Secured University Result System using Block Chain Features

Patel Zeel Vijaybhai patelzeel@gmail.com
Golait Shubham Nitin Shubhamgolait2015@gmail.com
Birendra Pratap Singh birenderpsingh21@gmail.com
Prof. S. B. Ahire
Department of Computer
NBN SSOE Pune, Maharastra, 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 are an exciting technological advancement in the information technology world. Block chain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of block chain as service to implement distributed database systems. The paper felicitates the requirements of building secure system and identifies the technological limitations of using block chain as a service for realizing such systems. The paper starts by evaluating some of the popular block chain frameworks that offer block chain as a service. We then propose a novel database system currently used by universities based on block chain 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 block chain-based application which improves the security and decreases the cost of hosting a worldwide application for universities.**

Keywords- **Nano fluid, Friction factor, heat transfer, Reynolds numbers.**

I. INTRODUCTION

1.Problem Definition:

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.

2.Basic Concept:

A block chain, 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 block chain 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 block chain 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 block chain records are not unalterable, block chains 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 block chain. Block chain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the crypto currency bit coin.

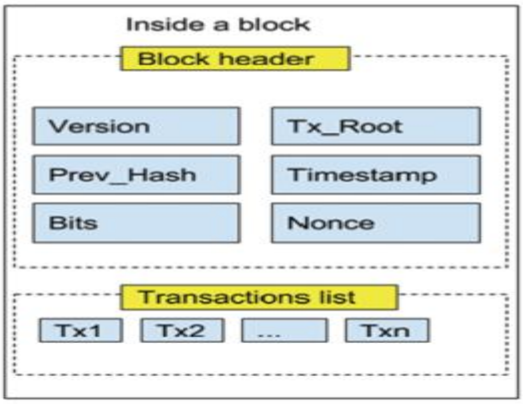

Fig.1. Bit Coin Block Chain.

II. RELATED WORK

In this paper, based on the block chain 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 [1].The purpose of this study is the presentation and the definition of a new system named Crypto-voting. We base this solution upon the Shamirs secret sharing approach, implemented using the block chain technology. We use this technology to integrate the management procedures of the phases and events of an 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 [2].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[3].

Algorithm:

1. Visual Cryptography

In this project we are going to use this algorithm for the authentication of the student as well as verification of the student through his identity card i.e. AADHAR

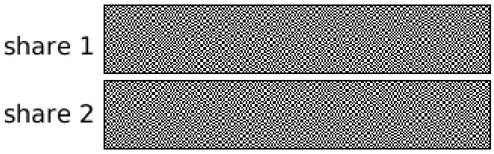

Fig .2 Share1 and share2 secret images.

share 1
+
share 2
WIKIPEDIA

Fig .3 Share1+share2 output after staking overreach other.

Share 1 image copy is shared to admin through mail.
Share 2 image copy is shared to the admin through mail.
When admin is logged in to the website then the share1+share2 images will generate a secret code visible which admin has to submit to proceed in result entry process.

2. Proposed System

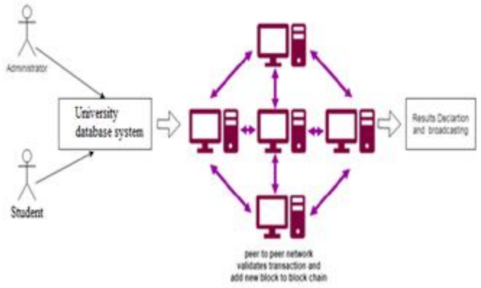
Administrator
Student
University database system
Results Declartion and broadcasting
peer to peer network validates transaction and add new block to block chain

Fig.4 Proposed System

In this architecture actually there are two working modules used

- Administrator
- Student

2. 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

3. Student

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

III. 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 block chain 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 todays scheme and offer new possibilities of transparency.

REFERENCES

[1]. An Database management based on Blockchain, Yi Liu and Qi Wang
[2]. Crypto-voting, a Blockchain based database System, Francesco Fusco, Maria Ilaria Lunes, Filippo Eros Pani and Andrea Pinna
[3]. Zerocash: Decentralized Anonymous Payments from Bitcoin, Eli Ben Sasson ; Alessandro Chiesa ; Christina Garman ; Matthew Green ; Ian Miers ; Eran Tromer ; Madars Virza, 2014 IEEE Symposium on Security and Privacy, IEEE,
[4]. SHARVOT: Secret SHARe-Based data management on the Blockchain, Silvia Bartolucci ; Pauline Bernat ; Daniel Joseph, 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Block chain (WETSEB), IEEE.
[5]. Secured data storage Using Block-Chain Service (Jushua I James):
[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. (2008). Anonymous voting by two-round public discussion
[8]. Feng Hao and Piotr Zielinski. A 2-Round Anonymous Veto Protocol.
[9]. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability.