Localized Peer to Peer Privacy Preserving Money Transfer with Android App and Private Blockchain

M.J.Jeyasheela Rakkini, K.Geetha, K.R.Sekar, R.Subramanian, V.Santhosh Kum, P.Kaniyan

Abstract*: *Peer to Peer money transfer in Android App with blockchain architecture is a very novel and holistic approach to transfer money within a small group of peers who lend, borrow and the transfer money from one person to another in e-wallets.Money transfer in blockchain is inevitable in the near future as it entails non- repudiation, security, transparency, preserves anonymous of users with Homomorphic encryption and the inherent tamper-proof nature of the distributed ledger of the blockchain makes it more resilient and robust. The transactions of all the peers are recorded in distributed ledger stored in real time cloud database Firebase with Homomorphic encryption.

Keywords: Wallet signature, Homomorphic encryption, Double spending attack, Blockchain.

I. INTRODUCTION

Blockchain, a decentralized architecture with tamper proof, append only log of transactions, non-repudiation has gained immense popularity and is a disruptive technology for all Fintech operations that involve transactions. With a blockchain, users can write entries into a record of information, and a community of users can control how the record of information is amended and updated. The distributed database created by blockchain technology grows as the number of transactions increase and is cryptographically secure. The most distinct and important features of blockchain technology.Authentication and authorization, vital to digital transactions, are established since they are the quintessential feature of blockchain technology. The transactions by blockchain are slow and are nowhere near the VISA which handles 50,000 transactions per second, but this android app can be suited for small peer.to peer members who do transactions like the women self-help groups, where the need for ledger maintenance is considerably reduced here every participant keeps an entire copy of the blockchain.It is a trust less, decentralized network with transparency of transactions. The blockchains can be broadly classified into permissioned blockchains and permission less blockchains. Permissioned Blockchains, for example the IBM Hyper ledger where the roles are strictly delineated for mining nodes and a normal nodes. The two prominent examples of permission less blockchains are Bitcoin and Ethereum, where everyone can participate in the consensus process.

Revised Manuscript Received on May 10, 2019

M.J.Jeyasheela Rakkini, School of Computing, SASTRA Deemed University, India
K.Geetha, School of Computing, SASTRA Deemed University, India
K.R.Sekar, School of Computing, SASTRA Deemed University, India
R.Subramanian, School of Computing, SASTRA Deemed University, India
V.Santhosh Kum, School of Computing, SASTRA Deemed University, India
P.Kaniyan, School of Computing, SASTRA Deemed University, India

The usage of cloud application (third-parties) i.e. Firebase a real time database, as part of our blockchain implementation might be vulnerable to attackers and data mining operations of sensitive data might be carried out by third party cloud service providers. To avoid this the data to be stored in firebase is encrypted using homomorphic encryption. Double Spending of digital currency is one of the major concern in blockchain Transactions. This violation may take down the entire blockchain and may lead to forking of blocks. Since blockchain is a blooming-technology which is still in its proof of Concept and pilot stages, there is no assurance for refunding of digital money. By chronologically ordering the transactions and validating them, the double spending attack has been cleverly avoided in our proposed method.Since Mobile nodes are limited to performance constraint, it takes high time to do everything with peer-to-peer technology. So, Firebase, a real time database was used to cut down that time and get time and storage efficiency. The Blockchain service provider can get the infrastructure from the cloud service provider and can provide it to the users. All the major cloud service providers provide blockchain service on paid basis. The fiat currency is used here which defies the need for real currency and a proof of concept implementation is done here.In all decentralised apps in Ethereum the permissionless blockchain,the fiat currency used is Ether and for each transaction ,there is a cost of each transaction which is termed as gas is considered. Here in our proposed work we were motivated with chamapesa app in Kenya which operates the blockchain modelled android app and is to be launched in September 2019 and the term chama stands for small groups in Kenya which serve solidarity lending,peer to peer lending ,microfinance services among the female members, who on a monthly basis save money, lend money, do transactions and keep a record of the transactions.

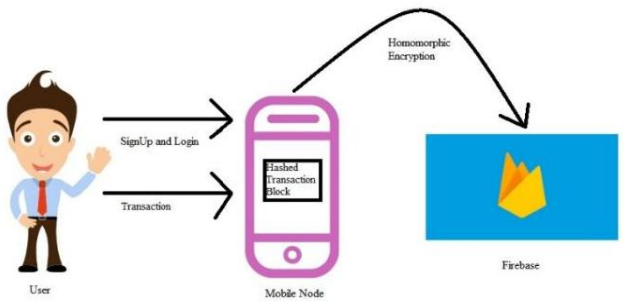

Fig.1.Workflow of the Localized Peer to Peer money transfer

The user data and the transaction details are encrypted with Homomorphic Encryption before the data is stored in firebase. Homomorphic encryption has been used to create other secure systems such as secure voting systems, collision-resistant hash functions, private set intersection, and private information retrieval schemes. Homomorphic encryption can be used for secure outsourced computation, for example, secure cloud computing services, and securely chaining together different services without exposing sensitive data.

II. RELATED WORKS

Sebastian Feld et al [1] discusses the deployment of Bitcoin's P2P network in distinct autonomous systems. The parameters considered are bitcoin peers, autonomous systems with routable peers, peer list of all connected peers in the autonomous systems, routable peers, non-routable peers and unreachable peers. The traversal of Bitcoin P2P peers in distinct autonomous systems and their statistics is exploited in this paper. Richard Dennis et al [2] discusses the scalability of blockchains and he emphasizes a time period during which the data from the blockchain is read and verified. Any transaction data before that time period is omitted. The time period data for 30 days is checked for availability, consistency and Integrity. The data gets updated and at the older time, the block gets deleted. The availability, consistency, and Integrity measures are considered against the traditional blockchain. The author has presented a paper on B-language and Z-language. Kongrath Suankaewmanee, et al [3] discusses about an android app that deploys the message passing process regarding transactions from one mobile user to all mobile users that are connected to a gateway. The miners take the unconfirmed transactions from a pool of transactions present in backlog and mine them and add it to the blockchain. The ID of the new block, previous block ID, timestamp, transaction, miner's, signature and public key are the quintessential features in a block. Po-Wei Chen, Bo-Sian Jiang, Chia-Hui Wang et al [4] discusses the payment collection of supervision system using pervasive Bitcoin digital wallet.This system can cost-effectively collect the payment and supervise the transactions between customer and merchandise store with NFC-enabled Android Apps. For this financial transaction, they used visa and blockchain technology. Finally, the digital wallet is implemented by android apps with interfaces of registration, login, insert, update, items listed in the shopping cart, confirmation to remove the item, Bitcoin payment confirmation activities of purchasing item confirmation, payment confirmation, transaction history, using blockchain explorer to validate the transaction stored in Bitcoin. Jingjing Gu et al [5] discusses the malware detection in mobile devices, so as to extract malware family features including software package feature, permission feature, application feature, and function call feature. This method can achieve higher detection accuracy in limited time with lower false-positive and false-negative rates. This malware can be analysed by static and dynamic based analysis with help of blockchain technology called de-centration. This can be implemented by secure sensitive methods such as Dynamic loading function, Java language, Encryption and decryption functions and Native Development Kit (NDK). Yuki Kano, Tatsuo Nakajima et al [6] discusses about the Blockchain mining work for making Blockchain technologies fit the ubiquitous, mobile computing environment. In this paper, a new solution to solve the mining problem by using a simple virtual currency service that allows a user to operate the service by giving the user a new incentive based on gamification. Mining work based on gamification of services consists of following elements such as Currency Unit, Communication protocol, Account, Transaction, Block and Mining Work. These technologies can be implemented by Graphic User Interface (GUI) of functions such as Account Registration and Login, Menu, Transaction, Publication, List Up account and Mining Work. Ahsan Manzoor et al [7] discusses the delay tolerant payment scheme on the ethereum Blockchain. A cash-less payment scheme for remote villages based on blockchains that allow maintaining a record of verifiable transactions in a distributed manner. The bank joins as a peer and monitors node behaviours, rewards miners and processes currency exchanges whenever the connectivity is available. These group of peers can be a conglomerateof three network nodes that consists of miners, full nodes and light nodes. The feasibility of the system design with a prototype implementation containing a private Ethereum blockchain with an intermittently connected bank node is implemented. He Zhu et al [8] discusses the blockchain-based architecture to make mobile edge application placement decisions for multiple service providers, based on a stochastic programming problem minimizing the placement cost for mobile edge application placement scenarios. All placement transactions are stored on the blockchain and are traceable by every mobile edge service provider and application vendor who consumes resources at the mobile edge. The potential security problems including service overlay, security, trusted classification policy, and secure encapsulation can be prevented. This can be implemented by using the edge chain algorithm. XiaoDong Zhang et al [9] discusses the security of the blockchain with mobile edge computing. The traditional solution to the security problem is based on centralized approach which requires a trusted central entity. In this paper the security architecture includes three layers to solve the large computational problem of blockchain. Santeri Paavolainen et al [10] discusses about the estimation on the cost and effects of attacks and spams.In this paper transaction history of the Ethereum blockchain is analysed and looked for the cost and effectiveness of a spam attack. In this method historical block characteristics, transactions and costs of a transaction spam attack are analysed.

III. IMPLEMENTATION

A. Real time database creation with Firebase

The implementation is done in Firebase and in Android Studio bundle 3.3. Google's Firebase which is a real time database has its data in JSON format and the data is displayed, synchronised across all its clients,web clients or mobile clients. The user of this app has to sign in and register their details like name, mobile number and password. The login phase needs the user to login the details of mobile number and pin number and login to the mobile application.

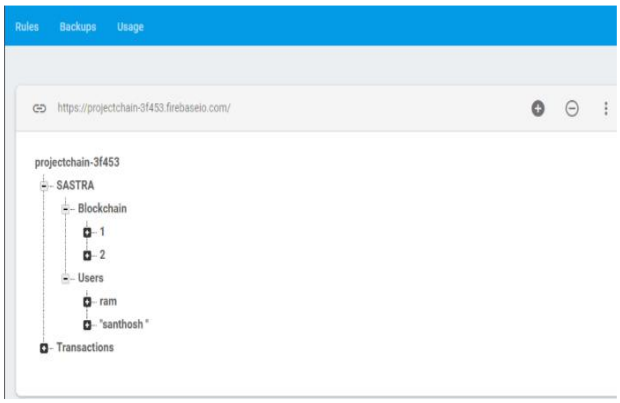

Fig.2: The Firebase with Block Details.

The blocks of each user, the number of users and the transactions of the user are stored in the Google firebase, a real time database as shown in Fig.2.Firebase, the cloud database has details of the group of users who wants to do their transactions in this Mobile-chain with the other registered users. The firebase has user details like his name, his phone number and pin number. The user details are validated and entered or else the users are asked to enter proper values. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signing transactions which is an asymmetric encryption. The Digital signature is used for secure transactions in which each user has a pair of keys, the private key and public key. The sender node signs the transaction and broadcasts it to other users. The receiver node will sign with his private key to get the transaction details and also broadcast it to other users. Proof of work consensus mechanism is used which requires all the nodes to participate in block generation and verification process. TheFig. 3 and Fig. 4. illustrates the Mobile Wallet application,they contain four modules they are Signup module, Login module, edit Contactor updation of details module and Transaction Module.

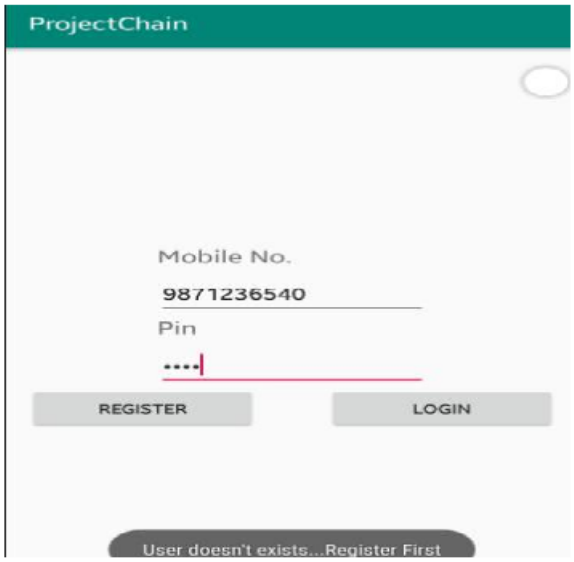

Fig. 3.The signup and registration in Firebase

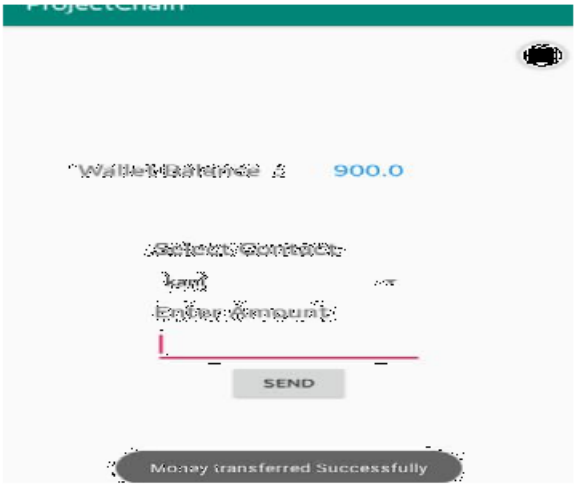

Fig. 4. Mobile Wallet Application.

The block of each user with the hash value of the block, merkle root, the nonce, hash value of the previous block, the time stamp shown in long number is demonstrated in Fig 3.The merkle root which has the hash of all the transactions beneath it is shown in Fig.4, which will enable new users to download the transactions. If a new user downloads the blockchain and if the transactions are broken during the download phase, the user can utilize the merkle tree for downloading the transactions. Proof of work consensus is reached here where a transaction is validated by more than 51% users in this peer to peer network. By chronologically ordering the time stamps of the transactions, the double spending attack is carefully avoided and thus forking of the chain is also prevented. Theblock chain architecture has a pool of transactions, where the first invalidated transaction is taken from the pool and validated by miners. Here we have considered all as miners, due to the small group of peers who do transactions among themselves in a transparent way. Money laundering is avoided because the transactions are auditable and also have provenance record and also this is micro-money sharing platform where if the transactions go above Rs.10, 000per day, theyare taxable. There is no such implementation of Metamask wallet in Mobile Applications, so we have devised this method. Metamask which is used for validating transactions in permission less block chains (Ethereum) and in decentralised applications has not been implemented in mobile applications.

Fig 5. The Block of users

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The user details like the username, the mobile number of the user are encrypted and stored in firebase with our Android app. The number of transactions of each user, from whom they have got money and with who they have transacted money are also shown in encrypted form. Thus the anonymity of the payer and the payee are maintained by this app.In Fig 5.The user details and the encrypted details are shown. The user validatiy of the chain is checked and shown in Logcat and the transaction details of a successful transaction,the public key of the user is shown in Fig 6 and Fig 7 respectively.

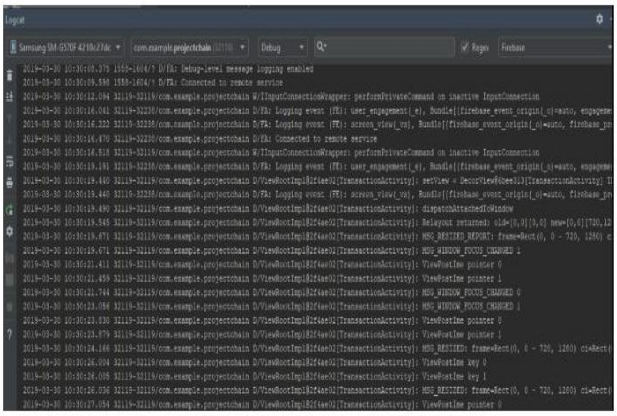

Fig 6.The Logcat of the transactions

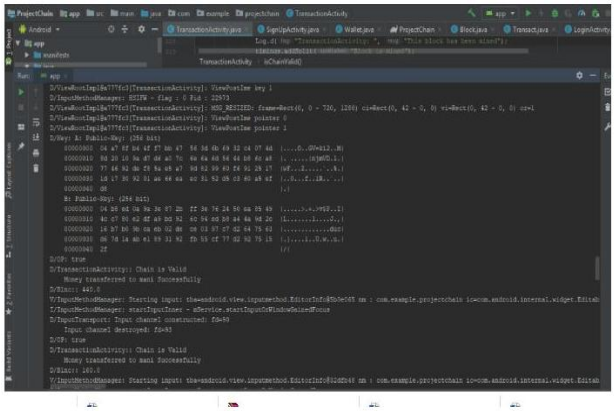

Fig 7.The Logcat of transactions with public key and private key

Homomorphic encryption is a form of encryption where the computation can be done in cipher text that yields the same result as when it is done in normal data. The data that is stored in cloud storage by the users can be stored using homomorphic encryption that yields for security and privacy preserving features. If the cloud service provider or any anonymous person if he wants to perform data mining operations, he can do it in encrypted data and not in the real data. Thus it is a privacy preserving decentralised mobile application.

Fig 8: The Encrypted user details in Firebase.

IV. CONCLUSION

The proposed approach, where homomorphic Encryption for data security is implemented in firebase with the blockchain architecture enabled transactions between the local peer to peer users who can have transactions between them without the need to go through the intermediate who skims a little part of the money for their transactions. The transparent nature of all the transactions and the innovative way of implanting it in an android app gives superiority of our work. Since Metamask works for DApps and not for mobile applications, we have chosen the firebase with data encrypted in it for our android application.

FUTURE WORK

The data mining operations can be carried out by the third party users with encrypted data, which is the quintessential feature of Homomorphic encryption. Any successful microfinance working model like Grameen Bank proposed by Professor Muhammad Yunus,a nobel price Laureat can be implemented as the future work of this app ,in our regional language provided there is regulation and support for digital currency. This system with no collateral and peer motivation will alleviate the poverty.

REFERENCES

1. Feld, Sebastian, Mirco Schönfeld, and Martin Werner.
2. "Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective." *Procedia Computer Science* 32 (2014): 1121-1126.
3. Dennis, Richard, Gareth Owenson, and Benjamin Aziz. "A temporal blockchain: a formal analysis." *2016 International Conference on Collaboration Technologies and Systems (CTS)*. IEEE, 2016.
4. Suankaewmanee, Kongrath, et al. "Performance analysis and application of mobile blockchain." *2018 international conference on computing, networking and communications (ICNC)*. IEEE, 2018.
5. Chen, Po-Wei, Bo-Sian Jiang, and Chia-Hui Wang. "Blockchain-based payment collection supervision system using pervasive
6. Bitcoin digital wallet." *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2017.
7. Gu, Jingjing, et al. "Consortium blockchain-based malware detection in mobile devices." *IEEE Access* 6 (2018): 12118-12128.
8. Kano, Yuki, and Tatsuo Nakajima. "An alternative approach to blockchain mining work for making blockchain technologies fit to ubiquitous and mobile computing environments." *2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*. IEEE, 2017.
9. Manzoor, Ahsan, et al. "A Delay-Tolerant Payment Scheme on the Ethereum Blockchain." *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(Wow Mom)*. IEEE, 2018.
10. Zhu, He, Changcheng Huang, and Jiayu Zhou. "Edge Chain: blockchain-based multi-vendor mobile edge application placement." *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018.
11. Zhang, XiaoDong, Ru Li, and Bo Cui. "A security architecture of VANET based on blockchain and mobile edge computing." *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 2018.
12. Paavolainen, Santeri, Tommi Elo, and Pekka Nikander. "Risks from Spam Attacks on Blockchains for Internet-of-Things Devices." *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2018.