Sinhgad Institutes

Review 1

Project Group :-
Under Guidance of Prof. Piyush Gawali

Members -
Vaibhav Aghav
Jay Dale
Devesh Sarda
Pramod Ghodke

Sinhgad Institutes

Title

"A Step Towards Cashless India Using Block Chain technology"

Sinhgad Institutes

Index

Sinhgad Institutes

Introduction

1) “Fearless, Paperless and Cashless” is one of the professed role of digital India. This progress towards goal was made in late 2016 when government took step to demonetize country.

2) According to 2019 study by Tuffs University the cost of cash in India, cash operations cost of the Reserve Bank of India and commercial banks are about 29 Crore annually

Sinhgad Institutes

Introduction

3) Shifting away from cash will make it more difficult for tax evaders to hide income.

4) The “1992 scam” is the biggest scam is one of the biggest example of banking scam in India.

5)The Government is also working on to reduce dependency on cash.

Sinhgad Institutes

Motivation

1) Banking and technology are very closely associated and innovations have changed banking drastically over the period of time.

2) 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 wit digital signatures.

3) One such disruptive innovation which is changing the banking sector globally Blockchain Technology (BCT).

Sinhgad Institutes

Problem Statement

"Development a software model for Cashless Economy using Block chain Technology in Java which will be secure and transparent."

Sinhgad Institutes

Concept

1) Block chain is shared distributed ledger which stores business transaction to a permanent unbreakable chain which can be viewed by the parties in a transaction.

2) Block chain technology has the potential to disrupt the financial business applications as it provides permanent and tamper proof recording of transactions in a distributed network.

Sinhgad Institutes

Current System

1)According to a report by Credit Suisse Group, 72% of India's consumer transactions take place in cash, double the rate as in China.

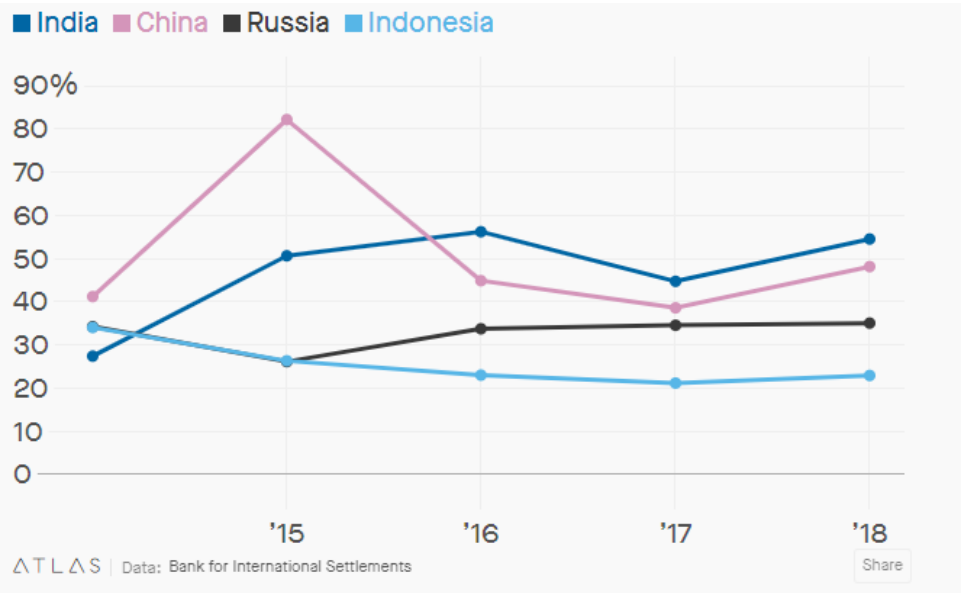
2)The total cases of frauds (involving Rs1 lakh and above) reported by banks and financial institutions (FIs) shot up by 28 per cent by value during 2018-19 despite the Reserve Bank of India (RBI) tightening the supervision.

3)The reasons for such failures are quite transparent. In essence, the sloppy regulatory oversights, weak supervision, absence of accountability, susceptibility to misuse by prominent figures and the ineptitude to learn from past mistakes keep adding to the woes of the financial system

Sinhgad Institutes

Proposed System

1)Digital transactions in India increased by 55% last year, compared with 48% in China and 23% in Indonesia, according to data from the Bank for International Settlements (BIS)



Sinhgad Institutes

Proposed System

2) The transactions made through Block Chain technology is more transparent and secure as compare to current system.

3) Due to this Covid situation many people are trying to make more cashless payment so to avoid frauds and to keep our money more secure via online transactions we have to use distributed system.

4)We are following distributive system for more safety and transparent transactions. It doesn't rely on a trusted third-party to process transactions.

Sinhgad Institutes

Objectives

1) To learn and Understand Block Chain Technology.

2) To learn and Understand Java programming language.

3) To learn and Understand SHA 256 for hashing

4) To learn and Understand AES for database encryption.

5) To learn and Understand distributed, decentralized concept using WLAN

6) To learn and Understand MySQL

Sinhgad Institutes

Scope

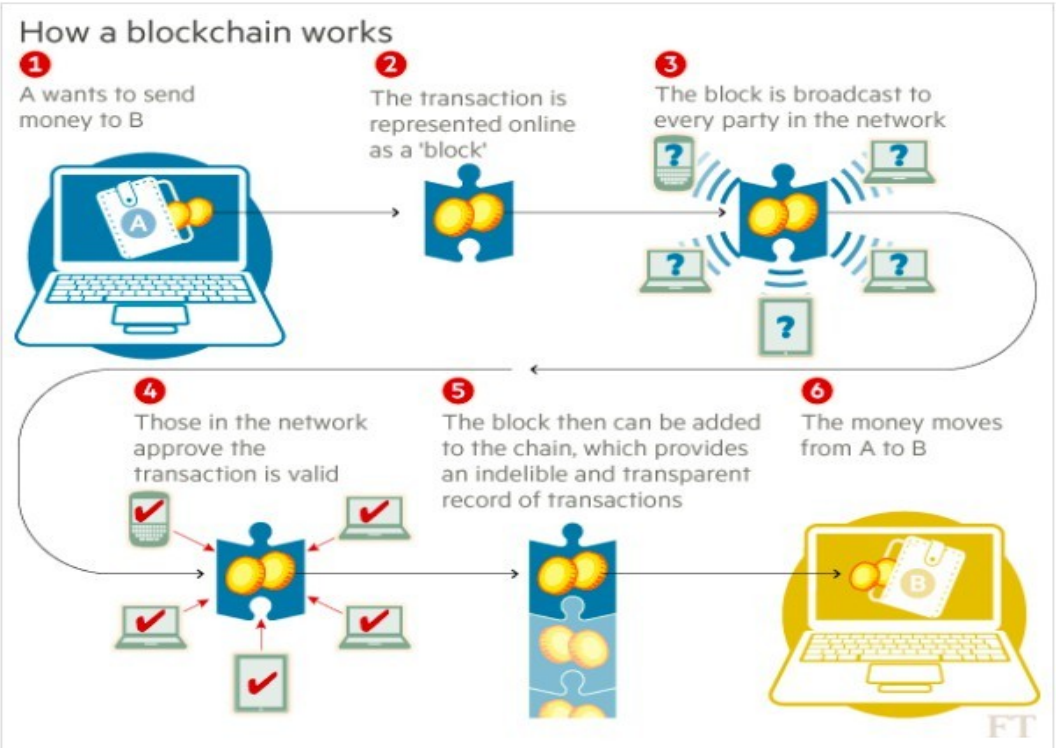
1) Project will be developed as a web and android based application using java which will communicate through WLAN.

2) In future it will require WAN and online storage space to host the application.

3) The current application will be limited to LAN as the web application will run as a local host using glassfish server.

Sinhgad Institutes

Block Diagram



Sinhgad Institutes

Block Diagram Explanation

1)When one person wants to send money to second person following things will happen:

2)Every database will get updated simultaneously(distributed)
Transaction information will be stored permanently in the block.
After which transaction will take place.

3) The database will be in the encrypted format.
So it is transparent but secure too.

Sinhgad Institutes

Software Requirements

1) JAVA DEVELOPMENRT KIT (JDK) 1.8
2) MYSQL
3) NETBEANS
4) APACHE TOMCAT/ GLASSFISH SERVER

Sinhgad Institutes

Hardware Requirements

- Processor : core i5
- RAM : 4GB
- Hard Disk : 320 GB

Sinhgad Institutes

Algorithms: SHA 256

1) SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits.
2) It is a keyless hash function; that is, an MDC (Manipulation Detection Code).
3) A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds

Sinhgad Institutes

Algorithms: AES

STEPS:

1) Derive the set of round keys from the cipher key.
2) Initialize the state array with the block data (plaintext).
3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of state manipulation
6) Copy the final state array out as the encrypted data (ciphertext).

Sinhgad Institutes

Algorithms: AES

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

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

9)This array we call the state array.

Sinhgad Institutes

References

[1] D. Mills et al., "Distributed ledger technology in payments, clearing, and settlement," *Finance and Economics Discussion Series 2016- 095*. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095.

[2]The Financial Industry Regulatory Authority Report, http://www.finra.org/sites/default/files/FINRA Blockchain_Report.pdf, January 2017

[3]http://economictimes.indiatimes.com/articleshow/61715860.cms?utm source=contentofinterest&utmmedium=text&utm_campaign=cppst,November 2017.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2009," 2012. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

Sinhgad Institutes

References

5] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang., "An overview of blockchain technology: Architecture, consensus, and future trends." *In 2017 IEEE International Congress on Big Data (BigData Congress), 2017* Jun 25 (pp. 557-564). Honolulu, USA, DOI: 10.1109/BigDataCongress.2017.85

[6] https://en.bitcoin.it/wiki/Transactions (visited on 05/28/2013).

[7] M. Ober, S. Katzenbeisser, and K. Hamacher., "Structure and Anonymity of the Bitcoin Transaction Graph". *Future internet*, 5(2):237–250, May 2013

[8] http://blockchain.info/de/wallet/send-shared (visited on 05/31/2013).

[9] M. Möser , "Anonymity of Bitcoin Transactions" , An Analysis of Mixing Services . *Münster Bitcoin Conference (MBC),* 17–18 July 13, Münster, Germany.

[10] V. Dhar and R. Roger, "FinTech Platforms and Strategy " MIT Sloan Research Paper No. 5183-16. Available at SSRN https://ssrn.com/abstract=2892098 or http://dx.doi.org/10.213 9/ssrn.2892098

Sinhgad Institutes

Thank You !