ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2022.0391

VALIDATION OF BLOCKCHAIN TRANSACTIONS IN WIRELESS SENSOR NETWORKS USING DENSE NEURAL NETWORKS

S. Brilly Sangeetha and K. Krishna Prasad
College of Computer Science and Information Science, Srinivas University, India

Abstract

The emergence of Blockchain is seen as a viable technology for enabling the improved Internet services. To authenticate information via transactions without the involvement of a third party, this decentralised, secure, and auditable approach is used. Blockchain technology is now being used in conjunction with Wireless Sensor networks (WSNs) to help bring about the fourth industrial revolution. In this paper, we analyse the difficulties in transaction throughput enhancement and block time reduction that arise in blockchain-enabled WSN networks. The study uses Dense Neural Networks to reduce the transmission delays. The simulations are conducted to test the viability of transactions and optimal distribution of transaction in WSN. Thus, Dense Nets enables optimal transactions of data from source to destination node via blocks.

Keywords:

Blockchain Transactions, Validation, Dense Neural Networks, Internet of Things

1. INTRODUCTION

The Internet of Things (IoT) is a collection of devices or sensors connected with internet [1] [2]. This is especially true for IoT devices. Applications based on the Industrial Internet of Things (IIoT) offer a variety of benefits, including increased quality of life and better knowledge of corporate processes (IIoT). By 2025, it is predicted that the overall number of IoT-enabled linked devices will reach 75.44 billion, representing a five-fold growth over the last ten years. First and foremost, the Internet of Things (IoT), which is enabled by global Internet technology, allows Internet services to be offered in a networked home environment.

It is necessary to note that the devices used in Internet of Things applications are constrained in a number of ways that are not particularly significant. It is difficult to accomplish desirable features including cost, reliability, energy efficiency, delay, security and privacy, when a large number of devices are connected to a network that does not have appropriate hardware support and does not have an acceptable energy supply, as explained above. When operating a large-scale dispersed IoT network, technologies such as Software Defined Networking (SDN) [3]–[7] can be the most successful in terms of providing control and operations while also providing security.

The blockchain, which is a critical technology that underpins Bitcoin and other crypto-currencies, has been in existence for nearly as long as the Internet has been in existence [8]-[13]. In recent years, there has been a great deal of discussion regarding the potential applications of this technology, particularly in the military. Supplier collaboration around mass customization in industrial automation, as well as increased supply chain visibility, are two concerns that are increasingly on the minds of manufacturing executives.

According to researchers, the industrial sector appears to have the most potential use for blockchain, because it is more difficult to modify current automation technologies. Transactions (TXs) can be carried out directly between peers without the requirement for a central authority to facilitate the process. Many organisations and services stand to gain significantly from this simple but powerful concept. This technology has the potential to cause significant disruption to organisation or business that relies on the current system as a key source of competitive differentiation. This development will have a significant impact on Internet of Things applications in the near future [14] [15].

Validating transactions, producing blocks, and adding additional blocks to the blockchain network are all required while transacting on the blockchain. The TXs maintained in the TX-Pools are validated by miners prior to being included in a new block, which is the central process of the blockchain. Initially, blocks are generated, and then TXs are sent to the individuals who have requested them from the requester. Validation of the results is accomplished by the use of a random or fee-based TX selection. When considering time-critical transactions, it is possible that even if the chances of being selected by random are equal or based on the bigger charge, it will be ineffective.

In this paper, we analyse the difficulties in transaction throughput enhancement and block time reduction that arise in blockchain-enabled WSN networks. The study uses Dense Neural Networks to reduce the transmission delays. The simulations are conducted to test the viability of transactions and optimal distribution of transaction in WSN. Thus, DenseNets enables optimal transactions of data from source to destination node via blocks.

2. BACKGROUND

A substantial amount of recent research in the field of blockchain has had an impact, and it offers a number of benefits to a wide range of businesses [1]-[5]. A large number of additional applications [6]-[10] are now being implemented as a result of its distributed methodology. The blockchain technology incorporates features such as anonymity, security, and data integrity into its design.

This makes it an ideal choice for the healthcare business [11] [12] because of its unique characteristics. One of the many advantages that blockchain technology can provide to the healthcare industry and biomedical systems is decentralisation. Other advantages include secrecy, security, and privacy, to name a few.

The Fig.1 demonstrates the structure of blockchains, which is necessary for transactions to take place. It is stated that transactional data sets are included in the block chain of a particular blockchain. A blockchain is created for each block, which serves as a header for all of the transactions that have taken place. Each block hash value, timestamp, nonce, and random number are all validated using a cryptographic procedure that is specific to that block data.

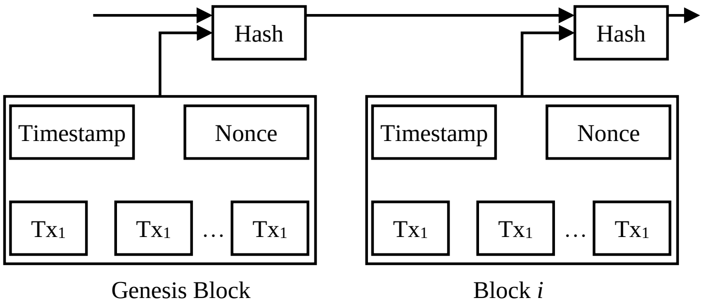

Fig.1. Blockchain Structure

The integrity of a block chain can therefore be checked by looking at the first block in the chain. The fact that the hash value of a blockchain changes at random based on block modifications is linked to the fact that it prevents the authentication of unlawful data. If the transaction and block are found to be authentic, a new block with a chain [15]-[17] will be added to the blockchain.

There are a variety of factors that can cause a time-critical transaction (TX) to be delayed in the blockchain system. The following are the considerations that must be taken into account when making a decision:

- ***Propagation Delay***: The propagation delay in the blockchain refers to the amount of time it takes for other miners to receive an announcement that a new block or transaction has been discovered during a period of activity to take place.
- ***Block Size and Miners***: The following are the miners' and block dimensions: Because the network block size is too small, it is unable to respond to requests in a timely manner. A miner TX-Pool soon fills up with pending TXs that have not yet been validated by the network. Another way to say it is that if there are fewer miners on a network, the likelihood of a TX being added to the current block is reduced.
- ***Speed of Web***: As a whole, a slow Internet causes all of the network participants to speed up, resulting in a slower Internet as a result overall.
- ***Memory-Pool***: When participants make use of temporary shared memory to store initially unconfirmed TXs, this memory pool is used to keep track of all TXs in the network, which is known as a queue.
- ***Attacks***: There have been an attack on the Blockchain [17] over years. An adversary in the spam attack constantly sends little TXs with low network costs to confuse it and the network. Sybil attacks can involve an infiltrating node generating a large number of false IDs and flooding the network with TXs and fake traffic bottlenecks, for example. When an attacker makes changes to the data included in a TX, this is referred to as a modifying TX. Furthermore, when a miner is susceptible to a compromised miner attack, any data saved in a TX is subjected to modification. Several assaults are carried out in an attempt to disrupt service and compromise the security of the system

3. PRELIMINARIES

When the transmission distance between the sender and receiver block increases, the attenuation of radio signal increases. The signal attenuation is calculated by RSSI circuit, which estimates the receiver signal coverage distance using the received signal power. The reduction of signal power at receiver is estimated and converted into an estimated distance. The distance d is calculated by an ideal radio propagation model, which is given by:

$$P_r\left(d\right)=\frac{P_\lambda G_t G_r \lambda^2}{4\pi^2 d^n L} \tag{1}$$

where

P_λ is regarded as the transmitted power,

G_t is regarded as the gain of transmitter antenna,

G_r is regarded as the receiver antenna gain,

L is regarded as the system loss and

λ is regarded as the system wavelength.

The RSSI distance estimation is given as below:

$$P_r\left(d\right)=P_r\left(d_0\right)+10\cdot\eta\cdot lof\left(\frac{d}{d_0}\right)+X_\sigma \tag{2}$$

where

d is considered as distance from transmitter to receiver block,

η is considered as path loss exponent, which estimates the reduction rate of RSSI with distance,

X_σ is regarded as the Gaussian random variable.

d_0 is considered as the power measured from the transmitting sensor block.

The power of reception between the transmitter and receiver block is given as below:

$$P_r=\frac{P_t}{d^\eta} \tag{3}$$

Hence, we can obtain,

$$P_r=A-10\cdot\eta\cdot\log\left(d\right) \tag{4}$$

where

P_r is considered as the signal power received in dBm,

A is considered as signal power estimated at meter from the receiver.

These equations are used to measure the distance easily. The path loss model determines the accuracy of RSSI measurement. Since, RSSI model is affected mostly by shadows, mobility, terrain and fast fading. Further, poor RSSI calibration affects the accurate RSSI calculation.

3.1 HOP COUNT ESTIMATION

The sensor blocks are deployed in such a way that each sensor block lies inside the neighbour blocks range i.e. block lying inside the neighbouring block range (R). By identifying the total number of hops i.e. hop count and total length of a single hop i.e. hop length, the distance d of communication between any two sensor blocks is given as,

$$d = hop\,count \times hop\,length \qquad (5)$$

The hop length tends to vary since the location of block often changes within its neighbouring block communicator range (*R*). Hence, the hop length may lead to improper results and this can be resolved to estimate the hop length in a better way if the total number of neighbour blocks or total number of local blocks (n_{local}) are known. This is given by:

$$hop\,length = R\left[1 + e^{-n_{local}} - \int_{-1}^{1} e^{\left(\frac{n_{local}}{\pi}\right)\arccos t - t\sqrt{1-t^2}}\,dt\right] \qquad (6)$$

The above computation works well if the value of n_{local} is always greater than 5. Thus, to measure the distance between the transmitter and receiver, the hop count is considered as the better metrics.

4. PROPOSED METHOD

In this section, we present an architecture of the blockchain WSN method, which are integrated to optimize the transactions by optimal selection of valid blocks. The valid blocks in the block chain network uses WSN to transmit the blocks in an optimal way using DRL, where DRL chooses the short routes as in following equations:

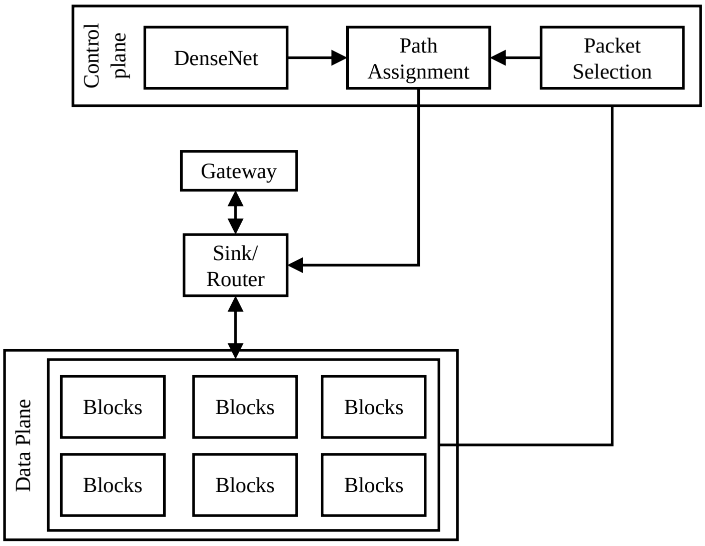

Fig.2. Architecture of blockchain transaction Validation

4.1 TRANSACTION RELIABILITY ESTIMATION

This is defined as the signal-to-noise relationship of the connection and is used to determine the reliability of the connection while assessing the connection quality. When the signal-to-noise ratio (SNR) is high, the bit error rate (BER) value is low, and the SNR is inversely proportional to the higher BER. The reduced mobility rate increases the reliability of the link in the blockchain computer, which is beneficial. The following blocks are contained within the following relationship:

$$SNR_{in} = \chi \cdot SNR_{in} + (1-\chi)SNR_{avg} + L_{st} \qquad (7)$$

where,

SNR_{in} is regarded as the SNR,

SNR_{avg} is regarded as the average SNR.

χ is regarded as the constant [0,1].

It is determined that the current SNR has a higher value. In addition, when the threshold value for SNR is dropped when compared to the current SNR, the quality of the connection is assigned a value of one, and vice versa, when the threshold value for SNR is increased.

4.2 RELIABILITY ESTIMATION OF BLOCKS

In blockchain computing, the stability of the block as well as the expiration period of the link are used to determine the trustworthiness of a block. In blockchain computing, the trustworthiness of a block is dependent on the stability of each block $N_s(\tau)$, which is affected by the expiration of a link $T_{LE}(\tau)$.

As a result, the reliability estimation factor $N_{rf}(\tau)$ is calculated as follows:

$$N_{rf}(\tau) = f\left(N_s(\tau), T_{LE}(\tau)\right) \qquad (8)$$

Block dependability is evaluated if stability > 0; this reduces the likelihood of routes failing in blockchain computing, which uses blocks with an adjustment topology to reduce route failure.

4.3 RESIDUAL ENERGY FACTOR ESTIMATION

The amount of energy consumed by each process is the most important aspect in determining the efficiency of server free computing. Overuse is avoided by the use of energy management technologies that boost leftover block energy in the system. In this case, the residual energy factor of the block $R_{et}(\tau)$ is computed as

$$R_{et}(\tau) = \frac{E_{rm}(\tau) - E_{pl}(\tau)}{E_T(\tau)} \qquad (9)$$

where, $E_{rm}(\tau)$ is regarded as the average energy spent, $E_{pl}(\tau)$ is regarded as the energy loss in each block, and $E_T(\tau)$ is regarded as the energy distribution over blocks.

4.4 LOCALIZATION OF BLOCKS

Messages of control are exchanged back and forth between the source and sink sensor blocks, which results in the formation of stable routes. In this study, we construct a stable path on the basis of position updates, successful packet delivery rates, and signal strength measurements. If the discovered path drops less than 10% of the total number of packets delivered during transmission, the path is considered stable. The term stable path refers to a channel with a high degree of connectedness. Those pathways that have a limited failure tolerance are referred to as unstable paths.

Because of the way the path is constructed, we will be able to rely on it at all times. This is an excellent strategy. Each of these three metrics is used to measure the length of the communication channel between two blocks.

The fault tolerant rate is the initial metric for finding the fault tolerance rate of the communication path in dynamic environment. It is denoted as (P_{fr}) and estimated as:

$$P_{f_r} = \sum_{n=1}^{N} HN_S + BLER + RHD \qquad (10)$$

where, HN_S is considered as the signal strength of sensor nodes for finding the stable paths, *LBER* is considered as the bit error rate of lowest order and *RHD* is considered as the minimum hop count value or regulated hop distance.

The estimation of PDR is hence given below (P_{dr}),

$$P_{d_r} = \frac{No.\ of\ pakcets\, received}{No.\ of\ packets\, sent} \times 100 \tag{11}$$

The neighbor block connectivity between the sensor blocks is the mixture of low bit error rate, minimum hop count, packet delivery ratio of each sensor blocks.

5. RESULTS AND DISCUSSIONS

The proposed method is evaluated and tested using Network Simulator tool. We set the traffic type to be a constant bit rate (CBR). The parameters settings are given in Table 1.

Table.1. Simulation parameters

Parameter	Value
Number of blocks	100
Number of sensor nodes	100
Simulation time	1000 s
Network size	200 × 200 m^2
Radio range	200 m
Packet size	256 bytes

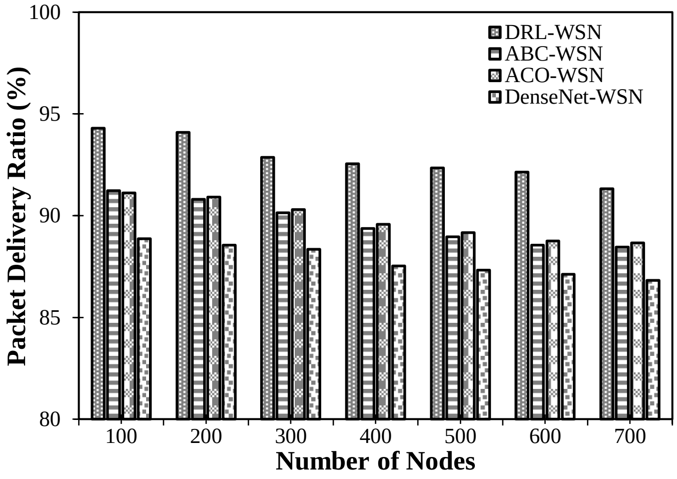

Fig.3. Packet Delivery Rate

The Fig.3 shows how the suggested method, when compared to existing methods, may be used to accurately detect the location of sensor blocks with a 90% success rate (Fig.3). Because of the existence of non-linear topology in the ACO, ABC, and DRL schemes, the position detection efficiency of these schemes is poor. Stabilized routes allow the BC-DenseNet technique to achieve its highest possible detection accuracy level. Even while moving at top speed, the maximum channel capacity and higher detection accuracy provided by a constant path allow for the identification of block movement.

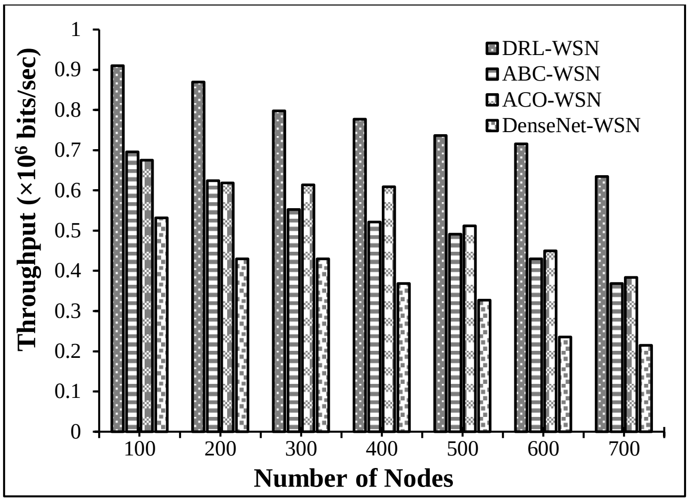

Fig.4. Throughput

The proposed BC-DenseNet has a number of advantages, including the ability to assemble clusters more quickly and update sensor block positions more quickly. Cluster creation is carried out during this phase by the cluster head, who is responsible for grouping all sensor block cluster members that are located within its cluster region with the highest feasible precision of position. A table update is used by the bridge members to communicate information about the positions of cluster members to the cluster head in order to maximise detection efficiency.

At the next stage, the proposed method is compared with existing methods like ACO, ABC and DRL in terms of throughput as in Fig.4. Variations in the sensor block mobility between 20 and 100 m/s are used to simulate the control overhead.

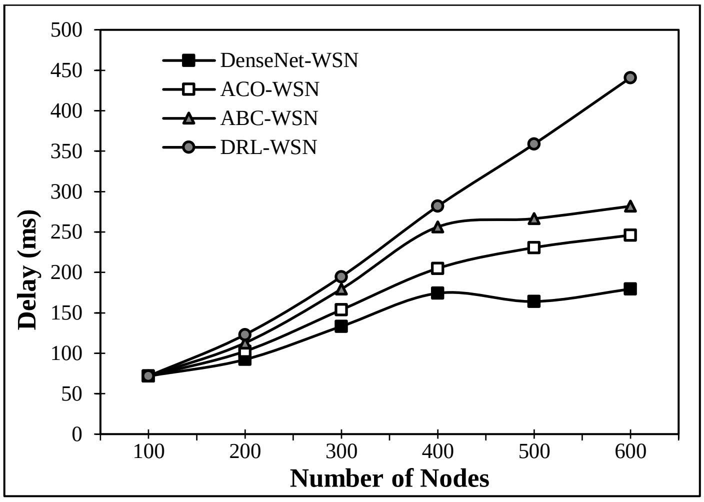

Fig.5. Delay

From the results, it can be inferred that proposed BC-DenseNet method obtains reduced delay in Fig.5 than ACO, ABC and DRL. The proposed method can build more stable paths with less computational effort by reducing the number of hops in the paths.

6. CONCLUSIONS

In this paper, we analyse the difficulties in transaction throughput enhancement and block time reduction that arise in blockchain-enabled WSN networks. The study uses Dense Neural Networks to reduce the transmission delays. The simulations are conducted to test the viability of transactions and optimal distribution of transaction in WSN. Thus, DenseNets enables optimal transactions of data from source to destination block via blocks.

REFERENCES

[1] D. Puthal, N. Malik, S.P. Mohanty and G. Kougianos, “Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems”, *IEEE Consumer Electronics Magazine*, Vol. 7, No. 4, pp. 6-14, 2018.

[2] S. Angraal, H.M. Krumholz and W.L. Schulz, “Blockchain Technology: Applications in Health Care”, *Circulation: Cardiovascular Quality and Outcomes*, Vol. 10, No. 9, pp. 1-15, 2017.

[3] B. Gobinathan, M.A. Mukunthan, S. Surendran, and V.P. Sundramurthy, “A Novel Method to Solve Real Time Security Issues in Software Industry using Advanced Cryptographic Techniques”, *Scientific Programming*, Vol. 2021, pp. 1-7, 2021.

[4] A.S. Hosen, S. Singh, P.K. Sharma and G.H. Cho, “Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network”, *IEEE Access*, Vol. 8, pp. 117266-117277, 2020.

[5] D. Puthal, N. Malik, S.P. Mohanty and G. Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems”, *IEEE Consumer Electronics Magazine*, Vol. 7, No. 4, pp. 6-14, 2018.

[6] R. Chaudhary, A. Jindal, G.S. Aujla and K.K.R. Choo, “Best: Blockchain-Based Secure Energy Trading in SDN-Enabled Intelligent Transportation System”, *Computers and Security*, Vol. 85, pp. 288-299, 2019.

[7] N. Arivazhagan, K. Somasundaram, D. Vijendra Babu and V. Prabhu Sundramurthy, “Cloud-Internet of Health Things (IOHT) Task Scheduling using Hybrid Moth Flame Optimization with Deep Neural Network Algorithm for E Healthcare Systems”, *Scientific Programming*, Vol. 2022, pp. 1-8, 2022.

[8] I.A. Omar, R. Jayaraman, K. Salah and S. Ellahham, “Applications of Blockchain Technology in Clinical Trials: Review and Open Challenges”, *Arabian Journal for Science and Engineering*, Vol. 46, No. 4, pp. 3001-3015, 2021.

[9] T.K. Agrawal, V. Kumar and Y. Chen, “Blockchain-Based Framework for Supply Chain Traceability: A Case Example of Textile and Clothing Industry”, *Computers and Industrial Engineering*, Vol. 154, pp. 1-12, 2021.

[10] I. Karamitsos, M. Papadaki and N.B. Al Barghuthi, “Design of the Blockchain Smart Contract: A Use Case for Real Estate”, *Journal of Information Security*, Vol. 9, No. 3, pp. 177-187, 2018.

[11] H. Rathore, A. Mohamed and M. Guizani, “A Survey of Blockchain Enabled Cyber-Physical Systems”, *Sensors*, Vol. 20, No. 1, pp. 282-291, 2020.

[12] J. Li, “Data Transmission Scheme Considering Block Failure for Blockchain”, *Wireless Personal Communications*, Vol. 103, No. 1, pp. 179-194, 2018.

[13] S.R. Maskey, S. Badsha, S. Sengupta and I. Khalil, “ALICIA: Applied Intelligence in Blockchain based VANET: Accident Validation as a Case Study”, *Information Processing and Management*, Vol. 58, No. 3, pp. 1-12, 2021.

[14] B.A. Scriber, “A Framework for Determining Blockchain Applicability”, *IEEE Software*, Vol. 35, No. 4, pp. 70-77, 2018.

[15] Q. Wang, Z. Jia and Z. Shao, “A Highly Parallelized Pim-Based Accelerator for Transaction-Based Blockchain in IoT Environment”, *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp. 4072-4083, 2019.

[16] S.M.H. Bamakan, A. Motavali and A.B. Bondarti, “A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria”, *Expert Systems with Applications*, Vol. 154, pp. 1-19, 2020.

[17] Y.T. Yang, L.D. Chou and C.C. Liu, “Blockchain-Based Traffic Event Validation and Trust Verification for VANETs”, *IEEE Access*, Vol. 7, pp. 30868-30877, 2019.