World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:10, 2019

Blockchain Security in MANETs

Nada Mouchfiq, Ahmed Habbani, Chaimae Benjbara

***Abstract*—The security aspect of the IoT occupies a place of great importance especially after the evolution that has known this field lastly because it must take into account the transformations and the new applications .Blockchain is a new technology dedicated to the data sharing. However, this does not work the same way in the different systems with different operating principles. This article will discuss network security using the Blockchain to facilitate the sending of messages and information, enabling the use of new processes and enabling autonomous coordination of devices. To do this, we will discuss proposed solutions to ensure a high level of security in these networks in the work of other researchers. Finally, our article will propose a method of security more adapted to our needs as a team working in the ad hoc networks, this method is based on the principle of the Blockchain and that we named ”MPR Blockchain”.

***Keywords*—Ad hoc networks, blockchain, MPR, security.

I. Introduction

WHILE there is a smart environment, advanced and improved information and communication technologies that can save time and deliver results faster [1], it has become critical to educate all members of the community about the need to maintain personal and safe sides; Which brings us to remember the security of the digital intelligent environment and privacy in the world, there is a change of confidence in the reliability of the Internet.

The current research is oriented towards the phenomenon of Internet of Things (IoT) associating both hard and soft aspects [2]. The combination of the Internet and emerging technologies has identified the concept of digital environment.

Nowadays, the phenomenon of information and communications technology infrastructures and vast flows of information have become essential in defining of modern life. Each challenge represents an ample and discreet notion where know-how and leadership in social work can be focused on new bold ideas, scientific discoveries and surprising innovations [3]. In the coming years, IoT will make the link between several intelligent devices.

Our team works on improving the performance of ad hoc networks (MANET, VANET, FANET, ...). Since ad hoc networks could integrate the new IoT technology, we will be able to take advantage of this type of network to improve ours. In this article, we will study security improved by the principle of blockchain in order to find a relevant solution increasing the security level of ad hoc networks.

To make the network more flexible and secure, blockchain is there as a series of techniques used in distributed networks [4] in order to maintain a consistent and secure database among all the components of this network.

The remainder of the paper is organized as follows. Section II: IoT, Section III: Blockchain, Section IV: Related Work, Section V: Discussion and Section 6: Our proposition.

II. IoT

A. IoT Definition

First, Internet of Things (IoT) is considered as emerging concepts and technologies [5]. At the same time he tries to transform certain concepts from which he can create new possibilities, with adapted scenarios.

The Internet of Things is defined as a gigantic entity that has services and technologies that allow communication between its various components [6], the IoT contributes to the optimization or the creation of new concepts whether for the companies or for individuals and in several areas namely:

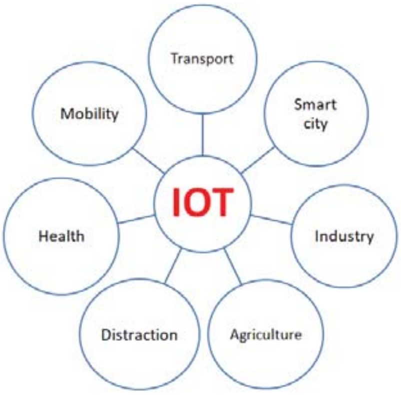

Fig. 1 IoT Domains

B. IoT Architecture

The architecture of the IoT network consists of 4 layers as shown in Fig. 2. This is not a standard architecture for IoT [7] but we will adopt it as a reference architecture since it is the most used and most accepted in order to identify and classify different security issues in IoT [8].

C. Challenges of IoT

The growing prevalence of intelligent systems embedded in virtually all types of consumer devices and the criticality of certain applications (such as monitoring, online health and network control) dictate the need for reliable security [9]. The problems associated with reliable security in IoT are motivated by the following factors:

- Problem of understanding: IoT systems are complex and less than understandable than normal systems.

N. Mouchfiq is with ENSIAS, Mohamed 5 University, Rabat, Morocco (e-mail: mouchfiq.nada@gmail.com).

A. Habbani is with ENSIAS, Mohamed 5 University, Rabat, Morocco (e-mail: habbani@ifride.com).

C. Benjbara is with ENSIAS, Mohamed 5 University, Rabat, Morocco (e-mail: benjbara@ifride.com).

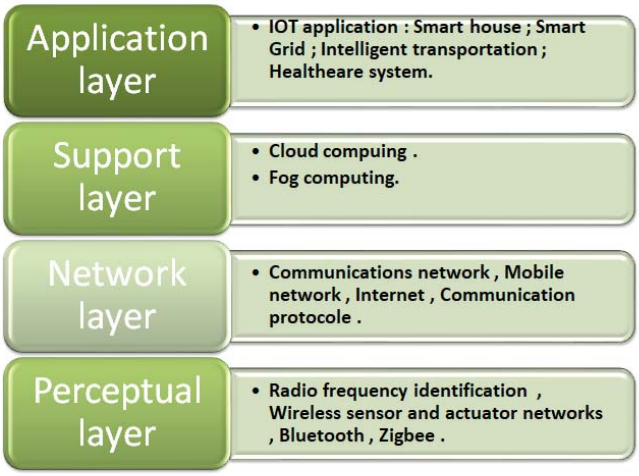
Application layer
• IOT application : Smart house ; Smart Grid ; Intelligent transportation ; Healtheare system.
Support layer
• Cloud computing .
• Fog computing.
Network layer
• Communications network , Mobile network , Internet , Communication protocole .
Perceptual layer
• Radio frequency identification , Wireless sensor and actuator networks , Bluetooth , Zigbee .

Fig. 2 IoT Architecture

- Distribution problem: IoT systems are known by their distribution over huge areas and in most cases are not sufficiently secure or controlled.
- Delimbing problem: IoT systems are deployed according to the specific choice of the provider so there is not a common standard for all systems.
- Addressing Problem: IoT systems opt for various endpoints and use multiple addressing schemes as needed, which makes these systems complex.
- Problem related to the limitation of battery: This is due to the variety of the functionalities of the IoT systems and which have a rather limited battery.
- Cost problem: IoT systems opt for platforms in the form of nodes that are inexpensive and of limited capacity, which does not allow the use of robust tools, namely the integration of fire.
- Architecture issue: IoT systems do not have standardized security tools and techniques and so far this principle has not been implemented yet.

D. *IoT Security Criteria*

- Confidentiality: Ensure that data packets and configuration parameter information are not accessed or appropriated to an attacker or disclosed to unknown entities.
- Integrity: ensure that the packets exchanged (or stored) have not been modified in an unauthorized manner (ensure that the data is not modified by unauthorized agents).
- Disponibility: Ensure that the packets exchanged are always available and that devices and agents are not prevented from having access to the information.

E. *IoT Security Technics*

IoT network security is more complex than traditional network security because the IoT network has more communication protocols, additional standards and features, and this complexity leads to hackers and malicious devices that can harm the network [10].The robust security techniques for IoT networks include:

- IoT authentication: Allows the management of several devices in the system either through passwords or simple keys or biometrics. In the context of the IoT, the authentication scenarios do not require the Human intervention, only machines can take care of it.
- IoT Encryption: Allows to reserve the integrity of the information in the network and makes it difficult to hack the system, that is, there is no standard encryption process in the IoT but what is common is the process life cycle and is essential for security management in general.
- IoT PKI: In the same framework of the concept of life cycle, the generation of private / public keys provided by the PKI since the hardware rating can restrict the choice of the key and these allow to ensure the desired level of security.
- IoT security analysis: This is an approach that aims to make operations at the level of IoT devices, namely: the collection, aggregation, monitoring and standardization of data and the creation of reports and alerts. This IoT security analysis approach detects attacks and intrusions that are not affected by traditional network security solutions.
- IoT API security: This notion is essential to ensure the integrity of the information flowing through the network and, to detect attacks that can threaten the system and to authenticate and authorize data matching between devices.

III. Blockchain

A. *Blockchain Definition*

The blockchain is a technology for storing information and transmitting in a transparent, secure and decentralized way. It looks like a large database that contains the history of all the exchanges made between its users since the creation of the blockchain. The great feature of the blockchain is its decentralized architecture as we mentioned above, in fact it is hosted by a single server but by some users. The components of the blockchain do not need intermediaries so that they can verify the validity of the chain and the information and are equipped with security procedures that protect the system [11].

Transmissions between network users are grouped in blocks and each of these blocks is validated by network nodes called ”minors”, based on criteria that depend on the type of blockchain. Once the block is validated, it joins the other blocks and is added to the block chain. The transaction is then visible to the receiver as well as the entire network.

B. *Blockchains Security*

The blockchain is in the form of a series of techniques used in decentralized networks in order to maintain a consistent database among all members. It is first proposed by Satoshi Nakamoto to abstract the basic techniques of the well-known digital currency, [12] that is to say the Bitcoin. Unlike the traditional centralized network structure, there are no fixed central nodes in networks based on block strings.

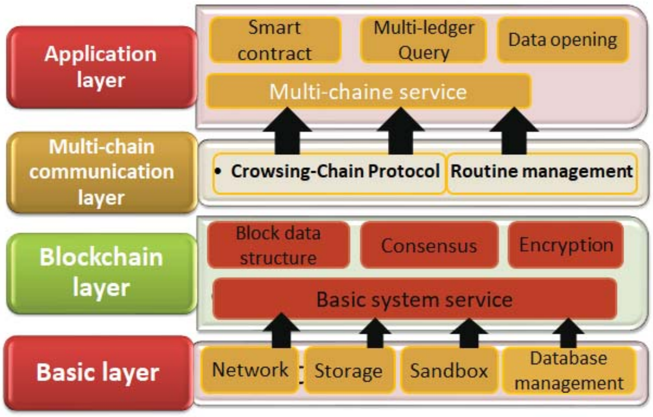

Fig. 3 Blockchain Architecture

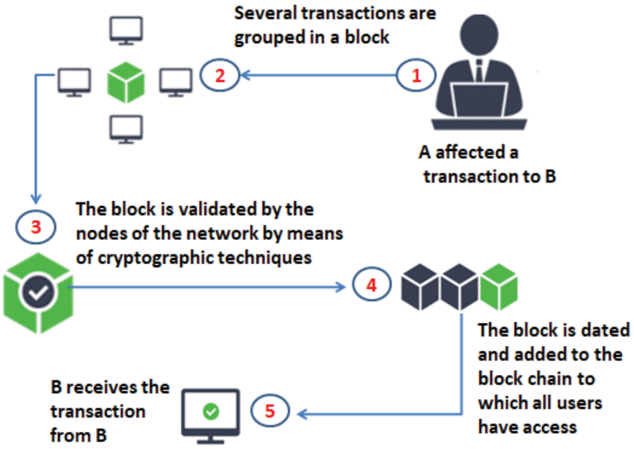
Several transactions are grouped in a block
1
2
A affected a transaction to B
3
The block is validated by the nodes of the network by means of cryptographic techniques
4
The block is dated and added to the block chain to which all users have access
5
B receives the transaction from B

Fig. 4 Operating principle of the Blockchain

All members of the network have relatively equal positions and store the same copy of blockchain. Due to the high security and reliability, blockchain has been applied in many applications scenarios and is considered one of the key techniques to promote the development of the world.

Blockchain mechanisms are ideal for this requirement as they support authentication and authorization, but availability can be provided by intrusion detection systems. Authorization and authentication may be considered an integral part of the integrity requirement.

When several nodes have the same blocks in their main chain,they are considered to have reached consensus.This subsection describes the validation rules of each block and how consensus is reached and maintained. We also explain some other consensus mechanisms that are currently used.

The consensus mechanism consists of two steps: block validation and the most extensive chain selection.These two steps are performed independently by each node. The blocks are broadcast on the network, and each node receiving a new block retransmits it to its neighbors. But, before this retransmission, the node performs a block validation to ensure that only valid blocks are propagated. There is an extensive checklist to follow including the following:

- Block structure
- Verifying if the header hash meets the established difficulty
- Block size within projected limits
- Verification of all transactions
- Checking the timestamp

IV. Related Work

A. Inter-Blockchain Report Model (Connection)

After carrying out the transaction operation [13], the routers as well as the routing tables are updated, the blockchain system of the router keeps all the addresses of each blockchain. This proposal (fig. 5) advances an interactive structure of the blockchain dedicated to the exchange of information from an arbitrary blockchain system.

The proposed protocol ensures the consistency of transactions and allows to have a high rate of blockchain, indeed, the proposed model performs the following operations:

- The communication of heterogeneous blockchains communicate based on traditional blockchain transactions.
- Once transactions cross, they are transferred by the nodes in router leblockchain.
- Transactions are performed without intermediaries and without the intervention of a third party since the routing tables contain credible information in such a way as to be maintained in the global blockchain system.

B. A Blockchain-Based Reputation System for Data Credibility Assessment in Vehicular Networks

This proposal [14] makes it possible to evaluate the credibility of the data through a ”reputation” system based on blockchain techniques. This allows the vehicle to judge the credibility of the messages received based on the reputation of the sender. each block is chained to the preceding one by storing the hash value of the one preceding it and the reputation value of each vehicle is calculated from the evaluations stored in the blockchain and the results that it has obtained agree precisely the role important that this approach plays in improving the safety of the VANETs (fig. 6).

V. Discussion

Our team focuses on ad hoc networks, specifically ad hoc mobile networks (MANETs), which are wireless networks with mobile components without infrastructure and perform the configuration on an ongoing basis. Each MANET component has the ability to move freely in the network and must each time have traffic related to its use and this is what gives the MANETs the particularity of acting both as a router and as a host. Our team works on olsr Optimized Link State Routing (OLSR) protocol, is a well-known manet protocol based on specific nodes called Multipoint Relays (MPRs). These specific nodes are in charge of the optimization of TC messages. The communication between the source (S) and the destination (D) is provided via intermediate nodes

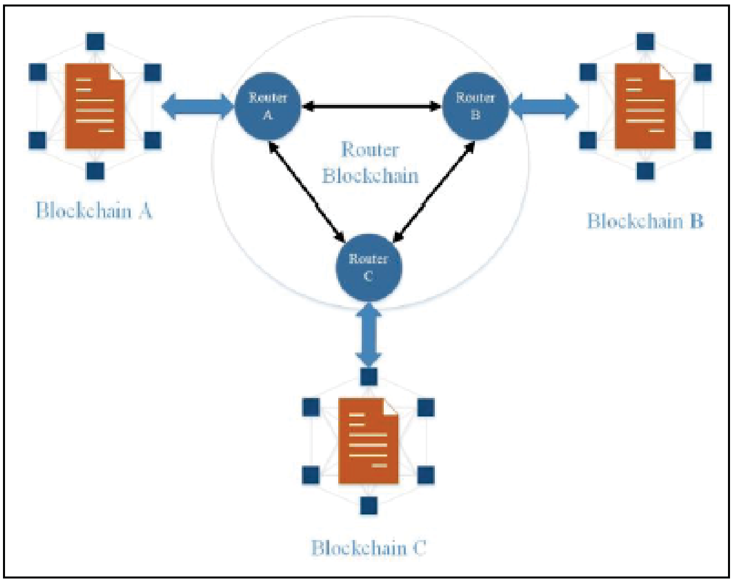

Fig. 5 Inter-Blockchain report model

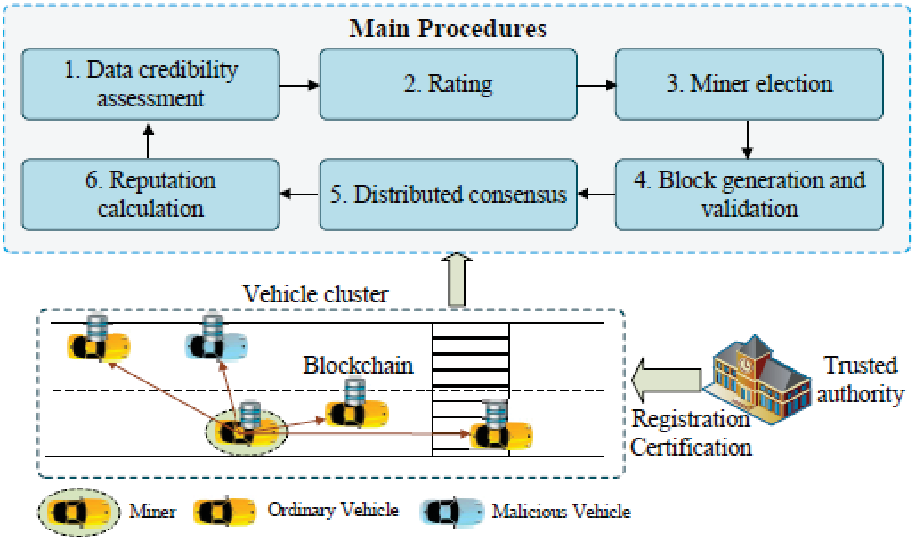

Fig. 6 Blockchain-based reputation system

(N) which select relay points among them based on several characteristics such as: energy level, stability of the node. take care of spreading control messages along the network in an optimized way.

Our team is working on improving the OLSR protocol in MANETs networks by proposing solutions to face the challenges of this type of network. Among the work done, there are those who study the optimization of the MPRs selection based on different criteria for example mobility quantification [15] and reducing broadcast redundancy [16].

In order to ensure the continuity of the team work and especially to ensure security for the network using the improved OLSR protocols developed in our team, we propose a method of security more adapted to our needs, this method is based on the principle of the Blockchain.

VI. Our Proposition

In a traditional Blockchain network, a MANETs network, the MPR plays the minor role. The MPR is elected by nodes (N) constituting its neighborhood and which are all equipped with a blockchain security algorithm.At each of these nodes (N), values are assigned:

- The previous hash: value referring to the previous node.
- TX list: historical transactions broadcast on the network.
- Nonce: takes place in each block as a solution to the mathematical problem.

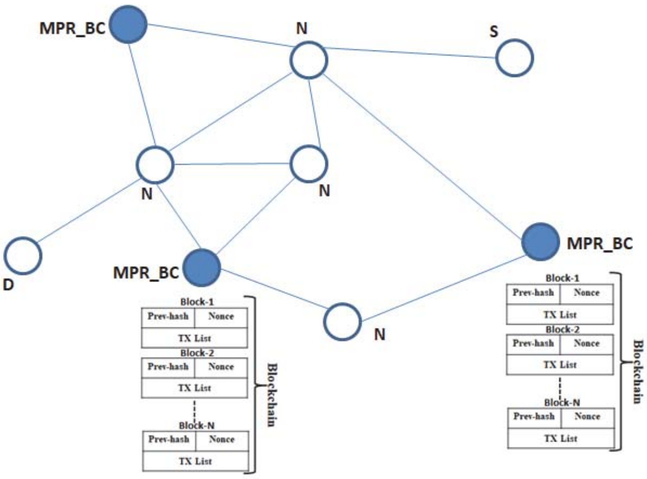

Fig. 7 ”MPR Blockchain” integrated in a MANETs network

After recording the values that correspond to each of the (N) nodes in the MPR, comes the choice of the hash algorithm to create the keys to complete the structure of the blockchain. Each MPR exchanges its own blockchain with the other MPRs present in the network and all the MPRs are based on transaction methods of the blockchain to ensure security in the network ,we will call them ”MPR Blockchain”. Finally, each MPR Blockchain calculates the credibility value of the network part which makes it able to detect malicious nodes among his neighbors.

VII. Conclusion

In this article, we discussed the definition of IoT, its architecture and infrastructure, and the security of IoT by citing security criteria. We also shed light on the work already done in the area of network security using blockchain technology and then presented our proposal. Our next work will deal with the implementation and simulation part of the Blockchain solution in the MANETs and compare them with the latest results obtained by the other members of the team working on the security side.

References

[1] M. A. Khan and K. Salah, *”IoT security: Review, blockchain solutions, and open challenges”*. Future Gener. Comput. Syst., vol. 82, p. 395-411, mai 2018.

[2] *”CONDENSE: A Reconfigurable Knowledge Acquisition Architecture for Future 5G IoT ”*. IEEE Journals Magazine . https://ieeexplore.ieee.org/abstract/document/7508921/.

[3] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu *”SDN-Based Data Transfer Security for Internet of Things”*. IEEE Internet Things J., vol. 5, no 1, p. 257-268, fvr. 2018.

[4] M. Swan, *”Blockchain thinking: The brain as a dac (decentralized autonomous organization)”*, in Proceedings of the Texas Bitcoin Conference, pp. 2729, 2015.

[5] H. Chourabi et al., *”Understanding Smart Cities: An Integrative Framework ”*, in 2012 45th Hawaii International Conference on System Sciences, 2012, p. 2289-2297.

[6] T. Forsyth *”Community-based adaptation: a review of past and future challenges ”*. Wiley Interdiscip. Rev. Clim. Change, vol. 4, no 5, p. 439-446.

[7] H. Nguyen-Minh, *”Contribution to the Intelligent Transportation System: security of Safety Applications in Vehicle Ad hoc Networks ”*. p. 159.

[8] I. Ali, S. Sabir, and Z. Ullah, *”Internet of Things Security, Device Authentication and Access Control: A Review ”*. vol. 14, no 8, p. 12, 2016.

[9] D. Minoli and B. Occhiogrosso *”Blockchain mechanisms for IoT security ”*. Internet of Things Journal 12 (2018).

[10] M. Grabovica, S. Popi, D. Pezer and V. Kneevi, *”CProvided security measures of enabling technologies in Internet of Things (IoT): A survey ”*. Zooming Innovation in Consumer Electronics International Conference (ZINC) 2016.

[11] Florian Wessling and Volker Gruhn *”Engineering Software Architectures of Blockchain-Oriented Applications ”*. 2018 IEEE International Conference on Software Architecture Companion (ICSA-C) 2018.

[12] S. Nakamoto. *”Bitcoin ”*. A Peer-to-Peer Electronic Cash System.bitcoin.org, 2008.

[13] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao and H. Kai, *”A Multiple Blockchains Architecture on Inter-Blockchain Communication ”*. IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C).

[14] Z. Yang, K. Zheng, K. Yang et V. C. M. Leung, *”A blockchain-based reputation system for data credibility assessment in vehicular networks ”*. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC).

[15] H. Amraoui and A. Habbani and A. Hajami, *”Mobility Quantification for MultiPoint Relays Selection Algorithm in Mobile Ad Hoc Networks”*. 5th International Conference on Multimedia Computing and Systems (ICMCS), p.278-283, September 2016.

[16] M. Souidi and A. Habbani and H. Berradi and F. El Mahdi, *”Geographic forwarding rules to reduce broadcast redundancy in mobile ad hoc wireless networks”*. Pers Ubiquit Comput, May 2018.