E wallet Architecture Using Block chain Technology

OBJECTIVE:

1. To implement a java based web application.
2. To implement AES.
3. To implement visual cryptography.
4. To implement block chain.
5. To implement distributed database system using WLAN.

DOMAIN: Security, Mobile Computing, Block chain Technology

ABSTRACT:

A cashless society describes an economic state whereby financial transactions are not conducted with money in the form of physical banknotes or coins, but rather through the transfer of digital information (usually an electronic representation of money) between the transacting parties. Cashless societies have existed from the time when human society came into existence, based on barter and other methods of exchange, and cashless transactions have also become possible in modern times using digital currencies such as bitcoin. However this article discusses and focuses on the term "cashless society" in the sense of a move towards, and implications of, a society where cash is replaced by its digital equivalent—in other words, legal tender (money) exists, is recorded, and is exchanged only in electronic digital form Such a concept has been discussed widely, particularly because the world is experiencing a rapid and increasing use of digital methods of recording, managing, and exchanging money in commerce, investment and daily life in many parts of the world, and transactions which would historically have been undertaken with cash

are often now undertaken electronically. Some countries now set limits on transactions and transaction values for which non-electronic payment may be legally used. Here in this paper we are going to discuss about how we can use block chain technology for digital economy for digital India.

Keywords: Below the abstract

INTRODUCTION

Today money is not safe in the form of cash neither in banks. Imagine this scenario: You invested Rs 10 lakh in a bank fixed deposit for tenure of 2 years. The interest every quarter for seven quarters was earned/received by you, but just a few months before the deposit was about to mature, the bank owing to multiplying financial troubles (which ultimately led to the banking regulator impose some controls) didn't pay your hard-earned money on the date of maturity. There are numerous such instances, where investors have lost their hard-earned money with banks ---owing to financial mismanagement at banks --- and consequently, the Reserve Bank of India (RBI) taking Prompt Corrective Action (PCA) against them. Currently, UCO Bank, United Bank of India, Central Bank of India, Indian Overseas Bank, Punjab & Maharashtra Co-operative (PMC) Bank, to name a few are under the PCA of the RBI. The track record of co-operative banks has been horrific. According to RBI data, there were 1,926 Urban cooperative Banks (UCBs) in 2004; and over the last 16 years, the RBI was compelled to merge 129 weaker cooperatives with stronger banks. Nearly 246 UCBs collapsed over the last 16 years. And this risk of default is only increasing; the potential risk is systemic and things could get out of hands quite quickly if timely measures aren't taken. The latest, i.e. the 21st edition of Financial Stability Report (FSR) released by the RBI, highlights several downside risks, although India's financial system remains stable. All major risk indicators, global risk, financial market risk, and expected macroeconomic risk, remain in the 'high' to 'very high' zone. RBI has cautioned all stakeholders (which includes depositors as well) about the potential rise in Gross Non-performing Assets (GNPAs) of the sector in the coming quarters. As the on-going pandemic has affected life as well as livelihood, its impact on credit growth, the asset quality of banks, and the capital adequacy of banks has been and is likely to be adverse. The process of deleveraging of corporate balance sheets, which was making steady progress during the pre-COVID times, got severely impacted by the

pandemic. Macro stress tests for credit risk indicate that the GNPA ratio of all SCBs may increase from 8.5 per cent in March 2020 to 12.5 per cent by March 2021 under the baseline scenario. If the macroeconomic environment worsens further, the ratio may escalate to 14.7 per cent under very severe stress, mentions the RBI's Financial Stability Report. According to the FSR, close to 67% of customers of Public Sector Banks (PSBs) and 49% of customers of private sector banks availed the moratorium facility as of April 30, 2020. Nearly 1/3rd of the loan book of private sector banks and 2/3rd of the PSBs was under moratorium. And this is very scary. Time and again, the government has assured that depositors' money with banks is safe; but please do not take such assurances too seriously. Given that NPAs of most banks are on a rise, your hard-earned money is not necessarily 100% safe with a bank. The financial stress in the Indian banking system (and debt market) is certainly building up, and this increase in the systemic level may blow off investors' money for no mistake on their part. The government introduced the Financial Resolution and Deposit Insurance (FRDI) Bill in the lower house of the Parliament in August 2017 but subsequently withdrew it in August 2018. This is because in the proposal of setting up a resolution corporation, the Bill had an extremely controversial bail-in clause, wherein it effectively permitted conversion of the term deposit with the bank into equity to recapitalize the bank if it fails. Bail-in is the opposite of bail-out. When a government bails out a bank, it primarily uses taxpayers' money to save that entity. In contrast, the bail-in clause permits using depositors' money to reduce the liability of the bank. Given the strong uproar in the media, the government had to back off on the proposal. Just before the COVID-19 pandemic hit the country in March, the government was pondering upon introducing the modified version of FRDI, rechristening it as Financial Sector Development and Regulation (FSDR) Bill. And now that the banking and financial sector has come under massive pressure amidst the coronavirus pandemic, the talks of setting up a resolution under the legislative framework of the new FSDR system has started gathering momentum. Non-Banking Financial Companies (NBFCs), insurance companies, capital market players, co-operative societies, regional rural banks, payment banks, will all come under the purview of the proposed resolution authority. "We need a structured mechanism with the legal backing to deal with stressed assets" opined RBI Governor, Mr Shaktikanta Das.So there is need of totally cashless system, which must be secure too so we are going to implement a gitial economy for digital India using BCT.

PROBLEM STATEMENT

To develop an android base application for e wallet architecture using block chain features using java programming language.

MOTIVATION

The digital innovations in the banking sector started with the introduction of money that replaced the barter system and then the gradual replacement of wax seal with digital signatures. One such disruptive innovation which is changing the banking sector globally is Blockchain Technology (BCT). Blockchain is shared distributed ledger which stores business transaction to a permanent unbreakable chain which can be viewed by the parties in a transaction. Blockchain technology has the potential to disrupt the nancial business applications as it provides permanent and tamper proof recording of transactions in a distributed network.

LITERATURE SURVEY

The Implementation of E-money in Mobile Phone: A Case Study at PT Bank KEB Hana

Didik Haryadi ; Harisno ; Victory Haris Kusumawardhana ; Harco Leslie Hendric Spits Warnars

Published in: 2018 Indonesian Association for Pattern Recognition International Conference (INAPR)

The purpose of this research is to examine the design of e-money and to propose some development ideas for e-money implementation. The system here employs electronic payment via QR code and encryption technology.

A Landscape of Cryptocurrencies

Zhaofang Li ; Qinghua Lu ; Shiping Chen ; Yue Liu ; Xiwei Xu

Published in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

The generated landscape, which reports the state of cryptocurrencies and can be used as a framework for cryptocurrency analysis, provides a breakthrough understanding of cryptocurrencies.

Security Management and Visualization in a Blockchain-based Collaborative Defense

Christian Killer ; Bruno Rodrigues ; Burkhard Stiller

Published in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

The goal of this project is to create a security management dashboard for BloSS that can be used interactively by cyber security analysts. DDoS attacks in defence systems are the subject of this research.

On the Effectiveness of Multi-Token Economies

Published in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

This paper discusses token classification, the rationale for implementing multi-token economies, and their efficacy. Steemit is examined as a representative example of multi-token economies. We explain how the multi-token economy works and show how it differs from other types of economies. We also propose criteria for evaluating multi-token economies.

Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract

Van-Cam NGUYEN ; Hoai-Luan PHAM ; Thi-Hong TRAN ; Huu-Thuan HUYNH ; Yasuhiko NAKASHIMA

Published in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

This paper proposed using BCT to implement the VAT system as an online system. In an online system, a distributed database system is used. BCT can protect the system from being hacked.

Analysis of the Possibilities for Improvement of BlockChain Technology

Daniela Mechkaroska ; Vesna Dimitrova ; Aleksandra Popovska-Mitrovikj

Published in: 2018 26th Telecommunications Forum (TELFOR)

The purpose of this paper is to investigate block chain technology. A study on the design and development of BCT was proposed in the paper. The feasibility of BCT was determined, and it was determined that BCT is a secure and efficient system.

EXISTING SYSTEM:

Existing system is based on cash economy and banking sector. Existing systems are centralized so there are chances of corruption, hacking etc.

PROPOSED SYSTEM:

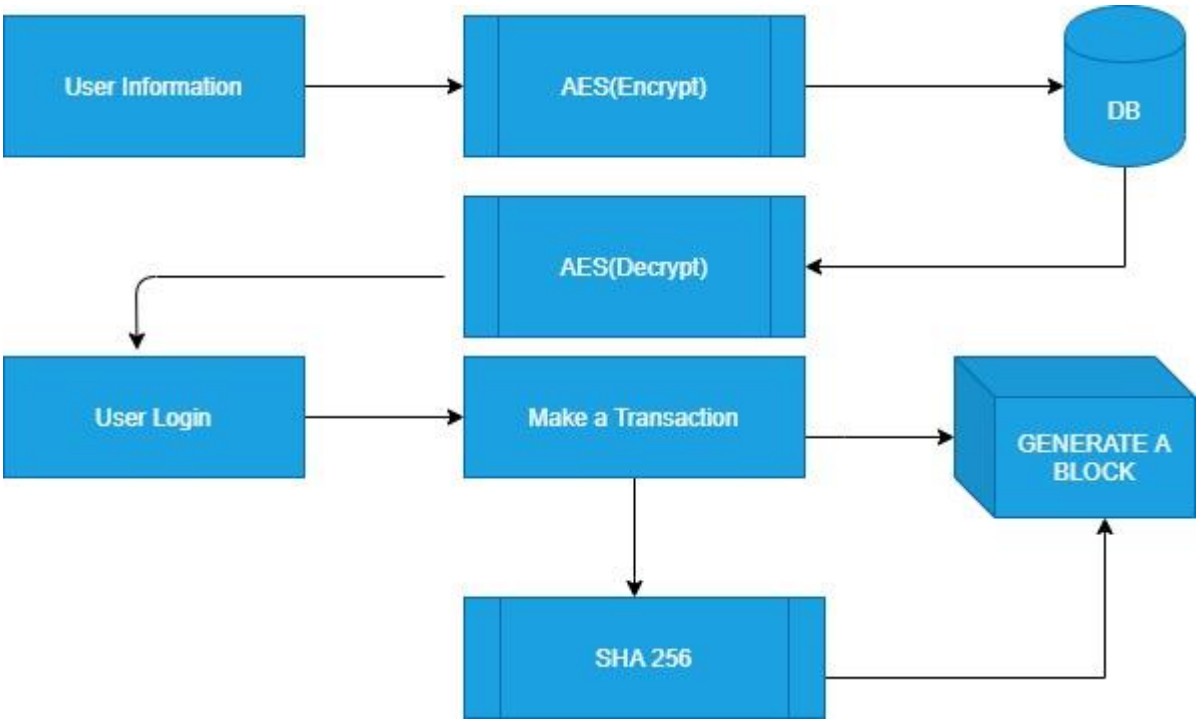

Fig: Proposed System

Whenever user does registration, the information will first feed to the AES block which will encrypt the information and then stores it to the database. When user does registration, it will require information from the database in the normal format and not encrypted so the information from the database will be decrypted and then user can perform login. After login user can transfer amount to some another user

which will generate a block of transaction which is a permanent record of transaction. In this way a block will be generated which can't be changed further.

MODULES

Hash Generation:

Step 1. Append Padding Bits. The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. ...

Step 2. Append Length. ...

Step 3. Initialize MD Buffer. ...

Step 4. Process Message in 16-Word Blocks. ...

Step 5. Output.

In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value.

As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

An MD5 hash is typically expressed as a 32 digit hexadecimal number

Database Encryption:

AES is used to encrypt the database.

The encryption process uses a set of specially derived keys called round keys.

These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted.

This array we call the state array.

STEPS:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.

- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation
- Copy the final state array out as the encrypted data (ciphertext)

SYSTEM REQUIREMENT SPECIFICATION

Hardware Requirement

1. Processor: Intel Core I3 or Higher

2. RAM: 4 GB or Higher

3. Hard Disk: 100 GB (min)

Software Requirement:

1. Operating System: Microsoft Windows 7 and Above

2. Programming Language: Java

3. IDE: Netbeans, Android Studio

SCHEDULE

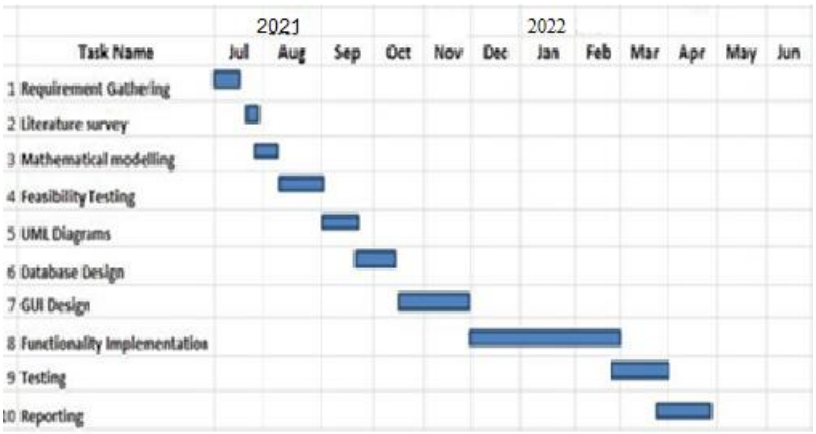

Table: Project Schedule

ADVANTAGES

1. Secure
2. Reliable
3. Immutable
4. Ant hacking
5. Transparent

LIMITATIONS

Requires more space.

APPLICATION OF THE PROPOSED SYSTEM

Educational Sector

Government Sector

Agricultural Sector

Enterprises

Organizations.

PURPOSE AND SCOPE

In future we will try for sponsorship from government and will implement a project on large scale with some domain and hosting space online.

REFERENCES

[1] F. Lv and S. Chen, "Research on Establishing a Traceability System of Quality and Safety of Agricultural Products Based on Blockchain Technology," Rural Finance Research, vol. 12, pp. 22-26, 2016.

[2] Y. Yang and Z. Jia, "Application and Challenge of Blockchain Technology in the Field of Agricultural Internet of Things," Information Technology, vol. 258, pp. 24-26, 2017.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2008.

[4] Y. Yuan and F. Y. Wang, "Blockchain: The State of the Art and Future Trends," Acta Automatica Sinica, 2016.

[5] Y. Yuan, T. Zhou, A. Y. Zhou, Y. C. Duan, and F. Y. Wang, "Blockchain Technology: From Data Intelligence to Knowledge Automation," Zidonghua Xuebao/acta Automatica Sinica, vol. 43, pp 1485-1490, 2017.

[6] Y.-b. Zhang, "The New Ecosystem of Cross-border E-commerce between EU and China based on Blockchain," China Business And Market, vol. 32, pp. 66-72, 2018.

[7] T. Hong, "Accelerating the Application of Blockchain in the Field of Agricultural Products E - commerce in China," Journal of Agricultural Information, pp. 18-20, 2016.

[8] Y. Yuan and F.-Y. Wang, "Parallel Blockchain: Concept, Methods and Issues," IEEE Acta Automatica Sinica, vol. 43, pp. 1703-1712, 2017.

[9] Andreas M A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014.

[10] Jerry B, Andrea C. Bitcoin: A Primer for Policymakers. Mercatus Center, George Mason University, 2013.

Project Guide Project Coordinator HOD