International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Blockchain based Decentralized Password less User Authentication System: A Survey

Rajdeep Singh[1], Yash Jain[2], Sankalp Khawade[3], Akshay Jinde[4], Shubham Zanwar[5]
[1,2,3,4]*Student, Dept. of Computer Engineering, SKN-Sinhgad Institute of Technology and Science, Lonavala, India*
[5]*Assistant Professor, Dept. of Computer Engineering, SKN-Sinhgad Inst. of Tech. and Science, Lonavala, India*

***Abstract*: With the advent of social media sites and digital payment systems, the security and privacy of the individuals becomes a lot more important. Interestingly most of the websites including the global players like Google, Facebook, Amazon, Paytm, etc. are all based on password-based authentication system. But the passwords pose a lot of threat as there are many ways of breaching the security and gaining access to sensitive information. In most of these websites, the data is stored on a centralized system called as a server. The whole system is under threat if the server goes down. One of the solutions for this problem is to use a decentralized system based on a blockchain. The blockchain is a distributed ledger of information to keep all the records with the help of a hash key. Using blockchain the user can be provided with a security key which is immutable and can be used to login into the system. This paper presents a method of creating an authentication system which uses blockchain and is far more secure than the existing password-based authentication system. The aim of the mentioned project is to fulfill the same by using PKI over multiple input methods backed by a Blockchain network.**

***Keywords*: Blockchain, authentication, password-less, privacy, access control, hashing, public key infrastructure, credentials, cyber security**

1. Introduction

We are living in a digital age and the internet has become an integral part of our lives. In this era of digitalization, where almost all the entities of the society are on the internet interacting with each other for varied reasons create massive information-base on the internet. The sensitive information of the public like details of their financial transactions, medical records, social media preferences, etc. are in the digital form on the internet and thus security and privacy of the users is an extremely important factor to be safeguarded for the benefit of the society.

The current password-based user authentication system consists of a lot of loopholes using which the security of the users can be breached. The following are the ways using which the security of the system can be compromised:

A. Brute force attack

The brute force attack is the simplest method to gain access to a site or server (or anything that is password protected). It tries various combinations of usernames and passwords again and again until it gets in [3].

B. Dictionary attack

In cryptanalysis and computer security, a dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

C. Shoulder surfing

In computer security, shoulder surfing[2] is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder.

D. SQL injection

SQL injection [3], also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

E. Man in the middle attack

In cryptography and computer security, a man-in-the-middle attack (MITM) [2] is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

2. Public key infrastructure

A. PKI implementation

PKI requires the 2 sides to have public and private key pair. The PKI manages these keys by verifying them through a certificate management authority, CA, who keeps the record of the valid certificate of the public. The most common approach to PKI is CA-based – specifically, the X.509 standard. CA is a trusted party, who will issue a signed certificate verifying an entity's ownership of a public key on request. In order to "trust" a CA, a device accepts a root certificate for that CA into its store. The metadata in a public key certificate typically comprises a version number, a validity period, a serial number, a URL that provides revocation information, an identifier that identifies the digital signature cryptosystem used to sign the certificate, and an identifier that identifies the CA that issued

the certificate. A hierarchical certificate chain stems from this root, in which any certificates signed using a trusted certificate are also trusted. WoT-based PKI is also widely used. Members of the network establish trust by verifying that others have a certificate signed by an entity in whom the verifier has previously established trust. Unlike in CA-based PKI, trust is decentralized in WoT – certificate issuance can be performed by any party [10].

B. PKI in blockchains

Blockchain was first introduced as the transaction record for the Bitcoin cryptocurrency in 2008[11]. Alternative blockchains have since been developed, including the Namecoin blockchain, on which Certcoin and PB-PKI are built. Namecoin works as a decentralized domain name server (DNS) which, unlike the Bitcoin blockchain, is able to store data, making it suitable for wider applications [Kalodner et al., 2015]. A blockchain is a public ledger to which events are posted and verified by network members, before being "mined" in an incentivized system in which members compete to complete some proof-of work – usually a cryptographic challenge. Blockchain has a unique combination of properties that make it suitable for a number of applications: it is decentralized (it is controlled through majority consensus of members), and the transaction record is reliable (events recorded in the past cannot be altered without the consensus of a majority of the network's mining power). Proposed and existing applications include smart contracts, reputation systems, and IoT device interactions. Many other Cryptocurrencies have been launched since the launch of Bitcoins [12]. Here we shall use the distributed and on chain storage feature of blockchain that will help us make PKI possible through it.

3. Modeling of the proposed system

A blockchain is a chain of blocks where every chain consists of a hash of complete chain prior to it [12]. The chain can hold more of such data as required. The blockchain currencies used this concept to store transactions in it providing an immutable storage. We will exploit this feature of the blockchain to store the user account details instead of a central database. In our system, we used 6 separate chains.

1) Hash Chain
2) User Information Chain
3) Request Chain
4) Blocked users
5) Logs
6) Privilege

Since we are building a complete user management system, we will need these, for basic features of user data, requests, blocked users/deleted accounts, rights and login logs. A large number of chains would make the system bulky but the segregation of information keeps it systematic and more secure and manageable. Hash chain would generally contain user ID, public key and Hashes.

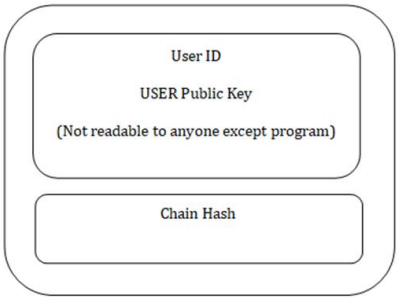

Fig. 1. User hash chain

The second chain contains user information such as name, contact details, address, profile, department, etc. in a similar fashion. Read-only accessible to all the users since it doesn't contain any kind of personal information. The third chain contains the new user account request with details such as User Info, Contact Info ID, and Hashes. A new user will need to send a joining request before they could actually start using the system. The request needs to be approved by the senior authority like the Database admin in traditional database systems. The roles will be mentioned in the Roles list which will again be hidden from everyone containing the user IDs and their corresponding roles or access levels. The Blocked chain will have a list of the ID of accounts that are disabled or blocked. This will restrict the users to join the network and help to track of the same. The log chain will have user log details similar to traditional logs.

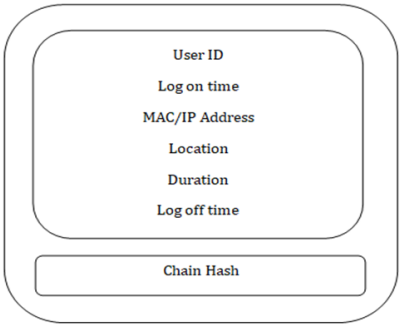

Fig. 2. Logs chain

The chained hash is always the hashes like in traditional blockchain systems.

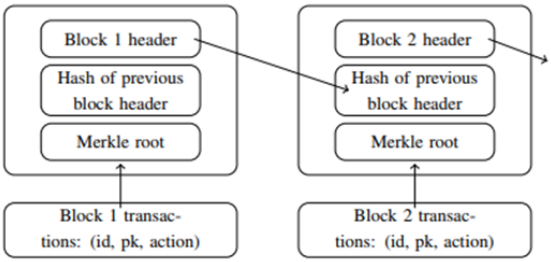

Fig. 3. Blockchain with a PKI structure

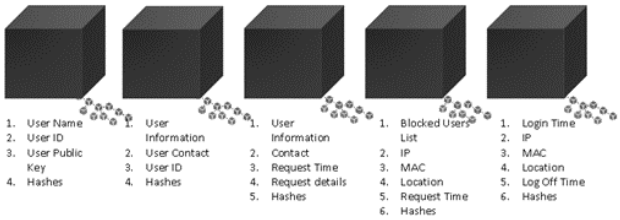

Fig. 4. List of chains with detail

The same deployment is more secure by making the communication SSL encrypted. Where there is no CA authority, every chain has a local copy of certificates and the same is distributed among all the nodes in the chain to ensure that every node has the same set of data removing the need to have a central CA authority, updates are shared mutually.

A. Modes to carry the key

The user is free to choose the mode of the key they wish to carry. The key can be in a form of smart card [13]. The smart card is one of the emerging key storage devices. Its security studies have proved it to be one of the best vaults available [14]. More ways available are Thumb drives, USB Drives, Files, Daily issued keys, Biometric DB, etc.

IV. ADVANTAGES OF IMPLEMENTATION OF PKI AS A BLOCKCHAIN

The first advantage of the implementation of PKI as a blockchain is that the certificates are not signed. This means that they are shorter, which reduces the time it takes to transmit a certificate backed by a CA certificate chain. Second, validation of a certificate and its CA certificate chain is trivial. A blockchain being a distributed ledger, the verifier has a local copy of the entire blockchain and looks up hashes of certificates in blockchain stores in the local copy, without network access. No signatures need to be verified. A blockchain PKI solves a longstanding problem of traditional PKIs by not requiring the use of a service that issues certificate revocation lists (CRLs) or responds to online certificate status protocol (OCSP) queries. CRLs can get very big. They must be stored by the verifier and updated over the network on a regular schedule. OCSP checks add network latency to certificate validation and leak the information that the subject is presenting the certificate to the verifier, destroying the feature of cryptographic credentials. Too often, if the revocation checking service is unavailable, verifiers skip revocation altogether. It should be noted that a blockchain PKI can be used to back plain blockchain certificates just as well as rich blockchain certificates and both use cases benefit from the above advantages of a blockchain PKI.

4. Advantages of the proposed system

1. The system is based on distributed nodes instead of a centralized system and hence the security of the system is enhanced.
2. There are no traditional passwords, instead of a PKI system which cannot be cracked in a short period of time.
3. There are no limitations, can be integrated with any system due to open request response API support.
4. No additional costs for servers, management, and maintenance.
5. No Licensing costs.

5. Conclusion

This is a description script of a project whose goal is to make the user management system secure by removing the concept of traditional alphanumeric characters and centralized authentication database. This system allows the user to select among multiple ways of password object as preferred including Files, Barcode, Smart Cards, etc. embedded with a private key of the user. The authentication will be provided by the blockchain network through the key object with the user instead of a central database. The user will be able to log in if more than 50% of the network nodes approves. This paper describes the model used to attain the same proving more benefits than traditional passwords and PKI systems with the same management features.

References

[1] Karen Lewison and Francisco Corella, “Backing rich Credentials with Blockchain PKI”, October 24, 2016.
[2] Davies, D. W., and Price, W. L, “Security for computer networks,” (John Wiley, New York, 1984.
[3] Denning, D.E.: ‘Cryptography and data security’ (Addison Wesley, Massachusets, 1982)
[4] Feistel, H., Notz, W. A., And Smith, J. L.: ‘Some cryptographic techniques for machine to machine data communications’, Proc. IEEE, 1975.63, (11). pp. 1545-1554.
[5] A. Evans Jr., W. Kantrowitz, E. Weiss, A user authentication scheme not requiring secrecy in the computer, Commun. ACM 17 (1974) 437–442.
[6] G.B. Purdy, A high security log-in procedure, Commun. ACM 17 (1974) 442–445.
[7] N. Haller, The S/KEY (TM) one-time password system, in: Proceedings of Internet Society Symposium on Network and Distributed System Security, Internet Society, 1994, pp. 151–158.
[8] N. Haller, The S/KEY one-time password system, RFC Technical Report 1760, February 1995.
[9] A Nash, W Duane, C Joseph PKI: Implementing and Managing- 2001.
[10] Louise Axon and Michael Goldsmith Department of Computer Science, PB-PKI: a Privacy-Aware Blockchain-Based PKI, University of Oxford, Parks Road, Oxford, UK.
[11] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. October 2008.
[12] CoinMarketCap. Crypto-Currency Market Capitalizations
[13] W Rankl, W Effing, Smart Cards – 2004.
[14] E.A. Dabbish, R.H. Sloan Examining Smart-card security under the threat of power analysis attacks – 2002.
[15] Remme.io, Distributed Public Key Infrastructure (PKI) protocol and Access Management DApps – 2018.