Authentication and Identity Validation Blockchain Application

Arun N, Mathiyalagan R, Suchithra

Department of Computer Science and Engineering, JAIN (Deemed-to-be University), Bengaluru, India
Email Id- 1n.arun@jainuniversity.ac.in, 2r.mathiyalagan@jainuniversity.ac.in, 3r.suchithra@jainuniversity.ac.in

ABSTRACT: The biggest obstacle to electronic migrations of many systems is the need to protect the details and to check the identity of users. Currently, the use of dual-factor authentication is based occasionally on a password. The problem with these approaches is that passwords are extremely insecure and authentication by two factors usually involves the sending of code via SMS or a third-party provider. The blockchain might be a solution to this problem. A 50 billion dollar currency is managed by blockchain. But authentication could be subject to the same cryptographic principles. Thus, blockchain authentication eliminates someone from maliciously modifying the ledger when they distribute a ledger to all network members. A majority of the network shall check its validity any time a block of data is attached to a chain. That guarantees the completeness of the ledger. You can then make sure to send passwords safely using public-key encryption, such as highly protected RSA encryption. The receiver could then search for an entry in the unchanged blockchain, which would result in a remarkably safe and reliable way of handling identity verification. These rules apply for the transformation into a stable, fast, reliable, and readily available service from the election process, state identifiers to dual-factor authentication.

KEYWORDS: Blockchain, Authentication, Network, Protection, Encryption, Data.

INTRODUCTION

The blockchain offers a solution for several safety concerns in our daily lives. Every day, there have been the challenge of proving our identity through the submission of credentials for an online service such as social network sites or a driver’s license to prove us who. Nonetheless, these approaches are old and committed to health. The new Yahoo hack of 500 million accounts is famously easy to crack email and password credentials. Drivers, on the other hand, are likely to send someone more details as they need. If a store needs to check your age then they must only know who you are and the date of birth, but not also the address, height, weight, color of your hair and the color of the eye. This is the data necessary which results for the theft of one's identity. To overcome this problem there is a need for an authentication system[1] that only provides access to certain data and eliminates the need for each service provider to store credentials for each customer would be the ideal solution. This approach can be offered by decentralizing ownership and offering a protocol that is universally available to verify your record in an immutable data chain. The data is stored in a shared directory rather than on an app basis. Where each single blockchain user downloads this shared directory and records any change in the transaction that has ever been made[2].

HOW SECURE IS THE BLOCKCHAIN?

The blockchain relies on three main pillars: consensus, dissemination, and trust. This is a problem that is designed to take a lot of the computational power to solve problems which can take years to be solved by a single person however, it take a few minutes for a network of computers. The corroboration of work linked to the block data is important for acceptance of the blocks. The chain can always be added to a transactions processed timely while the tampering data is secured. It is unlikely for someone to modify the blockchain because of the complexity of this issue[3]. To modify a block all successors must be redone and regenerated. It could be done in theory, where the user network agrees to be the longest
blockchain recognized. It forms the blockchains first foundation. The only way for an individual to successfully modify the chain by agreeing on the longest blockchain is to change a block and generate subsequent transaction blocks to form the new largest chain. Nevertheless, it becomes difficult to use as a proof of a work problem mathematically. As the user network adds blocks much more quickly than anybody could ever add blocks. The safety is therefore untrustworthy, which ensures that malicious parties do not harm the protocol in its essence without authenticating a transaction. Eventually, in a conventional blocks a booklet were made where the booklet is circulated to each user so that each user saves the booklet for security so that no one can change one point of data reality. Nevertheless, in conventional encryption if the certificate was violated, a malicious aggressor would substitute for the stored keys with user keys and thus allow him to disguise him as a plethora of user, where a single certificate authority could be the reality. Thus, it would make an impossible to breach the chain.

**BLOCKCHAIN IMPLEMENTATION TO SECURITY AUTHENTICATION**

With the advancement in the technology and on exploitation of the potential of the blockchain and develop a range of technology-based services. A blockchain ID would be the cornerstone of blockchain authentication. This ID is a chain block which can be checked by any third party and reveal details such as birth date. The details needed such as birth date can be displayed. The ECDSA (elliptic curve digital signature algorithm)[4] is the key to this verification. By applying an ID to the blockchain, a public key is by default bound by an authentication provider and passing the private key to the user. The user and the user alone can then sign a signature that can be checked against the public key in the blockchain[5]. This user identity would act as an authentication source. It would effectively be a one-stop portal accessible through any device while not owned by a single entity. Only a digital signature and ID from a user seeking access is required for a protected application. The app can then verify that the signature is correct and that you’re ID.

**IMPORTANCE OF THE BLOCKCHAIN TO THE PUBLIC**

The market is much important for this blockchain technology, with US retailers reportedly losing some $40 billion to fraud, partially because of our appalling recognition systems and insecurity. But switching to this decentralized system will be a long process and users have to have a way to secure their data and identities in the meantime. This is where the authentication of multifactor begins. Service providers will enable blockchain multi-factor authentication without having to scrap contemporary authentication techniques[6]. It would add another protection layer to applications and slowly introduce people to the advantages of blockchain. Just as easy to use as photographs can be automated, the whole process requires only that the user creates an ID and downloads an application that handles authentication handshakes. Nevertheless, the decentralized nature of the blockchain would allow the user to sign the request manually and return it, for usability it is most likely an application using this technology. Only take a picture of a QR code that codes the request and signs it and returns it to the secured client. At a time when our smartphones seldom leave our hands, it would be incredibly easy not just for the power user but also for the average consumer to embrace this form of two-factor authentication.

**DIFFICULTIES WITH THE TWO-STEP VERIFICATION**

Several solutions for two-factor authentication are currently being used. Nevertheless, the approaches are uncivilized and pose certain security threats. These are fairly widely adopted. One of the best practices is transmitting a code over SMS, emails, etc. This is great, but notoriously insecure SMS messages. In addition to spoofing the sender, a potential attacker could sniff messages of any number[7]. This is because if your attacker knows that your account uses SMS as a backup and your name, they can find their phone numbers listed online and then intercept those messages, gaining access to any code they send. By changing the SMS protocol itself, it is simple and omnipresent but impossible to protect. The other problem with the current authentication with two factors is the exclusive existence of the services. However, Google Authenticator methods are safe and user-friendly, but Google will have
access to all your two-factor codes. This alternative is far safer but returns the question of a single entity that owns authentication data. A Google violation could result in the leakage of all authentication codes. The problem is solved by the decentralized method of blockchain, since the chain is 100% open to the public, and no confidential data is stored directly on the blockchain.

**BLOCKCHAIN METHODOLOGY**

Blockchain authentication is a viable solution for identifying a recipient and where it belongs to. This function can also be extended on behalf of an individual to make a variety of safe transfers of data. The exchange of identity data without disclosure of unnecessary information is a feature closely connected to identity verification[8][9]. A consumer can also add data to the chain in addition to data sharing as evidence of a transaction without supplying the original transaction data. Any party can check a document against this entry and demonstrate that it is legitimate to encourage rapid and reliable data audits. The theory of message signing and hacking would be based on this approach. Most providers already use this technology to validate data safely without disclosure.

**APPLICATION OF BLOCKCHAIN**

1. Block chain security flow authentication-
   A generic authentication flow that has been tested and implemented relates to a block chain handshake oriented. The handshake means that both the authentication system and the user interacts with who they claim to be. In this case, the protected app is the authentication application and the user tries to access the protected application. This flow's first step is the same as every login. The user should not enter a password, however. A user would instead see a form on the secure username page, either show the authentication QR code or see the preferred authentication option in the user's records. The example of the QR code would be easier to set and simply encode the authentication request from the protected application. The first step of the handshake is this authentication order. The next move is to test the application and submit a response. This step contains many authentication steps. Firstly, the user verifies that the request data is legitimate, and who is expected of the protected website. This can be done with public-key encryption. This would make it possible for the secured client to sign the document and then to be checked publicly either by way of the blockchain or by a certificate authority. It would be reasonable to start using a certificate authority scheme for HTTS in TLS to facilitate quick transfers. Nonetheless, this can be turne
d into a completely encrypted database by building a blockchain User ID to validate it. Once this request was checked, the user would press on a button to search for authentication. Then a response would be created, signed and then returned to a certain route in the protected app. This request is then tested using public-key encryption on the secured device and the user logs in. The downside of using the blockchain is that it is decentralized fully. If you do not want to use the software to allow this process, you would simply create your own publicly available signature and file it in a form that the website verifies. This shows a decentralized system's true advantage. Since anyone can access the data and their private key is controlled by the user, you do not have to use a certain API as a user to support this request.

2. Block chain sharing of the data-
   A current identity search issue is that you need to provide more information than the program wants. The thing if your account is hacked and anyone can access the data in a way, they can start forging an identity with a lot of information. To solve that problem, this type of service can be supported by the previous authentication flow. For these proposals, a proposed format; first, for a specific data set, the protocol must establish a ' permission ' request. For example, the machine may submit the payment request if it wants to collect credit information. What could the user then see and determine if his credit card information is to be disclosed to this vendor? If they trust it, they will sign the document and submit the information packet. If their bank can send a signed payment packet and support block chain authentication, they can then forward the
websites to the bank and conclude this transaction[10]. In this way, the user cannot provide personal information to the store. It would tell the store that the data is sent by a particular person. Next, the site would see a signed and hacked version of these data on the blockchain. Once hazelnuts match up to the fingerprints, the shop will know that the data is associated with the person concerned and that the data is unchallenged, which will guarantee that the identified person owns the card fairly. A robust, stable and mainly distributed authentication and identity verification scheme could be developed with the implementation of the concepts.

3. Secure voting using block chain

One use of this technology could be safe and anonymous online voting, and it would be possible to make full use of existing systems. Just as the monetary system is based on transactions that exchange a limited amount of a particular resource, voting is a transaction system that allows everyone only 1 unit of the money and has to pay only one unit to cast a vote. The transaction system on which Bitcoin[3] is based therefore can be used to secure online voting. A system of government-issued wallets could be a possible solution to vote. One of these wallets would be obtained after verifying the identity and become the sole owner of the wallet. Every transaction would then use the block chain to ensure that no user spends more than once by voting, thereby ensuring that every person can vote only once. However, voting is needed not only to provide everyone with voting but also ensure that such a vote is anonymous. The block chain is completely public when all can trace a transaction back to an address. Nevertheless, anybody could not decide your actual identity by using government wallets because no information about a user's identity has to be included in a wallet. Of course, a potential attacker can trace the transaction back to your system or find it to be different from you. Or you might want this government wallet to be linked with a blockchain tag. This procedure, while quick, essentially means this transaction cannot be traced back to a given wallet. In these situations, a common anonymizing technique called bitcoin "Tumbling" may rely on this approach. The transition of a coin between networks of different wallets is efficient. Therefore, this coin seems to have been the possession of all in the catalog of transactions. The voting wallet might have this feature baked, ensures that everybody's vote is anonymous. This is why the original owner is being obscured and the original owner anonymized. This system would also alleviate concerns about a hacked voting system that became a common concern after this last 2016 election, in addition to simplifying voting and making voting faster and, therefore, increasingly likely to result. Through vote is publicly displayed and thus instantly auditable by using the blockchain. Therefore, any person could check all votes for a given candidate very easily and cheaply. Cheaper and routine checks are carried out in the voting process. To raise people's trust in the voting system.

CONCLUSION & FUTURE SCOPE

Although there are many applications for the blockchain, the blockchain cannot be assumed to be a perfect solution. There are still inconveniences and insecurities, as with any program. There is no 100% safe system, therefore this must be taken into account in discussions to adopt this technology. In the event of authentication, the problem remains that it can rely on a certificate type authority and therefore rely on a third party. To make sure an ID is the person it says, it requires more secure forms of verification than using social media posts, and so forth. Either a trusted authority shall distribute these identification documents or a third party shall securely audit a user's sensitive documents that can better verify the identification. As in the case of TLS certificate authorities, people would, therefore, have to trust that the documents are properly vetted by these authorities. A hash-based system could be used to store details of document usage so that someone can verify that the document is for a particular identity, but that document could be vulnerable and the author also would not want the plaintext on the blockchain to be accessible. This presents the current problem of trusting a third party. When elections, the question is whether a particular person uses his vote or not. The problem of people selling votes is made by making voting private and making voting too easily accessible. Click on a button to transfer your "vote coin" to somebody else, can this encourage people to sell their vote? Since the vote is anonymous, the ability to trace every vote to a particular person would be removed to make every vote legitimate. The
issuer of the vote would simply make sure everybody is controlled by a single vote. It could also facilitate the sale of a vote. In addition, certain people would benefit more than others. This would make it much more accessible for tech schemers and those with easy internet connections than the poorer areas, as they still have to drive to a voting place counterpart to make its exchange. For the protection of such protocols, transactions themselves can be regarded as being reliable enough to validate the identity and link data with a certain entity using the elliptic curve digital signature algorithm in public-key cryptography. But this essentially makes your key, the key to your identity. If anyone can take your key anyway, they are stealing your freedom. However, in this interim, an attacker would have full access to anything and would increase the risk that you would lose that key. You could re-associate another key with this identity. Also, while ECDSA is extremely secure, public-key encryption is tried and true, it is famously unpredictable whether people are using this info. However, the possibility of uses and advantages for society cannot be denied before a wide-ranging system of blockchain identities is created. As culture is more techno-centered and the internet is a better digital identity, and the world in which living is increasingly insecure and inadequate for contemporary ways of verification and identification. There is an unavoidable major overhaul of these systems and the blockchain is a possible way to address these issues.

REFERENCES

[1] C. H. Lee and K. H. Kim, “Implementation of IoT system using block chain with authentication and data protection,” in International Conference on Information Networking, 2018.

[2] B. Cresciello-dittmar, “Application of the Blockchain For Authentication and Verification of Identity,” Int. J. Adv. Sci. Eng. Inf. Technol., 2016.

[3] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, “Inclusive block chain protocols,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015.

[4] A. Anjum, M. Spony, and A. Sill, “Blockchain Standards for Compliance and Trust,” IEEE Cloud Comput., 2017.

[5] N. Rückeshäuser, “Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls,” Wirtschaftsinformatik 2017 Proc., 2017.

[6] B. C. Florea, “Blockchain and Internet of Things data provider for smart applications,” in 2018 7th Mediterranean Conference on Embedded Computing, MECO 2018 - Including ECYPS 2018, Proceedings, 2018.

[7] L. Wei et al., “Security and privacy for storage and computation in cloud computing,” Inf. Sci. (Ny.), 2014.

[8] A. Reed, M. R. Forehand, S. Puntoni, and L. Warlop, “Identity-based consumer behavior,” Int. J. Res. Mark., 2012.

[9] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Futur. Gener. Comput. Syst., 2017.

[10] T. Prathyusha, M. Kavya, and L. Akshita, “Block Chain Technology,” Int. J. Comput. Math. Sci., 2018.

[11] Natarajan, B., Obaidat, M.S., Sadoun, B., Manoharan, R., Ramachandran, S. and Velusamy, N., 2020. New Clustering-Based Semantic Service Selection and User Preferential Model. IEEE Systems Journal. DOI: 10.1109/JSYST.2020.3025407.

[12] Nataraj, S.K., Al-Turjman, F., Adom, A.H., Sitharthan, R., Rajesh, M. and Kumar, R., 2020.
Intelligent Robotic Chair with Thought Control and Communication Aid Using Higher Order Spectra Band Features. IEEE Sensors Journal, DOI: 10.1109/JSEN.2020.3020971.

[13] Babu, R.G., Obaidat, M.S., Amudha, V., Manoharan, R., and Sitharthan, R., 2020. Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. IET Networks, DOI: 10.1049/iet-net.2020.0122.

[14] Sitharthan, R., Yuvaraj, S., Padmanabhan, S., Holm-Nielsen, J.B., Sujith, M., Rajesh, M., Prabaharan, N., and Vengatesan, K., 2021. Piezoelectric energy harvester converting wind aerodynamic energy into electrical energy for microelectronic application. IET Renewable Power Generation, DOI: 10.1049/rpg2.12119.

[15] Sitharthan, R., Sujatha Krishnamoorthy, Padmanaban Sanjeevikumar, Jens Bo Holm-Nielsen, Raja Singh, and M. Rajesh. "Torque ripple minimization of PMSM using an adaptive Elman neural network-controlled feedback linearization-based direct torque control strategy." International Transactions on Electrical Energy Systems 31, no. 1 (2021): e12685. DOI: 10.1002/2050-7038.12685.