International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

SECURE DIGITAL ECONOMY USING BLOCK CHAIN TECHNOLOGY AND CRYPTOGRAPHIC TECHNIQUES

Mr.Gopal Bugad
U.G. student, Department Computer Engineering RMDSSOE, Pune, India.

Ms.Poonam Surwase
U.G. student,Department of ComputerEngineering RMDSSOE, Pune, India.

Mr.Rutul Khedkar
U.G. student,Department of ComputerEngineering RMDSSOE, Pune, India.

Ms. Raksha Kapse
U.G. student, Department of of Computer Enginnering RMDSSOE, Pune, India.

Ms.Manisha Desai
Assistant professor,
Department of Computer Engineering, RMDSSOE,
Pune, India

ABSTRACT: *The Indian government declared that the country's two highest-denomination bank notes will no longer be legal tender, headed by Prime Minister Narendra Singh Modi. The two denominations accounted for about 86 percent of all cash in circulation in India at the time. People who had banknotes were required to deposit them in the bank. The Indian government planned to prosecute tax evaders in the future with this move. If people with significant sums of "black money" tried to deposit the demonetized banknotes, they would be asked questions. Banking and technology are inextricably related, and technical advances have dramatically altered banking over time. The introduction of currency, which replaced the barter system, was followed by the gradual replacement of wax seals with digital signatures in the banking sector. Blockchain Technology is one such revolutionary innovation that is disrupting the banking industry around the world (BCT). Blockchain is a distributed ledger that stores business transactions in an unbreakable, immutable chain that can be accessed by all parties involved in the transaction. Since it offers permanent and tamper-proof storage of transactions in a distributed network, blockchain technology has the ability to disrupt financial business applications.*

Key Words: *AES, Cashless Economy, Encryption, Hash Algorithm, Security, encryption, SHA 256, etc.*

I. INTRODUCTION

India actually has the world's seventh-largest economy. According to the World Economic Forum, the number of digital transactions in India increased as a result of the demonetization policy, which is good news for the government, which will now be able to monitor the flow of money more easily. In turn, the increase in digital transactions in India is a boon for Blockchain and cryptocurrency. Bitcoin, the cryptocurrency that popularized Blockchain technology, is still used by about 0.5 percent of Indians. The Reserve Bank of India's Institute for Development and Research in Banking Technology, or IDRBT, announced plans to launch a new Blockchain platform in September of this year. India's central bank is the Reserve Bank of India. India could use Blockchain to digitize its national currency, the rupee, according to a study published by the IDRBT in January of this year. Given the benefits such as increased tax payments that India's demonetization policy has brought about through increased digital transactions, it's likely that the government will continue to push for a cashless economy. There are some hurdles, but it seems to be on the right track. If the Indian government, like every other government in the world, wishes to improve its cashless economy, it must find long-term solutions to the problems that come with introducing a cashless economy. Financial inclusion, high setup and processing costs, and transaction times are just a few of the problems Most citizens will need a bank account to survive in a cashless economy, based on today's cashless technology an uphill fight. To put it another way, you'll need an alternative to conventional financial services if you want to run a cashless economy. This is a good place to start learning about Blockchain. This supports the concept of a less costly method ofperforming digitaltransactions. If a cashless economy is ever tobecomethe norm, it will need to include a real-time component. Today's technologies have done an excellent job of reducing the time between the completion of a transaction and the availability of funds. However, it is still not to the point where the entire population will be encouraged to go digital. And this is yet another issue that Blockchain technology brilliantly solves.

II. PROBLEMDEFINITION

To develop of a software model for Cashless Economy using BCT in Java and android, which will be secure and transparent.

III. METHODOLOGY AND ALGORITHMICSTUDY

1)MD5 (Message-Digest algorithm 5)

In cryptography, MD5 (Message-Digest algorithm 5) could be a mainly used cryptographic hash function with a 128-bit hash value. MD5 has been employed or developed in a very more style of security applications and is additionally mainly want to check the integrity of files or the merchandise. The MD5 hash technique is described in "RFC 1321" together with a C implementation. MD5 is comparable to the MD4 hash. The padding is identical.MD5 works on 32-bit words. Let the desired message to be implemented is "M". The message "M" is padded so its length in bits is comparable to 448 modulo 512, that is, the padded message is a smaller amount than 64 bits of multiple of 512.Firstly, the padding consists of one 1 bit within the first column, followed by enough zeros to pad the message to the desired length till the 512 bit. Padding is often used, whether or not the initial length of M happens to equal 448 mod 512. As a result, there's a minimum of one little bit of padding, and at the most 512 bits of padding. The padded message may be a multiple of 512 bits and, it's also a multiple of 32 bits.

2) Advanced Encryption Standard (AES):

Advanced Encryption Standard (AES) Encryption is currently the simplest and standard encryption used. Advanced Encryption Standard, AES 256-bit also happens to be the best level of encryption and therefore the strongest available today.

The Advanced Encryption Standard key features are:
- Implementation of Block Encryption.
- It is 128-bit group encryption.
- It may be a symmetric algorithm.
- Requires just one encryption and decryption key.
- Provides data security for pretty much 20 to 30 years.
- Accessible worldwide.

3)SHA256: HashFunction

SHA-256 (secure hash algorithm) could be a cryptographic hash function with a digest length of 256 bits. it's a keyless hash function; that's, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 32 bits, each block requiring 64 rounds A cryptographic hash (sometimes called digest) may be a quite signature for a text or an information file. A hash isn't encryption it cannot be decrypted back to the initial text (it could be a one-way cryptographic function, and may be a fixed size for any size of source text). This makes it suitable when it's appropriate to check hashed versions of texts, as opposition decrypting the text to get the first version.

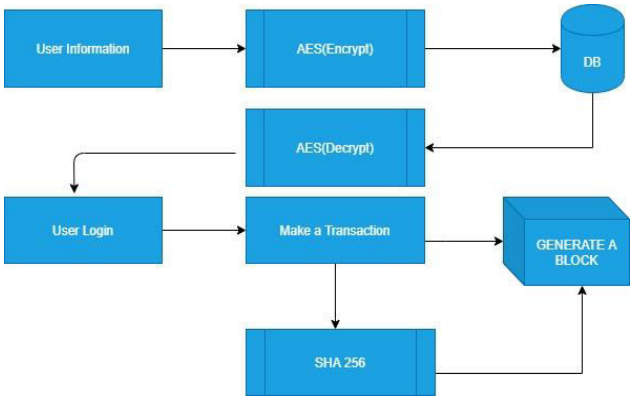
IV. PROPOSEDSYSTEM

In the proposed mode, there are two main building blocks which are given below:

- Encrypt or Decrypt the data
- Generate a Block of Transaction

Whenever user does registration, the information will first feed to the AES block which will encrypt the data and then stores it to the database. When user does registration, it will require data 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.

Fig: Proposed System



V. ExperimentalImplementation:

Step 1] After successfully run will appear login page,so from there admin will loginby using username and password which is also given already.

Step 2] After successfully admin login you have to add bank and user also.While adding bank and user you have to fill some required details.After that you will receive an email to both bank manager and user through your email id.

Step 3] After receiving email bank can login from web application and user can login from android application using username and password which is given through email.

Step 4] So after successfully login into android application user can make transaction of money successfully ,which is can see by bank by login into web application.Also you can see the transaction through android application.

Step 5] After successfully transaction user can logout.

VI. CONCLUSION :

With this proposed model, the cryptographic techniques and block chain technology used to implement a cashless economy system, will be the most secure, transparent, user-friendly, and free of corruption system ever devised. With the help of this proposed system, every transaction activity can be tracked, and intermediate bank corruption can be completely eliminated.

VII. REFFERENCES :

[1] Didik Haryadi,, Harisno, ,Victory Haris, Kusumawardhana, ,Harco Leslie Hendric Spits Warnars at Information System Management Department, BINUS Graduate Program-Master of Information System Management, "The Implementation of E-Money in mobile phone: A case study at PT Bank KEB HANA ", 7-09-@2018IEEE

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Steemit, https://steemit.com [Accessed 11 Mar. 2019]

[3] Christian Killer, Bruno Rodrigues, Burkhard Stiller,2019IEEE International Conference on Blockchain and Cryptocurrency (ICBC), "Security Management and visualization in a Blockchain based Collaborative Defense"

[4] Sean Kang,Kideok Cho, Kyle Park, "On the Effectiveness of Multi-Token Economies", 2019 IEEE

[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]Rahul Gupta,Cheshtha Kapoor,Jayesh Yadav at Computer Science Engineering Department Delhi Technological University Delhi, India, "Acceptance Towards Digital Payments and Improvements in Cashless Payment Ecosystem",5-7,2020@IEEE

[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.