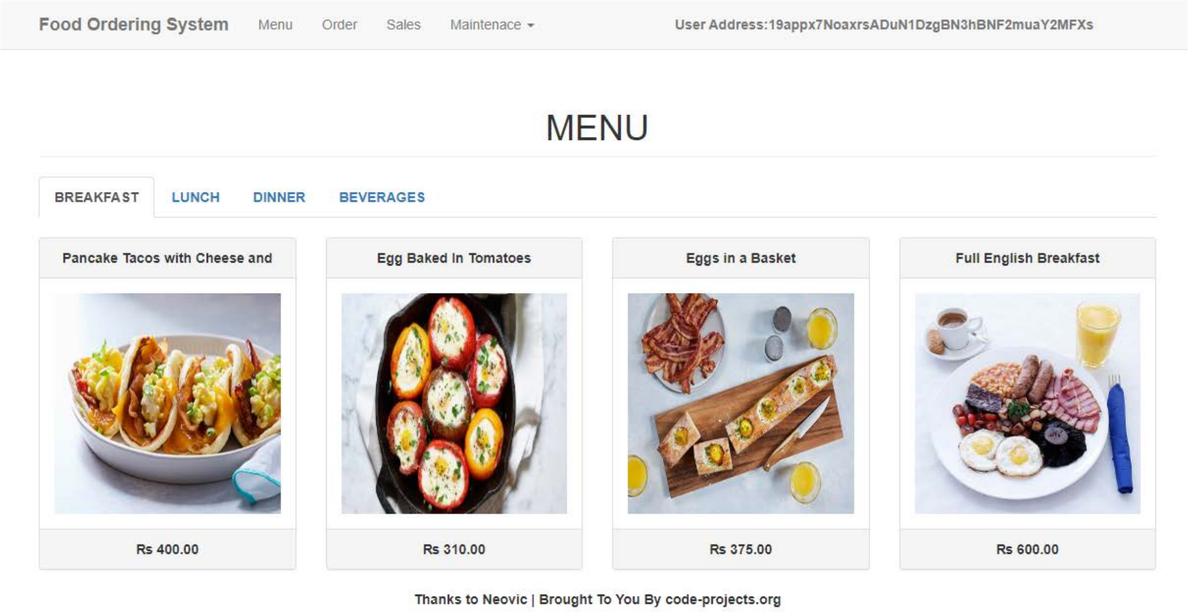
The steps to be followed for identity authentication are given in Figure 7. Information about these steps is given below.

1) **Login with username and password:** In this step, the user enters the username and password in the login module as shown in figure 6a. At this stage, users' information is manually added to web applications and then transferred to the blockchain.
2) **Sending username and password to the authentication service:** User-entered data is sent by the login module to the authentication service, which is also available on the S0.
3) **Validation by authentication service:** User-entered data is sent by the login module to the authentication service. The authentication service accesses the data stream called users through the MultiChain API and verifies the received username and password. If the result is correct, a 6-digit random code is returned to the login module.
4) **Sending back encrypted code:** The code sent by the service is shown to the user in the login module as shown in figure 6b. In this step, the user is expected to encrypt the code via the mobile application and return this encrypted data and public address to the authentication service. The entered code is encrypted with the “crypt” function of the PHP programming language. Meanwhile, to make encryption more complex, the user's private key previously paired in the mobile application is used as salt value. Within the scope of the authentication service, a web service is created that receives encrypted data and public address from mobile applications and returns true / false value as a result. SOAP (Simple Object Access Protocol) is used for data exchange between mobile application and authentication service. All requests to the authentication service are provided with SSL connection. Figure 5b and figure 5c show a screenshot of the mobile application to be used in this step.
5) **Verification of encrypted code:** In this step, the data encrypted with the user's private key is verified. A user who has logged into the system can create a public address for himself. This address created on blockchain also contains a private key. This private key and public address are shown to the user via QR code at the time of creation. After that, the address is mapped to the relevant user and used transparently in the blockchain network for many transactions. Public addresses and private keys are created on S0 server and this data is not shared with other nodes. This ensures that only the user and N0 node can access the private key.

   Encrypted data and public address is expected from the previous step. The authentication service can access the private key of this address via N0. The random code determined in the third step is encrypted with this private key and then this encrypted data is compared with the encrypted data sent by the mobile application. If these two data are the same, it is understood that the user sends the code correctly via the mobile application. Then, the user's public address, encrypted data and verification time are recorded in the data stream called sessions. Finally, encrypted data and public address are sent in response to the login module and mobile application.
6) **Redirection to web applications:** After receiving the positive result of 2FA from the authentication service, the user is notified via the login module as shown in figure 6c. At the bottom of the same screen, there are also links to web applications that are participating on the private network. Users will be able to access web applications thanks to these links containing encrypted data and public address received from the previous stage.
7) **Accessing web applications:** Encrypted data and public address are required to login to web applications. Web applications verify incoming encrypted data by accessing the data stream called sessions, which they have read permission in the blockchain. For this validation, a transaction is searched that matches the encrypted data in sessions stream. If a transaction is found and the time of the transaction is not older than 5 minutes (this value can be changed), the user of the public address in the relevant transaction can access the web application. Thus,

a user who login via the login module can access the web applications without having to login again and benefit from the ease of SSO.

The user who successfully completed the authentication steps can access the web applications in the chain. Figure 8 shows a screenshot of the user with the address "19appx7NoaxrsADuN1DzgBN3hBNF2muaY2MFXs" to access the food ordering system after authentication. This user is also be able to access other web applications in the private blockchain network without login again.



User Address:19appx7NoaxrsADuN1DzgBN3hBNF2muaY2MFXs

Thanks to Neovic | Brought To You By code-projects.org

Figure 8 Food ordering system

The web server hosting the food ordering system shown in Figure 8 is included in the private blockchain and read permission is given for session data stream. Thus, the encrypted code and public address transmitted to this application can be verified according to session data stream. When this verification is provided, the user associated with the public address is enabled to use the application.

4. Conclusions

In this paper, a blockchain-based SSO authentication system is designed and implemented for web applications. Detailed information about new and popular technologies such as blockchain, SSO, 2FA and identity authentication is provided. Technical information including screenshots of the combination of these technologies are given as well. There are many studies in the literature that offer identity authentication solutions with blockchain technology on IOT devices. But there are a limited number of theoretical applications for web applications. This study will be a pioneer for future studies and resolve the gap in this field. Thanks to the developed system, it is observed that SSO facilities can be offered in the private blockchain network for companies and institutions providing many web services. Recently, the 2FA method has been used through third-party applications like Google Authenticator and LastPass has been integrated with public addresses and private keys defined on the blockchain. For this integration, a mobile application has been developed that can securely store private key data. There is not such a study on this new method applied in the literature. In the future, it is aimed to work on the usage of a similar system in everyday life and monitoring its performance. In this study, MultiChain is used as the blockchain application. It will be useful to evaluate performance and effectiveness as a result of using other blockchain applications for similar purposes.

References

[1] L. Xiong, F. Li, S. Zeng, T. Peng, and Z. Liu, "A Blockchain-Based Privacy- Awareness Authentication Scheme with E_cient Revocation for Multi-Server Architectures," *IEEE Access,* vol. 7, pp. 125840-125853, 2019.

[2] Y. Ezawa et al., "Designing Authentication and Authorization System with Blockchain,*" in 2019 14th Asia Joint Conference on Information Security (AsiaJCIS),* pp. 111{118,2019.

[3] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography," *in 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET),* pp. 90{95, 2019.

[4] MultiChain | Open source blockchain platform." [Online]. Available: https://www.multichain.com/ . [Accessed: 15-Jan-2019].

[5] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing Blockchains: Characteristics and Applications," *in 11th IADIS International Conference on Information Systems,* pp. 49{57, 2018.

[6] Blockchain Distributed Ledger Market Size by Type, End-User," Allied Market Research Report, 2017. [Online]. Available: https://www.alliedmarketresearch.com/blockchain-distributed-ledger-market. [Accessed: 14-Nov-2018].

[7] S. Nakamoto, \Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986. [Accessed: 08-Nov-2018].

[8] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems,* vol. 88, pp. 173-190, 2018.

[9] M. Tanriverdi and A. Tekerek, "Implementation of Blockchain Based Distributed Web Attack Detection Application," *in 1st International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation, IISEC 2019 - Proceedings,* 2019.

[10] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financial Innovation*, vol. 2, no. 1-28, 2016.

[11] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question," *IT Prof.,* vol. 20, no. 2, pp. 62-74, Mar. 2018.

[12] MultiChain data streams | MultiChain." [Online]. Available: https://www.multichain.com/developers/data-streams/. [Accessed: 10-Mar-2020].

[13] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication," *IEEE Access,* vol. 6, pp. 32677-32686, Jun. 2018.

[14] B. S. Archana, A. Chandrashekar, A. G. Bangi, B. M. Sanjana, and S. Akram, “Survey on usable and secure two-factor authentication," *in RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings,* vol. 2018-January, pp. 842-846, 2017.

[15] Google 2FA." [Online]. Available: https://www.google.com/landing/2step/. [Accessed: 05-Mar-2020].

[16] LastPass - LastPass Authenticator." [Online]. Available:https://lastpass.com/auth/. [Accessed: 05-Mar-2020].

[17] S. Wang, R. Pei, and Y. Zhang, “EIDM: A Ethereum-Based Cloud User Identity Management Protocol," *IEEE Access*, vol. 7, pp. 115281-115291, Aug. 2019.

[18] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, “PTAS: Privacy- preserving Thin-client Authentication Scheme in blockchain-based PKI," *Future Generation Computer Systems*, vol. 96, pp. 185-195, Jul. 2019.

[19] C. Fromknecht and S. Yakoubov, “CertCoin: A NameCoin Based Decentralized Authentication System 6.857 Class Project," 2014.

[20] L. Axon and M. Goldsmith, “PB-PKI: A privacy-aware blockchain-based PKI," *in ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, vol. 4, pp. 311-318, 2017.

[21] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Ra_erty, “A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, pp. 1-21, Feb. 2020.

[22] S. Patel, A. Sahoo, B. K. Mohanta, S. S. Panda, and D. Jena, “DAuth:A Decentralized Web Authentication System using Ethereum based Blockchain," *in Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, 2019.

[23] A. Bakre and N. Patil, “Implementing Decentralized Digital Identity using Blockchain," *International Journal of Engineering Technology Science and Research*, vol. 4, pp. 379-385, 2017.

[24] H. Arslan and H. Aslan, “Blockchain based single sign-on support for IoT environments," *in 27th Signal Processing and Communications Applications Conference, SIU2019*, 2019.

[25] Best PHP Projects With Source Code Free Download [2020] Ideas,Video." [Online]. Available: https://itsourcecode.com/free-projects/php-project/php-projects-source-code-free-downloads/. [Accessed: 30-Mar-2020].

[26] Xamarin | Open-source mobile app platform for .NET." [Online].Available https://dotnet.microsoft.com/apps/xamarin. [Accessed: 01-Apr-2020].