



SECURE E WALLET ARCHITECTURE USING BCT

Siddhant Tyagi , Rutuja Pawar , Mayuri Uttarwar , Riddhi Padalkar , Prof. Mrs. Pradnya
Kasture

Dept of Computer Engineering, RMDSSOE, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT:

A cashless society is one in which financial transactions are conducted without the use of real money, such as banknotes or coins, but rather through the exchange of digital information (usually an electronic representation of money) between the parties involved. Since the birth of human civilization, cashless societies have existed, based on barter and other types of exchange, and cashless transactions are now possible with the usage of digital currencies like bitcoin. However, this article focuses on the term "cashless society" in the sense of a transition to a society in which cash is replaced by its digital equivalent—in other words, legal tender (money) exists, is recorded, and is only transferred in electronic digital form—as well as the implications of such a society. Such a concept has gotten a lot of attention, especially because digital methods of recording, managing, and exchanging money are becoming increasingly popular in commerce, investment, and everyday life in many parts of the world, and transactions that would have been done with cash in the past are now frequently done electronically. Non-electronic payment methods are now subject to transaction and transaction amount limits in some countries. We'll look at how block chain technology can be applied to the digital economy to help India become more digital in this post.

Keywords: digital economy, cashless, SHA256, AES, digital India, java, jsp, servlet, etc

I. 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 a totally cashless system, which must be secure too so we are going to implement a digital economy for digital India using BCT.

II. Literature Survey:

The trend towards use of non-cash transactions and settlement in daily life began during the 1990s, when electronic banking became common. By the 2010s digital payment methods were widespread in many countries,[which?] with examples including intermediaries such as PayPal, digital wallet systems such as Apple Pay, contactless and NFC payments by electronic card or smartphone, and electronic bills and banking, all in widespread use.[3] At this point cash had become actively disfavored in some kinds of transaction which would historically have been very ordinary to pay with physical tender, and larger cash amounts were in some situations treated with suspicion, due to its versatility and ease of use in money laundering and financing of terrorism. Additionally, payment with a large amount of cash has been actively prohibited by some suppliers and retailers,[5] to the point of coining the expression of a "war on cash".[6] The 2016 United States User Consumer Survey Study claims that 75% of respondents preferred a credit or debit card as their payment method while only 11% of respondents preferred cash.[7] Since the founding of both companies in 2009, digital payments can now be made by methods such as Venmo and Square. Venmo allows individuals to make direct payments to other individuals without having cash accessible. Square is an innovation that allows primarily small businesses to receive payments from their clients. By 2016, only about 2% of the value transacted in Sweden was by cash, and only about 20% of retail transactions were in cash. Fewer than half of bank branches in the country conducted cash transactions.[2] The move away from cash is attributed to banks convincing employers to use direct deposit in the 1960s, banks charging for checks starting in the 1990s, banks launching the convenient Swish smartphone-to-phone payment system in 2012, and the launch of iZettle for small merchants to accept credit cards in 2011.[2]

III. Proposed System:

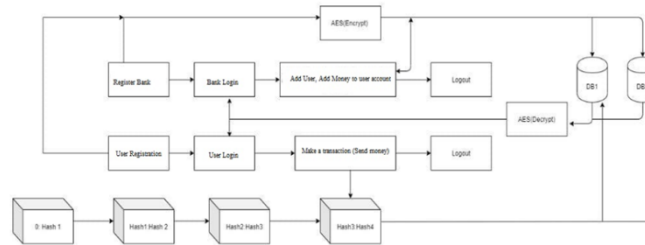


Fig: Proposed System

Whenever any transaction will occur in the system, the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the blocks is tempered the subsequent all the blocks hash must be changed . Such multiple copies are maintained at different servers , which will assure the data security and confidentiality. As everything is through the application interface, it will maintain the transparency in transaction.

Algorithm:

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).

Results:

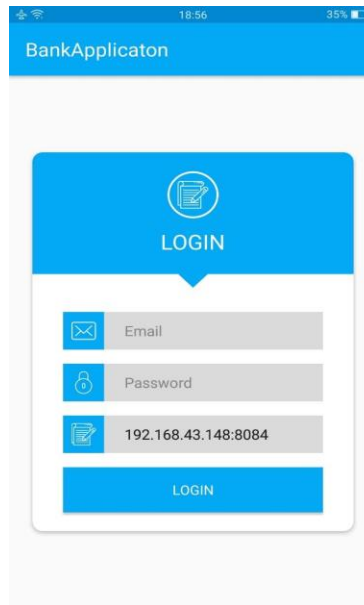


Fig: Login Page

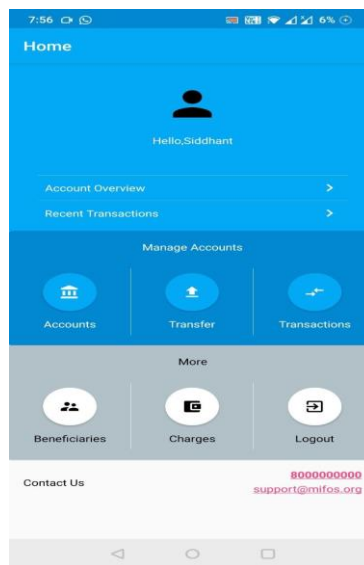
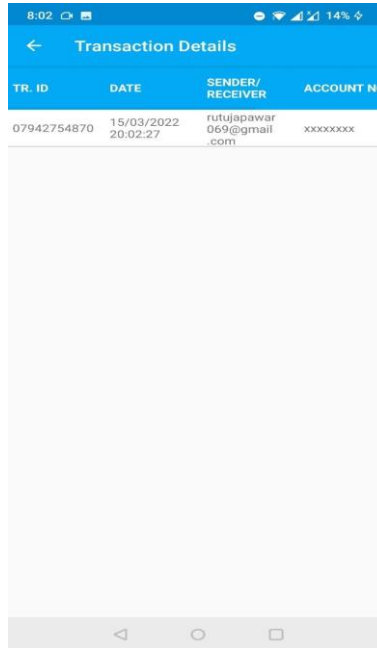


Fig: Dashboard



The image shows a mobile application interface for viewing transaction details. The screen has a blue header with a back arrow and the text "Transaction Details". Below the header is a table with four columns: TR. ID, DATE, SENDER/RECEIVER, and ACCOUNT NO. The table contains one row of data. The status bar at the top shows the time as 8:02, signal strength, Wi-Fi, and 14% battery. The bottom of the screen shows the standard Android navigation bar.

TR. ID	DATE	SENDER/RECEIVER	ACCOUNT NO
07942754870	15/03/2022 20:02:27	rutujapawar 059@gmail _com	xxxxxxxx

Fig: Transaction

IV. Conclusion:

Thus using BCT will be truly in the sense digital economy for digital India. We are going to use JSP & servlet technology to implement BCT features. AES will be used for databse encryption. SHA 256 will be used for hash generation.

References:

- [1] "THE COST OF CASH IN THE UNITED STATES" (PDF). The Fletcher School Tufts University. p. 9. Archived from the original (PDF) on 1 December 2016. Retrieved 17 December 2016.
- [2] Henley, Jon (June 4, 2016). "Sweden leads the race to become cashless society" – via www.theguardian.com.
- [3] "The UK is getting closer to becoming a completely cashless society". The Independent. May 21, 2015.
- [4] "Cashless-Society.org". Cashless-Society.org. Archived from the original on 2017-12-14. Retrieved 2017-01-27.
- [5] Tompor, Susan (4 September 2016). "A cashless society? Some retailers turn noses up at currency". USA Today. Retrieved 3 July 2020.
- [6] ""Negative" Interest Rates and the War on Cash". February 8, 2016.
- [7] "2016 User Consumer Study" .
- [8] <https://www.personalfn.com/dwl/are-you-assuming-money-in-bank-deposits-as-safe-watch-out>