BLOCKCHAIN SMART CONTRACT

PRIYANSHU RAJPUT

B.Tech Student, Department of Computer Science & Engineering Dronacharya College of Engineering, Gurugram, India

Abstract*: Privacy has become a major concern for many people around the world these days. As the number of technologies grows and privacy policies are updated, trust between individuals and those sitting behind computer screens that control algorithms on social media platforms is reduced. Everything from your money to social media is centralized. H. Often managed by a single organization, government or technology company. This leads to an unreliable and dictatorial form of leadership. However, blockchain technology seems to have a solution to these problems.*

General Terms-

Your common words should be any term that can be used standard separation of items submitted as pattern Blockchain, Security, Cryptography etc.

Keywords- *Smart Contract, Blockchain, Cryptography*

1. INTRODUCTION

The blockchain was developed in 2008 by an anonymous person using the pseudonym Satoshi Nakamoto. He published a technology white paper in 2009. Basically, a blockchain is a chain of blocks connected by a cryptographic hash. The first block in the blockchain is known as the "Genesis block". A block in a blockchain consists of three parts: data, hash, and previous hash. Primarily, blockchain technology is decentralized. H. Organizations are safer, immutable, distributed, and less malicious, especially in today's world, where everything seems to be in a closed algorithm because it is not controlled by a single organization. Smart contracts are one of the interesting concepts that are similar to real-world contracts but digital.
Use the blockchain as a building block. A smart contract is a line of code that is stored on the blockchain and is automatically executed only when certain conditions are met. The main goal of smart contracts is to reduce the need for intermediaries, brokers, scammers, and malicious random exceptions. Since we are using the blockchain as our main player, we are very secure and can execute transactions without any disadvantages. This white paper examines existing blockchain technology and how smart contracts eliminate the need for future.

2. SECURITY RISK TO DATABASES

The organization of the launched website is less than amazing various threats. Other serious threats are considered in this regard document. This list is taken from a white paper presentedby Imperva Application Protection Center

Legitimate Privilege Abuse

Violation of a legal right can be a form of abuse by website users, administrators or system administrator do anything illegal or unethical work. That's right, but it doesn't end there, anywhere misuse of sensitive data or unforgivable use of rights.

Excessive Privilege Abuse

When users are specified access permitsperforming other tasks that are not included in their work, which are dangerous the purpose can be achieved through such activities thus earning abuse of such rights. When we talk about such harassment, a university example can be cited when the administrator who is granted access to all databases and is entitled to this change therecords of any student. This can lead to abuse such as grade change, student marks or conversion of the amount of the fine charged to any student. As a result, all users those who perform different tasks are given this standard rights grant excessive access

Higher Rights

Excessive exposure leads to the detection of defective errors profit by invaders and may causechange rights e.g.

normal user given administrative access rights. Losses that may result in fraudulent accounts, money transfers, misinterpretations of other sensitive material analytical information. Such cases are also found to exist database functions, agreements and SQL statements.

Endangerment of the Website

Vulnerability to previous applications such as Widows 98, Windows 2000, etc. can cause dataloss from website, data corruption or service denial conditions. Because for example, blaster worm has created a denial of service conditions from the vulnerability found in Windows 2000.

SQL injection

Random SQL queries used by server maliciously the invader. In this attack the SQL statement is followed by a series identifier as input. That is verified by the server. If it happens can be confirmed it may be killed. With these unrestricted rights may be acquired by the aggressors as a whole database.

3.DATABASE SECURITY CONSIDERATION

Website Security Consideration

In order to eliminate security threats all organizations must explain the security policy. And that security policy should be the same strict enforcement. Strict security policy must be well contained defined safety features. Figure 2 shows the critical areas what needs to be considered is outlined below. [1] [3] [4]

Access Control

Access control ensures all connections to the site and other system components comply with policies as well controls defined. This ensures that no disturbances occur by any intruder outside or inside and thus, protects the database from potential errors - potential errors make a big impact like stopping factory operations. Access control also helps to reduce potential risks contributes to website security on large servers. Because for example, if any table was deleted by mistake or access fixed results can be supported or in specific files, access control can limit their removal.

Idea Policy

Idea policy is needed to protect data in a particular area level. It is possible when descriptions from specific data are in the type of analysis or facts that need to be protected from a certain

high level of security. It also determines the method of protection information that can be disclosed.

User ID / Verification

User identification and verification is a basic requirement for ensure safety as the identification method defines a set of people are not allowed access to the data and it provides complete accessibility method. Ensuring security, ownership verified and keeps sensitive data safe and secure edited by any normal user.

Accountability and auditing

Accountability and auditing are required to verify physical integrity of data that requires defined access data stored and controlled by research and recording to keep. It also helps to analyze the information stored on it verification servers, accounting and user access.

Encryption

Encryption is the process of concealing or converting information using cipher or code to be unreadable to all other people except those who hold the key information. The result of coded information is called as encrypted information. Data is an important asset of an organization. So its safety it is always a big challenge for the organization. In recent times the security of shared information was researched cryptographic view. A new framework was proposed in different keys used by different groups for encryption data stored in a variety of ways labeled as hybrid cryptography database (MCDB). [6] The various forms of government, non-governmental, and private as well many other organizations have sensitive data on web servers which really need protection from the invader or the invaders. To make the site secure with different security strategies improved. One of them is the encryption method. However encryption enhances protection but your implementation

decisions are also very important. Like you, how, when and where it should be nailed. . The following figure 4 shows where it iscrucifixion occurs.

Developing encryption techniques comes from something important questions and, such as how, when and where the encryption will be performed.

4. CONCLUSION

We have discussed about Blockchain, the need of Smart contract, why smart contract is important as well as a model of the working Password smart contracr on Blockchain, the features blockchain provides such as immutability, scalability, decentralization, transparency, builds sense, and much more. The model discussed consists of Blockchain, Consensus which is Proof of Work in our case, the importance of encryption, using aes-256-cbc, and finally the front-end application for easy interaction with the blockchain. The Password managers are very necessary to make sure you are safe online, using strong and different passwords for each login credentials. There is a lot of work that can be done in the field to make Password Manager to make them even more secure.

5. REFERENCES

[1] Satoshi Nakamoto (2008). Bitcoin: Peer-to-peer electronic cash system. https://bitcoin.org/ https://bitcoin.org/bitcoin.pdf.
[2] Polshakova, N. (2019). Secure password storage on the Bitcoin blockchain. https://cs.brown.edu/. https://cs.brown.edu/research/pubs/theses/capstones/2019/polshakova.nina.pdf。
[3] Brindha 、 S , Vishnudarshan, S. , Arsaad, S. , & Amp; Dinesh, A. (2020). Improvement of password system by blockchain. International Research Journal of Engineering and Technology (IRJET).
[4] Tse, D., Huang, K., Cai, B. , & Amp; Liang, K (2019). A robust password management systemusing blockchain technology. 2018 International IEEE Conference on Industrial Engineering and Engineering Management (IEEM). 10.1109 / IEEM 2018.8607284.
[5] Luevanos, C., Elizarraras, J., Hirschi, K. , & Amp; Yes, J (2018). Password manager security and usage analysis. 2017 18th International Conference on Parallel Distributed Computing, Applications and Technology (PDCAT). 10.1109/PDCAT.2017.00013
[6] Sousi、Ahmad-Loay; Yehya、Daliaandamp;ヨウディモハメドド。(2020) AES encryption: research and evaluation.
[7] Pitchaja M., Daniel Philemon, & amp; Praveen (2012). Implementation of standard extended encryption algorithms. International Journal of Scientific & amp; Engineering Research Volume 3, Issue 3, March-2012.
[8] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) algorithm for encrypting and decrypting data.