Blockchain Based Incentive Announcement Network for Communications Using VANET

N.Anudeep reddy[1*], N.Chaitra Sangeeth[1], B. Keerthi Samhitha[2], Suja Cherukullapurath Mana[2] and Jithina Jose[2]

[1*,1] UG Student, Department of Computer Science and Engineering,

Sathyabama Institute of Science and Technology, Chennai, India
[2] Assistant Professor, Department of Computer Science and Engineering,
Sathyabama Institute of Science and Technology, Chennai, India

anudeepreddyn226@gmail.com,
sangeethnekkanti064@gmail.com,samhitha711@gma
il.com,cmsuja@gmail.com,jithinajose@gmail.com

Abstract. Ad hoc vehicle networks (VANET) allow communications between vehicles and vehicles, especially , announcements produced by the vehicle. Cars may use these warnings to alert cars of road conditions in nearby areas. Thus, driving safety are often significantly increased. Their integrity must, however, be maintained. a replacement system for vehicle-generated announcements is introduced that's safe against external and internal attackers attempting to send fake messages. the utilization of a support mechanism supported multiple signatures risks internal attacks. In fact, this program guarantees that vehicles that volunteer for reliable announcements don't lose their rights.

Keywords: VANET, Blockchain, Vehicle Attacks, Incentive Mechanism

1   Introduction

The rapid increase in urban planning and the related traffic congestion, both academic and business, has highlighted MART cities. The VANET (Vehicle ad hoc network) vehicle announcement network has been promising vehicle communication systems because it offers a far safer experience in the field of vehicle driving [3]. In fact, it also helps to make traffic jams and incidents environmentally friendly while reducing costs on many of the public resources. Blockchain is a modern decentralized database system based on ledger[23]. Firstly, Satoshi applied Blockchain to Bitcoin, which is an e-cash network for peers. Afterwards, the corresponding speaker Blockchain gets more and more attention in e-commerce, growing attention. Especially because Blockchain-based Bitcoin has grown popular it has become a hot topic [1]. Moreover, every node manages the whole or a part of the framework database in Blockchain-based networks. Blockchain-based network data collection with the strong tamper-resistance and decentralization features that are useful in VANETs is therefore exciting. There are two key issues in developing an efficient vehicle communications network due to the increased data privacy[16].

First, ideally, all messages in VANETs must be sent anonymously because they usually contain confidential user information, such as number of cars, driving habits and consumer identities[17]. Nevertheless, sending messages secretly does not guarantee the authenticity of communications, limiting vehicle credit. Second, consumers are usually unable to transmit messages in VANETs if there are chances of infringing on their privacy[22]. Moreover, users do not benefit from receiving advertisements which also makes them unable to respond to messages [6].
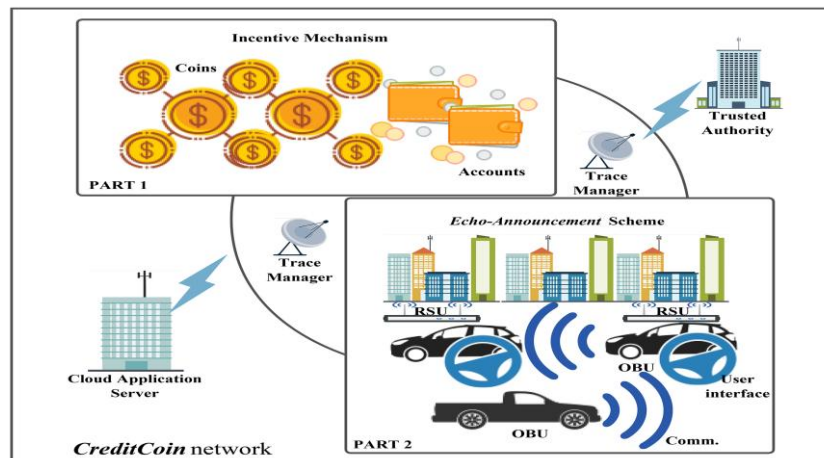
Fig. 1. The general idea of Credit Coin

The advancement of technology simplifies the lifestyle. Such systems can potentially also be used for our health[18]. ITS (Intelligent Transport Systems) work is also rising due to the growing issue of road accidents. In this region, many businesses worldwide invest as they know it is often the longer term. The VANET network is an important part of ITS. It's huge expectations of user has just hope to find answers to public safety issues. For VANET, accidents, flooding and harmful emissions in the air can be exacerbated. To do all of this, lots of work will be done to dismantle VANET's challenges. Movement of automobiles [3].

2   Related Work

Any process or physical event performed or shared between the participating nodes may be defined as a sharing and open public data base. Occurrence in the public database is verified based upon the accuracy of a large number of blockchain nodes[24,16]. The popularity of blockchain is attributed to the benefits of decentralization, anonymity, serial data structure, mutual security and transparency, immutability and tolerance to environmentally untrustful situations [2,4]. There are two types of nodes in the network[19,18]. A complete node is a node that stores and maintains the whole history of blockchain transactions. This explicitly and independently ends a transaction and authentically verifies all network transactions. The hash of the genesis block is accessible to any node in the blockchains network [2]. An earlier hash key is not in the sequence of genesis. When a new node is identified, it only knows the block of genesis, and will need to access all blocks from the genesis block to synchronize with the blockchains network. The blocks are clustered by inserting hashes from the preceding blocks into the current one, so that the hash The block is identical to the following one [2,5]. It is then safely exchanged with other nodes without the need for a central authority in a centralized P2P network. Sequential block hashes hold the transactions in order. It is therefore impossible without modifying the blocks and all future blocks to change the previous transactions [2,19]. Some of the previous works on the propagation of secure event messages concentrate on the VANET study[20,21].

The majority of voting mechanisms aim to address node security problems by seeking views from other nodes to determine the secrecy of a node. The problem with this kind of strategy is, however, whether the input nodes can be counted on. We assume that in our solution all information is kept in a centralized database of Blockchain [2].

In addition, automotive networks analyzes with the blockchain have been carried out with limitations. The simplification of centralized key management in a heterogeneous vehicle network is through a single blockchain system. The VANET and Ethereum blockchain technical concepts

allowed an open, independently regulated and decentralized network. They also used Ethereum's intelligent contract platform to run all manner of Ethereum blockchain applications. In comparison, the proposed work is for secure message transmission using a particular blockchain type in vehicle networks [25,2].

3   Overview of Blockchain

A blockchain is a centralized public ledger of all recorded activities conducted and exchanged between the participating nodes. It provides a transparent and verifiable record of each occurrence that has occurred [7]. The majority of network nodes agree to each case in the blockchain database. There are two main types of blockchains, i.e. public blockchains. The blockchain public is a transparent database in which anyone can enter and communicate with the network without the central authority's permission.

The private ledger, on the other hand, has a system of access control. It allows to monitor the network users and things like who can enter, access and write. The developer will set up a consensus community in the private blockchain. The private blockchain will thus combine to be centralized, leaving it vulnerable to a single failure. But the public ledger is a blockchain that is completely decentralized and has no single point of failure and can survive malicious attacks[7]. In a shared blockchain it aims to create a complete network after a full node is attached to its peers.
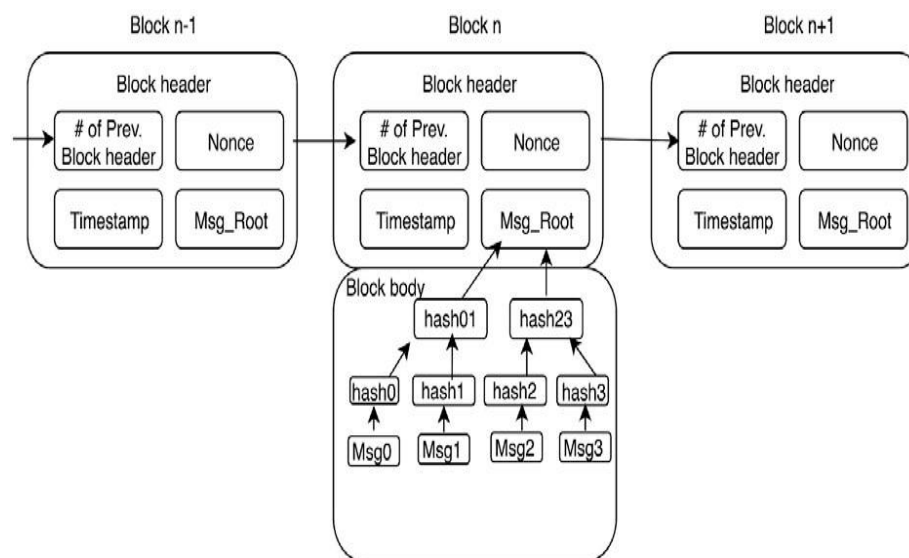

Fig 2. The structure of blocks in a blockchain

Blockchain Features
Immutability:
1. Immutability is one of the main characteristics of the blockchain. Since capturing and verifying a piece of information in the database, it cannot be updated or removed from the network. Also, it is not possible to add subjective information.
    Distributed and trusted environment:
2. Every additional node that can be distributed in a blockchain without central control to sync and verify all blockchain contents. It guarantees protection and avoids loss at a single point. It gives confidence in a stable setting.
    Protection and anonymity:
3. The blockchain gives users privacy. An encrypted network connection is given by a device. i.e. other users are not able to disclose user information. This means the private, safe and confidential personal information.
    Faster transfers:

4. A blockchain is incredibly easy to set up and the transactions are very easily validated. The handling of purchases or events takes only a few minutes.
Accurate data:
5. The data are secure, precise, trustworthy, timely and widely accessible due to the decentralized network in the blockchain. It is able to resist mistreatment and has no clear failing point.

Table 1. A Typical Scenario of Creditcoin

Phases	Initiator	Replier	Verifier
Phase 0	--	--	valid credit info by server
Phase 1	Hunt a mission for reward; valid credit info by server; **start forwarding**	--	Waiting
Phase 2	Waiting	**Receive details from phase 1; send for rewarding**	Waiting
Phase 3	Generate an announcement; **forward an AGP**	Receive a transaction from public address; wait to be confirmed	Waiting
Phase 4	Waiting	A consensus is reached by RSUs; transaction confirmed; get *coins*	Receive AGP; verify ring signatures successfully**, closing the mission**; pay *coins,* waiting to be confirmed by RSUs
Phase 5	**Mission is completed;** Receive a transaction from V, waiting to be confirmed by RSUs	Get balance; reset role	A consensus is reached by RSUs; pay *coins$_1$*; transaction confirmed
Phase 6	A consensus is reached by RSUs; transaction confirmed; get reward *coins$_1$* as	--	Get balance; reset role

	an incentive		
Phase 7	Get balance; reset role	--	--

4   Proposed Blockchain-Based Incentive Mechanism In Creditcoin

The proposed framework is based on address of these two challenges through the proposal, via an effective anonymous vehicle notification aggregation protocol, of a new privacy-preserving reward network called CreditCoin, which is built on Block-chain. In the unfamiliar environment, CreditCoin enables non-deterministic users to create and anonymize signatures and deliver an anonymous message [6]. On the other hand, CreditCoin allows users to share traffic information with Blockchain. Furthermore, CreditCoin transfers and account details are deceptive. CreditCoin also ensures anonymity as Trace's managing director of CreditCoin tracks the identity of malicious users in anonymous transactions secret.

The incentive mechanism used by the CreditCoin network is introduced in this portion. The mechanism works with the proposed Echo announcement protocol, with the goal of enabling users to make real announcements honestly [6]. The imple-mentation of this network first and then explain the meanings and protocols. Basic Concept have suggested to include four entities: trustworthy, trace, user, Roadside units and cloud-based application server. CreditCoin's proposed idea includes: the Trustworthy Authority, trace manager. A credit account, which stores reputational points, i.e. coins, is issued to every user. Users should forward and receive packages motivating their coins to be multiplied. This method is successful in crowd sourcing and unplanned networks, as demonstrated by current work. They are not, however, ideal for vehicle communications network privacy criteria. The use of Blockchain is based network in order that user behavior, without any lack of security, can establish accounting and monitor transactions.

The Table 1 represents the standard Creditcoin situation. A person is working as R or I within the network as we have indicated. Echo-Announcement Collaboration In particular, if new user, have few first coins and wishes to post a gratifying mission for information from a specific region one day, user must stay active. User can shift the role after saved some coins and later on for two reasons: One is that he / she wants to push more coins for a fulfilling mission; the other is that user is able to educate others. Since invitation costs are sent to honorable customers, it protects them by reducing unauthorized or irrelevant network requests. If a mission is made available by the number of coins, it can establish a task to obtain information about traffic. Until those with less satisfying coins the task of more coins is to be finished. This allows users to recompense more coins in their tasks. These opportunities promote the short-term movement of coins to continue to be involved in the CreditCoin network. CreditCoin also efficiently increases the availability and non-repudiation of car notes. Opponents will hardly change coins due to the voting system and hence Blockchain records.

5   Overview and Design Goals

The proposed framework system consists of four entities:

Initiator

Fig.3. Announcement Dashboard

Replier

Fig.4. Witness Dashboard

Verifier

Fig.5. Verify Announcement Dashboard

The Server stores and exchanges non-cryptographic knowledge within the network with the RSU also engages in the consensus voting process in the construction of the block chain. There are two sections of CreditCoin in order to build an efficient vehicle advertising network. The first component is a standard for advertising: the echo advertisement.

This protocol provides an authorization of thresholds and a certain degree of anonymity to ensure that anonymous ads in CreditCoin are secure. An initiator allows other observers to comply with the accompanying signature statements as Repliers and produces a note of signed traffic data and answers. The second part is a reward scheme based on Blockchain, which operates with Echo-Announcement. Through CreditCoin owner owns a multi-address credit account. The wallet

includes the names of coins. Traffic alerts from a given area are paid by consumers by charging some money for rewards[6]. In CreditCoin, a Cloud application server administers traffic allocations, and Blockchain transfers between users are forwarded. After transactions have been built, users transfer the transactions to nearby Roadside units, then the transactions are true for Roadside units. The Agreement System then checks the correct transactions. Finally, to the blocks of the chain are attached the correct transactions.

Fig.6. Credit coin report

The proposed research aims to establish a successful vehicle advertising network for VANETs. Design objectives CreditCoin has the following properties, depending on the suggested reward and echo-announcement: Enthusiasm: CreditCoin allows users to share details on traffic via advertisements. It is the network of car rewards in VANETs [6]. Data Protection: Requests, reports and transfers do not leave details (anonymity) about their origins. The Confidence: many honest witnesses (truthfulness) sign up to the announcements. Each consumer must handle a copy of the entire block chain of transactions according to threshold authentication and Blockchain and each transaction is connected to the phases of notification add-on. A source therefore cannot refuse to send (non-reputation) messages. Announcements are also rendered and transactions cannot be modified without authorization.

6   Conclusion

As a result several established routing protocols are available. The sophistication of the routing protocols is specified by different network characteristics. Protocols should be checked in real circumstances for the longer term. The majority of simula-tors still did not understand those factors. The VANET network is very critical, be-cause it is based on the road safety.

References

1. S. Nakamoto. (2008, Bitcoin: A peer-to-peer electronic cash system. Available: https://bitcoin.org/bitcoin.pdf
2. Rakesh Shrestha, Rojeena Bajracharya, Anish 1 P. Shrestha, Seung Yeob Nam. "A new type of blockchain for secure message exchange in VANET", Digital Communications and Networks,2019
3. Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges Sabih ur Rehman* , M. Arif Khan, Tanveer A. Zia, Lihong ZhengJ. Journal of Wireless Networking and Communications 2013
4. Z .Zheng, S. Xie, H.N. Dai, H. Wang Blockchain Challenges and Opportunities: A Survey Work Pap, December (2016), pp. 1-9
5. A.M. Antonopoulos Mastering Bitcoin First Edit. United States of America: OReilly Media, Inc. 2015
6. "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles",IEEE Transactions on Intelligent TransportationSystems, 2018
7. R. Shrestha et al., A new type of blockchain for secure message exchange in VANET, Digital

Communications and Networks, https://doi.org/10.1016/j.dcan.2019.04.003

8. Jithina Jose, SujaCherukullapurathMana, B.Keerthi Samhitha, "An Efficient System to Predict and Analyze Stock Data using Hadoop Techniques", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019

9. Subhashini, R., Keerthi Samhitha, B., Mana, S.C., Jose, J,"Data Analytics To Study The Impact Of Firework Emission On Air Quality: A Case Study", AIP Conference Proceedings. 2019

10. Samhitha, B.K., Mana, S.C., Jose, J., Mohith, M., Siva Chandhrahasa Reddy, L." An efficient implementation of a method to detect sybil attacks in vehicular ad hoc networks using received signal strength indicator", International Journal of Innovative Technology and Exploring Engineering, (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November, 2019

11. Mana, S.C., Samhitha, B.K., Jose, J., Swaroop, M.V., Reddy, P.C.K., "Traffic violation detection using principal component analysis and viola jones algorithms", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019

12. Subhashini, R., Jeevitha, J.K., Samhitha, B.K." Application of data mining techniques to examine quality of water", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-5S March, 2019

13. Surendran, R., Keerthi Samhitha, B.," Energy aware grid resource allocation by using a novel negotiation model", Journal of Theoretical and Applied Information Technology, 2014

14. Ramamoorthy, V., Divya, S., Mana, S.C., Samhitha, B.K.," Examining and sensing of artificial knee with multi sensors networks", Journal of Advanced Research in Dynamical and Control Systems, Volume: 10 | Issue: 11 Pages: 115-120, 2018.

15. R.Vignesh , B.Keerthi Samhitha, C.M Suja, S.Divya, "Privacy Preserving Ride Sharing Scheme with Global Social Network for vehicles using Big Data, Indian Journal of Science and Technology, Volume11(21),June 2018

16. Nagarajan, G., & Minu, R. I. (2015). Fuzzy Ontology based Multi-Modal semantic information retrieval. Procedia Computer Science, 48, 101-106.

17. Nagarajan, G., & Thyagharajan, K. K. (2012). A machine learning technique for semantic search engine. Procedia engineering, 38, 2164-2171.

18. Nagarajan, G., Minu, R. I., & Jayanthiladevi, A. (2019). Brain computer interface for smart hardware device. International Journal of RF Technologies, 10(3-4), 131-139.

19. Ananthi, S., Periwal, A., & PrinceMary, S. (2016). Data Security Based On Big Data Storage. Global Journal of Pure and Applied Mathematics, 12(2), 1491-1500.

20. Jancy, S., & Jayakumar, C. (2017, March). Various lossless compression techniques surveyed. In 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM) (pp. 65-68). IEEE.

21. Yarabarla, M. S., Ravi, L. K., & Sivasangari, A. (2019, April). Breast Cancer Prediction via Machine Learning. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 121-124). IEEE.

22. Saranya, E., Sam, B. B., & Sethuraman, R. (2017, August). Speech to text user assistive agent system for impaired person. In 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM) (pp. 221-226). IEEE.

23. Sterlin, C. S., Refonaa, J., & Ramalavanya, R. (2006). SECURE DATA OFFLOADING USING AUCTION BASED MECHANISM.

24. Surendran, R., KeerthiSamhitha, B.," Energy aware grid resource allocation by using a novel negotiation model", Journal of Theoretical and Applied Information Technology, 2014

25. Nagarajan, G., Minu, R. I., Vedanarayanan, V., Jebaseelan, S. S., & Vasanth, K. (2015). CIMTEL-Mining Algorithm for Big Data in Telecommunication,International Journal of Engineering and Technology (IJET), 7(5), 1709-1715.