International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secured University Results System using Block Chain Features

Rushikesh Pawar[1], Sambhaji Jadhav[2], Sainath Rodge[3], Naval Jakken[4]
[1,2,3]*Student, Dept. of Computer Engineering, G.H. Raisoni College of Engineering and Management, Pune, India*
[4]*Professor, Dept. of Computer Engineering, G.H. Raisoni College of Engineering and Management, Pune, India*

***Abstract*: Building a system for security of university results that satisfies the transparency of results has been a challenge for a long time. Distributed ledger technologies is an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed database systems. The paper elucidates the requirements of building secure system and identifies the technological limitations of using blockchain as a service for realizing such systems. The paper starts by evaluating some of the popular blockchain frameworks that offer blockchain as a service. We then propose a novel database s ystem currently used by universities based on blockchain that addresses all limitations we discovered. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a blockchain-based application which improves the security and decreases the cost of hosting a worldwide application for universities.**

***Keywords*: Block Chain, Cryptography, Data Security Framework, Bitcoin.**

1. Introduction

Nowadays a lot of cases are coming up regarding corruption in university results. Cases such as hacking into system and changing results, false mark sheets, are being observed. Hence the aim is to develop a system which would bring transparency in results of university.

A. Basic Concept

A blockchain, originally block chain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash). By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchain may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain. Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.

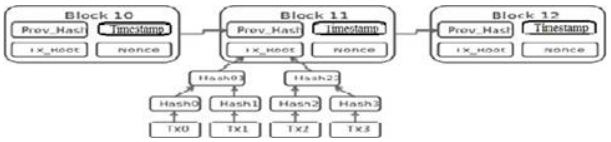

Fig. 1. Bitcoin block chain

2. Literature survey

In this paper, based on the blockchain technology, we propose a decentralized database management, without the existence of a trusted third party. Furthermore, we provide several possible extensions and improvements that meet the requirements in some specific cases.

The purpose of this study is the presentation and the definition of a new system named Crypto-voting. We base this solution upon the Shamir's secret sharing approach, implemented using the blockchain technology. We use this technology to integrate the management procedures of the phases and events of a database election. These events include the set -up of the system, the distribution of credentials, the results storage, the publication of results, and so on. In addition, our system aims to improve the methods of traceability and audit about results, with no middleman.

Bit coin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bit coin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zero coin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality. In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in zero - knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs). First, we formulate and construct decentralized anonymous

payment schemes (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security. Second, we build Zero cash, a practical instantiation of our DAP scheme construction. In Zero cash, transactions are less than 1 kB and take under 6 ms to verify - orders of magnitude more efficient than the less - anonymous Zero coin and competitive with plain Bit coin.

Recently, there has been a growing interest in using online technologies to design protocols for secure data management. The main challenges include privacy and anonymity and transparency throughout the result process. The in troduction of the blockchain as a basis for cryptocurrency protocols, provides for the exploitation of the immutability and transparency properties of these distributed ledgers. In this paper, we discuss possible uses of the blockchain technology to implement a secure and fair data management system. In particular, we introduce a secret share-based data system on the blockchain, the so-called SHARVOT protocol1. Our solution uses Shamir's Secret Sharing to enable on -chain.

Crypto currency, and its underlying technologies, has been gaining popularity for transaction management beyond financial transactions. Transaction information is maintained in the block-chain, which can be used to audit the integrity of the transaction. The focus on this paper is the potential availability of block-chain technology of other transactional uses. Block-chain is one of the most stable open ledgers that preserves transaction information, and is difficult to forge.

3. Related work

In this digital era, it is difficult for universities to maintain security. There is a need of some digital system on which one can rely on without any inconvenience. There is a need of some secure, fast, reliable and transparent system. Block chain is highly secure and recent technology which can change the face of university data management system.

Table 1
Comparison of the security services of different solutions

	Blockchain	Database	Distributed Database
Integrity of the Records	High	Moderate	Moderate
Availability	High	Low	Moderate
Fault Tolerance	High	Low	Low
Privacy	Low	High	Moderate

A. Project Objective

The system should ensure that integrity is maintained. The necessary mechanism should be employed in order to guarantee integrity. The system functionality should ensure that no one can falsify or modify the result of the particular subject by eliminating an actual result.

B. What is to be developed?

In the traditional University data management system, we have to face the following problems

1. A lot of manual work is present.
2. Results are centralized.
3. Lack of transparency in the results.
4. Compromising the security is very easy.

4. Proposed system

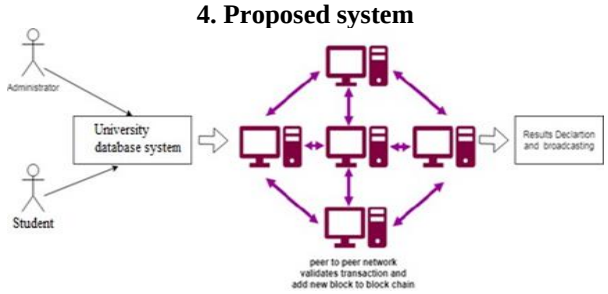

Fig. 2. Block diagram

System architecture is the design of the whole system architecture. The database system using block chain is made up of peer to peer network. Student is the person who is the user who access the system for viewing his result.

Administrator has control of the system. In this architecture actually there are two working modules used

- Administrator
- Student Administrator:

Here administrator is the authorized person of University who is responsible for the different activities:

1. Uploading student information
2. Verifying student information
3. Uploading result Information
4. Generating results
5. Date/ Time set by University
6. Schedule result display process
7. Declaring results

Student:

1. Registration
2. Uploading Self Information
3. Verifying Information
4. Login
5. View result

5. Other specifications

A. Advantages

- *Disintermediation:* The core value of a blockchain is that it enables a database to be directly shared without a central administrator. Rather than having some centralized application logic, blockchain transactions have their own proof of validity and authorization to enforce the constraints. Hence, with the blockchain acting as a consensus mechanism to ensure the nodes stay in sync, transactions can be verified and processed independently.

- *Secure:* Blockchain based system provides a secure way for database.
- Decentralized: Database is decentralized so that there is low chance of hacking attack.
- E-based: This is online process so that manual and traditional way is removed completely so there is no chance of fraud.
- Real time: Due to online this is the best to track the whole process in real time.
- Transparency: Provide transparency to the student and hides the privacy of student.

B. Applications

This proposed system can be used for in various areas like

- Organization
- Country
- College
- Firm

6. Conclusion

Nowadays a lot of malpractices are practiced regarding manipulation in the results of university exams. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement system for secure and transparent management of results using block chain algorithm. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient result handling scheme, while increasing the security measures of the today's scheme and offer new possibilities of transparency.

References

[1] Yi Liu and Qi Wang, "An Database management based on Blockchain."
[2] Francesco Fusco, Maria Ilaria Lunes, Filippo Eros Pani and Andrea Pinna, "Crypto-voting, a Blockchain based database System."
[3] E. B. Sasson *et al*., "Zerocash: Decentralized Anonymous Payments from Bitcoin," *2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 2014, pp. 459-474.
[4] Silvia Bartolucci; Pauline Bernat; Daniel Joseph, "Sharvot: Secret SHARe-Based data management on the Blockchain," 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), IEEE.
[5] Jushua I James, "Secured data storage Using Block-Chain Service."
[6] Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online].
[7] Feng Hao, P.Y.A. Ryan and Piotr Zielinski, "Anonymous voting by two-round public discussion," 2008.
[8] Feng Hao and Piotr Zielinski, "A 2-Round Anonymous Veto Protocol," 2006.
[9] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Intractability," Journal of Cryptology, 1(1):65-75 · January 1988.