A Review of Trust and Reutation Models Based on Block Chain Network

Geetu
Assistant Professor, Computer Science Department, Guru Nanak College, Budhlada
single.geetu@gmail.com

Abstract:

In recent years, the status of collaboration and advancement has turned out to be progressively significant. Research on the conduct of generation, training, and research associations has pulled in across the board consideration. Blockchain innovation is considered as another rebellious innovation following distributed computing, remote sensor systems, and huge information. It is profoundly worried by governments, money related foundations, and innovation organizations. Blockchain innovation is basically a specialized arrangement that on the whole keeps up a solid database through a decentralized, high-trust way. Blockchain WEB innovation has utilized in money related and different fields, yet in addition has an incredible potential for application in the fields of generation, training, and research. In this paper a novel model is proposed which immune the network against various attacks and ensure energy efficiency.

Keywords: Blockchain; Proof; Security; Trust; Reputation

1. Introduction

A trust based routing scheme deployment is important in wireless sensor networks to ensure security and efficiency. There exist a lot of trust based models in model scheme which are based on cryptographic systems and centralized model scheme, etc. However most of the routing models actually fail to identify the untrusted node in dynamic environment. In view to this problem, in this paper a trust and reputation model is proposed for routing in wireless sensor network (WSN) using block chain method with reinforcement learning. This scheme will improve the network security and efficiency. The block chain scheme is used to obtain non-tampered routing information from network nodes, as it is not feasible to tamper the network node information. The reinforcement learning model will help the network nodes to select more trusted and efficient links dynamically. In this paper, we introduce a novel trusted routing scheme based on blockchain and reinforcement learning for WSNs. In particular, we use the blockchain technology to provide a distributed routing information management platform that all the routing information is recorded on the blockchain through the blockchain token transactions. The scheme takes advantage of the decentralized, tamper-proof and traceable characteristics of the blockchain transactions to improve the trustworthiness of the routing information between the routing nodes. We exploit the reinforcement learning to learn the dynamic, reliable and extensive routing information from the blockchain network. A dynamically updated reinforcement learning model is generated in each routing node through the dynamically updated reward value brought by the action (scheduling) of each state (packet location), so as to help the routing nodes make better routing decisions and select the more reliable and efficient routing links.

2. Literature Review

Many of the research papers studied in the literature review are different for literature review done in synopsis as these are now some more specific research papers related to our study.

In [1] in their research proposed an agent based Secured Routing using Trusted neighbors in WSN. The proposed technique ensures high security by selecting the trustworthy neighbors and formulating the secured routes in the network using probability based trust model and MAC model. In this task, software agents play a pivotal role. The entire process of identifying trusted neighbors is divided into two phases:

ISSN: 2005-4297 IJCA

the first phase involves agents visiting all the neighbors one by one and determining their probability using trust model and in the second phase, MAC model is used to ensure the trusted neighbors.

In [6] suggested a minimal overhead trust management scheme in terms of memory and energy consumption. Instead of deriving the trust values of the neighboring nodes haphazardly, it employs a novel trust detector that monitors and alarms the nodes whose trust falls below a minimum threshold. This warning motivates the sensor nodes to improve its trust relationship with other nodes by analyzing and rectifying its packet forwarding behavior.

In [7] formulated an improved trust management system derived from the trust model in the iRTEDA protocol which is utilized to attain the secured data aggregation pertaining to the nature of relationship between the nodes in the network. The proposed trust model intends to efficiently utilize the second – hand information from the neighboring nodes and to attain the maximum level of security for aggregating the data and evaluating the trust and reputation of the nodes.

In [8] proposed a trust and reputation system called Eigen Trust for protecting a peer-to –peer network from the malicious users who circulate the inauthentic files in the network, which ultimately subvert the system. It presents a secure and distributed system in which a global trust value is assigned to each peer based on the peer's history of transactions. Whenever a peer i attempt to download a file from peer j, it rates the transaction as positive and negative based on the quality of file. These positive and negative ratings are added to formulate a local trust value of the peer from which file is downloaded. Local trust values of all the peers are normalized first and then aggregated using the recommendation of other peers also. This aggregated trust values are basically a global trust value which is then used by each peer in the network while communicating with other peers. Global trust values are used either for removing the malicious nodes in the system or rewarding the nodes which perform phenomenal in the network. Simulation results indicate that the proposed technique perform exceptionally well in reducing the number of downloads of inauthentic files in the system under various threat scenarios.

In [9] Came up with the Bayesian based trust management scheme (BTMS) which calculates both direct and indirect trust values for ever node in a wireless network. Direct trust values are calculated using Bayesian equation and indirect trust values which are calculated using entropy are only invoked when direct values are uncertain. The aggregated trust values are calculated by assigning weights to different recommenders depending upon their reputation system. Self-confidence factor is introduced using the aggregated trust values. Recommendation selection scheme is chosen so efficiently that it decreases the trust value of the malicious nodes in the system due to poor performance. This technique is effective enough to prevent from bad mouthing attack and ballot stuffing attack.

In [10] proposed an enhanced bio-inspired trust and reputation model for wireless networks. The proposed technique is an amalgamation of two techniques- BTRM-WSN (Bio-inspired trust and reputation management) [11] and Peer trust system [12]. BTRM-WSN employs the concept of ant colony optimization which is based on the pheromones to find the solution path in the system. Peer trust system is a trust and reputation model specially designed for dynamic peer-to-peer networks which aims at estimating the trustworthiness of the nodes by considering various factors. Simulation results exhibit drastic increase in the security of the network as it efficiently perceives benevolent nodes from malicious nodes in the network. The proposed technique behaves exceptionally well irrespective of the number of attackers in the system. The only drawback is that under highly secured environment, the energy consumption is high.

In [13] came forth a Beta-based trust and reputation system for wireless sensor networks. In this, beta distribution is used to simulate the node's reputation instead of binomial distribution as done in the previous papers which increases the efficiency of the system. Whenever a node wants to interact with other node, it calculates its reputation distribution based on the interaction information available. This is called direct trust value and then the indirect trust value obtained by sending the broadcast signal to the other node asking for its local trust value. Two types of trust are considered: communication trust and data trust. The proposed techniques audaciously shield the system from slander and collusion attacks by setting the appropriate weights and threshold values. Energy consumption is still a major issue that needs to be addressed.

In [14] introduced Multiple criterion decision making (MCDM) based trust and reputation system specially formulated for wireless mesh networks which is a coalescence of static and mobile entities and it is a challenge to ensure secure routing in such networks as these are devoid of any centralized administration. It is a combines the concept of trust as an uncertain entity [15] and TOPOSIS (Technique for ordered priority with similarity to ideal solution) [16].The technique TOPOSIS is based on the concept that the chosen solution should have the minimum distance from Positive ideal solution(PIS) and maximum distance from NIS (negative ideal solution). Initially, a decision matrix is formulated and ideal and non-ideal solutions are identified. After that, the separation between the ideal and non ideal solution is established, finally, a trusting system is built which is based on packet forwarding and recommendation system. Final trust value is calculated by combining the individual and recommended trust values. Extensive simulation done using c++ reveals that the proposed model effectively protects the network from malicious nodes.

The concept of 'Work' is introduced in [17] in which paper based geographical and energy aware routing (W-GEAR) is proposed for calculating trust and reputation in a wireless network. It uses a sink recognition mechanism for performing real time node data forwarding and differentiates between useful paper and useless paper. By doing that, it efficaciously protects the network from malicious nodes. Whenever a valid packet goes through the path all the way to the sink, each node in the path gets an incentive by increasing the reputation value and the path in which the invalid packet travels, each node's reputation value decreases. Paper is calculated based on the distance between the nodes. The proposed model is effective enough to cope the selective forwarding and data tempering attacks.

In [18] intends to ensure the security of the wireless multimedia sensor networks by assigning direct and indirect trust values to the nodes. The weight and trust value of the nodes are updated time to time. Firstly the nodes are clustered based on the power and distance between the nodes. There are two trust and reputation system: 1.Static trust and reputation system in which random weights and trust values are assigned to the nodes assuming that all the nodes are authorized. Malicious node detection is done using a certain formula. Trust values are updated as we route the packets from source to destination.

2. Dynamic trust and reputation system: As the position of the nodes is changing constantly. So instead of comparing the trust value of the node with the threshold value, the packet is directly routed to the node with the highest trust value. Packet loss is the parameter used for detecting the efficiency of the node. Loss of packets is used to identify the malicious nodes.

In [19] presented a novel technique suited for the sensor network and cloud computing integration. It aims at calculating and managing trust and reputation of the service provided by CSP (cloud service provider) and SNP (sensor network provider). It also helps the CSU (cloud service user) to choose CSP and CSP to choose SNP. CSU, CSP AND SNPs have several attributes which are taken into consideration while calculating the trust and reputation. The proposed technique is one –of-a-kind which addresses the problems of networks which incorporates both cloud computing and wireless networks.

In [20] presented a secure framework called GoNe (Good Network) for assessing the reputation of sensor nodes in the network. It employs a machine learning technique called SOM (self-organizing maps) specially designed for unsupervised neural architectures. The proposed framework is well-suited for the environments that produce humongous data and adverse in nature. It has various noteworthy features like it performs periodic assessment of nodes, provides security from many types of attacks and ensures privacy and security of the network. It also performs homomorphic encryption [21] in order to minimize the amount of data in the network and prevents network congestion.

2.1 Why Block chain scheme is used?

In case of any attack, assume the malicious node release a false queue length basically to obtain the information, and will not forward the information, and will not forward the information further will results in creation Black hole in network. Recently, Trust and Reputation models are used for routing where network nodes maintain trust value and keep track of its neighbours [4]. This scheme enables the nodes to select more reliable links, but due to information available only for neighbours nodes this scheme is not completely compatible with multi hop distributed WSN. To keeping in view above challenge a third party intermediary scheme is proposed, but a malicious node may attack and control third party system, therefore still secure routing is not ensured [20].

The Block chain is decentralized and has its own self organizing ledger system which make is suitable for Multi-hop distributed WSN. Four technical elements of block chain are [5-7]:

1. The distributed ledger will store all the transactions on block chain. Each transaction includes address of receiver, payload information, timestamp and smart control code and its result. This ledger is joined by multi-hop nodes at different locations. Each node in block chain maintains complete information can be tamper. Also all nodes in network can participate to check legality of transaction.
2. The asymmetric encryption and authorization mechanism technology of block chain also ensure data security and privacy. Information stored on block chain is public but the information regarding account identity is highly encrypted and can only be accessed by or under user authorization.
3. Consensus mechanism in block chain also prevents tampering. There exist many consensus algorithms like POW (Proof ofpaper), POS (Proof of Stack), POA (Proof of Authority), and POC (Proof of Capacity) [10]. In thispaper major mechanism that can be included in :
    a. PoW: Major crypto currency like bitcoin and litecoin used this consensus mechanism. This method relies on to carry out some mathematical operations which are done by a node to find a random number to obtain accounting right. A attacker node need more than 51% of network computing power to take over the block chain network control, which is almost not possible as resource utilization. Percentage of this scheme is too high.
    b. PoA: Improvement of PoW due to high complexity. In PoA mechanism a validator node is selected on basis of polling from other nodes. The validator only can validate the transaction then only upload on block chain network.

4. Smart contract is trusted and non-tampered data that will be executed automatically to update ledger status in block chain. These changes cannot be tampered as they are confirmed by specific consensus mechanism by which the block chain network agreed.

Therefore in this environment, a routing node can acquire correct reliable information is not limited to neighbour's only. A Re-inforcement learning is used which is a kind of machine learning algorithm which given feedback to node before selection of link [18-20].

3. Proposed Threat Model

In this paper various assumptions are:

a. The block chain network is trusted network, where no attacker can take over the network control by controlling more than half nodes.
b. The routing nodes are untrusted and all nodes are vulnerable to be attacked by malicious node.
c. A malicious node can falsely claim to send data packets to a node or may deny receiving packs received from other nodes.
d. A malicious routing node can broadcast false route information in network live route length information that affect network.
e. A routing node can only act as a malicious or normal node i.e. no mean intermittent.

3.1 Non-consideration Factors

a) In this paper the collision attack between two routing nodes will not be considered to avoid invalid block chain transactions.
b) Occasional abnormal behaviour by a network model will not be considered for example node did not be transmitting data on time, due to channel busy or loss of wireless connectivity.

4. Methodology of Proposed Model: Block Chain – Based Network Architecture

The proposed framework is divided into two components; one is routing networks other is block chain network. This framework will consist of three entities: Routing Nodes (R), Sever Node (S) and Terminal Device. The routing network consists of routing nodes and terminals. Each node has its Local area network to connect secure terminals. Also it is responsible for receiving and sending packets to other nodes. The source terminal will sent packet to forward to destination terminal to Routing Node (R_i). R_i

forward packets by selecting next hop R_π which is calculated on the basis of information obtained, using learning model. Then packet is delivered to destination terminal through node $R_{t.}$

In this paper PoA consensus algorithm is used. In Figure 1, red lines indicates PoA block chain network, which consist of server and routing nodes. The two entities of PoA are:

1. **Validator:** These are pre-authenticated nodes in network which are responsible for the verification paper in block chain. The validator node has high rights and unique block chain address. The major task of validator is to execute smart contract, verify block chain transactions. A new validator can only be added when more than 50% of nodes vote in favour. In case malicious nodes try to become a new validator node, it automatically kicked out as it can attack only a single block at a time. So there is no case that 50% majority will be given to attacker.
2. **Minions:** These are less privileges node which do notpaper, but execute contract and query. These are normal nodes of network known as Minions in block chain and they have unique block chain address. In this network the WSN nodes are both static and dynamic. For example Server nodes are static whereas Routing nodes are dynamic. But any node entry or exit does not affect system as information is updated dynamically using block chain.

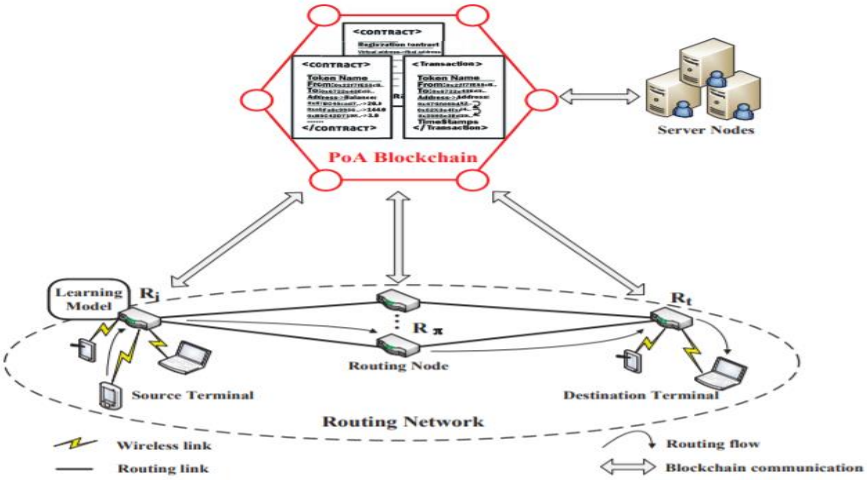

Figure 1 Framework of Block Chain Based Network

In contrast with traditional networks, each node in proposed scheme is registered on registration contract after entering in block chain network. The source node will forward data to next hop in block chain network. Then block chain network confirm Routing information (address of next hop, number of packets, timestamps). Then this information is confirmed by server node through block chain consensus mechanism and updated on block chain. The learning model regularly extracts this information from network and accordingly select best next hop based on Trust and Reputation.

4.2 Block Chain Network Procedure

To effectively operate block chain network the information of routing network must be transferred to block chain network. The information is recorded in contracts, named as Registration, Token, and Block chain transaction contract. These contracts are verified then released to block chain network. All these contracts manipulated by pre-authenticated server nodes, then result given to block chain network.

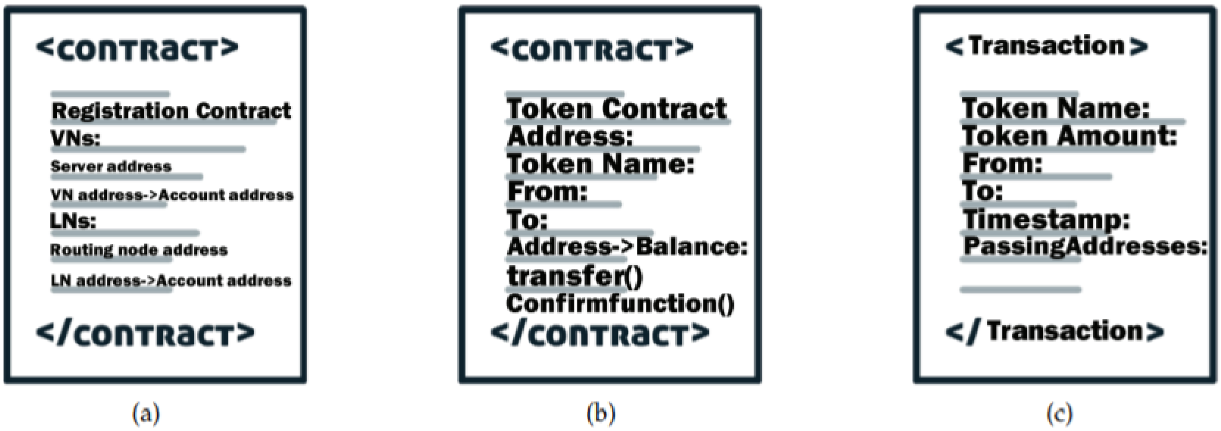

Figure 2 Contract Formats for Registration, Token and Transaction

Algorithm procedure of registering a node:

Input: ba (Block chain address of contract caller) and pa (Physical address of contract caller)

Output: Result of Registration (r) after execution

```
Mapping map :
        Blockchain .address ⟶ physical address
Mapping State
        Blockchain .address ⟶ 0 or 1
While true do
{The contract is waiting for contract caller to trigger}
 r ⟵ NULL ;
 If state (ba) = 1 then r ⟵ failure ;
 else map (ba) = pa;
State(ba) =1;
r ⟵ success ;
end if;
end while ;
```

Here state=1 indicate that node is already registered and operation fails. Concept of this code is that the block chain address never be changed in case a malicious node tries to attack changing its physical address, still registration fails as pa will not mapped with ba.

4.2.1 Token Contract

Each node in network will generate token's by giving co-related variables on block chain, like token balance B_r ,block chain address and destination node token R_T. As contract release, it will automatically generate supply of tokens for release. The routing nodes transmit tokens and record on block chain. The implementation details of one complete token transaction and we divide a token transaction into three processes:

a) Initialize number of data packets in R_i as p and in next hop as R_{TT} as i.e. B_{Ri} = P and B_{RTT} = q. R_i transfer n unit of data to $R_{TT,}$ in traditional routing network acknowledgement is shared by R_{TT} to confirm data received and token balance is B_{Ri} = P – n and B_{RT} = q + n. And other nodes do same by checking trust from trust from neighbours and keep sending data. In case R_{TT} is malicious, it drops packets then B_{RTT} = q. This cannot guarantee trustworthiness routing.

b) In this proposed paper, the routing process is validated by the block chain network instead of neighbour's nodes. Once the data packets are transmitted, R_i trigger the "transfer" function on token contract to indicate change in static including amount of token n sent to R_{TT} to block chain network. The R_{TT} trigger confirms function after receiving the n data packets.

c) After confirmation of data receiving, the token contract check whether n = n'.i.e. sent = received. In case n =! n' the balance of B_{Ri} = P and B_{RTT} = q will not updated. The complete transaction is verified by PoA consensus of server node, i.e. if more the half authenticated node of server authenticate transaction, then only it will be uploaded on block chain network. The stipulation is that the transaction must be done in single time slot, as incomplete, failed and cancelled transactions will not recorded in block chain network.

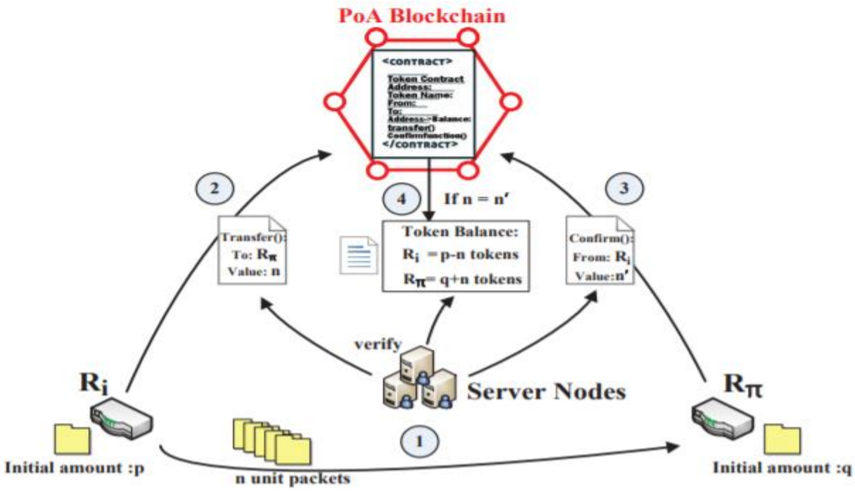

Figure 3 Token Transactionpapering

5.3 Reinforcement Learning

Further to optimize the network performance and decisions, the reinforcement learning technique is used. This technique will learn dynamically from the available information in the network and will help the source node to select best next trustworthy hop node. The proposed learning model will obtain all the information from block chain network, which includes: t_1 = timestamp of token transaction, t_t = array representing complete transactions and n_1 = transfer token time.

5.3.1 Reinforcement Learning Algorithm

Input: Environment (E); Action Space (A), Initial State (x_0); Reward Discount (β); Learning Rate (α);
Output: Policy (π);

```
$Q_t(x, a) = 0$; $P(x, a) = \frac{1}{A(x)}$;
$x = x_{0;}$
$for\ T = 1,2, \ldots \ldots do$
$A = \pi^P(x)$;
$R$ = Reward by rating action $A$;
$X^1$ = next state by routing action $A$;
$A^1 = \pi(x^1)$;
$Q_t(x, a) = Q_t(x, a) + \alpha(r + \beta Q_t(x^1, a^1) - Q_t(x, a))$;
$\Pi(x) = \arg\max_{ak} Q_t(x, a_k)$;
Now $x = x^1$;
End for;
```

6. Security Analysis of proposed paper

This scheme is based on PoA block chain method. In this network routing and server nodes jointly maintain transactions. The proposed scheme ensures trustworthy secure routing as:

1. **PoA Consensus method**: The network is based on proof or authority i.e. any change require authentication from more than 50% of server nodes to upload information on block chain network.
2. **Routing Information** Source: In proposed network the node acquire information from block chain network not from neighbours as in traditional networks. So the information is always true and consistent as block chain network cannot be tampered.

3. **No Single Point Attack**: Proposed network is not based on any 3rd trusted party for routing, but authentication from multiple server nodes require, so it prevent single point entry.
4. **No Re-Transmission**: The token contract specifies the routing node address mapped only to one physical address in one time slot, so no transaction can occur in same time slot for the involved nodes.
5. Self- Adaptability: The reward value based on learning is very low for a malicious node. So it will never be selected as next hop, but best hop will be chosen.

7. Conclusion

In this paper, a trusted routing scheme based on the blockchain and reinforcement learning is proposed to provide a trusted routing environment and improve the performance of the routing network. As a decentralized system, the blockchain network provides a feasible scheme for routing information management and a platform for reinforcement learning of routing scheduling. Proposed method will use the blockchain token to represent the routing packets, and each routing transaction is released to the blockchain network through the confirmation of the validator nodes. By making every routing transaction recorder traceable and tamper-proof, routing nodes can obtain dynamic and trusted routing information on the blockchain network. We also describe the detailed reinforcement learning model to adaptively choose the best routing path and avoid the routing links with malicious nodes. The implementation of proposed paper will return best possible results.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin. pdf (accessed on 25 February 2019).
2. Ali, S.; Wang, G.; Bhuiyan, M.Z.A.; Jiang, H. Secure Data Provenance in Cloud-Centric Internet of Things via Blockchain Smart Contracts. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 991–998.
3. Zheng, Z.; Xie, S. Blockchain Challenges and Opportunities: A Survey. Int. J. Web Grid Serv. 2018, 14, 352–375.
4. Pieroni, A.; Scarpato, N.; Di Nunzio, L.; Fallucchi, F.; Raso, M. Smarter city: smart energy grid based on blockchain technology. Int. J. Adv. Sci. Eng. Inf. Technol. 2018, 8, 298–306. [CrossRef]
5. Gómez-Arevalillo, A.D.L.R.; Papadimitratos, P. Blockchain-based public key infrastructure for inter-domain secure routing. In Proceedings of the Internationalpapershop on Open Problems in Network Security (iNetSec), Rome, Italy, 30–31 May 2017; pp. 20–38.
6. Li, J.; Liang, G.; Liu, T. A Novel Multi-link Integrated Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication. KSII Trans. Internet Inf. Syst. 2017, 11.
7. Ramezan, G.; Leung, C. A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts. Wirel. Commun. Mob. Comput. 2018, 2018, 4029591.
8. Angrish, A.; Craver, B.; Hasan, M.; Starly, B. A Case Study for Blockchain in Manufacturing: “FabRec”: A Prototype for Peer-to-Peer Network of Manufacturing Nodes. arXiv 2018, arXiv:1804.01083.
9. Bach, L.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 IEEE 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.
10. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Available online: http://blockchainlab.com/pdf (accessed on 25 February 2019).
11. Boyan, J.A.; Littman, M.L. Packet routing in dynamically changing networks: A reinforcement learning approach. In Proceedings of the 6th International Conference on Neural Information

Processing Systems (NIPS'93), Denver, CO, USA, 29 November–2 December 1994; pp. 671–678.

12. Subramanian, D.; Druschel, P.; Chen, J. Ants and reinforcement learning: A case study in routing in dynamic networks. In Proceedings of the Fifteenth International Joint Conference on Artifical Intelligence (IJCAI'97), Nagoya, Japan, 23–29 August 1997; pp. 832–839.
13. Al-Rawi, H.A.A.; Ming, A.N.; Yau, K.L.A. Application of reinforcement learning to routing in distributed wireless networks: A review. Artif. Intell. Rev. 2015, 43, 381–416.
14. Gupta, Y.; Bhargava, L. Reinforcement Learning based Routing for Cognitive Network on Chip. In Proceedings of the International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4–5 March 2016.
15. Gao, J.; Shen, Y.; Ito, M.; Shiratori, N. Multi-Agent Q-Learning Aided Backpressure Routing Algorithm for Delay Reduction. arXiv 2017, arXiv:1708.06926.
16. Sutton, R.S.; Barto, A.G. Reinforcement Learning: An Introduction; MIT Press: Cambridge, MA, USA, 2018
17. Ren, J.; Yue, S.; Zhang, D.; Zhang, Y.; Cao, J. Joint Channel Assignment and Stochastic Energy Management for RF-Powered OFDMA WSNs. IEEE Trans. Veh. Technol. 2018.
18. Ren, J.; Zhang, Y.; Deng, R.; Zhang, N.; Zhang, D.; Shen, X. Joint channel access and sampling rate control in energy harvesting cognitive radio sensor networks. IEEE Trans. Emerg. Top. Comput. 2016.
19. Zhang, D.; Chen, Z.; Zhou, H.; Chen, L.; Shen, X.S. Energy-balanced cooperative transmission based on relay selection and power control in energy harvesting wireless sensor network. Comput. Netw. 2016, 104, 189–197.
20. Zhang, D.; Chen, Z.; Awad, M.K.; Zhang, N.; Zhou, H.; Shen, X.S. Utility-optimal resource management and allocation algorithm for energy harvesting cognitive radio sensor networks. IEEE J. Sel. Areas Commun. 2016, 34, 3552–3565.
21. Kumar, N.; Singh, Y. Routing protocols in wireless sensor networks. In Handbook of Research on Advanced Wireless Sens