NATIONAL CONFERENCE
ON RECENT ADVANCEMENTS
IN
COMMUNICATION, ELECTRONICS
AND SIGNAL PROCESSING

RACES '19

15th March 2019

ORGANIZED BY
DEPARTMENT OF ELECTRONICS AND
COMMUNICATION ENGINEERING

Velammal Engineering College
Velammal Nagar, Ambattur-Redhills Road, Chennai- 600 066, Tamilnadu
Phone: 044-39666005/6/7, 39666020 Fax: 044 -26591771 Mobile: 9445257427, 9884711794
Email: ncraces2019@gmail.com
Website:www.velammal.org

IMPLEMENTATION OF BLOCK-CHAIN TECHNOLOGY FOR STUDENT DATABASE IN JAVA PLATFORM

L.Ashok Kumar, M Prudhvi Ram, P Jayasankar Reddy, B Praveen Kumar,
ashok2002ttd@gmail.com; maddinaprudhviram@gmail.com ; jayasankarreddy.pulasani@gmail.com;
praveenkumar333007@gmail.com; ECE Department, Panimalar Institute of Technology,Chennai.

***Abstract*- As of now the emerging trend in technology is never complete without having a secure platform for its applications and Block-Chain technology promises this cryptography features by employing secured hashing algorithms. This Block-Chain technology uses distributed technology unlike the centralized databases in typical internet model which made it theoretically 51% unhackable in near future. Who knows in future Block-Chain Technology may replace the whole internet model. Don't doubt it for a couple of reasons. Firstly it has potential features which are more than enough to replace the current internet model and secondly a huge number of companies are investing in this Block-Chain Platform. In this paper, we are going to integrate the Oracle database to implement Block Chain Technology for basic student database in java platform and consequently implementing for any relational database. Further with these works, we are willing to monitor big data such as stock market transactions etc.**

INTRODUCTION

The ultimate goal of this project is to use basic concepts of the implementation behind the Blockchain and similar digital ledger techniques in JAVA platform and beyond its application to crypto-currency. Thereafter to use this Block-Chain technology to build non-compromising databases under any circumstances. Block-Chain is a trending new technology to work on and we are trying to mention a basic background study over this field in here. In the last ten years, Since when Satoshi Nakamoto published and deployed block-chain this interesting and practically un-hackable concept came into existence in 2008 [1].

The usage of Block-Chain and other digital ledger techniques, their pros and cons, applications, security and privacy issues were closely monitored in order to come up with the idea of this project. Identifying and exploring the possible directions for the future use of Block-chain beyond crypto-currency is a major concern for this course of monitoring the developments in Block-chain technology. Block-chain which is the backbone of the Bitcoin crypto-currency system, is arguably the most important feature for building the foundation for developing most of security and privacy that is being employed in many other fields which include smart contracts [2], public services [3], Internet of Things (IoT) [4], reputation systems [5] and security services[6].

The POW(proof of work) concepts bring up the mathematical challenge(difficulty of continuing the chain of blocks by calculating hashes required for next block before genuine user founds is an ideal situation) to any intruder who tries to enter this Block-Chain without authentication to mine particular block or any other block and this ensures Block-Chain security by maintaining a digital record of transactions that are considered as unchangeable when once validated.

Further, This Block-Chain uses an alterable Public Key to record the user identity and this gives an extra layer of privacy for that user who makes transactions through Block-Chain. As of now, Block-Chain has been implemented in various fields and it made us undertake this opportunity to add an extra layer of security in our platforms which we are using right now by employing Block-Chain concepts and by injecting the Block-chain into our platforms. Thus we came up with this project to Implement a database in java platform using Block-chain concepts.

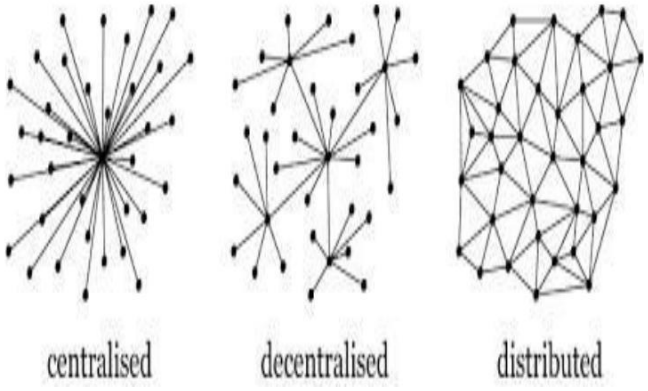

Fig.I.1

WHAT THE BLOCK-CHAIN TECHNOLOGY CAN DO FOR US

Some future consumer applications that share the vision of BCT sound like science fiction, but some of the more practical and realistic sounding possibilities for the technology include

(1). Various non-financial activities which include but not limited to online voting, absolute messaging are possible with BC without the fear of being tampered.

(2). Distributed cloud storage systems, Proof Of Location, healthcare and so on [7].

(3). Implementation of Block-Chain for increasing security, to check the disadvantages associated with this BC and later on, later on, to develop solutions for Block-Chain enabled enhanced security applications.

BENEFITS OF BLOCK CHAIN

The potential benefits that need to be mentioned about blockchain are :

(1). Secured and tamper-proof.
(2). Practically Unhackable.
(3). Reliable, easy to deploy and easy to maintain.
(4). Minimal requirements or resources needed for deploying chain.

IV. OUR CONTRIBUTION

We have combined the concepts of both Block-Chain and a relational database(in our project Oracle database) to deploy a student data precisely grades in java platform without compromising on privacy.

Simply speaking we are just trying to deploy the chain structure in this platform and we are not denying a chance for future deployments in various categories, In the matter of fact, we already have different ideas to sort things out.

In our project, the only administrator can alter changes in the database and once chain deployed in full length, not even admin can change without being found.

BASIC CONCEPTS

Let's understand a few terms before diving into this project. Mostly these are the exact terms or the idea behind the terms that we have used in our project.

Hash:

It's the most important aspect of our project. We have used the inbuilt message digest library in java in order to get hashed output. We have used SHA-256(Secured Hashing Algorithm-256bit) in our project which generates each message that is fed into it to 64-digit hexadecimal number.

For easy understanding, we can compare the hash to that of our fingerprint. Since only one fingerprint can unlock something similar way that only particular data can have a certain hexadecimal number of its own which is highly unpredictable on looking at the output that is generated after applying SHA-256.

It also adds mathematical difficulty if someone tries to hack that particular data. The output generated by this SHA is just like one-way traffic just because without knowing what parameters used in the function or the input value its nearly impossible to crack and hence reverse engineering is quite difficult in this case. If someone tries so then it will be just like generating fingerprint without the possessing original fingerprint.

For example: Just by adding a (.) at the end we can see that hashes changed drastically.

Sha256[Block Chain] =
7e7eb1d0b9472461ae6b448e274285004cbb111c898cbd97d4a94480fe489933

Sha256[Block Chain.] =
fa1482a66e7c4ef1e983fa866684e3ff041b79bd49b39abe574f86263805760f

Block-Chain:

On seeing the name itself we can say that it is the combination of blocks or simple chain of blocks. These blocks are deployed in such a way that each and every block. Technically speaking we would like to define it as a decentralized computational and informational platform that enables various permissioned domains in which no user needs to trust each other to co-operate, co-ordinate and to participate in any decision-making process.

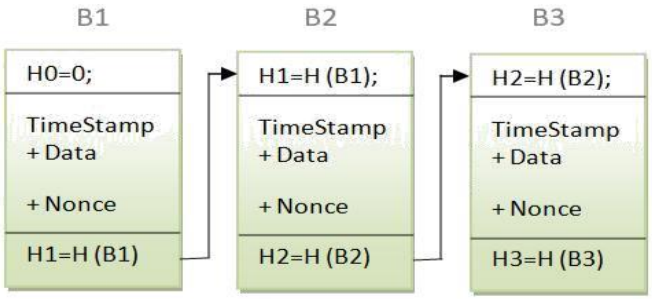

Fig.V.b.1

Difficulty:

It is the exact concept of time-delay that is employed in BC(Block-Chain). It is simply how difficult to mine particular block with the target that is being set for matching a hash. Roughly it takes (+10min to +15minutes) to generate a block in BTC Block-Chain. During this time delay, it uses some of its nodes to validate and the no. of nodes required to check truly based on the size of the BTC transaction.

The difficulty level in public BC depends on time consumed for generating last 2016 blocks. If time consumed is lesser than the span of two weeks then the difficulty is raised and if time consumed is greater than the span of two weeks then the difficulty is decreased. Difficulty level indicates no. of zeroes that are added in front of a hexadecimal number the more the no. of difficulty the lesser chance to get the exact hash.

Cryptography:

The way of encrypting or decrypting something such that only intended parties with the right key or password can view the message can be called as cryptography.

In the case of BC(Block-Chain) which is used to cover the sender details and to make sure that the previous records in the chain are untampered. Of all the ways available to encrypt we choose SHA-256 in our sample project as that of bitcoin blockchain.

e. Proof-Of-Work(POW):

POW(Proof of work) is a consensus strategy used in the Bitcoin network [1]. It's the concept which adds value to the bitcoin. Simply each system or machine spends its computational power along with electricity to mine a block and the block that is mined can be called as a POW and the miners get a fraction of transaction for mining/adding that block to Block-Chain. We have used the mining concept in our project just to check whether the mined blocks are valid or not.

Timestamp:

It fetches the time that is exactly available to it in year-month-date-hour-minutes-seconds format and converts it into subsequently to an unsigned integer value that is no. of seconds from the standard first of January 1970. (For example Tuesday, 05-Mar-19 21:07:07 UTC is 1551820027. That is for the mentioned time 1551820027seconds counted). This concept is being employed in various cases including patent forms. In our project, we employed this function so as to find any changes made to the database.

g. Nonce:

It's the random number just like OTP or simply the random number that is generated by authenticator application that is intended to find the particular hash in order to generate a block in the intended/targeted time or lesser than the targeted time. We have used nonce too in our Chain.

VI. CATEGORIES OF BLOCK-CHAIN

The BC can be classified into 3 categories:

(1). PUBLIC BC :

It is just like that of Bitcoin and Ethereum.

(2). PRIVATE BC:

It can be called as a permission BC since every participant needs to get permission from an administrator.

(3). CONSORTIUM BC :

These are the chains that organizations can develop using platforms like Hyper-Ledger or any other platform to meet their own requirements. This can be closely related to the chain we have developed [8],[9].

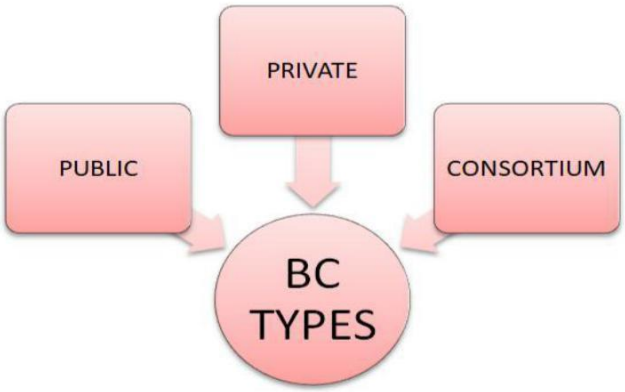

Fig.VI.1

VII. EXISTING SYSTEM

It's limited to most of the crypto-currencies like Bitcoin and a trend has started to implement smart contracts through BCT. It tends to lose some of its cryptographic features when tried to implement in various platforms.

VIII. PROPOSED SYSTEM

Provides a convenient platform by using both the Java platform and Oracle database without losing its cryptographic features.

IX. HARDWARE REQUIREMENTS

(1). Minimum Disk space (primary) 4GB, 128GB/+(SECONDARY)
(2). PROCESSOR: Intel Core i3 and above OR AMD FX 4100 and above.

SOFTWARE REQUIREMENTS

(1). Windows 8/8.1/10 (Any version).
(2). JDK, Oracle database 11g express edition,(Oracle dev tools).
(3). ojdbc6.jar file.
(4). google-gson-2.6.1jar/newer versions.

XI. OVERVIEW

First of all, we have just implemented a basic blockchain in java platform. google-gson-2.6.1jar/newer versions. A database with admin privileges is created. Further through code we have created and saved students marks details in the Oracle database.

In our final move, we have just imported the student table from oracle database to java by interfacing Java with Oracle database using OJDBC 6 jar file to display output in blocks. We used google-gson-2.6.1jar just to make sure that everything the code takes its inputs must follow the same order for each time it runs.

XII. CONCLUSION

As this technology advances, there may be more struggles to face or they may be better solutions but, one thing is for sure that it may take at least 10-15 years to use this technology to its full capability. We are further willing to test apply our method for bank transactions and for monitoring a trading platform. There is an urgent need to empower people about this new interesting technology and we think we have played a part in it. To the better and secured future may this Block-Chain lay a better way ahead.

XIII. REFERENCES

Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013.

Y. Zhang and J. Wen, "An IoT electric business th protocol Procmdeledingsbasedofon18 theof bitcoin," International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.

M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for the educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL2015), Lyon, France, 2015, pp. 490–496.

C. Noyes, "Bitav: Fast anti-malware by distributedblockchainconsensusand feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.

G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.

"Consortium chain development." Available at:https://github.com/ethereum/wiki/wiki/Consortium-Chain- Development.

"Hyperledger project," 2015. Available at https://www.hyperledger.org/