BLOCKCHAIN BASED TRANSACTION MANAGEMENT SYSTEM

M.Nithya
Department of CSE
Sri Sairam
Engineering College
Chennai

A.H.Praveen
Department of CSE
Sri Sairam
Engineering College
Chennai

C.Harshavardhan Reddy
Department of CSE
Sri Sairam
Engineering College
Chennai

S.S.Sudharsan
Department of CSE
Sri Sairam
Engineering College
Chennai

ABSTRACT

IoT-based E-commerce is a new business model that relies on autonomous transaction management on IoT devices.The management system towards IoT-based E-commerce demands autonomy, lightweight and legitimacy.As blockchain is an innovative technology that is competent in governing the decentralized network, we adopt it to design the autonomous transaction management system on IoT E-commerce. However current blockchain solutions, most namely cryptocurrencies, have fatal drawbacks of non-supervisability and huge computational overhead, and hence cannot be directly applied on IoT-based E-commerce.In this paper, we propose a blockchain based normalized autonomous transaction settlement system for IoT-based E-commerce.The provision for the Bank sector to supervise without compromising the individual users privacy rights, can monitor and if needed oversee the transaction.IoT device in a merchant's premises can run a block chain server to record and keep track of the transaction that is happening in the merchants business. The bank layer will have details about the transaction between the users. The users actual identity is protected by introducing a digital identity layer. The official can access the bank layer with consensus from the bank involved and oversee the transaction.

Keywords
Internet of Things (IoT), Blockchain,
E-commerce,Python,Java

1. INTRODUCTION

Internet of Things (IoT) is a collective set of technologies that connects and organizes a network of lightweight devices. Recently, the concept of IoT-based E-commerce is emerging as a new trading model, which realizes person-to-machine (P2M) or even machine-to-machine (M2M) transactions, rather than person-to-person (P2P) transactions as in the conventional Ecommerce.

For example, Amazon Dash is a one-click button that automatically purchases the assigned product. This is a typical example of extending the E-commerce from P2P to P2M transaction model. Additionally, CEO of JD.com, the Chinese E-commerce giant, has just made a full autonomous commitment, expecting robotics and M2M algorithms to eventually take over its supply chain. In addition, in 2017 JD successfully built the world's largest fully autonomous logistics center in Shanghai. It is therefore reasonable to imagine the future of E-commerce, where all levels of settlements are completed in a purely autonomous and M2M fashion. However, current IoT based E-commerce systems are often constructed with a crowd of fragmented and lightweight IoT devices. To govern this scattered structure, an autonomous, accountable and lightweight M2M framework must be deployed. Blockchain's ability on governing decentralized networks makes it especially suitable for designing a self-management system on IoT devices. Guaranteed by rigorous cryptography, current blockchain solutions can establish trust and run in a self-governed way without the need of a central authority. Additionally, its hash-connected chain data structure achieves almost-perfect data integrity. Transaction data can thus be stored and shared with great confidence. Further enhancement of IoT device autonomy can be done using smart contracts, which serve as digital contracts reinforced by codes.

1.1 Problem Statement

To develop a secure system and accountable transaction using blockchain and IoT in e-commerce application.

2 LITERATURE SURVEY

[1] We present a technique for Merkle tree traversal which requires only logarithmic space and time1. For a tree with N nodes, our algorithm computes sequential tree leaves and authentication path data in time Log2(N) and space less than 3Log2(N), where the units of computation are hash function evaluations or leaf value computations, and the units of space are the number of node values stored. Relative to this algorithm, we show our bounds to be necessary and sufficient. This result is an asymptotic improvement over all other previous results (for example, measuring cost = space time). We also prove that the complexity of our algorithm is optimal: There can exist no Merkle tree traversal algorithm which consumes both less than O(Log2(N)) space and less than O(Log2(N)) time. Our algorithm is especially of practical interest when space efficiency is required, and can also enhance other traversal algorithms which relax space constraints to gain speed.

[2] The fast advance of wireless networking, communication, and mobile technology is making a big impact to daily life. The significant increase of mobile device users in the recent years causes a strong demand on secured wireless information services and reliable mobile commerce applications. Since wireless payment is a critical part of most wireless information services and mobile commerce applications, how to generate secured mobile payment systems becomes a hot research topic in both the e-commerce research community and wireless commerce industry. This paper proposes a peer-to-peer wireless payment system, known as P2P-Paid, to allow two mobile users to conduct wireless payment transactions over the Bluetooth communications. The system uses a 2-dimensional secured protocol, which not only supports the peer-to-peer (P2P) payment transactions between two mobile clients using Bluetooth communications, but also supports the related secured transactions between the payment server and mobile clients. This paper provides a system overview about system functional features, system architecture, and used technologies. Moreover, an integrated security solution for the P2P-Paid system is described. Our first phase implementation is reported and application examples are given to demonstrate the functions and feasibility of this system.

[3] The bitcoin protocol can encompass the global financial transaction volume in all electronic payment systems today, without a single custodial third party holding funds or requiring participants to have anything more than a computer using a broadband connection. A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs block chain. If Bitcoin transactions can be signed with a new sighash type that addresses malleability, these transfers may occur between untrusted parties along the transfer route by contracts which, in the event of un- cooperative or hostile participants, are enforceable via broadcast over the bit coin block chain in the event of uncooperative or hostile participants, through a series of decrementing time locks.

[4] Crypto currencies, such as Bitcoin and 250 similar alt coins embody at their core a block chain protocol a mechanism for a distributed network of computational nodes to periodically agree on a set of new transactions. Designing a secure block chain protocol relies on an open challenge in security, that of designing a highly scalable agreement protocol open to manipulation by byzantine or arbitrarily malicious nodes. Bitcoin's block chain agreement protocol exhibits security, but does not scale: it processes 3–7 transactions per second at present, irrespective of the available computation capacity at hand. In this paper, we propose a new distributed agreement protocol for permission-less block chains called ELASTICO. ELASTICO scales transaction rates almost linearly with available computation for mining: the more the computation power in the network, the higher the number of transaction blocks selected per unit time. ELASTICO is efficient in its network messages and tolerates byzantine adversaries of up to one-fourth of the total computational power. Technically, ELASTICO uniformly partitions or parallelizes the mining network (securely) into smaller committees, each of which processes a disjoint set of transactions (or "shards"). While sharding is common in non-byzantine settings, ELASTICO is the first candidate for a secure sharding protocol with presence of byzantine adversaries. Our scalability experiments on Amazon EC2 with up to 1; 600 nodes confirm ELASTICO's theoretical scaling properties.

[5] Security and privacy are huge challenges in Internet of Things (IoT) environments, but unfortunately, the harmonization of the IoT-related standards and protocols is hardly and slowly widespread. In this paper, we propose a new framework for access control in IoT based on the block chain technology. Our first contribution consists in providing a reference model for our proposed framework within the Objectives, Models, Architecture and Mechanism specification in IoT. In addition, we introduce Fair Access as a fully decentralized pseudonymous and privacy preserving authorization management framework that enables users to own and control their data. To implement our model, we use and adapt the block chain into a decentralized access control manager. Unlike financial bitcoin transactions, Fair Access introduces new types of transactions that are used to grant, get, delegate, and revoke access. As a proof of concept, we establish an initial implementation with a Raspberry PI device and local block chain. Finally, we discuss some limitations and propose further opportunities.

[6] The block chain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not least Bitcoin. Each such project can be seen as a simple application on a decentralized, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalized manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

[7] Online underground economy is an important channel that connects the merchants of illegal products and their buyers, which is also constantly monitored by legal authorities. As one common way for evasion, the merchants and buyers together create a vocabulary of jargons (called "black keywords" in this paper) to disguise the transaction (e.g., "smack" is one street name for "heroin" [1]). Black keywords are often "unfriendly" to the outsiders, which are created by either distorting the original meaning of common words or tweaking other black keywords. Understanding black keywords is of great importance to track and disrupt the underground economy, but it is also prohibitively difficult: the investigators have to infiltrate the inner circle of criminals to learn their meanings, a task both risky and time consuming. In this paper, we make the first attempt towards capturing and understanding the ever-changing black keywords. We investigated the underground business promoted through blackhat SEO (search engine optimization) and demonstrate that the black keywords targeted by the SEOers can be discovered through a fully automated approach. Our insights are two-fold: first, the pages indexed under black keywords are

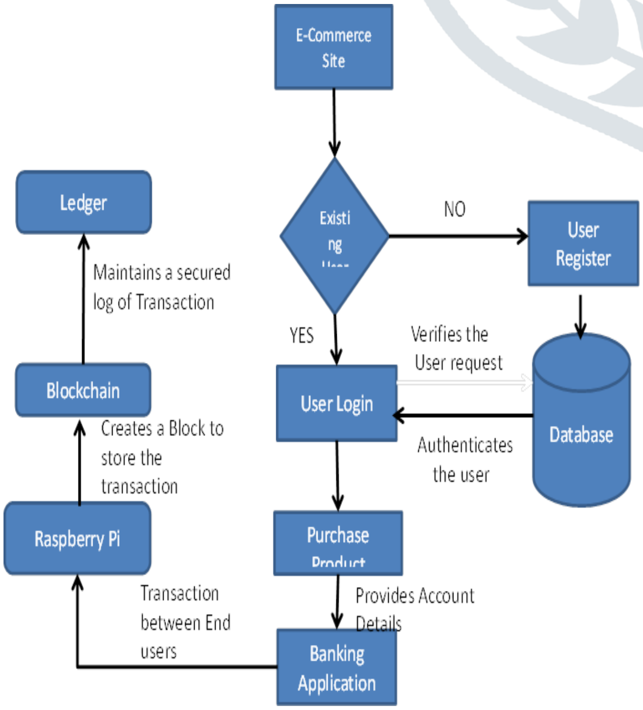
more likely to contain malicious or fraudulent content (e.g., SEO pages) and alarmed by off-the-shelf detectors; second, people tend to query multiple similar black keywords to find the merchandise. Therefore, we could infer whether a search keyword is “black” by inspecting the associated search results and then use the related search queries to extend our findings. To this end, we built a system called KDES (Keywords Detection and Expansion System), and applied it to the search results of Baidu, China’s top search engine. So far, we have already identified 478,879 black keywords which were clustered under 1,522 core words based on text similarity. We further extracted the information like emails, mobile phone numbers and instant messenger IDs from the pages and domains relevant to the underground business. Such information helps us gain better understanding about the underground economy of China in particular. In addition, our work could help search engine vendors purify the search results and disrupt the channel of the underground market. Our co-authors from Baidu compared our results with their blacklist, found many of them (e.g., long-tail and obfuscated keywords) were not in it, and then added them to Baidu’s internal blacklist.

3 SYSTEM ARCHITECTURE

The overall system design consists of following major modules:

(a) E-Commerce Application
(b)Business transaction application
(c)Transaction:Block chain implementation
(d)Approval:BlockChain in Raspberry Pi

A hypothetical ecommerce store is created where some goods were transacted between users and that financial transactions stored initially in database.Bank should be involved in financial transaction.The transaction shoule be later added on bloch chain as transaction.Each transaction stored as a block in block chain.Each block is linked with previous block and the digital signature of the previous block is included in the current block.Blockchain is implemented in python.Bloch chain is implemented in three layers.Raspberry pi is used for the iot device to implement blockchain.



4 EVALUATION OF SYSTEM

4.1 Advantages

The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system. . Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous.Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes. Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated

4.2 Applications

This idea can be used extensively in
e-commerce transaction for secured payment which increases the trust between the customer and vendor.Banking sector can also maintain ledger for the valid transaction that prevents the changes made by any third party users.

5 CONCLUSION

Thus the the system provides a secured transaction system with the help of blockchain which is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

6 FUTURE ENHANCEMENTS

In future the project can be extended by implementing this secured payment system for every online transaction by increasing the encryption efficiency of the details such a way that no intruder any decrypt or corrupt it.

7 REFERENCES

[1] M. Szydlo, “Merkle tree traversal in log space and time,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2004, pp. 541–554.

[2] J. Gao, K. Edunuru, J. Cai, and S. P. D. Shim, “P2p-paid: a peer-to-peer wireless payment system,” in Mobile Commerce and Services, 2005. WMCS’05. The Second IEEE International Workshop on. IEEE, 2005, pp. 102–111.

[3]] J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments,” draft version 0.5, vol. 9, p. 14, 2016.

[4] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 17–30.

[5] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “Fairaccess: a new blockchain-based access control framework for the internet of things,” Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.

[6]G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[7]] H. Yang, X. Ma, K. Du, Z. Li, H. Duan, X. Su, G. Liu, Z. Geng, and J. Wu, “How to learn klingon without a dictionary: Detection and measurement of black keywords used by the underground economy,” in 2017 IEEE Symposium on Security and Privacy (SP), May 2017, pp.

751–769.

[8] F. Tian, “An agri-food supply chain traceability system for china based on rfid & blockchain technology,” in Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016, pp. 1–6.