Survey on Identification Of Black/Fake Currency Using NFC&Blockchain

Mr. Hari Krishna K
Post Graduate
Sathyabama Institute Of Science and Technology
Chennai, Tamil Nadu

Ms. Aaradhana Deshmukh
C-DAC
Pune, Maharashtra

Mrs. Vaishali Maheshkar
Principal Technical Officer
C-DAC
Pune, Maharashtra

Dr. N.M. Nandhitha
Dean School of Electrical and Electronics
Sathyabama Institute Of Science and Technology
Chennai, Tamil Nadu

BhupendraPratad Singh
Project Engineer
C-DAC
Pune, Maharashtra

Abstract: ***Counterfeit currency is a hindrance to the economy. For the growth of the country's economy there needs to be some fit approach to eradicate these counterfeits from the system. Iot devices are used in many applications to track and monitor, always collecting data. NFC is one such device that can be used for tracking the money that flows in and out of the system. This can be done by placing NFC chips on the currencies. Since 2009blockchain has gained tremendous momentum being used in various applications across different platforms. Blockchain has been a promising approach to securing your transactions on a decentralized database. This paper aims to understand these technologies and propose an approach using both these technologies to track the genuine currency from fake ones.***

Keywords: Blockchain; Nodes; PBFT; IoT; Ethereum; Fake currency; NFC; QR; Counterfeit; Currency detector;

I. INTRODUTION

2016 India's Demonetization Drive created the necessary jolt for the economy. Circulation of counterfeit currency is huge pull back for a country's economy. But replacing old notes with new ones can not be the only solution to counterfeiting. Instead this will always give counterfeiters the time to make new counterfeits. Many approaches have been to identify counterfeits but all lack in some way or the other. Exploring modern approaches to this problem have given some promising techniques to eradicate counterfeits.

Many popular approaches use IoT devices to track counterfeits. Latest approaches include mixing it with blockchaintechnology.Blockchain got really popular since its initial use in the creation of Bitcoin by Satoshi Nakamoto in 2009[2]. Earlier it was a technique used for timestamping digital documents that was originally introduced in 1991. Since then it has gained massive momentum in various industries. It is also know as a distributed ledger that can be viewed as a solution to distributed transactions. Even today many organizations are using enterprise-grade databases

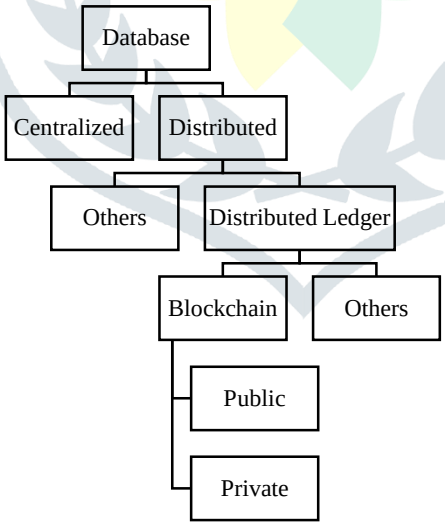

Fig 1: Database Technology Tree

which can be replaced with blockchain as it requires lower costs and infrastructure.

Particularly blockchain's immutability and distributed properties gives it advantage of reducing human errors and human intervention due conflictions[1]. There are certain points to note while implementing blockchain as a solution like,

1) Centralized DBs are a drawback as they are less secure and cannot handle huge amounts transactions.
2) When data moves across the system it will change
3) The data is redundant so that all stakeholders can improve its performance
4) The location of the data is distributed over many locations

5) Not all stakeholders will be allowed to change the data
6) Requirement of personal data protection

Blockchain can be applied to various applications[24] like fraud prevention, data verification, insurance etc.

NFC enables two electronic devices to communicate with eachother over a range of 4-10cm. Today all smartphones come with NFC chips allowing contactless transfers and payments. Several uses can be done using NFC chips as they are easy to program.

II. BLOCKCHAIN

[i]Blockchain is a distributed ledger that is available to anyone on the network. It stores information in the form of blocks that form a chain. It is assumed that each node on the network behave in a Byzantine manner[1]. This will allow stronger security than other databases out there. Each block will have the data, a hash value of its own and the hash value of the previous block. The data depends on the type of application it is, say for banking it would be transaction information like sender, receiver and amount.This technology provides security by this hash. If any of the block gets tampered then it will cause the hash to change which would in turn make the rest of the blocks in the chain invalid since they won't be pointing to the right hash valued block. Other ways for the blockchain to be secured is through proof-of-work(PoW) mechanism and by being distributed. This makes the blockchain to have a peer-to-peer(P2P) network allowing anyone to join. So whenever someone joins the network they get the full copy of the blockchain and is also updated when a new block is added to the network

This also helps to keep the nodes verified and in order. Addition of a new block will be updated by all nodes only if they create a consensus on whether the block is not tampered with and every node agrees on attaching it to their blockchain. So to successfully tamper with any block, one would have to control about 50% of the P2P network. There have been adversary controlling attacks by only controlling 25% of the P2P network[3]. Most blockchain applications use different variants of PoW as it safeguards fromSybil attacks[4]. Blockchain platforms are divided into either they require permission to read or not, or permission to write or not[5].

Bitcoin is a popular public blockchain example In this network each node broadcasts a set of transactions it will perform to other nodes. Here some nodes are called the miners that are responsible for collecting transactions into their blocks.

BlockchainTechnology	Platform	Language	Data Model	Consensus Protocol	Application
Hyperledger[7]	Docker	Golang, Java	Key-value	PBFT	General Applications
Bitcoin[2]	Native	Golang, C++	Transaction-based	PoW	Crypto-currency
Litcoin[8]	Native	Golang, C++	Transaction-based	PoW	Crypto-currency
Etherum[9]	EVM	Solidity	Account-based	PoW	General Applications
Parity[10]	EVM	Solidity	Account-based	Trusted-Validators	General Applications
HydraChain[11]	Python, EVM	Solidity	Account-based	Trusted-Validators	General Applications
BigchainDB[12]	Native	Python	Transaction-based	Trusted-Validators	Digital Assets

Table 1: Popular Blockchain Technologies

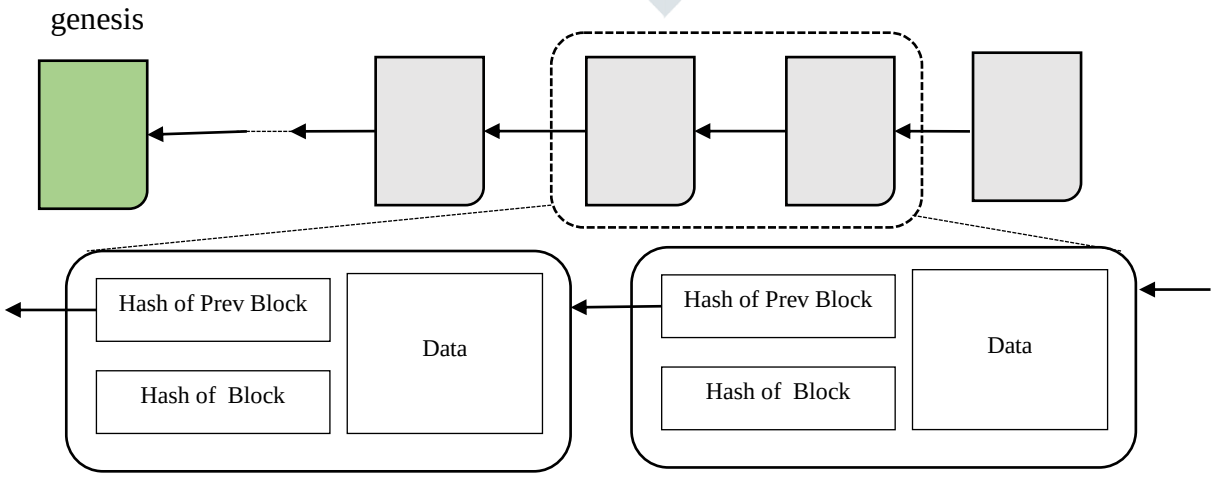

Fig 2: Blockchain Structure

Hyperledger is a popular example of private blockchain. This network employs various consensus protocols like PoS(Proof-of-Stake)[14][25], PoW[15][25], PoA(Proof-of-Authority)[10], PBFT[16], Parity[10] so on. Hyperledger uses PBFT consensus protocol[13].PBFT has 3 phases, (1) Pre-prepare phase: a leader broadcasts a value that must be committed by all other nodes, (2) Prepare phase: All other nodes will verify the values they will validate and (3) Commit phase: When 2/3rd of the nodes commit on a value, all such values are confirmed.

Blocks are evolving. One of the recent discoveries was smart contracts, which are simple programs that are inside the blocks and can automatically exchange data under certain conditions. Smart Contracts was coined by Nick Szabo in 1997. It is a distributed ledger that stores digital contracts. Since they reside inside the blockchain they inherit some of its properties like,

1) Immutability: When a contract is created it cannot be changed after that. This protects it from being tampered with.
2) Distributed: The output of the contract is validated by very node in the network.

This means that if one node attempts to tamper with a block without validation from all other nodes then its action will be marked invalid, thus safe guarding the block.This makes smart contracts practically impossible to tamper with. Ethereum[9] was first designed to support it. Bitcoin[2] also supports but with certain limitations.

Consensus Protocol	Network Settings	Description
PoS[14]	Public	Depending on the stake the node holds, they can create a new block.
PoW[15]	Public	A leader node will decide on the validation of the blocks
PoA[10]	Private	A round-robin election of authority nodes are made who can propose the new blocks.
PBFT[16]	Private	A voting is done among the nodes by assigning weights to the votes.

Table 2: Popular Consensus Protocols

III. TECHNIQUES TO IDENTIFY COUNTERFEIT CURRENCY

A. Fake Note Detector Machine

It is a machine that will examine the currency inserted. It will scan the ultraviolet properties and the magnetic ink present on the back. If a counterfeit is found the machine will cease to work and immediately notify the authorities of it. It is easy to use but using this approach has its limitations like we can't have the machine wherever we want, maybe only at ATMs and Banks.

B. Counterfeit Detector Pen

It is a pen that has iodine-based ink. Genuine currencies are printed on cotton fiber based papers that do not have starch(which reacts to iodine). When iodine reacts with food based paper it creates a black stain else if reacts with genuine notes no discolouration occurs. But this test will fail if the counterfeit is not a starch based paper and therefore this approach is less effective.

C. Counterfeit Money Detector

It is a mobile based application that allows detecting fakes under an ultraviolet light. Since the user of the application must see and validate the authenticity he must have knowledge of counterfeit currencies before hand.

IV. LITERATURE SURVEY

Alekhya[16] et. al proposed a technique to identify counterfeit notes based on their RGB components. They had stored images of real notes and they compare them to images clicked to check whether they are real or fake. Chakraborty[17] et. al proposed a technique that involved various steps like image acquisition, feature extraction and classification. After the image was acquired it was tested with different methods like ultraviolet light, MATLAB algorithm, counterfeit detection pen etc. Klein[18] et. al proposed to check the features of the note through a designed Optical Security Device that can detect the texture, identify the demographic variables. They approach was able to test about 74% right detection of counterfeit notes. Vishnu[19] proposed Principle Component Analysis(PCA) technique to extract features from images and calculate their mahalanobis distance and determine whether they are real or fake. Renuka[20] et. al identified that there was noise present in the images they acquired, so proposed a technique to compute the extent of colour matching which allowed in smooth process of rejecting fake notes.Park[22] et. al proposed a NFC based approach to allow secure payments. A signature RTD(Record Type Definition)-based transaction authentication is done to protect personal information which won't be tampered with.Vivek[23] et. al proposed a RFID tagging system to keep track of counterfeit notes.

Technology	Standard	Data Rate	Security	Application
NFC	ISO/IEC 14443	424kbps<20cm	Encrypted on smartcard app	Smartcard
RFID	ISO 18000	8-640kbps	Weak encryption, password, authentication	Smart tag

WiFi	IEEE 802.11	54 Mbps	WPA2	Internet Connection
Bluetooth	Up to 5.0	2.1 Mbps	Pairing & Link generation, PIN, SSP	Smartwatch, Headphone, Speaker
ZigBee	IEEE 802.15.4	40-250 kbps	AES encryption	Smarthome

Table 3: Popular IoT Technologies

V. PROPOSED WORK

To track counterfeit currencies, we have proposed to introduce NFC chips to be attached to the notes for tracking. The chip will record information like the serial number, amount of that note and expiry date to track their rotation cycle. The proposed application will work in three different scenarios, (1) when a currency to put for checking, it will be checked with the chip record information against the server information, (2) if people are using smartcards, the application is also designed to store transaction details on the server and finally (3) users can use QR codes for making transactions, such information will also be stored on the server. The application also allows users to report fake currency to the server. The money being used through scanning QR code would be deducted from the user'saccount. He will notified when some amount is being deducted.

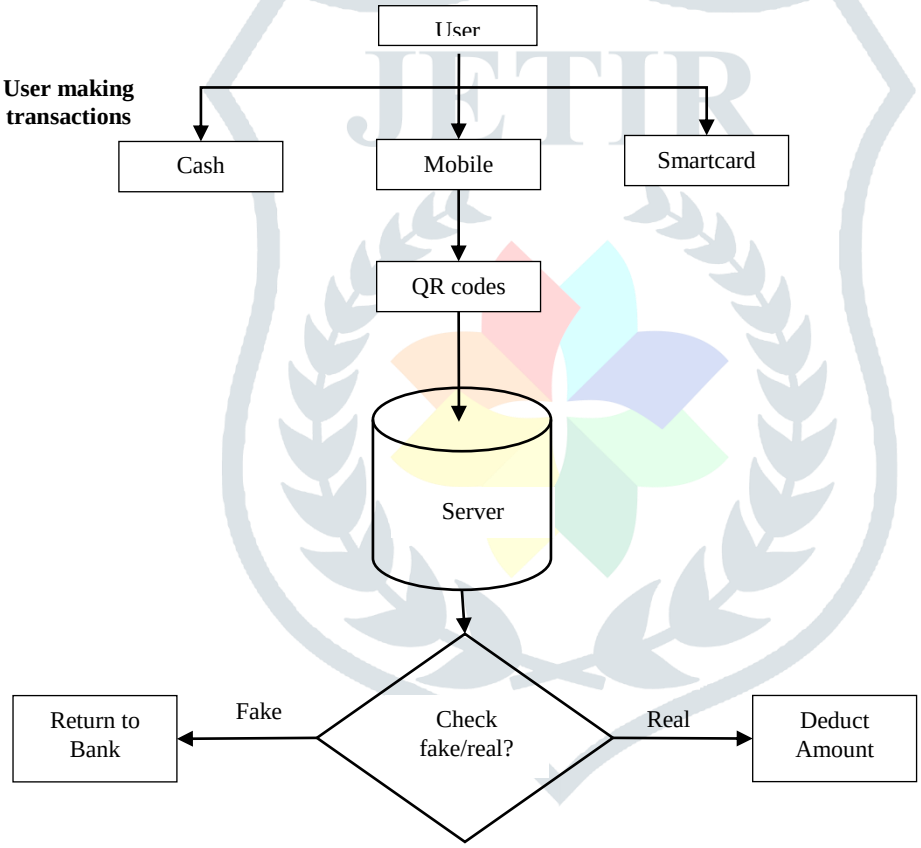

Fig 3: Proposed Work

VI. CONCLUSION

Existing approaches to identifying counterfeits are already prone to counterfeiters to tamper with. They can easily imitate the original currency to pass the test of checking its authenticity. Validating currencies through conventional methods require specialized devices for checking authenticity. But there is no effective technique to do so since all have some limitations. Modern digital solutions to this problem are complementing existing approaches. Our proposed work aims to embed NFC chips into the currency to guarantee successful monitoring of them in and out of the system.

VII. REFERENCES

[1] Dinh, Tien Tuan Anh, et al. "Untangling blockchain: A data processing view of blockchain systems." IEEE Transactions on Knowledge and Data Engineering 30.7 (2018): 1366-1385.
[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[3] Eyal, Ittay, and EminGünSirer. "Majority is not enough: Bitcoin mining is vulnerable." Communications of the ACM 61.7 (2018): 95-102.

[4] Vu, QuangHieu, Mihai Lupu, and Beng Chin Ooi. Peer-to-peer computing: Principles and applications. Springer Science & Business Media, 2009.
[5] Hileman, Garrick, and Michel Rauchs. "2017 Global Blockchain Benchmarking Study." (2017).
[6] Wibowo, Satriyo, and Ery Punta Hw. "Blockchain Implementation Assessment Framework, Case Study of IoT LPWA Licensing in Indonesia." 2018 International Conference on ICT for Smart Society (ICISS). IEEE, 2018.
[7] "Hyperledger fabric v0.6.0," https://github.com/hyperledger/fabric/releases/tag/v0.6.0-preview.
[8] "Global decentralized currency," https://litecoin.org/.
[9] "Ethereumblockchain app platform," https://www.ethereum.org/.
[10] Ethcore, "Parity: next generation ethereum browser," https://ethcore.io/parity.html.
[11] "Hydrachain: Permissioned distributed ledger based on ethereum," https://github.com/HydraChain/hydrachain.
[12] "Bigchaindb: a scalable blockchain database," https://github.com/bigchaindb/bigchaindb.
[13] Hyperledger, "Blockchain technologies for business," https://www.hyperledger.org.
[14] "Proof of stake," https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.
[15] "Tendermint: Blockchain app development simplified," http://tendermint.com/.
[16] Alekhya, D., G. Devi Surya Prabha, and G. VenkataDurga Rao. "Fake currency detection using image processing and other standard methods." IJRCCT 3.1 (2014): 128-131.
[17] Chakraborty, Kishan, et al. "Recent developments in paper currency recognition system." Int. J. Res. Eng. Technol 2 (2013): 222-226.
[18] Klein, Raymond M., Simon Gadbois, and John J. Christie. "Perception and detection of counterfeit currency in Canada: note quality, training, and security features [5310-01]." PROCEEDINGS-SPIE THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING. Vol. 5310. International Society for Optical Engineering; 1999, 2004.
[19] Vishnu, R., and Bini Omman. "Principal component analysis on Indian currency recognition." Computer and Communication Technology (ICCCT), 2014 International Conference on. IEEE, 2014.
[20] Renuka N, Shreya S, Trupti T, Chirayu Y, Suraj K, "Currency Recognition and Fake Note Detection", International Journal of Innovative Research in Computer and communication Engineering(IJIRCCE), 2016, Vol.4, Issue 3.
[21] Rupali D, Akash G, Prajyoti K, Pranali S, Anand P, "Design of Counterfeit: Currency Detector", National Conference on Innovations in IT and Management(NCI^{2}TM), 2014.
[22] Park, Sung-Wook, and Im-Yeong Lee. "Transaction Authentication Scheme Based on Enhanced Signature RTD for NFC Payment Service Environments." Platform Technology and Service (PlatCon), 2016 International Conference on. IEEE, 2016.
[23] Vivek D.U, Harsha N, Neeraj S, Harshada B, "A Survey on Authentication, Counterfeit Note Detection& Automatic Printing System", International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE), 2017.
[24] Gatteschi, Valentina, et al. "To Blockchain or Not to Blockchain: That Is the Question." IT Professional 20.2 (2018): 62-74.
[25] Kim, Jun-Tae, JunghaJin, and Keecheon Kim. "A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority)." 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018.

i