A NOVEL SOLUTION FOR BANKING SECTORS TO MAKE SECURE TRANSACTION USING BLOCK CHAIN TECHNOLOGY

K.ELAIYARANI[1],KRISHNA KUMAR C[2]
[1]Assistant Professor, Department of ECE,
[2]Assistant Professor, Department of CSE,
[1,2]DhanalakshmiSirinvasan College of Engineering and Technology, Chennai

Abstract—Effective information retrieval system in hospital is a web app which can be used in hospitals to upload patient details. Using this web app upload patient details for first time and generate a user ID for the particular patient for center use also. This user ID can be used by the patient for later use in any hospital which are linked by this web app. The proposed web app can reduce the time for the patients and the hospital workers for center use. Also, this web app can be used in any hospitals if the patient had a user ID. In this web app we provide security using Advanced Encrypted Standard algorithm. Our major goal is to link many hospitals in a single web app and to provide the details similarly. The proposed web app provides user ID for the patients and it is easier to break anywhere.

1. INTRODUCTION

A blockchain is a distributed transaction ledger. The blockchain itself is composed of blocks, with each block representing a set of transactions. As a data structure, a blockchain has several interesting properties. First, blocks are provably immutable. This is possible because each block contains a hash, or numeric digest of its content, that can be used to verify the integrity of the containing transactions. Next, the hash of a block is dependent on the hash of the block before it. This effectively makes the entire blockchain history immutable, as changing the hash of any block n − i would also change the hash of block n. The blockchain itself does not depend on a central, trusted authority. Rather, it is distributed to all nodes participating in the network. Because no centralized authority may verify the validity of the blockchain, a mechanism for reaching network consensus must be employed. In Bitcoin, a Proof of Work function is used to ensure network consensus. This strategy requires that any node wishing to add a block to the blockchain must complete a computationally expensive (but easily verifiable) puzzle first. At a high level, this ensures consensus of the network because there is an opportunity cost (the computation time) to building a block. There are several other techniques used, such Proof of Stake and Proof of Activity, but all are designed to drive the network to consensus on blockchain validity. Miners are nodes that assemble the blocks and add them to the blockchain. It is through the miners that the consensus strategy is enacted, usually via some incentivization protocol. In Bitcoin, for example, miners are incentivized by collecting transaction fees and also by a reward for adding the block to the blockchain. In general, however, there should exist an incentive for them to only build on top of valid blocks, which in turn drivesthe entire network to consensus.

2. EXISTING SYSTEM

Most banking systems in the world, built on a centralized database, are more vulnerable to cyberattack because once hackers attack the one system they get full accesswhich takes a service charge and is subject

togreater regulation and higher costs due to the prevalence of fraud.The traditional bank system uses centralized cloud for storing customer information that means we are placing a very large amount of trust in these third parties, particularly sensitiveinformation like account details transaction etc.

3. PROPOSED SYSTEM

The blockchain application changes the paper-intensive international trade finance process to an electronic decentralized ledger that gives all the participating entities. The blockchain application changes the paper-intensive international trade finance process to an electronic decentralized ledger that gives all the participating entities, including banks, the ability to access a single source of information. It also allows them to track all documentation and validate ownership of assets digitally, as an un-alterable ledger in real time.Blockchain provides a very high level of safety and security when it comes to exchanging data, information, and money. It also allows users to take advantage of the transparent network infrastructure along with low operational costs with the aid of decentralization.These characteristics make blockchain reliable, promising and in-demand solution for the banking and finance industry.The system would allow only authorised participants to access the data and keep a log of all the logging entries.

4. MODULES

USER MODULE: When the user registering for banking service the system will auto generate a unique account number and IFSC code.Also we will generate a public key and a private key to ensure the secured transaction. We use sha-256 one-way hashing algorithm is used for generating keys.The public key will be shared to the network and private key kept secrete.

MINER MODULE: Mining involves the use of computers to run hashing algorithms to process the most recent block, with the information needed in mining found in the block's header.The blockchain network sets a target value for this hash – the target hash - and miners try to determine what this value is by testing out all possible values.Cycling through solutions in order to guess the nonce is referred to as proof of work, and the miner who is able to find the value is awarded the block and paid.The target hash is adjusted periodically. The hash functions used to generate the new target have specific properties designed to make the blockchain secure.

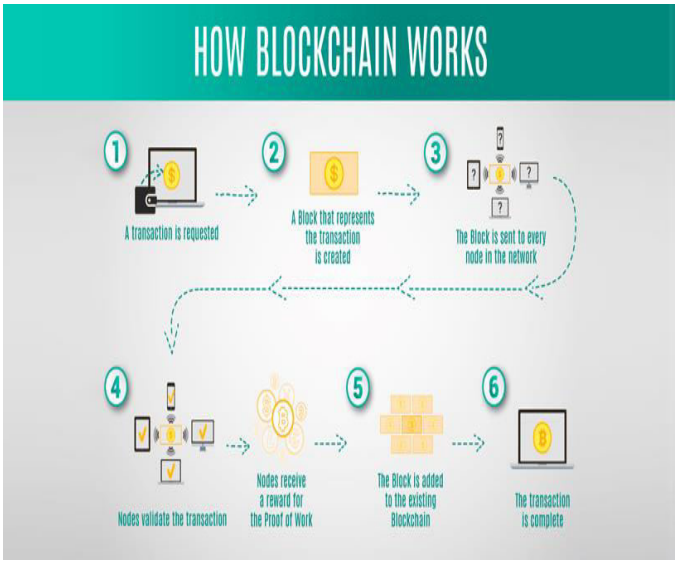

Fig.1 Working of Blockchain

5. ALGORITHMS

SHA-256 ALGORITHM: The hash concept is actually quite simple. It's the amount of jargon used that confuses people. Simply stated, **a hash function takes some input data and creates some output data.**In order to produce a private key, which is a randomly selected number, is multiplied using an elliptic curve to produce a public key. This public key is then put through the SHA-256 hashing algorithm.

AES: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

6. SYSTEM TESTING

System testing is a critical aspect of Software Quality Assurance andrepresents the ultimate review of specification, design and coding. Testing is aprocess of executing a program with the intent of finding an error. A good test isone that has a probability of finding an as yet undiscovered error. The purpose oftesting is to identify and correct bugs in the developed system. Nothing iscomplete without testing. Testing is the vital to the success of the system.In the code testing the logic of the developed system is tested. For thisevery module of the programis executed to find an error. To performspecification test, the examination of the specifications stating what the programshould do and how it should perform under various conditions. Unit testingfocuses first on the modules in the proposed system to locate errors. This enablesto detect errors in the coding and logic that are contained within that modulealone. Those resulting from the interaction between modules are initially avoided.In unit testing step each module has to be checked separately.System testing does not test the software as a whole, but rather thanintegration of each module in the system. The primary concern is thecompatibility of individual modules. One has to find areas where modules havebeen designed with different specifications of data lengths, type and data elementname. Testing and validation are the most important steps after theimplementation of the developed system. The system testing is performed toensure that there are no errors in the implemented system. The software must beexecuted several times in order to find out the errors in the different modules ofthe system.

Validation refers to the process of using the new software for the developed system in a live environment i.e., new software inside the organization,in order to find out the errors. The validation phase reveals the failures and the68bugs in the developed system. It will be come to know about the practicaldifficulties the system faces when operated in the true environment. By testingthe code of the implemented software, the logic of the program can be examined.A specification test is conducted to check whether the specifications stating theprogram are performing under various conditions. Apart from these tests, thereare some special tests conducted which are given below:

Peak Load Tests: This determines whether the new system will handle thevolume of activities when the system is at the peak of its processing demand. Thetest has revealed that the new software for the agency is capable of handling thedemands at the peak time.

Storage Testing: This determines the capacity of the new system to storetransaction data on a disk or on other files. The proposed software has the requiredstorage space available, because of the use of a number of hard disks.

Performance Time Testing: This test determines the length of the timeused by the system to process transaction data.In this phase the software developed Testing is exercising the software touncover errors and ensure the system meets defined requirements. Testing may
be done at 4 levels

- Unit Level
- Module Level
- Integration & System
- Regression

UNIT TESTING

A Unit corresponds to a screen /form in the package. Unit testing focuseson verification of the corresponding class or Screen. This testing includes testingof control paths, interfaces, local data structures, logical decisions, boundaryconditions, and error handling. Unit testing may use Test Drivers, which are69control programs to co-ordinate test case inputs and outputs, and Test stubs,which replace low-level modules. A stub is a dummy subprogram.

VALIDATION TESTING

In this requirement established as part of software requirements analysisare validated against the software that has been constructed. Validation testingprovides final Assurance that software meets all functional, behavioral andperformance requirements. Validation can be defined in many ways but a simpledefinition is that validation succeeds when software Function in a manner thatcan be reasonably by the customer.

1. Validation test criteria
2. Configuration review
3. Alpha and Beta testing (conducted by end user)

MODULE LEVEL TESTING

Module Testing is done using the test cases prepared earlier. Module isdefined during the time of design.

INTEGRATION & SYSTEM TESTING

Integration testing is used to verify the combining of the software modules.Integration testing addresses the issues associated with the dual problems ofverification and program construction. System testing is used to verify, whetherthe developed system meets the requirements. System testing is actually a seriesdifferent test whose primary purpose is to full exercise the computer base system.Where the software and other system elements are tested as whole. To testcomputer software, we spiral out along streamlines that broadens the scope oftesting with each turn.The last higher-order testing step falls outside the boundary of softwareEngineering and in to the broader context of computer system engineering.Software, once validated, must be combining with order system Elements (e.g.70hardware, people, databases). System testing verifies that all the elements Meshproperly and that overall system function/performance is achieved.

1. Recovery Testing
2.Security Testing
3.Stress Testing

REGRESSION TESTING

Each modification in software impacts unmodified areas, which resultsserious injuries to that software. So, the process of re-testing for rectification oferrors due to modification is known as regression testing.

Installation and Delivery: Installation and Delivery is the process of deliveringthe developed and tested software to the customer. Refer the support procedures.

Acceptance and Project Closure: Acceptance is the part of the project by whichthe customer accepts the product. This will be done as per the Project Closure,once the customer accepts the product, closure of

the project is started. Thisincludes metrics collection, PCD, etc.

7.CONCLUSION

Block chain technology could have a tremendous impact on the proceduresfor concluding and confirming transactions, managing cash, and optimizingassets, as well as many other business processes which altogether account forbillions of dollars in annual expenses for banks today. The solutions developedare much faster and more reliable than most block chain-based solutions on themarket. I do our best to ensure that our technology is developed and implementednot only by companies in the IT sphere, but also in real sectors of the economy.Banking is one of the most promising spheres to benefit from the advantages ofblock chain. Block chain makes it possible to reduce timeframes that havebecome accepted and established, such as the time from a loan application beingapproved to the funds actually being received, the time required for interbank or international transfers to be carried out, the time required for processing andconfirming personal information, and so on.

8.THE FUTURE OF BLOCKCHAIN BANKING

Block chain and distributed ledgers have a bright future. As real-time,open- source and trusted platforms that securely transmit data and value, they canhelp banks not only reduce the cost of processing payments, but also create newproducts and services that can generate important new revenue streams. The biggest key to turning block chain's potential into reality is a collaborative effortamong banks to create the network necessary to support global payments. Banksneed to look at the bigger picture and work together and with non-banks to helpdefine the backbone that can underpin a universally accepted, ubiquitous globalpayment system that can transform how banks execute transactions.

REFERENCE

[1]Al-Riyami S.S. and Paterson K.G. (2003), 'Certificateless public keycryptography', in Asiacrypt, Springer, Vol. 2894, pp. 452–473.

[2] Sahai A. and Waters B. (2005), 'Fuzzy identity-based encryption', inAdvances in Cryptology–EUROCRYPT, Springer, pp. 457–473.

[3] Atzori L., Iera A. and Morabito G. (2010), 'The internet of things: A survey', Computer networks, Vol. 54, pp. 2787–2805.

[4] Dziembowski S., Faust S., Kolmogorov V., and Pietrzak K. (2015), 'Proofsof space', in Annual Cryptology Conference,Springer, pp. 585–605

[5] Goldfeder S., Gennaro R., Kalodner H., Bonneau J., Kroll J.A., Felten E.V.and Narayanan A. (2015), 'Securing bitcoin wallets via a new dsa/ecdsa threshold signature scheme'.

[6] Hofmann E, Strewe UM, Bosia N. Supply chain finance and blockchaintechnology: the case of reverse securitisation. Springer; 2017.

[7] Alketbi A, Nasir Q, Talib MA. Blockchain for government services-use cases, security benefits and challenges. In learning and technologyconference 2018 (pp. 112-9). IEEE.

[8] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure andlightweight

certificate less signature scheme for IIoT environments," IEEETrans. Ind. Informat., vol. 14, no. 8, pp. 3701-3711, Aug. 2018.