gazi JOURNAL OF ENGINEERING SCIENCES

Gazi AKADEMİK YAYINCILIK

GAZİ
JOURNAL OF ENGINEERING SCIENCES

Blockchain-Based Secure Authentication Solution for Web Applications

Mustafa Tanrıverdi*

Submitted: 18.10.2023 Revised: 17.11.2023 Accepted: 08.12.2023 doi:10.30855/gmbd.0705081

Keywords: Blockchain, security, authentication, web application, Web3, ethereum, MetaMask

* Gazi University,
Faculty Of Applied Sciences,
Management Information Systems
06560 - Ankara, Türkiye
Orcid: 0000-0003-3710-4965
e mail: mustafatanriverdi@gazi.edu.tr

*Corresponding author:
mustafatanriverdi@gazi.edu.tr

ABSTRACT

In the age of information and technology, web applications have become an important part of daily life. The communication of these web applications, where important personal and corporate information is managed, with the outside world is provided by authentication methods. Today, most applications use the traditional username-password method for authentication. This method, which is vulnerable to brute force attacks, causes serious security vulnerabilities. In this method, since most users use the same login credentials in different applications, an attack can affect many applications. Some applications also prefer to rely on third-party systems such as Google and Facebook for authentication. Due to their nature, these systems have risks such as data security problems and single point failure. For more security in the authentication area, studies have been carried out on the Two-Factor Authentication (2FA) method This method has serious disadvantages such as GSM network problems, SMS cost or centralization. To overcome these problems, blockchain is appropriate solution thanks to its distributed, transparent, secure and immutable structure. In an important and sensitive issue such as identity control, it is thought that it may be risky to present blockchain technology, which is still under development, as the only method. Considering the current situation, in this study, a proposal has been made to offer a secure blockchain-based solution as an alternative to the authentication methods that currently work for web applications. The new technologies and tools used in the proposed solution are explained with visuals.

Web Uygulamaları için Blokzinciri Tabanlı Güvenli bir Kimlik Doğrulama Çözümü

ÖZ

İçinde bulunduğumuz bilgi ve teknoloji çağında web uygulamaları günlük yaşamının önemli bir parçası haline gelmiştir. Önemli kişisel ve kurumsal bilgilerin yönetildiği bu web uygulamalarının dış dünya ile irtibatı kimlik doğrulama yöntemleri ile sağlanmaktadır. Günümüzde çoğu uygulama kimlik doğrulama için geleneksel kullanıcı adı-şifre yöntemini kullanmaktadır. Kaba Kuvvet (Brute force) saldırılarına karşı savunmasız olan bu yöntem ciddi güvenlik açıklarına neden olmaktadır. Bu yöntemde çoğu kullanıcı aynı giriş bilgilerini farklı uygulamalarda kullandığından dolayı bir saldırı birçok uygulamayı etkileyebilmektedir. Bazı uygulamalar da kimlik doğrulaması için Google ve Facebook gibi üçüncü taraf sistemlere güvenmeyi tercih etmektedir. Bu sistemler de veri güvenliği ve tek nokta hatası gibi nedenlerden dolayı riskler barındırmaktadır. Kimlik doğrulama alanındaki daha fazla güvenlik için iki Faktörlü Kimlik Doğrulama (2FA) yöntemi üzerinde çalışmalar yapılmıştır. Bu yöntemin de GSM şebeke problemleri, SMS maliyeti, merkezi yapılara bağımlılığı gibi sorunları bulunmaktadır. Bu yaşanan sorunların üstesinden gelmek için blockchain, dağıtık, şeffaf, güvenli ve değişmez yapısı sayesinde uygun bir çözüm olarak karşımıza çıkmaktadır. Kimlik doğrulama gibi önemli ve hassas bir konuda henüz gelişimi devam eden blokzinciri teknolojisini tek yöntemin olarak sunulmasının da riskli olabileceği düşünülmüştür. Mevcut durum değerlendirildiğinde bu çalışmada halihazırda hizmet veren web uygulamaları için çalışan kimlik doğrulama yöntemlerine ek olarak blokzinciri tabanlı güvenli bir çözümün alternatif olarak sunulmasına ilişkin bir öneride bulunulmuştur. Önerilen çözümde kullanılan yeni teknoloji ve araçlar görsellerle desteklenerek açıklanmıştır.

Anahtar Kelimeler: Blokzinciri, güvenlik, kimlik doğrulama, web uygulaması, Web3, ethereum, MetaMask

To cite this article: M. Tanriverdi, “Blockchain-based secure authentication solution for web applications,” *Gazi Journal of Engineering Sciences,* vol. 9, no. 3, pp. 477-489, 2023. doi:10.30855/gmbd.0705081

1. Introduction

The Internet has grown quickly, and as a result, many uses, including online payments, smart homes, online commerce, online public affairs, etc., have become essential to people's everyday lives [1]. However, at the same time, the complexity and vulnerabilities of the Internet bring along several security concerns and people pay close attention to information security [2]. Today, many services are provided through web applications. Most of the information transmitted and stored through web applications that provide these many services contains personal, commercial and even confidential information of the state and will be targeted by hackers in the future as in the past [3]. For this reason, authentication, which refers to the verification of the User's identity on the Internet, plays an important role in protecting information security [4].

Authentication of users is usually provided by their own usernames and passwords. Users often use multiple applications, and two-thirds of these users reuse the same IDs and passwords for easier memorization [5]. Although this situation provides great convenience to users, it poses a potential security risk for both them and web applications. Authentication with username and password is the simplest and easiest method to implement, but it is not resistant to replay attacks [6]. This method is especially vulnerable to brute force attacks and user passwords can be captured by hackers. Simple passwords created by users also increase the probability of success of these attacks. The security of the SMS verification method via mobile phone is also relatively high, but SMS may not be received when the network signal is not good, which may cause users to wait. In addition, the cost of SMS verification method is relatively high [3]. Thanks to the developments in recent years, many applications can be accessed via third party authentication platforms like Google and Facebook, as depicted in Figure 1. These centralised solutions have serious problems such as privacy, security issues, single point of failure and poor transparency. Moreover, with these authentication methods where only username and password are used, web applications have become more vulnerable to threats [7]. Lightweight Directory Access Protocol (LDAP) provides a high level of security, single sign-on (SSO) and ease of use for users by managing user information in a central directory [8]. However, single point of failure problems encountered in this method cause access to applications to stop completely.

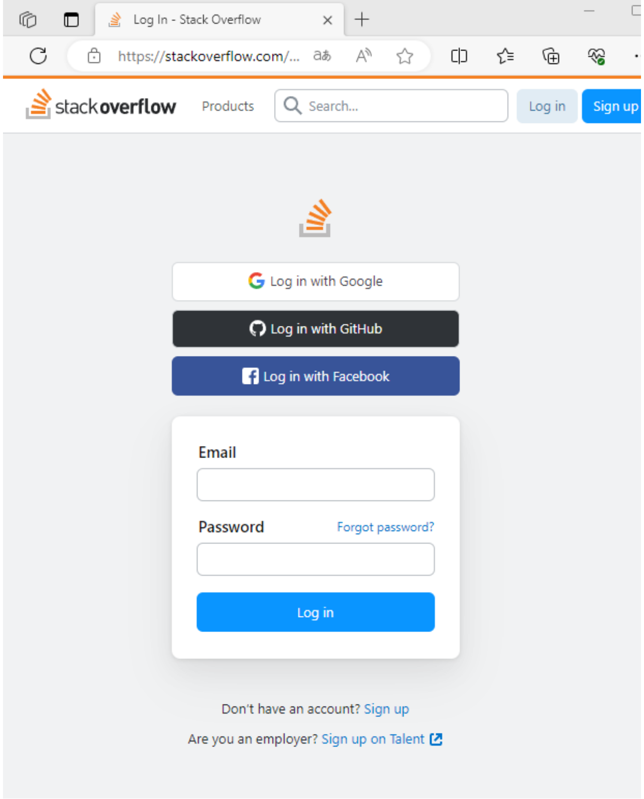


Figure 1. authentication with third party applications such as Google etc.

It is thought that blockchain technology is the most appropriate and secure solution to overcome problems such as the vulnerability of traditional username and password authentication which is still mostly used in the field of authentication in web applications, the inappropriateness of SMS authentication in terms of access and cost, and the problematic structure of third parties such as Google etc. in terms of centralisation and transparency.

Blockchain, which was first recognized in 2008 with the publication of a paper by a person or a group with the name Satoshi Nakamoto [9], is a cutting-edge technology that applies to many fields of computer science, including cryptography-based digital signature and distributed consensus mechanisms [10]. Due to its decentralized and open architecture, blockchain allows peer-to-peer data exchange in a secure and encrypted way, without the need for a centralized authority. Founded as the foundation of digital currencies, blockchain technology has revolutionized many areas of life in recent years, from finance and supply chain to health care, public services and education. Despite the services and opportunities offered by blockchain, there are still various challenges [11]- [13]. For example, according to Saberi et al. (2018), blockchain is still considered an immature technology as it is still in the early stages of its development [14]. Therefore, it still suffers from various issues related to scalability, interoperability, security, and privacy. There is also the problem of how to integrate blockchain technology into existing systems [15].

As in other fields, blockchain-based solutions are encountered in the field of identity control in the literature and IT (Information Technology) world. In addition to the advantages of blockchain, decentralised structure and autonomous operation, it is difficult to find an interlocutor on the other side in cases such as problems in the management of credentials or the reversal of an accidental transaction. In addition, for the use of blockchain in identity control, qualified professionals are needed for integrations with existing applications and continuous updating as it is a developing technology. The low number of competent personnel and access to these personnel is also an important problem. Considering the possibility of problems such as performance and scalability in real-world applications running on blockchain networks, it is thought that it may be risky to carry out the entire workflow in the field of identity control over blockchain.

For the reasons stated above, it is thought that it may be risky to transfer the authentication of web applications, especially those that are already running and have many users with different profiles such as age and technology usage skills, to a completely blockchain-based solution. Instead, it would be better to offer a secure blockchain-based authentication method as an option in addition to the existing authentication methods. When the literature is examined, there is no study in which a blockchain-based method is presented in addition to the existing authentication methods. Within the scope of this study, current literature on blockchain and authentication is given and a solution is proposed to offer a blockchain-based secure authentication option as an alternative on applications that perform authentication with traditional methods.

2. Literature Review

2.1. Brute force attack

Brute force attacks constitute an important part of cyber-attacks. They target systems that use the username-password authentication method, which is still widely used in web applications [16]. Brute force is a type of attack that enables the capture of targeted login information by trial and error in different combinations. Hackers usually use automated software to try these combinations. Brute force attacks rely on weak login credentials. If you have a simple and predictable password, hackers can use automated software to enter your site [17]. Frequently used password data is utilised in this software. For example, "rockyou.txt" file containing 14 million password data is used in attacks [18].
Brute force attacks are increasing. At the end of 2021, a 160 per cent increase in brute force attacks was recorded. It is stated that the recent Optus data breach in Australia was caused by a brute force attack [19]. If the website is compromised by a brute force attack, it can lead to the following consequences [17].

- The hacker can steal your private data.
- The hacker can add malware to your site.
- It will reduce web credibility.
- The hacker can remove your content completely.

2.2. Blockchain

Blockchain was born with Bitcoin at a time when some world-famous banks went bankrupt and people's trust in banks was shaken and panicked [20]. Blockchain was first defined in 2008 by a person or group under the pseudonym Nakamoto as a distributed ledger structure where each record is saved in a distributed platform and shared by participants in the network [9]. Reyna et al. [21] describe blockchain as a "distributed, transparent, and immutable data warehouse" where data is stored on the basis of an agreement between participants. As stated by Glaser [22], blockchain serves as a public and anonymous database allowing participants to maintain records of their assets without requiring any intermediaries or central authorities. Johar et al. [23] define blockchain as a distributed ledger technology protected by cryptography to deal with trust issues that users have long faced. Lewis [24] stated that the difference between blockchain and traditional databases is that in blockchain, operations such as adding and verifying records are performed by participants through the consensus mechanism on the P2P network.

One of the most important services provided by blockchain technology is smart contracts. It is believed that smart contracts can replace traditional contracts by decentralising work within predetermined rules on a blockchain network [21]. In other words, smart contracts are computer codes that exist transparently on the blockchain network, cannot be changed and are automatically executed. Smart contracts provide significant advantages in terms of cost, speed and security by eliminating banks, notaries and similar third parties. It is believed that smart contracts, which are already used in many areas, have great potential and will become more popular and widespread in the future.

We can divide the development of blockchain from its emergence until today into three stages [25]- [27]. The first stage is the blockchain 1.0 stage, where blockchain is considered as the technology that forms the infrastructure of Bitcoin and other digital currencies. Following digital currencies, the period in which blockchain is applied to financial applications in the form of smart contracts is called Blockchain 2.0. In recent years, the application of blockchain in many areas such as health, agriculture, education, public administration, internet of things is called blockchain 3.0.

Existing blockchain systems are divided into three categories: public blockchain, private blockchain and consortium blockchain [28].

Public blockchain: A public blockchain is an open platform where individuals, whether associated with organizations or acting independently, can participate, add records, and engage in mining activities. This type of blockchain operates without restrictions, which is why it is often referred to as a permissionless blockchain. The public chain is completely open and transparent and does not contain any private validation nodes. In this blockchain, anyone can download all the chain data and start mining, so you can ensure that there are many active copies of the chain. This increases the security and consistency of the blockchain network. In a distributed structure without any control mechanisms, the consensus protocol must do a lot of work when making changes to the chain due to the increased amount of data on the existing network.

Private blockchain: A blockchain structure that is managed by a person or group, allowing sharing and data exchange between people in one or more organisations is called a private blockchain. It can also be called permissioned blockchain because people without special permission cannot join the chain. A node's participation and access to the network is based on rules set by the group that manages the network. This reduces compliance with the decentralised and transparent nature of the blockchain.

Consortium blockchain: A consortium blockchain is a blockchain network characterized by its partial privacy and permissioned nature. In this type of blockchain, a specific group of nodes, predetermined in advance, partake in the processes of block validation and consensus as decision-makers, rather than being controlled by a single organization. These nodes decide who can join the network and who can mine. For block verification, a multi-signature scheme is used, where only blocks signed by authorised nodes are considered valid. The federation decides whether the network is public or restricted and whether everyone on the network has permission to read and write data. While Blockchain technology holds significant potential, its widespread adoption could encounter several challenges. One of these challenges lies in the energy consumption and substantial investment in computing resources associated with Blockchain systems utilizing the "Proof of Work" consensus protocol. For example, as of 2021, the Bitcoin blockchain using the "proof of work" protocol consumes more electricity than many countries [29]. At the same time, the excessive demand for many computer components, such as graphics cards used in Bitcoin mining, has led to a significant increase in their prices. Similarly, storing and verifying all data in the blockchain by all participants can lead to insufficient performance under high transaction loads. In a blockchain system, transactions performed by users are transparently shared and encrypted. By analysing this publicly shared data, it is possible to access the relationships between accounts or the real identities of users. In addition to the difficulties encountered in the implementation and dissemination of applications, new skills may be needed as new technologies develop. Blockchain continues to evolve as a new technology and researchers and companies are working hard to overcome these challenges.

2.3. Authentication with blockchain

Today, many services are provided over the Internet, and authentication processes are very important for service providers. It is no secret that current authentication systems have many problems. For example, many service providers rely on third-party authentication providers that have emerged in recent years to provide access to user information and services. However, whether it is third-party authorised login or traditional username and password login, it can be subject to various network attacks [30]. To overcome these problems, the following facilities can be provided if blockchain is used for authentication.

- Due to the decentralised nature of blockchain, service providers do not need a trusted central authority.
- The information stored within the blockchain is tamper-proof, which serves as a deterrent against certain illegal activities.
- When service providers are granted access to participate in private blockchains with permissions, users gain the advantage of accessing these services using a single account. This streamlines and enhances account management, offering greater ease and efficiency for users.
- The functionality of public and private keys in blockchain allows users to send their credentials securely. Instead of transmitting credentials directly to the service provider, users can encrypt the information with their private key, ensuring a higher level of security during data transmission.

Blockchain-based authentication technology has been the focus of researchers' attention in recent years [31], [32]. It was first proposed in 2014 by Conner et al. [33]. They introduced a blockchain-based Public Key Infrastructure (PKI) system named Certcoin, aiming to address specific security concerns. The transparency inherent in blockchain technology gives rise to concerns regarding user privacy in this solution. Furthermore, a privacy-conscious blockchain Public Key Infrastructure (PKI) guarantees user anonymity by implementing short-lived online public keys, a concept proposed by Axon and Goldsmith[34]. This work ignores storage and efficiency while ensuring user privacy. In the following years, the development of blockchain technology, improvements in performance and storage, and the use of smart contracts have made significant contributions to the authentication process.

When the literature is examined, it is possible to see many blockchain-based authentication and authorisation studies for Internet of Things (IoT) devices. Jiang et al. [32] and Khalid et al. [35] can be used as examples of these studies. There is a limited amount of network application research in this area. One of the few recent studies in this area is by Ezawa et al [36]. In this study, authentication and authentication are provided more securely by using blockchain-based PKI structures and smart contracts through authentication and authorisation servers. In this study, the fact that network users have to enter information such as public key certificates, random numbers and signatures on the login screen is considered extremely inconvenient in terms of data security and ease of use. In another study in this area, Xiong et al. [31] propose a privacy-sensitive authentication system suitable for multi-server environments, although it suffers from single point failure due to the centralised architecture. In addition to defending against various malicious attacks, the proposed system meets many security requirements such as mutual authentication and user anonymity. The solution proposed in this work is a theoretical framework and cannot be applied to any specific scenario. Ethereum-based cloud user identity management protocol was developed by Wang et al [30]. In this work, as in the work of Xiong et al. [31], network users were required to enter their key data and encrypted hash values on the login screen. Patel et al. [37] also developed a decentralized web authentication system using a prototype of an Ethereum-based blockchain system called DAuth. This study employed users' private keys and smart contracts to improve security and privacy. Similar to the research in this field, this study has limitations regarding the use of internet users in their daily lives. Petcu et al. [38] conducted a study on secure and decentralised authentication on the Ethereum network in accordance with the concept of Web3, which has been defined as the new decentralised version of the Internet in recent years. The researchers developed and experimentally implemented an end-to-end authentication application for web applications with Java and JavaScript languages. This authentication method, which is provided by connecting to the public Ethereum network through the MetaMask wallet application, was compared with 2FA and SMS authentication. These three methods were compared in 50 consecutive experimental logins and the proposed method was found to be much more efficient than the others. Chen et al. [39] proposed a framework called XAuth to provide security and privacy in authentication using Public Key Infrastructure (PKI) and Multiple Merkle Hash Tree protocols. Security analyses and experimental results for XAuth using Zero-Knowledge Proof (ZKP) Algorithm for encryption and blockchain-based IPFS for storage have shown that XAuth is effective and suitable in practice. Olanrewaju et al. [40] also conducted a study in which three options were presented for authentication: traditional username-password, one-time generated and used tokens, and digital certificates. According to the experimental results of this study, which uses Oracle database and Amazon cloud services as infrastructure, it is stated that it is more efficient in terms of performance and memory usage.

3. Proposed Solution

In this section, a solution proposal is given to provide a blockchain-based secure option in addition to the authentication controls made with username-password, LDAP or third-party applications in web applications currently in service. Blockchain is generally operated in two types of networks, private and public. The installation, maintenance and management of private networks are carried out by a specific person, group or institution. These networks move away from the structure and philosophy of blockchain in terms of decentralisation, openness to everyone and transparency. They also require investment and management costs for hardware, installation and maintenance. Public networks, on the other hand, allow application development in a public and fully decentralised environment without requiring any investment costs. Bolivar et al. [41] also stated that public networks will be easier to manage and less costly compared to private networks. Mohammed and Vargas [42], in a qualitative study in which 15 domain experts from the academic and management fields were interviewed, stated that factors such as the type of blockchain used (public-private) and the developer community behind it will affect the difficulty of integration studies. For this solution proposal, the public Ethereum network was deemed appropriate as a blockchain. The most important reason for this is that the Ethereum network operates in a completely decentralised, secure and automated manner without any investment and maintenance costs. One of the most important reasons why the public Ethereum network is preferred is that it has the potential to serve as an infrastructure where decentralised applications will increase in the future with web3, which we can express as the new version of the Internet, and where people can own the content on the Internet. According to the data in the Etherscan web application, where all transactions made in the Ethereum network can be monitored, there are 245 million active users in the Ethereum network and approximately 100 thousand new users create Ethereum accounts every day [43]. When the transaction density is analysed, 1000 verified smart contracts are created daily on the Ethereum network and more than 1 million transactions are made on average. Looking at these numbers, it is seen that decentralised web3 applications are increasing and the Ethereum network plays a major role in this.

People can manage their accounts on public blockchain networks from mobile devices and browsers using wallet applications such as MetaMask [44] and TrustWallet [45]. Thanks to these wallet applications, people can use their blockchain addresses for tasks such as authentication and data management on the internet. Nowadays, in addition to e-mail and third parties such as Google, some applications add the option to log in with blockchain accounts through these wallets. The most widely used among these wallet applications is MetaMask. In 2023, there are 21 million monthly active users using MetaMask wallet application [46]. In this study, it was deemed appropriate to use the MetaMask application to access the Ethereum network.

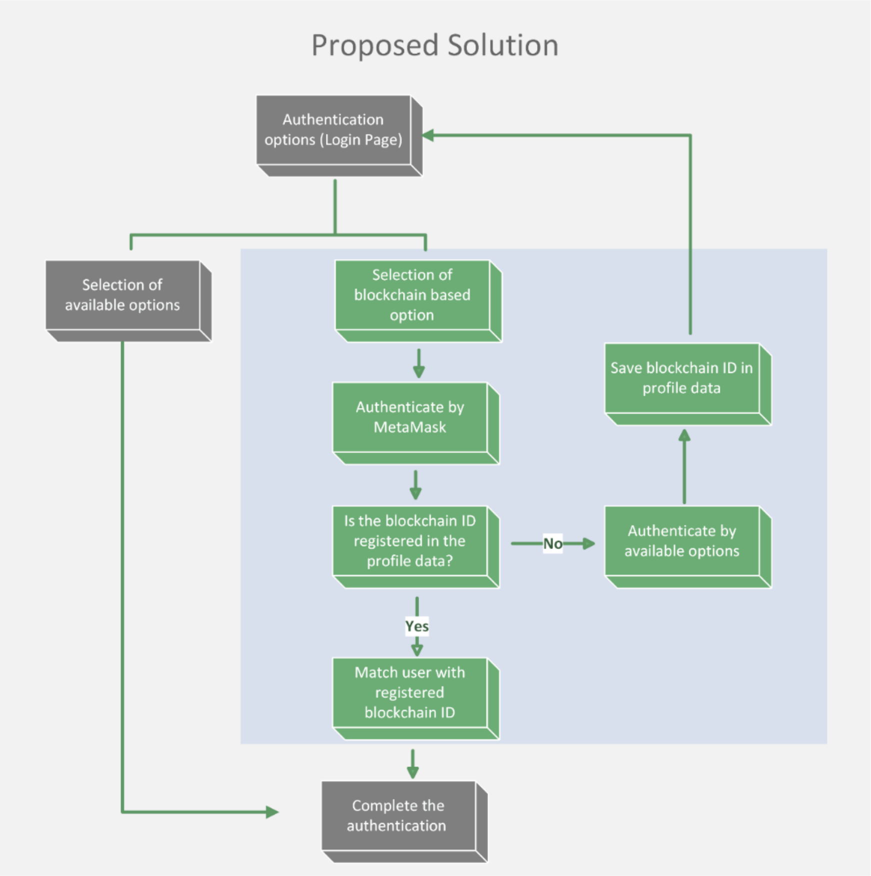

Proposed Solution
Authentication options (Login Page)
Selection of available options
Selection of blockchain based option
Authenticate by MetaMask
Is the blockchain ID registered in the profile data?
No
Yes
Authenticate by available options
Save blockchain ID in profile data
Match user with registered blockchain ID
Complete the authentication

Figure 2. General structure of the proposed solution

Figure 2 shows the general structure of the proposed solution. With this solution, a blockchain-based secure method is added as an option in addition to the authentication methods currently provided by username-password, LDAP or third parties such as Google. In this structure, users can continue to use the current authentication methods if they wish. Here, users can also select a blockchain-based authentication on the login page of the web application if they wish. In the first step, the user who chooses the blockchain-based authentication option on the login page is expected to access his address in the Ethereum network with the MetaMask application. The user who chooses this option must first install the MetaMask plugin in the browser and create an address on the Ethereum network. When the Ethereum network is accessed by successfully logging in with MetaMask in the browser, the address information in this network is used as the ID value and transmitted to the web application. In the next step, it is checked whether this blockchain ID value is saved in the profile information by any user. If this blockchain ID is saved in a profile, the user with that profile is identified and the authentication process is successfully completed. If no profile associated with this blockchain ID is found, it is understood that the user has chosen the blockchain-based authentication method for the first time and is directed to add the blockchain ID to the profile information. For this, a small development is needed to add the blockchain ID field to the profile information in the web application, such as e-mail, mobile phone, etc. fields. In this way, the user will be able to log in with the currently working authentication methods and register their own blockchain ID from the profile information page. After this process, the user who is directed to the login screen will now be able to use the blockchain authentication method and enter the web application.

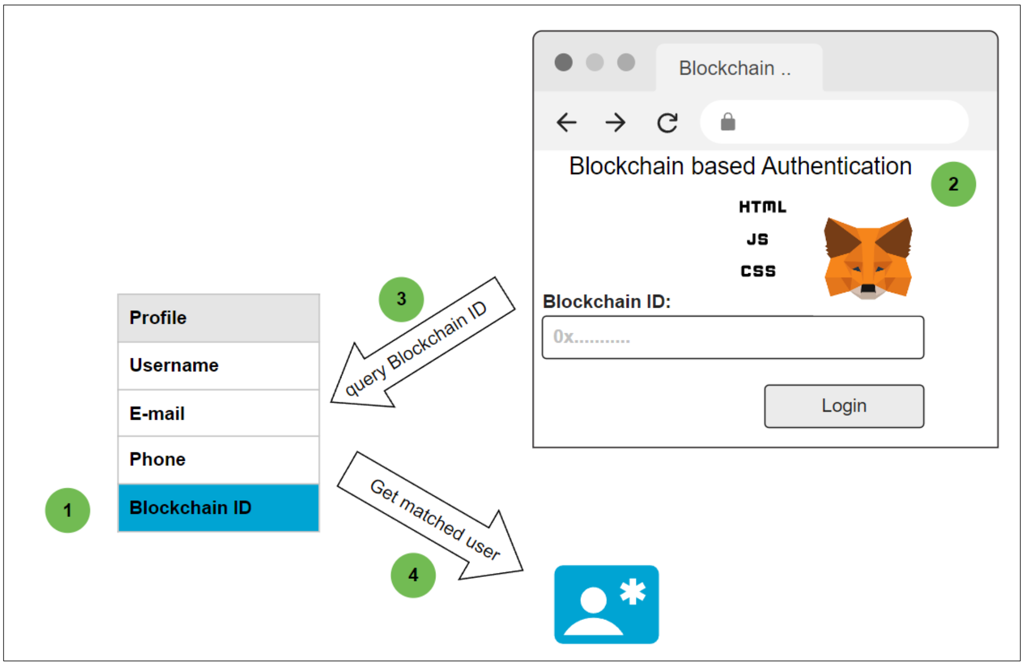


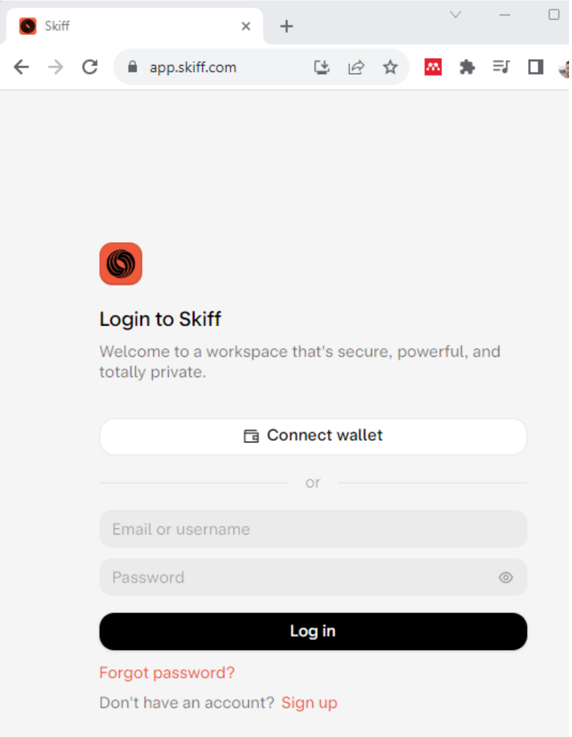
Figure 3. Integration of the proposed solution

Figure 3 shows a visualisation of how the proposed solution can be integrated into an already running web application. In this visualisation, the technical improvements needed are sequentially and numbered. In the first step, another field named "Blockchain ID" should be added to the table where user profile information is stored in the database of the web application and the user should be able to update this field from the profile screen. The Blockchain ID value should be defined as a "unique key" while saving it to the profile table, so that an ID value can only be used by one user. In the second step, a new web page should be created that calls the MetaMask plugin and obtains the user's Blockchain ID value as a result of the process. There are many libraries that allow this to be done in HTML, JavaScript and CSS. To develop this page, one can make use of the publicly available resource repository developed by Marountas, J. [47]. On this screen, brute force attacks can be prevented because the MetaMask plugin provides secure control instead of the structure that allows hackers to try passwords over and over again. In the third step, the user's Blockchain ID should be queried in the profile table. If the Blockchain ID does not match any user, a warning should be shown to the user trying to log in to save this blockchain ID value to his profile. In the fourth step, after the login process is completed, the information of the user whose blockchain ID value is matched in the profile table should be transferred to the next step.

In the introduction, Figure 1 shows a visualisation of the username-password and third-party authentication on the Stackoverflow website. In Figure 4, it is seen that Skiff website, which provides webmail service, offers users wallet applications as an option for authentication, thus taking precautions against cyber-attacks [48]. It is thought that the solution presented in this study will contribute to the increase of these examples.

4. Discussion

It can be said that this solution, which is presented as an alternative to currently working authentication methods, is very advantageous in terms of initial and management cost, implementation process, privacy, data security and resilience against attacks. This method can be quickly integrated into a web application by making use of many repositories and documentation on the internet without requiring any hardware or licence costs. An expert staff with software skills may be sufficient for this. Since there is no third party in this method, it can be considered reliable in terms of data security and privacy. One of the most important advantages of this method is that it is resistant to attacks such as brute force etc. thanks to the wallet applications and blockchain structure used. This solution is not dependent on the MetaMask app, other alternative wallet apps can also be used to access the blockchain network. Unlike other methods, in this method, users must have the ability to create an account in the blockchain network with wallet applications and to manage this account correctly.



Login to Skiff

Welcome to a workspace that's secure, powerful, and totally private.

Don't have an account? Sign up

Figure 4. Authentication option with wallet applications on the Skiff website.

In the table below, the presented method and other authentication methods are compared in terms of providing resistance against cyber-attacks, data privacy, initial and management cost, and not being affected by the single point of failure.

Table 1. Comparison of authentication methods

Authentication method	**Resistance against cyber attacks**	**Data privacy**	**Free (start-up and management cost)**	**Not affected by single point of failure**
Traditional username and password	✗	✗	✓	✓
E-mail- LDAP	✗	✗	✓	✗
SMS	✓	✓	✗	✗
2FA	✓	✓	✓	✗
Proposed Blockchain based solution	✓	✓	✓	✓

Traditional username and password authentication is vulnerable to cyber-attacks such as Brute force. At the same time, it can be considered weak in terms of data privacy and data security because users generally use the same login information for many applications. This method does not require any start-up and management costs and is not affected by single point errors since it usually runs in the database of the application. Authentication via e-mail and LDAP are also not fully resistant to cyber-attacks. Since these systems are usually provided by third parties, data confidentiality cannot be ensured and become inoperable in case of single point of failure. SMS, which is the only method that brings additional cost to operate among the authentication methods, is successful in data confidentiality and resistance to cyber-attacks, but it becomes unable to respond to single point of failure. The 2FA method, which has become widespread in recent years, can also be considered resistant to attacks and successful in terms of data privacy. At this point, the fact that Google infrastructure is generally preferred for 2FA service brings a significant risk in terms of data privacy and being affected by single point of failure. It can be said that the blockchain-based authentication method, which is presented as an alternative to the existing methods within the scope of the study, is successful and has a high potential for the future in terms of resistance to cyber security attacks, data privacy, not requiring any start-up and management costs, and not being affected by single point errors due to its distributed structure.

5. Limitations and Future Works

The advantages of public blockchain networks such as decentralisation, autonomous operation and no start-up and management costs are mentioned. In the presented solution, the Ethereum network, which is widely used in IT sector and academia and has a large developer base behind it, was preferred as a public blockchain network. In order for the solution to be valid, the Ethereum network must be operational, in other words, if the Ethereum network is shut down or stops providing service for any reason, the authentication option will also become inoperable.
In the proposed solution, users are expected to have the ability to create accounts on the Ethereum network with wallet applications such as MetaMask, manage their accounts and access these accounts on web browsers. In addition, there will be no solution for problems that may arise in this process in terms of password security, backing up and transferring account information, since there is no interlocutor in the Ethereum network.

Looking at the studies on blockchain in the literature, it can be said that blockchain has found application in many sectors and has become one of the main technologies. Considering the number of uses of the Ethereum network and MetaMask application mentioned in the previous sections and the increase in these numbers, it can be said that they play an important role in the popularisation of blockchain technologies. Today, information and communication technologies are developing and spreading very rapidly. Blockchain cryptocurrency, smart contract, NFT and Metaverse applications, which are considered as Web3 applications with their distributed and transparent structure, have recently entered our lives rapidly in many areas [49]. In the future, it is predicted that people will prefer Web3 applications that adopt trust in information systems instead of third-party intermediaries and applications. In the future, it is thought that there will be a need for solutions that eliminate the dependency on centralised systems and work on decentralised infrastructures as in this study.

It will be much more beneficial to implement the solution proposed in this study in real life. At the end of such an implementation process, it may be possible to access important information about the difficulties experienced by users when using the blockchain-based authentication solution, their attitudes towards this solution, and performance and efficiency.

6. Conclusion

Nowadays, web applications are used extensively by people in many areas, and a significant part of the attacks on web applications are made in the field of authentication, which is the gateway of these applications to the outside. In web applications, authentication is usually done through traditional username-password or third parties such as Google and Facebook. Authentication with username-password can be vulnerable to cyber-attacks as a result of easily guessable passwords or misuse. Third-party applications, on the other hand, carry risks in terms of privacy, data security and single point of failure. When the literature and sector studies are examined, it is seen that the most suitable way to solve these problems is blockchain-based methods thanks to their features such as secure, decentralised and autonomous operation.

It may be inconvenient to use blockchain technology, which is still in the development stage, as the only option in an important and sensitive area such as authentication. Instead, it is thought that it would be more appropriate to present a blockchain-based method as an option in addition to the existing methods. In order to fill this gap in the literature, this study proposes a blockchain-based secure identity management solution as an alternative for web applications that currently serve with traditional methods. New concepts and technologies such as Ethereum public network and MetaMask wallet application used in the proposed solution are explained and the general structure of the solution is explained with visuals. The steps to be followed in order to add a blockchain-based authentication option to an existing web application are also explained in a sequential manner. Compared to traditional authentication methods such as username and password, e-mail, LDAP, SMS, 2FA, etc., the proposed method has a significant advantage in that it is not affected by single point of failure due to its distributed structure. Thanks to the structure of the Ethereum network and the use of the MetaMask tool, the proposed method shows great resistance to cyber-attacks. The fact that blockchain networks work in an automated manner and are not under the control of any person or institution is extremely important in terms of data privacy and security. The method presented in this study is proposed to work as an alternative to existing authentication methods. In this way, when a problem is encountered in the existing centralised methods, the proposed system will be a life saver for web applications.

In addition, thanks to this method to be implemented as an alternative, it is thought that the service disruptions encountered due to the density experienced during special periods such as some announcements and registration periods made through web applications can be prevented.

Conflict of Interest Statement

The author declares that there is no conflict of interest.

References

[1] A. Szymkowiak, B. Melović, M. Dabić, K. Jeganathan, and G. S. Kundi, "Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people," Technology in Society, vol. 65, p. 101565, May 2021. doi:10.1016/J.TECHSOC.2021.101565

[2] W. Liang, Y. Wang, Y. Ding, H. Zheng, H. Liang, and H. Wang, "An efficient blockchain-based anonymous authentication and supervision system," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2492–2511, Sep. 2023. doi:10.1007/S12083-023-01518-5/FIGURES/6

[3] J. Zhu, Y. Wei, and X. Shang, "Decentralized Dynamic Identity Authentication System Based on Blockchain," *Proceedings - 2021 International Conference on Networking Systems of AI, INSAI 2021*, 2021, pp. 1–4. doi:10.1109/INSAI54028.2021.00012

[4] 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)*, 2019, pp. 90–95. doi:10.1109/CCET48361.2019.8989361

[5] L. Xiong, F. Li, S. Zeng, T. Peng, and Z. Liu, "A Blockchain-Based Privacy-Awareness Authentication Scheme with Efficient Revocation for Multi-Server Architectures," *IEEE Access*, vol. 7, pp. 125840–125853, 2019. doi:10.1109/ACCESS.2019.2939368

[6] K. Greene, D. Rodgers, H. Dykhuizen, K. McNeil, Q. Niyaz, and K. Al Shamaileh, "Timestamp-based defense mechanism against replay attack in remote keyless entry systems," *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, vol. 2020-January, Jan. 2020, doi:10.1109/ICCE46568.2020.9043039

[7] M. Tanriverdi, "Design and Implementation of Blockchain Based Single Sign-On Authentication System for Web Applications," *Sakarya University Journal of Computer and Information Sciences*, vol. 3, no. 3, pp. 343–354, Dec. 2020. doi:10.35377/SAUCIS.03.03.757459

[8] R. F. Sari and S. Hidayat, "Integrating web server applications with LDAP authentication: Case study on human resources information system of UI," *2006 International Symposium on Communications and Information Technologies, 2026*, pp. 307–312. doi:10.1109/ISCIT.2006.340053

[9] S. Nakamato, "Bitcoin: A Peer-toPeer Electronic Cash System." *bitcoin.org*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Oct. 15, 2023].

[10] X. Li, Z. Zheng, and H. N. Dai, "When services computing meets blockchain: Challenges and opportunities," *Journal of Parallel and Distributed Computing*, vol. 150, pp. 1–14, Apr. 2021. doi:10.1016/J.JPDC.2020.12.003

[11] C. Delgado-Von-eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," *Applied Sciences 2021,* vol. 11, no. 24, p. 11811, Dec. 2021. doi:10.3390/APP112411811

[12] J. Park, "Promises and challenges of Blockchain in education," *Smart Learning Environments*, vol. 8, no. 1, Dec. 2021. doi:10.1186/S40561-021-00179-2

[13] R. Raimundo and A. Rosario, "Blockchain System in the Higher Education," *European Journal of Investigation in Health, Psychology and Education 2021,* vol. 11, no. 1, pp. 276–293, Mar. 2021. doi:10.3390/EJIHPE11010021

[14] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, Apr. 2018. doi:10.1080/00207543.2018.1533261

[15] A. A. Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission," *Applied Sciences 2021,* vol. 11, no. 22, p. 10917, Nov. 2021. doi:10.3390/APP112210917

[16] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Medard, "Centralized vs Decentralized Targeted Brute-Force Attacks: Guessing with Side-Information," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3749–3759, 2020. doi:10.1109/TIFS.2020.2998949

[17] P. G. Shah and J. Ayoade, "An Empricial Study of Brute Force Attack on Wordpress Website," *Proceedings - 5th International Conference on Smart Systems and Inventive Technology*, 2023, pp. 659–662. doi:10.1109/ICSSIT55814.2023.10060966

[18] R. A. Grimes, *Brute-Force Attacks: Hacking Multifactor Authentication*. New Jersey: Wiley, 2020, pp. 295–306. doi:10.1002/9781119672357.CH14

[19] A. Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, and C. A. Sari, "Website and Network Security Techniques against Brute Force Attacks using Honeypot," *Proceedings of 2019 4th International Conference on Informatics and Computing,* Oct. 2019. doi:10.1109/ICIC47613.2019.8985686

[20] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," *IEEE Access*, vol. 11, pp. 64679–64696, 2023. doi:10.1109/ACCESS.2023.3289598

[21] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018. doi:10.1016/j.future.2018.05.046

[22] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," *HICSS*, 2017. [Online]. Available: https://www.semanticscholar.org/paper/Pervasive-Decentralisation-of-Digital-A-Framework-Glaser/859d0535e16095f274df4d69df54954b21258a13. [Accessed: Oct. 15, 2023].

[23] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey," *Applied Sciences 2021,* vol. 11, no. 14, p. 6252, Jul. 2021. doi:10.3390/APP11146252

[24] A. Lewis, "So, You Want to Use a Blockchain for That?" *CoinDesk*, Jul. 16, 2022. [Online]. Available: https://www.coindesk.com/want-use-blockchain/. [Accessed: Oct. 15, 2023].

[25] K. Burgess, "The Promise of Bitcoin and the Blockchain," *Consumers' Research Primary*, 2015. [Online]. Available: https://www.academia.edu/23117440/The_Promise_of_Bitcoin_and_the_Blockchain_A_product_of. [Accessed: Oct. 15, 2023].

[26] M. Swan, *Blockchain: Blueprint for a New Economy*. California: O'Reilly Media, 2015. doi:10.1109/CANDAR.2017.50

[27] 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, p. 28, Dec. 2016. doi:10.1186/s40854-016-0049-2

[28] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, Jul. 2018. doi:10.1109/MCE.2018.2816299

[29] BBC News, "Bitcoin consumes," *BBC News*, Feb. 10, 2021, [Online]. Available: https://www.bbc.com/news/technology-56012952. [Accessed: Oct. 15, 2023].

[30] 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. doi:10.1109/access.2019.2933989

[31] L. Xiong, F. Li, S. Zeng, T. Peng, and Z. Liu, "A Blockchain-Based Privacy-Awareness Authentication Scheme with Efficient Revocation for Multi-Server Architectures," *IEEE Access*, vol. 7, pp. 125840–125853, 2019. doi:10.1109/ACCESS.2019.2939368

[32] 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. doi:10.1016/j.future.2019.01.026

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

[34] 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*, SciTePress, 2017. pp. 311–318. doi:10.5220/0006419203110318

[35] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, *A decentralized lightweight blockchain-based authentication mechanism for IoT systems: Cluster Computing*. New York: Springer, 2020, pp. 1–21. doi:10.1007/s10586-020-03058-6

[36] Y. Ezawa, M. Takita, Y. Shiraishi, S. Kakei, M. Hirotomo, Y. Fukuta, M. Mohri, M. Morii, "Designing Authentication and Authorization System with Blockchain," *14th Asia Joint Conference on Information Security (AsiaJCIS)*, IEEE, Aug. 2019, pp. 111–118. doi:10.1109/AsiaJCIS.2019.00006

[37] S. Patel, A. Sahoo, B. K. Mohanta, S. S. Panda, and D. Jena, "DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain," *International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, Institute of Electrical and Electronics Engineers Inc., 2019. doi:10.1109/ViTECoN.2019.8899393

[38] A. Petcu, B. Pahontu, M. Frunzete, and D. A. Stoichescu, "A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology," *Applied Sciences 2023*, vol. 13, no. 4, p. 2231, Feb. 2023. doi:10.3390/APP13042231

[39] J. Chen, Z. Zhan, K. He, R. Du, D. Wang, and F. Liu, "XAuth: Efficient Privacy-preserving Cross-domain Authentication," *IEEE Transactions on Dependable and Secure Computing*, 2021. doi:10.1109/TDSC.2021.3092375

[40] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, "A Frictionless and Secure User Authentication in Web-Based Premium Applications," *IEEE Access*, vol. 9, pp. 129240–129255, 2021. doi:10.1109/ACCESS.2021.3110310

[41] M. P. Rodríguez Bolívar, A. Pozzebon, A. Mohammad, and S. Vargas, "Barriers Affecting Higher Education Institutions' Adoption

of Blockchain Technology: A Qualitative Study," *Informatics 2022,* vol. 9, no. 3, p. 64, Aug. 2022. doi:10.3390/INFORMATICS9030064

[42] A. Mohammad and S. Vargas, "Challenges of Using Blockchain in the Education Sector : A Literature Review," *Applied Sciences*, vol. 12, no. 13, Jul. 2022. doi:10.3390/APP12136380

[43] Etherscan, "Ethereum Charts and Statistics | Etherscan," *etherscan.io,* [Online]. Available: https://etherscan.io/charts. [Accessed: Sep. 15, 2023].

[44] Metamask, "MetaMask," *metamask.io*, [Online]. Available: https://MetaMask.io/. [Accessed: Oct. 15, 2023].

[45] Trust Wallet, "Trust Wallet," *trustwallet.com,* [Online]. Available: https://trustwallet.com/.[Accessed: Oct. 15, 2023].

[46] MetaMask, "MetaMask Statistics 2023," *earthweb.com*, Mar. 16, 2023. [Online]. Available: https://earthweb.com/MetaMask-statistics/#Detailed_MetaMask_Statistics_2023. [Accessed: Oct. 15, 2023].

[47] Pragathoys, "GitHub pragathoys," *github.com*, Apr. 28, 2022. [Online]. Available: https://github.com/pragathoys/web3-simple-login-with-MetaMask. [Accessed: Sep. 18, 2023].

[48] Skiff, "Skiff-Log in with MetaMask," *skiff.com*, Fab. 12, 2021. [Online]. Available: https://skiff.com/blog/log-in-with-metamask. [Accessed: Oct. 16, 2023].

[49] A. Zohar, "Bitcoin," *Communications of the ACM*, vol. 58, no. 9, 2015. doi:10.1145/2701411