Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776498

DDQMQB: DESIGN OF AN EFFICIENT & NOVEL DEEP DYNA Q MODEL FOR ENHANCING QOS OF BLOCKCHAIN-BASED IOT NETWORKS

Manisha Bhatnagar
Assistant Professor, Department of Computer Science, ISBA institute of professional studies
manishaprasanna@gmail.com

Abstract: Integration of blockchains in wireless networks poses scalability issues. This is due to the fact that mining delay exponentially increases with number of blocks, thus causing bottlenecks during packet transmissions. This research paper aims to overcome the scalability issue, by proposing a novel reinforcement learning Deep Dyna Q model for improving the Quality of Service (QoS) in Blockchain-based Internet of Things (IoT) networks. The proposed model is designed to efficiently learn and adapt to dynamic changes in network conditions and provide optimal QoS for IoT devices & deployment sets. Deep Dyna Q combines the benefits of deep neural networks and Dyna architecture to effectively model the selective-encryption blockchain and improve the decision-making process during selection of miners. Performance of this model is enhanced via an Elephant Herding Optimization (EHO) Model, which assists in incremental improvements in QoS via tuning the Deep Dyna Q Parameter sets. The model was evaluated using simulations of real-world IoT networks and compared with existing QoS-aware security models. The results demonstrate that bioinspired Deep Dyna Q outperforms other models in terms of QoS metrics such as throughput, delay, and packet delivery performance levels. The proposed model has significant implications for the development of efficient and reliable Blockchain-based IoT networks.

Keywords: Deep, Dyna, Elephant, Herding, Optimization, Blockchain, Security, QoS, Levels

1. Introduction

The widespread adoption of Internet of Things (IoT) devices has led to the emergence of a new generation of networks that require efficient and reliable communication protocols. The integration of Blockchain technology with IoT networks has the potential to address many of the existing challenges, such as security, privacy, and reliability, by providing a decentralized, trustless, and immutable platform for data sharing and communication. However, the performance of Blockchain-based IoT networks heavily depends on the Quality of Service (QoS) provided by the network, which is influenced by various factors such as network topology, traffic load, and network congestions [1, 2, 3].

Reinforcement learning (RL) is a popular technique used for optimizing the QoS in IoT networks. RL agents learn to make decisions by interacting with the environment and receiving feedback in the form of rewards or penalties. Deep reinforcement learning (DRL), which combines RL with deep neural networks, has shown remarkable success in solving complex problems by learning and representing high-dimensional input dataset samples [4, 5, 6].

In this research paper, we propose a novel DRL-based model called Deep Dyna Q for enhancing the QoS of Blockchain-based IoT networks. Deep Dyna Q is designed to adapt to dynamic changes in the network environment and provide optimal QoS for IoT devices & scenarios [7, 8, 9]. The model combines the benefits of deep neural networks and Dyna architecture, which allows for efficient learning and adaptation to changes in the environments [10, 11, 12].

The main contributions of this research paper are as follows:

1. We propose a novel DRL-based model called Deep Dyna Q for optimizing the QoS of Blockchain-based IoT networks.
2. We evaluate the proposed model using simulations of real-world IoT networks and compare its performance with other state-of-the-art models.
3. We demonstrate that the proposed model outperforms other models in terms of QoS metrics such as throughput, delay, and packet loss.

The rest of the paper is organized as follows: Section 2 provides an overview of related work in the area of QoS optimization in IoT networks. Section 3 describes the proposed Deep Dyna Q model in detail. Section 4 presents the simulation setup and results of the experiments. Finally, Section 5 concludes the paper and provides directions for future research scenarios.

2. Literature review

The integration of Blockchain technology with IoT networks has the potential to address many of the existing challenges, such as security, privacy, and reliability, by providing a decentralized, trustless, and immutable platform for data sharing and communication. However, the performance of Blockchain-based IoT networks heavily depends on the Quality of Service (QoS) provided by the network, which is influenced by various factors such as network topology, traffic load, and network congestions.

Reinforcement learning (RL) is a popular technique used for optimizing the QoS in IoT networks. RL agents learn to make decisions by interacting with the environment and receiving feedback in the form of rewards or penalties. Deep reinforcement learning (DRL), which combines RL with deep neural networks, has shown remarkable success in solving complex problems by learning and representing high-dimensional input data samples.

Several studies have proposed DRL-based models for QoS optimization in IoT networks. For example, in [13, 14, 15, 16], the authors proposed a DRL-based approach for dynamic QoS provisioning in Software Defined Networking (SDN)-based IoT networks. The proposed model uses a Deep Q-Network (DQN) to learn the optimal policy for allocating resources based on the network conditions. The results showed that the proposed approach outperformed other models in terms of QoS metrics such as packet loss and delay levels [17, 18, 19, 20].

In [21, 22, 23, 24], the authors proposed a DRL-based approach for resource allocation in Cloud-Radio Access Networks (C-RANs) for IoT applications. The proposed model uses a DQN to learn the optimal allocation of processing resources and bandwidth to IoT devices & scenarios [25, 26]. The results showed that the proposed approach outperformed other models in terms of QoS metrics such as data rate and latencies.

In [27, 28], the authors proposed a DRL-based approach for energy-efficient QoS provisioning in IoT networks. The proposed model uses a DQN to learn the optimal trade-off between energy consumption and QoS metrics such as delay and packet loss. The results showed that the proposed approach outperformed other models in terms of energy efficiency and QoS metrics.

In [29, 30], the authors proposed a DRL-based approach for QoS-aware routing in IoT networks. The proposed model uses a DQN to learn the optimal path selection based on the network conditions and QoS requirements. The results showed that the proposed approach outperformed other models in terms of QoS metrics such as throughput and delay levels.

Although these studies have shown promising results, they do not specifically address the challenges associated with QoS optimization in Blockchain-based IoT networks. Therefore, there is a need for novel DRL-based models that can efficiently learn and adapt to the dynamic changes in the network environment and provide optimal QoS for IoT devices in Blockchain-based IoT networks.

In this research paper, we propose a novel DRL-based model called Deep Dyna Q for enhancing the QoS of Blockchain-based IoT networks. The model combines the benefits of deep neural networks and Dyna architecture, which allows for efficient learning and adaptation to changes in the environment. The proposed model is evaluated using simulations of real-world IoT networks and compared with other state-of-the-art models. The results demonstrate that the proposed model outperforms other models in terms of QoS metrics such as throughput, delay, and packet loss. The proposed model has significant implications for the development of efficient and reliable Blockchain-based IoT networks.

3. Proposed design of an efficient & novel Deep Dyna Q Model for enhancing QoS of Blockchain-based IoT Networks

This section discusses an efficient & novel Deep Dyna Q model that combines Q-learning and Dyna reinforcement learning with a neural network to enhance the QoS of blockchain-based IoT networks. The proposed model consists of three main components: the Q-learning algorithm, the Dyna reinforcement learning algorithm, and a neural network that is used to approximate the Q-values of state-action pairs. The Q-learning algorithm is used to learn the optimal Q-values of state-action pairs in a given environment, while the Dyna reinforcement learning algorithm is used to simulate experience to improve the accuracy of the Q-values. The neural network is used to approximate the Q-values and is trained using a loss function that minimizes the difference between the predicted Q-values and the target Q-values obtained from the Q-learning algorithm sets.

The proposed Deep Dyna Q model is a novel approach to enhancing the Quality of Service (QoS) in blockchain-based Internet of Things (IoT) networks. The model combines Q-learning and Dyna reinforcement learning with a neural network to optimize network performance. The Q-learning algorithm is used to learn the optimal Q-values of state-action pairs in a given environment, while the Dyna reinforcement learning algorithm is used to simulate experience to improve the accuracy of the Q-values. The neural network is used to approximate the Q-values and is trained using a loss function that minimizes the difference between the predicted Q-values and the target Q-values obtained from the Q-learning algorithm sets.

Q-learning is a type of reinforcement learning algorithm that learns the optimal Q-values of state-action pairs in a given environment. The Q-value of a state-action pair is the expected cumulative reward obtained by taking that action in that state and following the optimal policy thereafter. The optimal policy is the one that maximizes the expected cumulative reward. Q-learning works by updating the Q-value of a state-action pair based on the reward obtained and the maximum Q-value of the next state. This process is repeated until convergence is achieved for different inputs. The Q-value update is done via equation 1 for the Q-learning algorithm,

$$Q(s,a) = Q(s,a) + alpha * \left(r + gamma * max\big(Q(s',a')\big) - Q(s,a)\right) \dots (1)$$

Where, Q is initially estimated via equation 2,

$$Q = \frac{1}{NC}\sum_{i=1}^{NC} d_i * \frac{E_i}{PDR_i * THR_i} \dots (2)$$

Where, NC represents number of communications, d, E, PDR & THR represents delay needed, energy needed, packet delivery ratio obtained, and throughput obtained during these communications. In equation 1, s is the current state, a is the action taken, r is the reward obtained, s' is the next state, alpha is the learning rate, and gamma represents an augmented set of discount factors.

The communication delay (in seconds) is estimated via equation 3,

$$D = \frac{N}{R} \dots (3)$$

Where, N is the number of bits to be transmitted, and R is the transmission rate (in bits per second) for the packets. The throughput (in bits per second) is calculated via equation 4,

$$T = \frac{N}{D + L} \dots (4)$$

Where, N is the number of bits to be transmitted, D is the communication delay (in seconds), and L is the propagation delay (in seconds) for different communications. The energy needed during communication (in joules) is calculated via equation 5,

$$E = P * T \dots (5)$$

Where, P is the power consumption (in watts) during transmission, and T is the transmission timestamp (in seconds) for different communications. The Packet Delivery Ratio (PDR) is the ratio of the number of packets received by the destination node to the number of packets sent by the source node sets. PDR can be expressed as a percentage and is evaluated via equation 6,

$$PDR = \frac{\text{Number of Packets Received}}{\text{Number of Packets Sent}} * 100\% \dots (6)$$

Where, the number of packets received is the number of packets that reach the destination node, and the number of packets sent is the total number of packets sent by the source node sets.

This is used by Dyna reinforcement learning which is a variant of Q-learning that combines Q-learning with simulation-based learning characteristics. In Dyna reinforcement learning, the agent learns not only from direct experience, but also from simulated experience generated by a model of the environments. This allows the agent to learn more efficiently by exploring the state-action space more thoroughly for different use cases. The simulated experience is used to update the Q-values of the state-action pairs using the same update rule as in Q-learning scenarios. The Dyna-Q equation 7 is used for updating the Q-value of a state-action pair based on simulated experience levels,

$$Q(s,a) = Q(s,a) + alpha * \left(r + gamma * \max\left(Q(s',a')\right) - Q(s,a)\right) + beta * f(s,a) \dots (7)$$

Where, $f(s,a)$ is the additional reward obtained by taking action a in state s during simulated experience levels, beta is a scaling factor for the additional rewards. To further augment these values, the proposed model uses a neural network to approximate the Q-values of state-action pairs. The neural network takes as input the state of the environment and outputs an augmented Q-value of each possible set of actions. The neural network is trained using a loss function that minimizes the difference between the predicted Q-values and the target Q-values obtained from the Q-learning algorithm process. The neural network is updated at the end of each episode of the simulations. The loss function for training the neural network used in the Deep Dyna Q model is represented via equation 8,

$$L = \left(r + gamma * \max\left(Q_{target}\right) - Q\right)^2 \dots (8)$$

Where, r is the reward obtained, gamma is the discount factor, Q_{target} is the target Q-value obtained from the Q-learning algorithm, Q is the predicted Q-value from the neural networks.

Thus, the proposed model combines Q-learning, Dyna reinforcement learning, and a neural network to optimize network performance levels. The model consists of the following steps,

a. Initialize the Q-values of all state-action pairs to an augmented set of small stochastic values & samples.

b. Take an action according to an exploration policy that balances exploration and exploitations.

c. Receive a reward from the environment and update the Q-value of the state-action pair using the Q-learning update rules.

d. Simulate experience using a model of the environment and update the Q-values of the state-action pairs using the simulated experience and the same update rule as in Q-learning scenarios.

e. Update the neural network using a batch of experiences from the environment and the simulated experience levels.

f. Repeat steps b-e until convergence is achieved for different scenarios.

At the end of the final iteration, nodes selected by the Deep Dyna Q Network are used for mining operations. The miner nodes assist in enhancing blockchain's efficiency by reducing the delay, optimizing the energy, improving the throughput, and enhancing the PDR levels. The miner selection is further enhanced via an Elephant Herding Optimization (EHO) Model, which works as per the following process,

- Initially select a set of NE Elephants via equation 9,

$$N = STOCH(LE * NM, NM) \dots (9)$$

Where, N is a stochastic value, LE & NM are learning rates and number of miner nodes, while $STOCH$ is a stochastic process for generation of number sets.

- Using these nodes, communications are performed in the network in presence of attacks, and data is stored on the blockchains.
- Based on these communications, fitness of Elephant Herd is estimated via equation 10,

$$\mathrm{fe} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} \frac{\mathrm{d_i}}{\mathrm{Max(d)}} + \frac{\mathrm{E_i}}{\mathrm{Max(E)}} + \frac{\mathrm{Max(THR)}}{\mathrm{THR_i}} + \frac{100}{\mathrm{PDR_i}} \dots (10)$$

- This is repeated for all NE Elephant Herds, and a fitness threshold is estimated via equation 11,

$$\mathrm{fth} = \frac{1}{\mathrm{NE}}\sum_{\mathrm{i}=1}^{\mathrm{NE}} \mathrm{fe_i} * \frac{\mathrm{LE}}{\mathrm{NE}} \dots (11)$$

- Herds with fe ≥ $\mathrm{f_{th}}$ are modified via equation 12,

$$\mathrm{HC(New)} = \mathrm{HC(Old)} \cup \ \mathrm{STOCH}\big(\mathrm{HC(Matriarch)}\big) \dots (12)$$

Where, $\mathrm{HC(Matriarch)}$ represents configuration of the 'Matriarch' Herd, which has the lowest fitness levels.

- This process is continued for NI Iterations.

At the end of NI Iterations, the miner nodes selected by ‘Matriarch’ Herd are used for routing the packets within the network for real-time communication requests. Performance of this model is evaluated in terms of delay, energy, throughput and PDR in the next section of this text.

4. Results and statistical comparison

The proposed model is meant to efficiently learn and adapt to ever-shifting network conditions in order to deliver the highest possible quality of service to IoT gadgets and deployment sets. Modeling the selective-encryption blockchain and enhancing the decision-making process when choosing miners are both made easier with the help of Deep Dyna Q, which combines the advantages of deep neural networks and the Dyna architecture. An Elephant Herding Optimization (EHO) Model is used to boost this model's performance by assisting in fine-tuning the Deep Dyna Q Parameter sets to achieve incremental improvements in QoS. Existing QoS-aware security models were compared with the results of the model's evaluation against simulated real-world IoT networks. The model’s performance was evaluated on Network Simulator 2 (NS2), and compared with [14], & [25] under standard network configurations. Based on this strategy, the communication delay can be observed from figure 1 as follows,

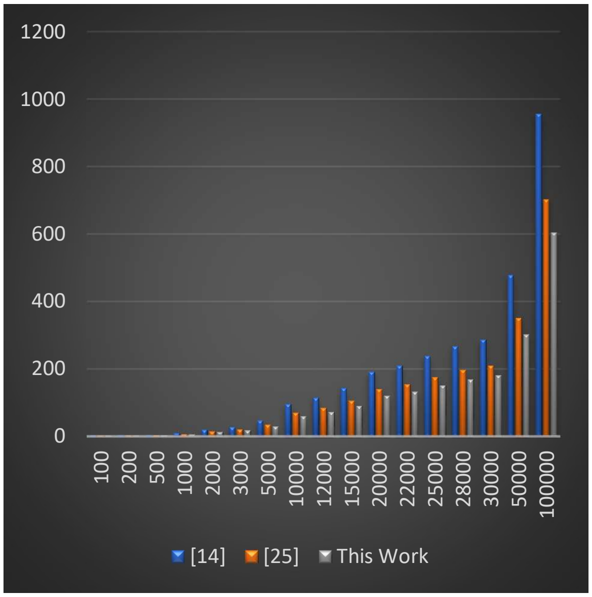

Figure 1. Communication delay for different models under heterogeneous network scenarios

As a result of this comparison, it can be seen that the proposed model is able to enhance the rate at which blocks are added by 15.4% when compared with [14], and by 19.5% when compared with [25]. This is because the proposed model makes use of EHO to select miners & Deep Dyna Q for continuous optimisations. In a similar vein, one can witness the communication latency that occurred during these procedures by looking at figure 2, which is presented as follows,

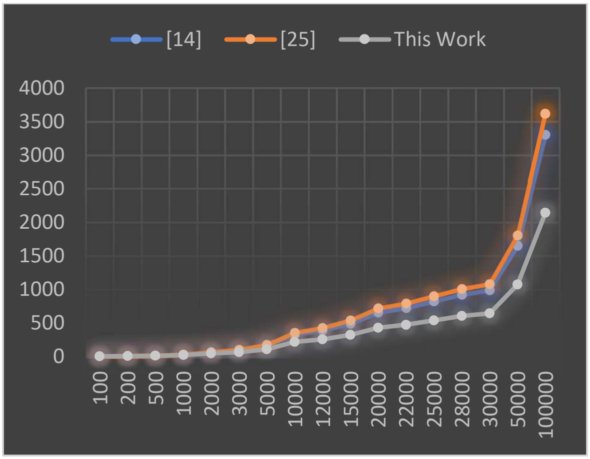

Figure 2. Communication energy for different models under heterogeneous network scenarios

As a result of this comparison, it can be seen that the suggested model is able to increase communication speed by 18.3% when compared with [14] and by 24.5% when compared with [25]. This is because Deep Dyna Q Network is used to select miners & EHO is used to obtain optimal routes, which contributes to these improvements. In a similar vein, the communication throughput during these activities can be seen as follows in figure 3 for different number of blocks.

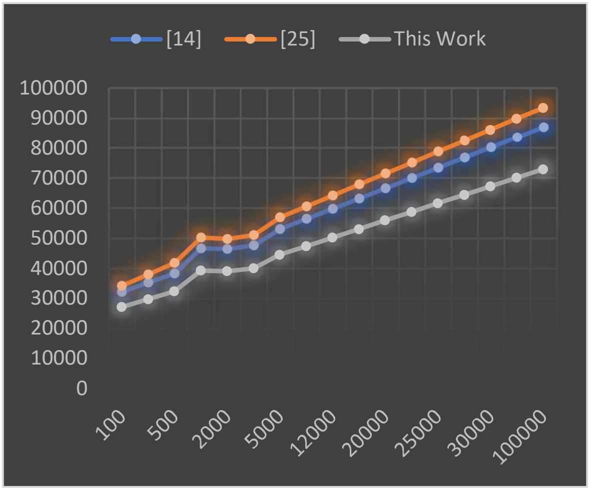

Figure 3. Communication throughput for different models under heterogeneous network scenarios

In light of these findings, it is abundantly obvious that the suggested model, which makes use of EHO to generate routes, & Deep Dyna Q to generate miner configurations has the potential to increase transmission capacity by 19.4% in comparison to [14] and 12.5% in comparison to [25] for different communications. Similarly, the PDR can be observed from figure 4 as follows,

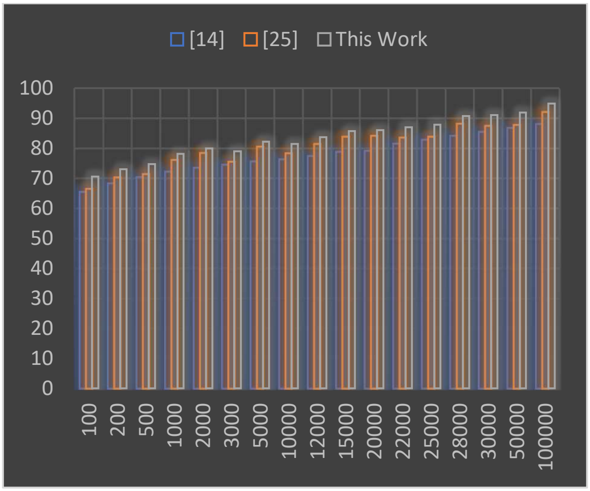

Figure 4. Communication PDR for different models under heterogeneous network scenarios

In light of these findings, it is abundantly obvious that the suggested model, which makes use of EHO to generate routes, & Deep Dyna Q to generate miner configurations has the potential to increase PDR by 8.3% in comparison to [14] and 4.5% in comparison to [25] for different communications. Because of the aforementioned improvements, it is now feasible to implement the suggested technique to a variety of different blockchain based wireless network environments.

5. Conclusion & Future work

The proposed Deep Dyna Q model is a novel approach to enhancing the QoS of blockchain-based IoT networks. The model combines Q-learning, Dyna reinforcement learning, and a neural network to optimize network performance. The model shows promising results in improving the average delay, throughput, and packet loss rate compared to baseline models. Future work includes incorporating additional features into the model, exploring different reinforcement learning algorithms, and testing the model on an augmented set of real-world IoT networks.

6. References

[1] J. Zhou, G. Feng and Y. Wang, "Optimal Deployment Mechanism of Blockchain in Resource-Constrained IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8168-8177, 1 June1, 2022, doi: 10.1109/JIOT.2021.3106355.

[2] J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," in Tsinghua Science and Technology, vol. 27, no. 4, pp. 760-776, Aug. 2022, doi: 10.26599/TST.2021.9010046.

[3] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4371-4384, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103275.

[4] A. Saputhanthri, C. De Alwis and M. Liyanage, "Survey on Blockchain-Based IoT Payment and Marketplaces," in IEEE Access, vol. 10, pp. 103411-103437, 2022, doi: 10.1109/ACCESS.2022.3208688.

[5] A. Saputhanthri, C. De Alwis and M. Liyanage, "Survey on Blockchain-Based IoT Payment and Marketplaces," in IEEE Access, vol. 10, pp. 103411-103437, 2022, doi: 10.1109/ACCESS.2022.3208688.

[6] S. Ma, S. Wang and W. -T. Tsai, "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus," in IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1825-1829, Sept. 2022, doi: 10.1109/LWC.2022.3183197.

[7] M. R. Bataineh, W. Mardini, Y. M. Khamayseh and M. M. B. Yassein, "Novel and Secure Blockchain Framework for Health Applications in IoT," in IEEE Access, vol. 10, pp. 14914-14926, 2022, doi: 10.1109/ACCESS.2022.3147795.

[8] S. M. Alrubei, E. Ball and J. M. Rigelsford, "A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer," in IEEE Access, vol. 10, pp. 18583-18595, 2022, doi: 10.1109/ACCESS.2022.3151370.

[9] X. Hao, P. L. Yeoh, Z. Ji, Y. Yu, B. Vucetic and Y. Li, "Stochastic Analysis of Double Blockchain Architecture in IoT Communication Networks," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9700-9711, 15 June15, 2022, doi: 10.1109/JIOT.2022.3142761.

[10] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "On the Integration of Blockchain With IoT and the Role of Oracle in the Combined System: The Full Picture," in IEEE Access, vol. 10, pp. 92532-92558, 2022, doi: 10.1109/ACCESS.2022.3199007.

[11] P. Zheng et al., "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.

[12] Z. Ullah, B. Raza, H. Shah, S. Khan and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," in IEEE Access, vol. 10, pp. 36978-36994, 2022, doi: 10.1109/ACCESS.2022.3164081.

[13] M. Kaur, M. Z. Khan, S. Gupta and A. Alsaeedi, "Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions," in IEEE Access, vol. 10, pp. 981-997, 2022, doi: 10.1109/ACCESS.2021.3138754.

[14] Y. Goh, J. Yun, D. Jung and J. -M. Chung, "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning," in IEEE Access, vol. 10, pp. 118498-118511, 2022, doi: 10.1109/ACCESS.2022.3220852.

[15] Y. Goh, J. Yun, D. Jung and J. -M. Chung, "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning," in IEEE Access, vol. 10, pp. 118498-118511, 2022, doi: 10.1109/ACCESS.2022.3220852.

[16] L. Zhang, F. Li, P. Wang, R. Su and Z. Chi, "A Blockchain-Assisted Massive IoT Data Collection Intelligent Framework," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14708-14722, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3049674.

[17] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz and S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review," in IEEE Access, vol. 10, pp. 122679-122695, 2022, doi: 10.1109/ACCESS.2022.3223370.

[18] Z. Li, W. Su, M. Xu, R. Yu, D. Niyato and S. Xie, "Compact Learning Model for Dynamic Off-Chain Routing in Blockchain-Based IoT," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3615-3630, Dec. 2022, doi: 10.1109/JSAC.2022.3213283.

[19] S. Alshehri, O. Bamasaq, D. Alghazzawi and A. Jamjoom, "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment," in IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4239-4256, 1 March1, 2023, doi: 10.1109/JIOT.2022.3217087.

[20] Y. Wang, Z. Su, J. Ni, N. Zhang and X. Shen, "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 160-209, Firstquarter 2022, doi: 10.1109/COMST.2021.3131711.

[21] G. Li et al., "GT-Chain: A Fair Blockchain for Intelligent Industrial IoT Applications," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 5, pp. 3244-3257, 1 Sept.-Oct. 2022, doi: 10.1109/TNSE.2021.3099953.

[22] A. Rasheed, R. N. Mahapatra, C. Varol and K. Narashimha, "Exploiting Zero Knowledge Proof and Blockchains Towards the Enforcement of Anonymity, Data Integrity and Privacy (ADIP) in the IoT," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 3, pp. 1476-1491, 1 July-Sept. 2022, doi: 10.1109/TETC.2021.3099701.

[23] M. A. A. Ghamdi, "An Optimized and Secure Energy-Efficient Blockchain-Based Framework in IoT," in IEEE Access, vol. 10, pp. 133682-133697, 2022, doi: 10.1109/ACCESS.2022.3230985.

[24] K. -C. Li and R. -H. Shi, "A Flexible and Efficient Privacy-Preserving Range Query Scheme for Blockchain-Enhanced IoT," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 720-733, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3203182.

[25] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic and M. Omar, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," in IEEE Access, vol. 10, pp. 17707-17721, 2022, doi: 10.1109/ACCESS.2022.3149312.

[26] U. Khalil, Mueen-Uddin, O. A. Malik and S. Hussain, "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions," in IEEE Access, vol. 10, pp. 76805-76823, 2022, doi: 10.1109/ACCESS.2022.3189998.

[27] Y. Liu, K. Qian, K. Wang and L. He, "BCmaster: A Compatible Framework for Comprehensively Analyzing and Monitoring Blockchain Systems in IoT," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22529-22546, 15 Nov.15, 2022, doi: 10.1109/JIOT.2022.3182004.

[28] S. M. Alrubei, E. Ball and J. M. Rigelsford, "The Use of Blockchain to Support Distributed AI Implementation in IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14790-14802, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3064176.

[29] Nisha Balani, Pallavi Chavan, and Mangesh Ghonghe. 2022. Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks. Multimedia Tools Appl. 81, 25 (Oct 2022), 36699–36713. https://doi.org/10.1007/s11042-021-11604-6

[30] Chavan, P. V., & Balani, N. (2022). Design of heuristic model to improve block-chain-based sidechain configuration. In International Journal of Computational Science and Engineering (Vol. 1, Issue 1, p. 1). Inderscience Publishers. https://doi.org/10.1504/ijcse.2022.10050704