# Performance Analysis of Blockchain-Based Internet of Vehicles Under the DSRC Architecture

Qilie Liu[1(✉)], Liang Lin[1], Yun Li[1], and Yongxiang Liu[2]

[1] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
{liuql,liyun}@cqupt.edu.cn, linliangsure@foxmail.com

[2] School of Economics and Management, North China Electric Power University, Beijing, China
yongxiangL@126.com

**Abstract.** Blockchain technology has shown great potential in the Internet of Vehicles (IoV) in solving the problems of data sharing and information traceability. Understanding the relationship between the IoV communication architecture and the blockchain can facilitate designing dedicated blockchain enabled IoV systems. In this paper, a two-layer wireless blockchain network architecture based on Dedicated Short Range Communication (DSRC) is proposed. Then the M/G/1 queuing model is used to analyze the delivery process of the transaction under the unsaturated condition, and the Markov model is established to analyze the unicast service process. Finally, the verification process of the block in the Tangle consensus network is deduced. The simulation results show that the network load, channel conditions, queuing and backoff service processes in the wireless environment have a significant impact on the delay and throughput of the blockchain network, which further proves that the wireless environment is the main reason for limiting the performance of the Tangle blockchain network.

**Keywords:** Blockchain · IoV · DSRC · M/G/1

## 1 Introduction

The rapid development of Internet of Vehicles (IoV) technology has brought a richer driving experience to the drivers. However, in order to improve the user

Q. Liu—The work is supported by the National Natural Science Foundation of China (61671096), Chongqing Natural Fund Key Project (No. cstc2019jcyj-zdxmX0008), Chongqing Science and Technology Innovation Leading Talent Support Program (CSTCCXLJRC201908), Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJZD-K201900605), and State Grid Corporation of China Technology Project (No. 5418-201971184A-0-0-00).


H. Gao et al. (Eds.): ChinaCom 2020, LNICST 352, pp. 112–126, 2021.
https://doi.org/10.1007/978-3-030-67720-6_8

experience, smart car equipment vendors as the service subjects need to collect various data to analyze user requirements, which brings about the problems of data storage, data transmission and privacy leakage. Besides, the traditional IoV architecture relies on centralized data management and needs to face single points of failure and data leakage risks. With the generation of cryptocurrency Bitcoin [1], blockchain technology is proposed as a revolutionary technology to build a distributed and tamper-resistant digital ledger. In the case of removing the third-party institutions, the users who do not trust each other can conduct transactions through the blockchain. The key technologies of blockchain mainly include digital encryption, time stamp server, consensus mechanism, smart contract and incentive mechanism, etc., which can be applied to the fields of cryptocurrency, Internet of Things (IoT), smart city, energy transaction [2,3], etc.

In the IoV, on the one hand, the blockchain consensus mechanism is used to store and verify data, so that the data cannot be tampered with. On the other hand, smart contracts can be used to code complex logical ideas in the IoV, which can improve system execution efficiency.

However, the current application of blockchain in the IoV still faces many challenges. First, extending the blockchain to the IoV need to consider consideration of a suitable consensus mechanism. The traditional consensus mechanism based on Proof of Work (PoW) requires huge computing power, which is not friendly to the IoV nodes with low storage and computing capabilities. In order to solve the problems of limited storage space and computing power, currently, a blockchain consistency mechanism Tangle based on a Directed Acyclic Graph (DAG) algorithm has been widely studied [4]. It supports micro-transactions and has high throughput characteristics, and can be well adapted to the IoT environment. In addition, how to reduce the impact of mobility on network performance is also a challenge when applying blockchain to the IoV.

Nowadays, researchers have done a lot of work on the related issues. In [5], the author analyzed how the blockchain was extended to the IoV and presented a model of the outward transmission of vehicle blockchain data, but the analysis of the blockchain network is defective. In [6], the author established an analysis model of the IoV system based on blockchain. Based on the system model and performance analysis, the author designed an algorithm to determine the optimal full function node deployment for blockchain system under the criterion of maximizing transaction throughput. In [7], the author analyzed the security performance of a wireless blockchain network with malicious interference, and discussed the probability of successful block transmission. In [8], the author used three key indicators to study how mobility affects the performance of the blockchain system in the IoV. The model assumed that the consensus of the blockchain was carried out on moving vehicles. In [9], the author theoretically analyzed the impact of the 802.11 transmission protocol on the performance of the blockchain system, and proposed a random model to analyse the probability of a successful double-spending attack. And in [10], it analyzed why the Tangle blockchain is more suitable for IoT systems than PoW and Proof of Stake (PoS), and discussed the potential problems and challenges of Tangle in the IoT.

Most of the above work consider placing the consensus layer on the fixed IoT nodes, but ignore the mobility of the IoV nodes which will undoubtedly bring about delay fluctuations and reliability problems to the consensus of the blockchain network. Besides, the existing work has not analyzed the performance of the blockchain network on the more mature Dedicated Short Range Communication (DSRC) architecture. Therefore, based on the above work, this article proposes to extend the Tangle blockchain into the IoV. The main contributions are as follows:

- Research the extension of blockchain technology to the IoV under the DSRC architecture, propose a two-layer wireless architecture to avoid the impact of mobility on the blockchain network, and analyzes the blockchain transaction delivery model based on Carrier Sense Multiple Access (CSMA/CA) mechanism.
- We theoretically studied the delay and throughput performance of extending the Tangle blockchain to the IoV. First, we established the M/G/1 queuing model to analyze the delivery process of the transaction, and obtained the average transaction delivery delay and the average number of retransmissions; Then we deduced the block verification process in the Tangle consensus network. Considering the network load, node distribution and channel conditions, the confirmation delay of the transaction from being issued to be verified and the network throughput are obtained.

The rest of this paper is structured as follows. Section 2 introduces prepare knowledge and discusses the system model; Sect. 3 theoretically analyzes the performance of blockchain network in IoV systems, including the wireless transmission model and the blockchain verification process; Sect. 4 presents the evaluation of the proposed model; Finally, Sect. 5 concludes this paper.

## 2 Preliminaries and System Model

### 2.1 DAG Based Tangle Blockchain

The Tangle blockchain has been proved to be a very potential distributed network solution. According to reference [4], we know that Tangle uses DAG data structure to store blocks in the network, and each block unit in DAG only contains one transaction. A new transaction entering the Tangle needs to be packaged into block and verifies the two blocks at the end of the DAG. Each block has its own weight and cumulative weight. The cumulative weight is the sum of the own weights of all other blocks that directly and indirectly verify the block. The execution process of the consensus algorithm is the growth process of the cumulative weight, which is related to the load of the network. The block verification delay refers to the time when the cumulative weight reaches the verification threshold.

### 2.2 System Model

For the IoV network with random distribution and mobility characteristics, if the blockchain consensus layer is placed at the bottom mobile node, this will bring huge challenges to the reliability and delay of the blockchain network, e.g., double-spending attacks are caused by communication delays. In order to reduce the impact of the vehicle mobility on the blockchain network, this paper proposes a two-layer network model with consensus layer moving up. In the model, vehicles as light nodes are only responsible for delivering transactions to the blockchain network, and the fixed Road-Side Unit (RSU) is consensus node, running the blockchain consensus algorithm. In this paper, it assumes that the number of light nodes is subject to $2\beta L_s$ Poisson distribution [11]. $\beta$ is the unit mileage density of the node in the IoV, the unit is vehicle/m; $L_s$ is the carrier sensing coverage area of the all node, which is determined by the wireless transmission protocol. There are $n$ nodes within the carrier sensing coverage area of the consensus node, which can be expressed as

$$P(n, L_s) = e^{-2\beta L_s} \frac{(2\beta L_s)^n}{n!} \tag{1}$$

Light nodes communicate with neighboring light nodes and consensus nodes through 802.11p wireless transmission protocol. When a light node delivers a transaction to a consensus node, it first needs to compete with other light nodes within its own carrier sensing coverage area, and obtain the right to use the channel through the CSMA/CA mechanism. Only when the nodes meet the two prerequisites that the channel is idle and the backoff counter is 0 can participate in the channel competition. The above process can be modeled as a queuing process, which will be discussed in detail in the next section. The consensus node sends the received blockchain block to other consensus nodes through a wired channel to complete the consensus.

To illustrate the system model of the proposed framework, the detail steps in the Fig. 1 are as follows.

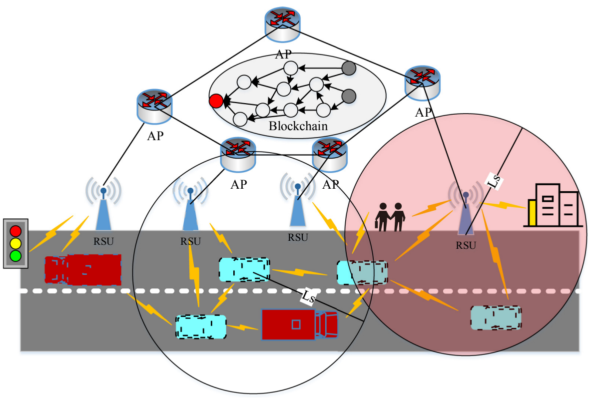


**Fig. 1.** System model

1) Light nodes classify the data transactions collected by their respective sensors, which can be divided into one-way transactions $id|type|pk|sig$ and two-way transactions $id|type|pk.1|sig.1|pk.2|sig.2$ according to the logic type. The content includes transaction id, transaction business type, transaction information, and signatures of the publisher and recipient. It is assumed that the number of transaction arrivals of each light node follows the Poisson distribution with the parameter $\lambda$.
2) The delivery process of blockchain transactions is divided into two stages. The first stage is that light nodes send the transaction to consensus nodes through one-hop unicast. In this process, multiple transactions are first queued in the MAC layer, and monitor the channel to obtain communication resources. Since it is a process of queuing to be served, this paper models it as an M/G/1 queuing system [12]. Therefore, the probability of $k$ transactions reaching the queuing system in time $t$ is

$$P(k,t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t} \tag{2}$$

In this paper, the wireless transmission environment is non-ideal, wireless signals are susceptible to various interference sources, such as buildings and communication distances, and the data packet errors can be caused by channel fading. Therefore, we discusses the channel fading by introducing the packet transmission error probability, and its calculation formula is

$$P_e = 1 - (1 - P_{ber})^{H+L} \tag{3}$$

where $P_{ber}$ is the error probability and $H + L$ is the size of the data packet.
3) The second stage is that the consensus node packs the transaction into the block, then verifies, records, and finally forwards them through the wired communication. According to the network traffic entering the consensus node, which is related to the first stage, the verification process can be divided into low load and high load.

Our analysis framework can be extended to other scenarios with mobility and resource constraints, i.e., the Unmanned Aerial Vehicle (UAV) IoT environment. Note that the focus of this paper is on the uplink transmission from the light node to the consensus node, mainly to analyze the confirmation delay of the transaction being successfully verified. Downlink performance analysis can be done in a similar way.

## 3 Problem Analysis

To study the performance of the network when extending the blockchain to the IoV, we will focus on the system delay. The transaction confirmation delay $T_s$

represents the time from when the transaction is issued to being verified, which can be expressed as

$$T_s = T_w + T_v \tag{4}$$

$$T_w = T_q + T_{st} \tag{5}$$

$T_w$ represents the time delay for the transaction to be delivered to the blockchain network. The queuing time $T_q$ is the duration when the transaction reaches the MAC layer cache queue and it enters the CSMA/CA backoff process. The service time $T_{st}$ is the time from entering the CSMA/CA backoff process to successful transmission after queuing, which is determined by wireless environment factors. $T_v$ represents the block verification delay after the transaction enters the blockchain network, that is, the delay when the cumulative weight reaches the verification threshold. Through the Tangle white paper [4], we know that the block verification delay is greatly affected by the transaction load, so it is necessary to study the delivery efficiency and consensus mechanism of transactions in a wireless environment. This section will first analyze the delivery process of transactions in a wireless environment, and then analyze the block verification process.

### 3.1 Probability Analysis of Transaction Delivery Process

Considering that the delivery of a transaction in a wireless environment is a process of queuing and waiting for service, this paper models it as an M/G/1 queuing model. The transaction generated by the light node of the blockchain first reaches the MAC layer cache queue, and then the light node obtains the right to use the channel through the CSMA/CA back-off mechanism to send the transaction. The back-off process is the service process of the queuing system.

When the light node has a transaction that needs to be uploaded to the blockchain network, it is first necessary to detect whether the wireless channel is idle according to the back-off mechanism. The back-off counter decreases by 1 when it detects that the wireless channel is idle in each slot time $\sigma$, otherwise it stays suspended. When the counter reduces to 0, the transaction is sent. If a collision occurs while sending the transaction, the next back-off stage is entered. In this paper, we assume that each back-off stage has the same back-off window and allow the transaction to be retransmitted until the receiver successfully receives it. Because the actual environment is an unsaturated network, the queue may enter the idle period after sending the transaction. Based on the above analysis, we model the backoff behavior of a light node as a Markov process [13].

Since the transaction arrival rate of light nodes obeys the Poisson distribution with the parameter $\lambda$, it can be known that the probability that no transaction arrives in the cache queue is

$$P_{idle} = 1 - exp(-\lambda h) \tag{6}$$

Where $h$ is the average slot time length, which will be analyzed later. Within the carrier sensing range of the sending node, the probability that at least one node sends a transaction is

$$P_{tr} = 1 - \sum_{k=0}^{\infty} (1-\tau)^k e^{-2\beta L_s} \frac{(2\beta L_s)^k}{k!} = 1 - e^{-2\beta L_s \tau} \quad (7)$$

where $\tau$ represents the probability of a node sending a transaction at a slot time.

Define $P_m$ as the probability that the transaction sent by the light node will fail due to the collision and error at any slot time, i.e., the probability of entering the next back-off stage. It can be expressed as

$$P_m = PP_e + P(1-P_e) + (1-P)P_e \quad (8)$$

where $P = 1 - e^{-(2\beta L_s - 1)\tau}$ is the probability that the back-off counter reaches 0 and the channel is detected busy again.

According to the above analysis, we can write the probability expression of a light node sending a transaction in a generic (i.e., randomly chosen) slot time as

$$\tau = \left[ \frac{W_0(1+P_m) + (1-2P_{tr})}{2(1-P_{tr})} + \frac{1-\rho}{1-P_{idle}} \right]^{-1} \quad (9)$$

where $\rho$ is the service intensity of the queuing system, which will be analyzed later. Considering (9) is a complicated process, we choose to use an iterative algorithm to solve it. The specific implementation of the algorithm is introduced in the next section.

Therefore, according to (6)–(9), the average length of a slot time can be expressed as

$$h = (1-P_{tr})\sigma + P_{tr}P_m(T_c[i] + T_e[i]) + P_{tr}(1-P_m)T_s[i] \quad (10)$$

where $T_c[i]$ and $T_e[i]$ represent the delay of collision and transmission error in unicast, respectively, and the successful transmission delay is $T_s[i]$. These can be expressed as

$$\begin{cases} T_s[i] = T_e[i] = T_{RTS} + T_{SIFS} + T_\delta + T_{CTS} + T_{SIFS} + T_\delta \\ +T_{SIFS} + T(H+L) + T_\delta + T_{ACK} + T_{AIFS[i]} + T_\delta \\ T_c[i] = T_{RTS} + T_{AIFS[i]} + T_\delta \end{cases} \quad (11)$$

where $T_\delta$ represents the data propagation delay.

In 802.11p, the Enhanced Distributed Channel Access (EDCA) mechanism is adopted, and Arbitration Inter-frame Spacing ($AIFS$) is used instead of Distributed Inter-frame Spacing ($DIFS$). For different priorities of transactions, the calculation formula of $AIFS$ is as follows

$$AIFS[i] = AIFSN(AC[i]) * \sigma + SIFS \quad (12)$$

Among them, $AIFSN$ is mainly for distinguishing the grade of the transaction, $AC[i]$ represents the type of the transaction, $SIFS$ is the interval between short frames.

The average number of retransmissions in the back-off mechanism is an important indicator for analyzing the transaction delivery efficiency of light nodes. Define $P_n$ as the probability that the transaction is successfully sent after $n$ back-off stages. Since each back-off process is independent of each other, $P_n$ can be expressed as

$$\begin{cases} P_0 = 1 - P_m \\ P_1 = (1 - P_0)P_0 \\ P_2 = (1 - P_0)(1 - P_1)P_0 \\ \ldots\ldots \\ P_n = \prod_{i=0}^{n-1}(1 - P_i)P_0 \end{cases} \tag{13}$$

Finally, the average number of retransmissions caused by collision and error in the process of back-off service can be obtained

$$N_w = \sum_{n=0}^{\infty} nP_n \tag{14}$$

### 3.2 Daley Analysis of Transaction Delivery Process

On the basis of the probability analysis in the previous section, in order to obtain the average delay of the delivery process in this section, we first need to obtain the service time distribution of the MAC layer. In this paper, we use the Probability Generating Function (PGF) to approximate service time distribution [14]. Denote $q_i$ as the steady state probability that the transaction service time is $i\sigma$. Let $Q(z)$ be the PGF of $q_i$, which is

$$Q(z) = \sum_{i=0} q_i z^i \tag{15}$$

Due to the simplicity of the symbols in the $z$ transform domain and the one-to-one correspondence between $Q(z)$ and $q_i$, we discusses how to calculate $Q(z)$ instead of $q_i$ alone, so $Q(z)$ can be expressed as

$$\begin{aligned} Q(z) = [PH_c(z) + (P_m - P)H_e(z)]^{\lfloor N_w \rfloor} \tfrac{1}{W_0} \sum_{k=0}^{W_0-1} H_b^k(z) + (1 - P_m) \\ H_s(z) \sum_{i=0}^{\lfloor N_w \rfloor} \{[PH_c(z) + (P_m - P)H_e(z)]^i \tfrac{1}{W_0} \sum_{k=0}^{W_0-1} H_b^k(z)\} \end{aligned} \tag{16}$$

$\lfloor N_w \rfloor$ refers to the rounding operation for the number of retransmissions; $H_c(z) = z^{T_c}$ refers to the time distribution transfer function that causes the transmission failure due to the collision during the transmission process of the transaction; $H_s(z) = z^{T_s}$ refers to the time distribution transfer function that makes the transaction transmitted successfully; $H_e(z) = z^{T_e} = z^{T_s}$ refers to the time distribution transfer function that causes the transmission failure of the transaction due to the channel error code; $H_b(z)$ is the transfer function of the time distribution occupied by the back-off process of the competitive channel. In the scenario conditions of this paper, it can be represented as

$$H_b(z) = (1 - P_{tr})z^{\sigma} + P_{tr}P_m z^{T_c+T_e} + P_{tr}(1 - P_m)z^{T_s} \tag{17}$$

By differentiating the above (17), we can get the expression and variance formula of the average service time expressed as non-saturated system as follows.

$$\begin{cases} E[T_{st}] = \sum\limits_{i=0} q_i i\sigma = \left.\frac{dQ(z)}{dz}\right|_{z=1} \\ Var[T_{st}] = \left.\frac{d^2Q(z)}{dz^2}\right|_{z=1} \end{cases} \tag{18}$$

From the Pollaczek-Khintchine (P-K) expression, the average queuing time of the sending node can be obtained in the unsaturated case.

$$E[T_q] = \rho + \frac{\rho^2 + \lambda^2 Q''(z)\Big|_{z=1}}{2(1-\rho)} \tag{19}$$

To derive the average service time distribution, probability $\tau$ must be determined. However, the calculation of $\tau$ depends on the service parameter $\rho = \frac{\lambda}{\mu}$, where $\mu$ is the service rate of the queuing system. Hence, we apply an iterative algorithm to calculate $\tau$ and $\rho$. The iteration steps are shown in Algorithm 1.

**Algorithm 1.** Time delay double iteration algorithm

1: Initialization: Assume that in the case where the load is saturated with $\rho = 1$, i.e., there are always transaction packets arriving in the queue, the idle state in the Markov model at this time will be removed.
2: **repeat**
3: Through formulas (6)–(19), the value of $\tau, P_{tr}, h, P_{idle}, P_m, N_w$ can be obtained by the first-level iterative algorithm.
4: Bring the value iterated in 3 into the PGF function of the service time to obtain the average service time $E[T_{st}]$, the service rate $\mu = \frac{m}{E[T_{st}]}$, and the average queue time $E[T_q]$ of the queue, where $m$ is the maximum number of transactions in a wireless transmission.
5: **until** Update $\rho' = \frac{\lambda}{\mu}$, if $|\rho' - \rho| < \varepsilon$, $\varepsilon$ is a predefined minimum error value, output $\rho = \rho'$, and the iteration is completed; otherwise, bring $\rho = \rho'$ into step 2 and repeat the iterative algorithm.

### 3.3 Daley and Throughput Analysis of Block Verification Process

Through the analysis of the above two subsections, the average number of retransmissions and the average delivery delay of the transaction delivery process have been obtained. Based on this, this section will study the verification process of transactions in the blockchain network, and analyze the verification delay $T_{st}$ and network throughput.

After completing the queuing and back-off process in the wireless environment, the transaction reaches the consensus node firstly, and then is packaged into blocks. Define $N_c$ is the number of all consensus nodes. And then, the consensus node broadcasts blocks to the blockchain network through a wired channel to complete the consensus, and that all blocks in the queue can be broadcast at once. From the above analysis, it can be concluded that the throughput of the wireless environment is the average block arrival rate $\lambda'$ of consensus nodes in the blockchain. Since the consensus nodes are independent of each other, we assume that the block enters the blockchain network satisfying the Poisson distribution, and the assumption will be more reasonable when the number of consensus nodes increases [15].

In the Tangle network, unlike PoW, blocks will not enter the waiting verification pool, but is directly added to the DAG structure of each consensus node. The cumulative weight is the symbol of block verification. Let $W(t)$ be the expected value of the cumulative weight of the block at time $t$, and $L(t)$ be the number of tips of the unverified block. The blockchain network update time is $D$, so the number of tips in the system after a broadcast is

$$L(t) = 2N_c\lambda' D = \begin{cases} 4\beta L_s \lambda N_c D, \rho < 1 \\ \frac{4\beta L_s N_c m D}{E[T_{st}]h}, \rho \geq 1 \end{cases} \tag{20}$$

Since the block arrival rate will affect the block verification delay in the Tangle blockchain network [16]. For this reason, We will discuss the block verification process in saturated and unsaturated wireless environments, respectively. According to the block arrival rate, the cumulative weight verification of the block is divided into low frequency $W_l^{unsat}(t)$ and high frequency $W_h^{unsat}(t)$, as shown in Fig. 2. The verification of low frequency is a linear process with parameter $\lambda_l'\omega$, and the verification of high frequency is first an exponential process, and then a linear process with parameter $\lambda_h'\omega$.

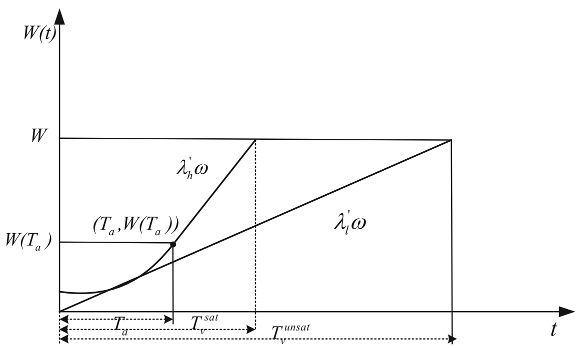


**Fig. 2.** The cumulative weight growth process of Tangle

Therefore, the cumulative weight under unsaturated wireless environment can be expressed as

$$\begin{cases} W_l^{unsat}(t) = \omega\lambda_l' N_c \\ W_h^{unsat}(t) = \begin{cases} 2exp(0.352\frac{t}{D}), t < T_a \\ 2exp(0.352\frac{T_a}{D}) + \omega\lambda_l' N_c(t - T_a), t \geq T_a \end{cases} \end{cases} \tag{21}$$

The critical point of the adaptation period and the linear period is $(T_a, W(T_a))$, where $T_a = \frac{D}{0.352}\ln(2\lambda_l' N_c D)$ represents the end of the adaptation period. If the cumulative weight value of each block reaches $W$, it is deemed to be successfully verified. Thus the block verification delay under the unsaturated wireless environment can be expressed as

$$T_v^{unsat} = \begin{cases} \frac{W}{\omega N_c \lambda_l'}, \lambda_l' N_c D \leq 1 \\ \frac{D}{0.352}\ln(2\lambda_l' N_c D) + \frac{W - W(T_a)}{\omega N_c \lambda_l'}, \lambda_l' N_c D > 1 \end{cases} \tag{22}$$

Similarly, in a saturated situation, due to the high block arrival rate, the blockchain network will directly enter the high frequency stage, i.e., the cumulative weight of the block will go through the exponential growth adaptation period and linearity at the speed $\lambda_h'\omega$ growth period. Therefore, the cumulative weight under the saturated wireless environment can be expressed as

$$W_h^{sat}(t) = 2exp(0.352\frac{T_a}{D}) + \omega\lambda_h' N_c(t - T_a) \tag{23}$$

where $T_a = \frac{D}{0.352}ln(2\lambda_h' N_c D)$ represents the end time of the adaptation period at high frequency, and the block verification delay $T_v^{sat}$ under the saturated wireless environment can be obtained.

$$T_v^{sat} = \frac{D}{0.352}ln(2\lambda_h' N_c D) + \frac{W - W(T_a)}{\omega N_c \lambda_h'} \tag{24}$$

For the entire network, the $\rho < 1$ state means that the network is unsaturated, the throughput continues to increase linearly; due to the limitation of channel capacity and delivery efficiency in wireless environment, $\rho \geq 1$ indicates the network reaches saturation state and its throughput tends to be stable.

$$TPS^{dag} = \begin{cases} 2\beta L_s \lambda N_c, \rho < 1 \\ \frac{2\beta L_s N_c m}{E[T_{st}]}, \rho \geq 1 \end{cases} \tag{25}$$

## 4 Simulation Results

To verify the model proposed in this paper, it is modeled and simulated in MATLAB according to the actual environmental requirements and the 802.11p protocol standard. The system parameters are set as follows: the number of consensus nodes is $N_c = 10$; the communication coverage $L_s = 100\,\text{m}$ is controlled by the transmission protocol; the data transmission rate in the wireless channel is 12 Mbps; and the maximum number of transactions for one wireless transmission is set as $m = 32$, the data packet size $E[H + L]$ is 1024. In the blockchain network, the weight of each block is set as $\omega = 3$, and the verification threshold is assumed to be $W = 800$. In this paper, in order to evaluate the performance of the IoV network based on the Tangle blockchain, the influence of parameters, such as the distribution of light nodes, transaction load, and channel attenuation, which are analyzed respectively.

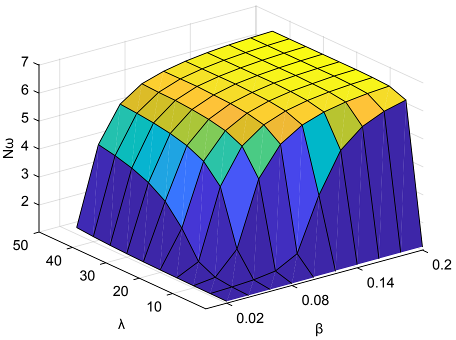


**Fig. 3.** Average number of retransmissions of transaction delivery

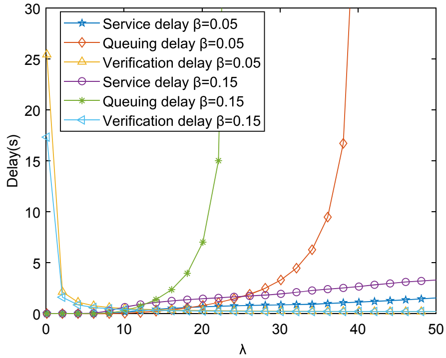


**Fig. 4.** Transaction queuing delay, service delay, and block verification delay

This article uses a three-dimensional graph to analyze the delivery process of blockchain transactions from light nodes to consensus nodes under the combined effect of the arrival rate $\lambda$ and node distribution $\beta$. As shown in Fig. 3, when $\lambda$ is fixed, as $\beta$ increases, the average number of retransmissions increases rapidly. In the same way, after fixing $\beta$, the amplitude of $N_w$ also increases with the increase of $\lambda$. But it can be clearly seen that $\beta$ has a greater impact on the average number of retransmissions than $\lambda$. This is because $\lambda$ increases the arrival probability of transactions in the queue and indirectly leads to collision when sending transactions. However, $\beta$ directly leads to collision by increasing the distribution density of competing nodes. This result is also matched with our previous analysis in (7)–(8). The average number of retransmissions $N_w$ is an important indicator that the wireless environment affects the performance of the blockchain network. As analyzed in (13)–(16), when $N_w$ increases, it means that the average service time $T_{st}$ for transaction delivery becomes larger, and the delivery efficiency decreases, which eventually leads to the block arrival rate of the blockchain network becomes lower in (20).

Figure 4 shows the trend of network queuing delay, service delay and block verification delay with the transaction arrival rate when the light node distribution is 0.01 and 0.15. As shown in the figure, when $\lambda$ increases to about 25 and 37, the transaction queuing delay $T_q$ increases suddenly, which means that the network is saturated with load. This result is matched with our previous analysis in (19), because the probability of the arrival of transactions in the queue increases with $\lambda$, which exceeds the maximum service intensity $\mu$ of the queuing system, so new transactions need to be queued to be served. In addition, since $\lambda$ will indirectly lead to collisions when the transaction is sent, it can also be seen that the service delay $T_{st}$ has a certain increase. Meanwhile, we can also see that $\beta = 0.05$ enters the load saturation stage later than $\beta = 0.15$. Additionally, the figure also shows the trend of block verification delay $T_v$. According to (14)–(16), when the load is low, the cumulative weight of each block increases slowly, and the block verification delay is large. In contrast, with the increase of $\lambda$, the accumulative weight growth rate becomes larger, and thus the block verification delay becomes smaller. Finally, when the network enters the load saturation, the verification delay will stabilize.

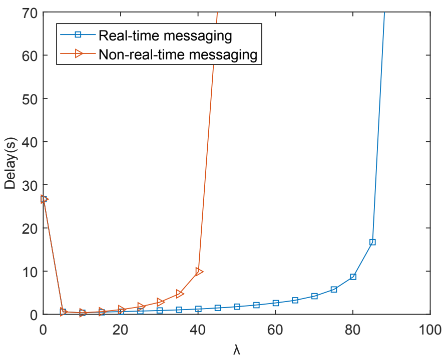


**Fig. 5.** Confirmation delay of different priority transactions

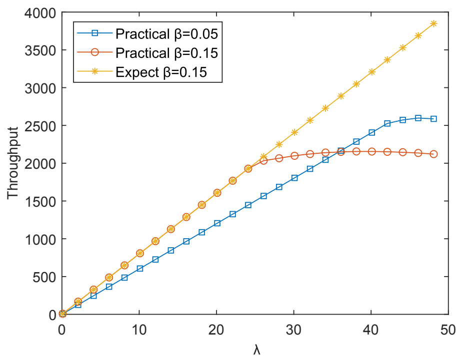


**Fig. 6.** Throughput performance

In Fig. 5, we can get the trend of the confirmation delay $T_s$ of different priority transactions. According to (10)–(12), due to the EDCA mechanism of 802.11p, transactions with higher real-time requirements are assigned a higher transmission priority, thereby reducing their service time in the queuing system. From the verification in the figure, the confirmation delay of real-time transactions is lower than that of non-real-time transactions, and it enters the load saturation state later. At the same time, it can be clearly seen in the figure that the confirmation delay of the transaction undergoes a process of falling firstly and then rising, which is caused by the consensus mechanism and the wireless environment, which have been explained in Fig. 4.

In Fig. 6, when the transaction arrival rate is low, the wireless network does not reach the saturated load and the probability of retransmission caused by collision is small, so the delivery efficiency of light node transactions is higher. At this time, the throughput growth rate of $\beta = 0.15$ is higher than that of $\beta = 0.05$. As the transaction arrival rate increases, in the case of $\beta = 0.15$, the practical situation is different from the expect situation in [17], and the throughput performance of the network will eventually stabilize after $\lambda$ reaches 25. When the maximum value is reached, the throughput will drop to a certain extent due to $E[T_{st}]$, which verifies the analysis in (25). Meanwhile, when the network load is saturated, a larger node distribution density is more likely to collision during transaction delivery, resulting in lower throughput than a blockchain network with a lower node density.

## 5 Conclusion

In this paper, we studies the performance of the IoV based on the Tangle blockchain, and analyzes how the wireless environment affects the transaction delivery process and consensus process in the Tangle blockchain, which takes into account of the more mature wireless transmission protocol standard DSRC. The simulation results prove: 1) The confirmation delay of the transaction has undergone two stages. In the first stage, the blockchain consensus mechanism leads to a higher confirmation delay, and as the network traffic increases, the confirmation delay decreases. In the second stage, the limitation of the wireless environment causes the confirmation delay to increase; 2) The throughput of the Tangle blockchain network cannot rise infinitely. In fact, as the node distribution density and network load continue to increase, the delivery efficiency of transactions decreases. The throughput of the network eventually stabilizes. The model proposed in this paper shows that it is feasible to extend the Tangle blockchain to the IoV under the DSRC architecture, but its performance is affected by its own consensus mechanism and wireless environmental factors. In the future work, as the IoV standard gradually matures, it will consider studying the blockchain network under the 5G communication architecture. At the same time, the blockchain under the heterogeneous network is also worth studying in the future.

## References


1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
2. Lei, A., Cruickshank, H., Cao, Y., et al.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things **4**(6), 1832–1843 (2017)
3. Kshetri, N.: Can blockchain strengthen the Internet of Things? IT Prof. **19**(4), 68–72 (2017)
4. Sergio, D.L.: DagCoin: a cryptocurrency without blocks. https://bitslog.com/2015/09/11/dagcoin
5. Jiang, T., Fang, H., Wang, H.: Blockchain-based internet of vehicles: distributed network architecture and performance analysis. IEEE Internet Things J. **6**(3), 4640–4649 (2018)
6. Sun, Y., Zhang, L., Feng, G., et al.: Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment. IEEE Internet Things J. **6**(3), 5791–5802 (2019)

7. Xu, H., Zhang, L., Liu, Y., et al.: RAFT based wireless blockchain networks in the presence of malicious jamming. IEEE Wirel. Commun. Lett. **9**(6), 817–821 (2020)
8. Kim, S.: Impacts of mobility on performance of blockchain in VANET. IEEE Access **7**, 68646–68655 (2019)
9. Cao, B., Li, M., Zhang, L., et al.: How does CSMA/CA affect the performance and security in wireless blockchain networks. IEEE Trans. Ind. Inform. **16**(6), 4270–4280 (2020)
10. Cao, B., et al.: When Internet of Things meets blockchain: challenges in distributed consensus. IEEE Netw. **33**(6), 133–139 (2019)
11. Yao, Y., Rao, L., Liu, X.: Performance and reliability analysis of IEEE 802.11p safety communication in a highway environment. IEEE Trans. Veh. Technol. **62**(9), 4198–4212 (2013)
12. Yin, X., Ma, X., Trivedi, K.S.: An interacting stochastic models approach for the performance evaluation of DSRC vehicular safety communication. IEEE Trans. Comput. **62**(5), 873–885 (2013)
13. Bianchi, G.: Performance analysis of the IEEE 802.11 distributed coordination function. IEEE J. Sel. Areas Commun. **18**(3), 535–547 (2000)
14. Guo, H., Zhao, H., Shuai, Z.Z.: Platoon architecture VANETs workshop communication process and performance analysis. J. Softw. **30**(4), 1121–1135 (2019)
15. Hao, S., Zhang, H.: Theoretical modeling for performance analysis of IEEE 1901 power-line communication networks in the multi-hop environment. J. Supercomput. **76**(4), 2715–2747 (2019). https://doi.org/10.1007/s11227-019-03065-4
16. Li, Y., et al.: Direct acyclic graph-based ledger for Internet of Things: performance and security analysis. IEEE/ACM Trans. Netw. **28**(4), 1643–1656 (2020)
17. Cao, B., Zhang, Z.H., Feng, D.Q.: Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digit. Commun. Netw. **6**(4), 480–485 (2020)