A Survey on Blockchain-Based Routing in Communication Networks

Patikiri Arachchige Don Shehan Nilmantha Wijesekara
Department of Electrical and Information Engineering,
Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka
e-mail: nilmantha@eie.ruh.ac.lk

Article Info

Article history:

Received Feb 13, 2024
Revised Mar 9, 2025
Accepted Mar 19, 2025

Keyword:

Routing
Blockchain
Routing automation
Blockchain-based routing
Smart contracts

ABSTRACT

Routing in communication networks involves the transmission of packets among network nodes by making routing decisions constructed upon diverse protocols that can depend on various metrics. Blockchain systems made up of concatenated blocks inherently preserve the faithfulness, assure the non-deniability, and assure the obscured individuality of their transactions/blocks through the incorporation of distributed unanimity mechanisms and cryptographic techniques. In the present literature, it clearly lacks a review manuscript on the broad scope of blockchain-based routing; thus, we fill that gap by studying Blockchain-based Routing (BBR) under numerous routing techniques, identifying the concept under 5 divisions, and then in-depth scrutinizing the reviewed work based on blockchain-correlated, routing-correlated, and network-correlated characteristics. We collected a premature sample of 83 articles by cherry-picking articles for qualification requirements explored in scientific databases, employing an in-depth and extended quality assessment approach. As per the appraisal, BBR improves the overall routing performance and security through the storage of routing decisions and updates securely, automatic routing with the aid of smart contracts, providing authentication for secure routing, providing reputation-based routing, and blockchain-based onion routing. In-depth scrutinization reveals that 45.5% of BBR frameworks utilize blockchain for storing routing decisions and updates; 93.2% employ linear blockchain architecture; 20.5% employ proof-of-work consensus; 100% dynamic routing; 72.8% decentralized routing; 93.2% single path routing; 86.4% table-based; and 20.5% are designed for IoT networks. Finally, we disclose the possibilities and impediments of the idea of BBR, identify review gaps, and then render proposals to conquer them.

Corresponding Author:

Patikiri Arachchige Don Shehan Nilmantha Wijesekara,
Department of Electrical and Information Engineering,
Faculty of Engineering, University of Ruhuna,
Galle 80000, Sri Lanka
Email: nilmantha@eie.ruh.ac.lk

1. INTRODUCTION

Routing is a fundamental function in networking that involves the forwarding of a packet or a flow from a source equipment to a destination equipment. In multi-path routing, multiple paths are found among the source equipment and the destination equipment, whereas in single-path routing, the best path is found [1]. In sensor networks, data aggregation routing involves data aggregation at intermediate nodes as a means to reduce communication overhead and energy consumption [2]. Routing in modern communication networks is dynamic and can adapt to changing conditions in the network, such as changes in its topology, which has features such as automatic failure handling [3]. For instance, routing in software-defined networking often involves maintaining a flow table consisting of information about available routes (next hop) as a means to reach different destinations, which is computed and installed by the centralized controller [4]. Specifically, in link state routing, shortest path algorithms such as Dijkstra are employed in each router, which maintains a network topology graph [5]. However, static routing is still employed in fixed-wired networks, where network administrators define the routing table of each forwarding element explicitly [6].

A routing decision can be made based on different techniques. Specifically, optimization can be assisted in making routing decisions by minimizing or maximizing network parameters like latency, throughput, etc. under a set of constraints as a means to select optimum paths [7]. Furthermore, distance vector and path vector routing approaches compute a cost metric to reach different destinations and exchange the resulting routing tables with neighbors periodically [8]. Moreover, the routing of flows can be prioritized in sequence and/or in multiple paths based on the quality of service as a means to reach the same destination based on the service requirements [9]. Similarly, artificial intelligence can be employed for analyzing and predicting network traffic to make routing decisions based on the analysis of predictions [10]. There are numerous routing performance evaluation metrics, including packet delivery factor, latency, communication cost, mobility resilience, etc., that can be employed to evaluate the effectiveness of a given routing approach [11]. Additionally, in wireless adhoc and sensor networks, probabilistic routing makes use of probability distributions as a means to make routing decisions [12], such as the prediction of link lifetimes.

A blockchain necessarily consists of a concatenation of blocks connected together in a single-path or multi-path based on the architecture of the peer-to-peer ledger system [13]. Specifically, transactions/blocks are attached in mutual association by a given block/transaction that maintains the hash signature of one or more parent transactions/blocks, making them resistant to change [14]. Precisely, they incorporate a unanimity mechanism, including but not limited to proof-based unanimity or vote-based unanimity, for substantiating the blocks within the group of nodes before a transaction/block is added to the peer-to-peer ledger system [15]. Moreover, they use cryptographic hash functions to assure faithfulness and digital signatures to assure transaction non-deniability [16]. Additionally, they have the potential to blend robust cryptographic techniques, including but not limited to privacy-enhancing proofs and post-quantum cryptography for bolstering security vs. quantum ambushes [17], reinforcing the features of secrecy guaranteeing in blockchain. Although pure blockchain by heredity does not use cryptographic techniques, including but not limited to public key cryptography, for assuring secrecy guaranteeing, it is not totally secrecy guaranteeing given that blockchain transactions are with obscured individuality, meaning that transactions are pinpointed by a cryptographic pseudo address in contrast to the real addresses of users [18]. Besides, the depth of secrecy preservation can be varied based on the peer-to-peer ledger category: non-public, cooperative-networked, and publicly-accessible. A publicly-accessible blockchain is the traditional fully distributed blockchain, whereas non-public and cooperative-networked blockchains have a certain depth of autocratic authority, providing better isolation and access control over data than a publicly accessible blockchain [19].

The concept of blockchain-based routing is a new approach to routing that has revolutionized traditional routing. In this appraisal, we show that blockchain-based routing can be one of 5 types. In the first category, blockchain is employed for secure storage of routing decisions and updates as a means to prevent routing threats, including grey hole, black hole, BGP, etc., scrutinizing the features of high integrity, transparency, and trustworthiness of blockchain (ISRchain, TRAQR, etc.) [20], [21]. Secondly, blockchain has been employed to automate the routing process by employing Smart Contracts (SCs) to implement a conventional routing technique to generate routes. Specifically, in [22], SCs have been employed to provide the topologies of each controller as a means to build a global reputation for crossing-domain routing with multiple controllers in an IoT unmanned aerial vehicle network. Thirdly, blockchain facilitates secure routing by helping to provide robust authentication. Specifically, blockchain based authentication attempts to prevent malicious nodes from engaging in routing through proper node registration with or without the aid of a certificate authority [23]. Forthly, blockchain is employed for reputation/trust-based routing that employs reputation-based mechanisms for improving routing reliability by calculating trust values of nodes based on their behavior using consensus approaches, where blockchain can further facilitate providing alarms after detecting malicious nodes based on reputation scores calculated [24]. The final category of blockchain-based routing is blockchain-based onion routing, where a token-based approach is employed for securing privacy and anonymity in routing with the aid of encryption and validation processes [25].

Let's now contrast this survey with previous ones. In the midst of composing this appraisal, as far as we know, there is only one review paper reviewing specifically secure inter-domain routing using a broader gateway protocol with the aid of blockchain [26]. The preceding work only focuses on inter-domain routing and does not identify blockchain routing aspects in a broader scope. Thus, the absence of a review manuscript is evident in the broader scope of blockchain-based routing in communication networks so far. Therefore, this paper addresses that gap by studying blockchain-based routing under numerous routing techniques, identifying blockchain-based routing categories in high-level (5-fold concepts reviewed above), analyzing the reviewed work using blockchain and routing-specific attributes, and finally providing proposals for identified impediments.

Figure 1 displays the content outline of this investigation.

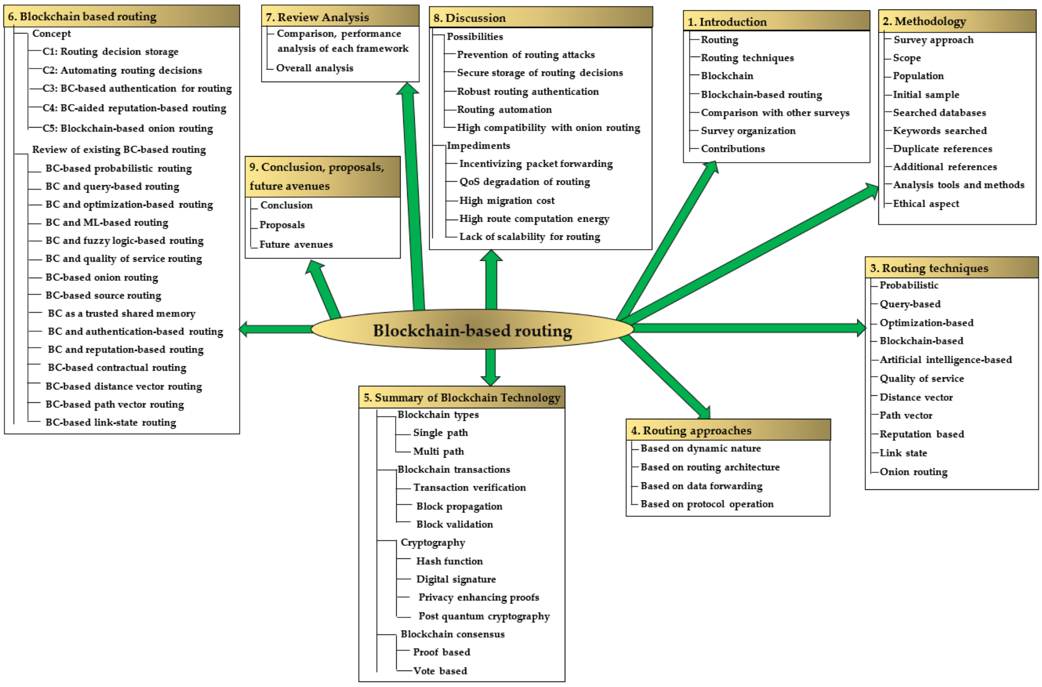

Blockchain-based routing
1. Introduction
Routing
Routing techniques
Blockchain
Blockchain-based routing
Comparison with other surveys
Survey organization
Contributions
2. Methodology
Survey approach
Scope
Population
Initial sample
Searched databases
Keywords searched
Duplicate references
Additional references
Analysis tools and methods
Ethical aspect
3. Routing techniques
Probabilistic
Query-based
Optimization-based
Blockchain-based
Artificial intelligence-based
Quality of service
Distance vector
Path vector
Reputation based
Link state
Onion routing
4. Routing approaches
Based on dynamic nature
Based on routing architecture
Based on data forwarding
Based on protocol operation
5. Summary of Blockchain Technology
Blockchain types
Single path
Multi path
Blockchain transactions
Transaction verification
Block propagation
Block validation
Cryptography
Hash function
Digital signature
Privacy enhancing proofs
Post quantum cryptography
Blockchain consensus
Proof based
Vote based
6. Blockchain based routing
Concept
C1: Routing decision storage
C2: Automating routing decisions
C3: BC-based authentication for routing
C4: BC-aided reputation-based routing
C5: Blockchain-based onion routing
Review of existing BC-based routing
BC-based probabilistic routing
BC and query-based routing
BC and optimization-based routing
BC and ML-based routing
BC and fuzzy logic-based routing
BC and quality of service routing
BC-based onion routing
BC-based source routing
BC as a trusted shared memory
BC and authentication-based routing
BC and reputation-based routing
BC-based contractual routing
BC-based distance vector routing
BC-based path vector routing
BC-based link-state routing
7. Review Analysis
Comparison, performance analysis of each framework
Overall analysis
8. Discussion
Possibilities
Prevention of routing attacks
Secure storage of routing decisions
Robust routing authentication
Routing automation
High compatibility with onion routing
Impediments
Incentivizing packet forwarding
QoS degradation of routing
High migration cost
High route computation energy
Lack of scalability for routing
9. Conclusion, proposals, future avenues
Conclusion
Proposals
Future avenues

Figure 1. Content outline of investigation on blockchain-based routing.

1.1. Contributions to already existing literature

- We labelled and briefly described a summary of different routing techniques (Section 3).
- Routing approaches in telecom networks are briefly described (Section 4).
- A summary of the blockchain system is showcased (Section 5).
- Appraise already existing blockchain-based routing frameworks in telecom networks (Section 6).
- Scrutinize meticulously on the appraised blockchain-based routing frameworks (Section 7).
- The possibilities and impediments of blockchain-based routing are communicated (Section 8).
- Proposals and future avenues for employing blockchain-based routing are showcased (Section 9).

2. METHODOLOGY

We performed a systematic literature review in order to search for solutions to two research questions: Q1: "What are the existing blockchain-based routing frameworks?" and Q2: "What are the trends, strengths, weaknesses, gaps, and future directions of blockchain-based routing in communication networks?". Specifically, we utilized a mixed-method quality assessment approach with narrative synthesis.

This appraisal probes into the current research on blockchain-based routing in communication networks circulated within the academic realm over the sweep of time, operating with an in-depth and extended practice [27]. Precisely, it explores numerous aspects of routing and peer-to-peer ledger schemes. Hence, all primary investigative studies and website content disseminated to the research community on routing, blockchain-based routing, and blockchain comprise the total population in the present work's scope. However, total population references are laborious to review in the present work. Therefore, by operating with complying keywords and qualification requirements, we stockpiled 86 references from investigative studies and website content.

We explored Google Scholar academic search engine, IEEE Xplore electrical engineering repository, ScienceDirect scientific database, ACM internet library, Wiley internet library, and MDPI information lookup engine. The keywords we commonly employed were "Routing" OR "Blockchain-based probabilistic routing" OR "Blockchain-based query-based routing" OR "Blockchain- and optimization-based routing" OR "Blockchain and machine learning-based routing" OR "Blockchain and fuzzy logic based routing" OR "blockchain-based quality of service routing" OR "blockchain-based onion routing" OR "Blockchain-based source routing" OR "Blockchain trusted shared memory routing" OR "Blockchain and authentication-based routing" OR "Blockchain-based secure routing" OR "Blockchain-based contractual routing" OR "Blockchain-based distance vector routing" OR "Blockchain-based path vector routing" OR "Blockchain based link state routing" OR "Blockchain".

Various elements for cherry-picking the articles composed the qualification requirements. The first qualification requirement states that the citing article must be composed in English, and after that, it necessitates high relevancy to the keyword. After that, with a view to improving the reliability of the conducted appraisal, scholarly journals were given precedence by way of contrast with conference proceedings and initial research papers. However, we weren't biased against academic articles by a dedicated publishing agent inside the qualification requirements; instead, we viewed all publishers identically. The last qualification requirement defines that a dedicated citing article must be released in the interim period of years from 1980 up to 2023.

The premature sample was reduced to 83 citing articles as a result of the finding that 3 citing articles were mirrors. Precisely, we cited notations and explanations appertaining to the diverse subjects discussed in this appraisal using 25 citing articles. To contrast this appraisal with precedent appraisals, we subsequently included 1 extended appraisal article in the selection of writings, acquiring the complete quantity of citing articles to 109.

Owing to the low size of the study, we used manual forms to extract information from the articles by reading them manually. The method utilized in this review is qualitative synthesis and does not involve any meta-analysis; therefore, there was no requirement to use PRISMA that demands multiple reviewers and extensive documentation, which does not align well with the utilized study method.

To scrutinize present blockchain-based routing in communication networks belonging to various elements, including but not limited to blockchain characteristics, routing characteristics, network characteristics, and capabilities, we operated the spreadsheet data structure for the appraisal’s qualitative review. Precisely, we generated charts operating with the MS data analysis tool to impartially scrutinize appraisal data correlated with routing-based and blockchain-based elements.

Ethics are unconnected, as this appraisal is associated with network routing.

3. A SUMMARY OF DIFFERENT TYPES OF ROUTING TECHNIQUES

Routing in communication networking involves sending a packet or a collection of packets (flow) from a given source equipment to a destination equipment, either using a single path or multiple paths. The single-path multi-hop routing concept, where a flow is routed from source equipment A to destination equipment G through a set of intermediate equipment, is pictorially displayed in Figure 2.

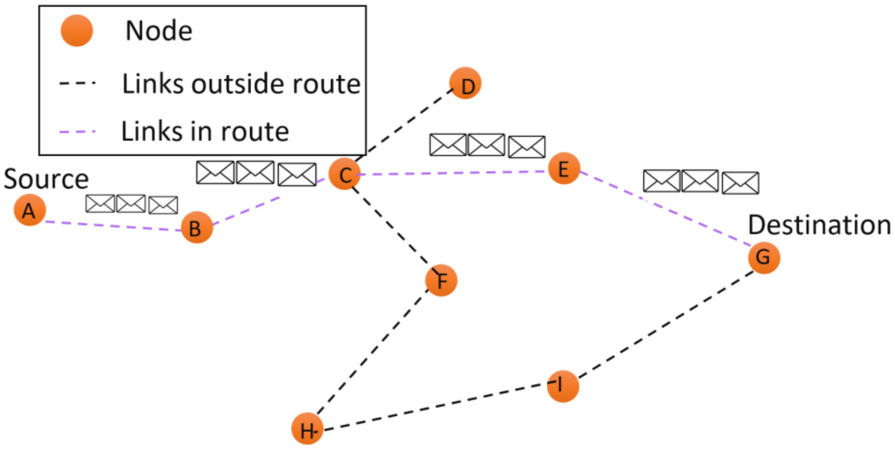


Figure 2. Single path routing concept.

Different types of routing techniques are reviewed in the following subsections. Note that a given routing framework can be designed using a combination of two or more of the following techniques.

3.1. Probabilistic routing

In probabilistic routing, randomization and probability are employed to make routing decisions. This is typically employed in wireless adhoc networks and sensor networks, where nodes may randomly select a neighboring node to forward a packet relying upon a probability distribution. For delay-tolerant networks, a low-latency and high packet delivery ratio scheduling probabilistic routing protocol using encounter history and transitivity has been employed in internet of things networks to improve storage and transmission performance [28]. Similarly, another probabilistic routing algorithm uses the limiting number of replications using the record of encounters to project the meeting probabilities between two pieces of equipment with low replications, reducing the communication overhead [29]. Thus, this technique does not have fixed routes and can be helpful in networks with dynamic network topologies, such as vehicular adhoc networks [30].

3.2. Query-based routing

In query-based routing typically implemented in wireless adhoc networks, sink nodes use queries to communicate with neighbors (the region of interest) and gather data from neighboring nodes. Two approaches for query-based routing are directed diffusion and Sensor Protocol for Information via Negotiation (SPIN). Directed diffusion focuses on data itself rather than addresses, where nodes express interest in data by broadcasting interest packets, which are propagated through the network based on gradient, and data is sent through the reverse path of the interest packets. However, directed diffusion can expose sensitive information if relay nodes are unreliable. For the sake of solving those problems, an energy trust model that assesses the residual energy and faith of nodes for secure directed diffusion routing for transmitting confidential data using a credible communication path has been studied in [1]. In SPIN, nodes send queries to neighboring nodes, and node respond if they have the information requested. Similar to SPIN, QWRP is a query-based routing approach with a virtual wheel to limit the broadcasting of the location of the sink nodes and has an angle-based forwarding approach to enhance information delivery [31].

3.3. Optimization-based routing

Optimization-based routing attempts to find the optimum routing by minimizing or maximizing certain network parameters like latency, throughput, packet delivery ratio, etc. under given constraints. Common optimization tactics include linear programming, non-linear programming, particle swarm optimization, genetic algorithms, etc. Ant colony optimization has been employed to select optimal routes between the cluster head and base station in a clustering-based routing approach by considering distance, residual energy, and node degree, where butterfly optimization is used for cluster head selection [32]. Moreover, some have used routes obtained from an adhoc OnDemand multipath distance vector protocol to optimize using a genetic algorithm with a fitness function that implements the shortest path, maximum residual energy, and low traffic under random packet losses [33].

3.4. Blockchain-based secure routing

Blockchain-based routing involves employing blockchain to improve trustworthiness, integrity, and transparency in routing decisions. We discuss the blockchain-based routing concept and existing frameworks in detail in Section 5.

3.5. Artificial intelligence-based routing

Artificial intelligence-based routing techniques use either machine learning or fuzzy logic to make routing decisions by analyzing and generating knowledge regarding network traffic, conditions, historical data, etc. to predict future trends or knowledge on the present network to make routing decisions based on that knowledge. These techniques can adapt to changing network conditions, patterns, or anomalies that traditional algorithms may not be able to detect. Likewise, fuzzy logic has been employed to identify the weight of the strategy of order selection by resemblance to the optimal solution algorithm in an intelligent multi-attribute routing approach as a means to find the next hop for packet forwarding in a two-layered software-defined vehicular network [34]. In [35], machine learning has been employed to detect network contention, predict wireless link lifetime and link delay, and decide the mode of a hybrid routing approach that forwards packets using high-stability links, either using a shortest path or least delay approach.

3.6. Quality of service routing

In quality-of-service routing, data packet forwarding is prioritized and chosen by employing quality-of-service parameters like bandwidth, latency, jitter, reliability, etc. Specifically, low-latency paths for video data traffic and high-bandwidth paths for data traffic may be selected. QROUTE is an efficient quality-of-service-aware routing scheme that has low route computation time in the controller of a software-defined overlay network that employs quality-of-service metric-based forwarding in the data plane [9]. Likewise, a multipath routing protocol finds an optimum path and alternative paths between a given source equipment and destination equipment in a cognitive adhoc network employing various routing metrics to choose quality of service paths with higher stability [36].

3.7. Distance Vector Routing (DVR)

In DVR, each router manages a routing table that stores the distance metric (cost) to reach different destinations in the network. These routing tables are exchanged among the neighbors periodically to update the routing information. DVOR is a distance vector-based exploitative routing approach that uses a query method to compute distance vectors for underwater acoustic nodes, where packets are forwarded based on distance vectors, which has avoided the issues of void area and long detour [8]. FD-AOMDV is a fault-tolerant multipath AODV routing protocol that has a lower delay for path sprinting and finds path disjoints in such a manner that routing overloads are significantly decreased [37].

3.8. Path Vector Routing (PVR)

PVR maintains a vector of autonomous system numbers that a route has traversed, preventing routing loops in determining a path from source to destination. Broader Gateway Protocol (BGP) is a PVR strategy that facilitates network administrators to define policies. Symmetric cryptography has been employed to protect paths from alteration in a routing framework that utilizes BGP [38]. Some have used a snapshot of the network topology to compute routing paths using BGP for an autonomous system without using the complex message passing employed in conventional BGP, which has been effective in reducing the computation workload [39].

3.9. Reputation-based routing

Reputation-based routing is employed in peer-to-peer networks such as blockchain and considers the reputation of routing paths when making routing decisions. A reputation score is calculated for each piece of equipment based on its historical performance, reliability, etc. and is employed to assess the trustworthiness of the node. This approach can reduce the addition of malicious nodes to routing paths, improving routing security. In [40], node activity such as packet forwarding, activity changes, etc. is monitored to estimate a trust and reputation score to be employed in a quality of service-aware routing scheme. Likewise, in another reputation-based routing scheme, each piece of equipment assigns a reputation score for other equipment in the network, and reputation scores are employed in finding better routing paths as a means to minimize packet loss rates, which has been effective in the company of selfish nodes [41].

3.10. Link State Routing (LSR)

In LSR, each router in the network sustains a database of the network topology and is employed to compute the shortest path to reach destinations using algorithms such as the Dijkstra shortest path algorithm. This approach is adaptive to dynamic network topology changes; however, it is resource intensive and less scalable [42]. In optimized link state routing, multipoint relays broadcast messages through the duration of the flooding procedure to generate link state information and minimize flooded control messages, where partial link state information is released by multipoint relays reporting links between themselves and selectors, and routes are computed using link state information [5]. Multipath-optimized LSR uses the multipath Dijkstra algorithm to search numerous paths, and link metrics and cost functions are used for route computation with additional route recovery and loop detection techniques [43].

3.11. Onion routing

Onion routing is a privacy-preserving routing approach where the routing traffic is anonymized by encrypting it in multiple layers such that intermediate nodes can decrypt one layer and are aware of the previous and next nodes in the route. Thus, this approach hides the source and destination of routing to improve anonymity. However, this approach is complex and can cause high latency. Location-based dynamic relay groups are formed to act as cryptographic relays satisfying anonymity requirements using pseudo-IDs for onion routing in vehicular adhoc networks [44]. Recently, the reply mechanism of onion routing has been secured using updatable encryption and non-interactive arguments to authenticate payloads and has been effective against reply manipulation in onion routing [45].

Table 1 displays a summary of existing literature on different routing techniques.

Table 1. A summary of existing literature on different routing techniques.

Routing technique	Framework	Methodology	Performance
Probabilistic	Delay tolerant routing [28]	Encounter history and transitivity	Low latency and high packet delivery ratio
	Limited replication routing [29]	Probability prediction by history of encounters	Reduced communication overhead due to low replicas
Query-based	Diffusion routing (SPIN) [1]	Energy trust model for trust nodes energy assessment	Secure routing
	QWRP [31]	Virtual wheel with limited broadcasting	Energy consumption reduction with good data delivery

Routing technique	Framework	Methodology	Performance
Optimization-based	Cluster-based routing [32]	Butterfly and ant-colony optimization	High energy efficiency with higher alive nodes
	Multipath AODV routing [33]	Genetic algorithm	Maximize residual energy under packet losses
Artificial intelligence	Hybrid routing [35]	Deep learning to predict link lifetime and delay	Low latency, cost and high PDR with respect to Dijkstra, AODV
	Multi-attribute routing [34]	Fuzzy logic with TOPSIS algorithm	Improved PDR, reduced latency in urban environments
Quality of service	QROUTE [9]	QoS based forwarding	Low route computation time in control plane
	Multipath QoS routing [36]	Routing metrics to select stable QoS paths	Low packet drop probability, high throughput
Distance vector	DVOR [8]	Use query mechanism to computed distance vectors	Good packet delivery ratio, energy efficiency
	FD-AOMDV [37]	Finds disjoint multipaths	Reduced routing overloads and latency
Path vector	SPV for BGP [38]	Symmetric cryptography to secure paths	22 times faster than S-BGP
	BGP [39]	Avoids complex message passing	Acceptable running time with correct routing
Reputation-based	QoS routing [40]	Node activity-based reputation	20% high throughput, 10% low overhead, delay
	Source routing [41]	Assign and find paths using reputation score	Minimize packet losses under effects of selfish nodes
Link state	Optimized link state routing [5]	Uses multipoint relays, flooding, & link state info	Effective in large and dense adhoc networks
	Multipath OLSR [43]	Uses multipath Dijkstra, link and cost metrics	Suitable for large, mobile, dense networks
Onion	Anonymous location-based routing [44]	Pseudo IDs using cryptographic relays	Better PDR, latency, and number of transmissions
	Onion routing with replies [45]	Updatable encryption and non-interactive arguments	Effective against reply manipulation

4. A SUMMARY OF DIFFERENT ROUTING APPROACHES

A given routing technique will belong to an approach related to each of the routing classifications listed below.

- Classification based on dynamic nature
- Classification based on network architecture
- Classification based on data forwarding
- Classification based on protocol operation

Each of these routing classifications and approaches belonging to each classification will be briefly discussed in the following sub-sections.

4.1. Routing approaches based on dynamic nature

4.1.1. Static routing

In static routing, the network managers manually set up the routing table for every piece of network equipment in the network. This approach is employed in fixed-wired networks that have a fixed network topology, as it does not involve automatic adaptation to changes in the network environment using routing protocols. A comparison of static and dynamic routing for satellite networks has shown that static routing has performed better regarding newly started call blocking, having longer in-progress call probabilities since the pre-calculated routing table in static routing is less vulnerable to abrupt topological changes [6].

4.1.2. Dynamic routing

This approach involves routing protocols that adapt to the dynamic network topology to update routes as the network topology changes. This also facilitates automatic failover handling by rerouting traffic when existing routers fail. Even though this approach is scalable, the communication overhead is high and less predictable. Most of the modern routing techniques in dynamic networks are dynamic in nature. Specifically, in intelligent transportation systems, dynamic routing using k-means for clustering as a means to exchange routing information among clusters, including an ant colony optimization for obtaining paths for multimedia access, has been feasible [3].

4.2. Routing approaches based on routing architecture

4.2.1. Centralized routing

In centralized routing, a centralized controller is responsible for computing routes by using the network statistics collected and distributing the packet forwarding rules to the routers. As an example, in [46], a centralized routing approach in software-defined networking, considering QoS parameters and prioritizing flows, has achieved a better balance in channel resource load.

4.2.2. Distributed routing

In distributed routing, the end nodes of the network exchange information related to routing as a means to derive packet forwarding rules without the involvement of a centralized entity. This involves both multi-hop routing that typically exists in ordinary networks and single-hop transmissions that typically exist in underwater networks [47]. Distributed routing approaches are often employed in mobile adhoc networks and wireless sensor networks. In [48], a fuzzy logic-driven, energy-efficient reactive protocol is employed to select the most trusted nodes that can be employed as a metric for distributed routing using an adhoc on-demand distance vector in a mobile adhoc network to improve the network lifetime.

4.2.3. Hierarchical routing

In hierarchical routing, there is a hierarchy of controllers responsible for routing packets in nodes under each one's domain. The regional controllers lie at the base of the hierarchy and are responsible for making routing optimizations in their domain, and at the top of the hierarchy, there is a centralized authority. A hierarchical network architecture with inter-autonomous system routing and quality of service, which has a main controller acting as a broker and maintaining a global network view with a hierarchy of controllers, has been proposed in [49].

Centralized, distributed, and hierarchical routing concepts are pictorially displayed in Figure 3.

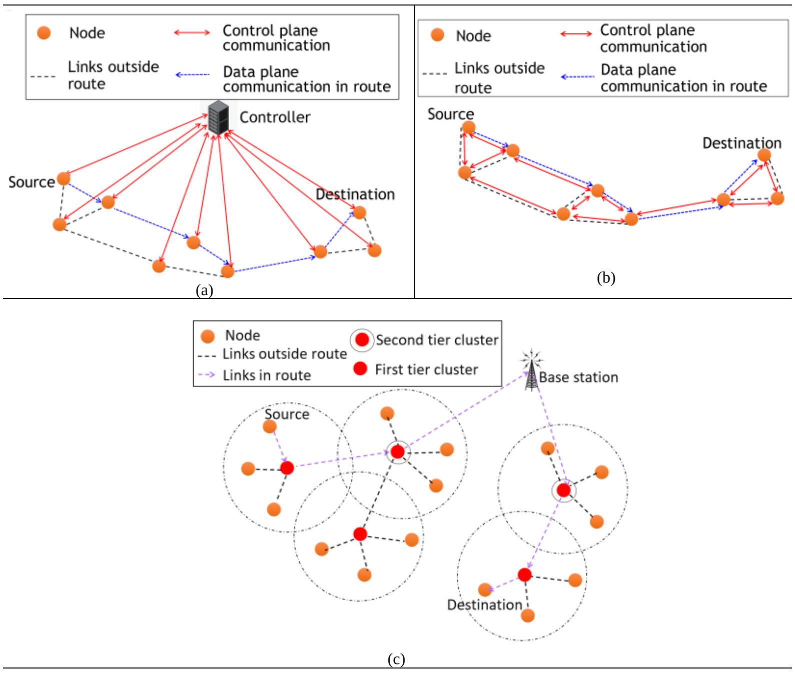


Figure 3. Routing architectures (a) Centralized (b) Distributed (c) Hierarchical.

4.3. Routing approaches based on data forwarding

4.3.1. Single-Path Routing (SPR)

SPR involves finding a single path from a given source to a destination based on a routing protocol or by manual configuration. This approach has limited adaptability due to failure or resource constrainment, such as high congestion in a given path, which can limit the network's performance. Moreover, this approach is poor in load balancing compared to that of multi-path routing (under a high number of multipaths) [50].

4.3.2. Multi-path routing

In MPR, numerous paths are found between the source and the destination using routing protocols. Thus, multi-path routing offers load balancing by distributing network traffic across multiple paths, balancing the workload of the network nodes. Moreover, redundancy and fault tolerance are higher in this approach than in single-path routing. A topology change-aware multipath AODV routing protocol that can adapt to node mobility while supporting quality of service employs a stable path selection algorithm considering node resources and link stability probability predictions [51]. Furthermore, multipath routing has been feasible considering environment and residual energy, where routes are selected by having the best trade-off among energy conservation, latency, and survivability, avoiding routing through danger zones [52].

4.4. Routing approaches based on protocol operation

4.4.1. Source routing

Source routing is an approach where the source equipment determines the complete routing path that the packet should travel from the source equipment to the destination equipment without relying on intermediate equipment. However, the approach should reduce mathematical computations since they can contribute to unnecessary depletion of energy [53]. This approach has fine grained control over the routing path, and the source node has high responsibility. Dynamic source routing is composed of route discovery and maintenance for required destinations of the network, ensuring routing is loop-free and does not require routing information in the intermediate nodes that operate in an on-demand manner, allowing routing packet overhead to scale automatically [54]. Work in [55] uses the information on residual power of network nodes and transmission power dissipation for control and data channel transmissions to implement a power-aware source routing protocol that has been effective in improving network lifetime.

4.4.2. Table-based

In table-based routing, a routing table is sustained at each piece of network equipment, containing all information about available routes with corresponding cost metrics to reach different destinations. Note that these routing tables are constructed using routing protocols. Upon the reception of a packet by a router, the packet header will be inspected and searched in the routing table for a match with the destination address. Upon finding a match, the packet will be forwarded through the corresponding port to the next hop found in the matched entry. Work in [56] proposes to use a backup routing table for the adhoc on-demand distance vector routing protocol using a multi-criteria decision-making technique storing alternative routes for the indirect peers, considering hop count, bandwidth, and remaining energy as decision criteria. Moreover, in software-defined networking, the OpenFlow protocol is employed to update the flow tables in switches using an adaptive or proactive approach, once flow rules are formulated using a routing technique [57].

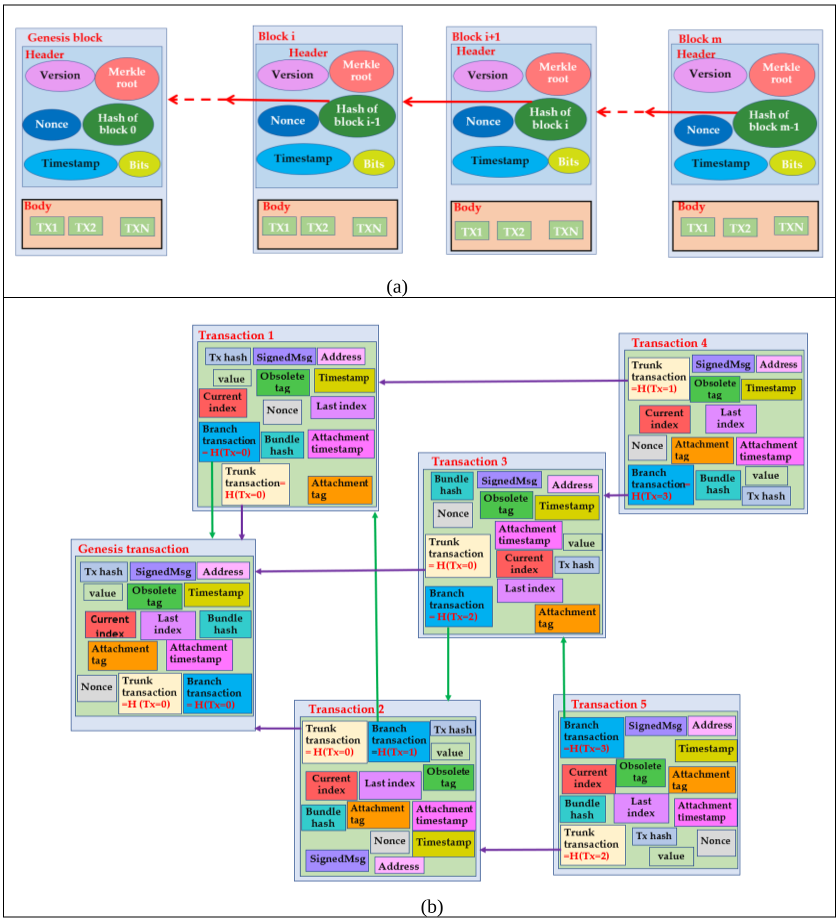
4.4.3. Data aggregation

Data aggregation routing is often employed in sensor networks where data from multiple sources having the same destination is aggregated in an intermediate node before transmitting to the destination to reduce communication overhead and conserve energy. Q-learning has been employed to maximize rewards defined in terms of sensor-type-depending data aggregation, energy for communication, and remaining energy as a means to obtain the routing path in an energy-efficient, data aggregation-conscious routing algorithm [58]. Secure data aggregation is performed using principal component analysis, and a source location privacy-preserving randomized routing technique is employed for routing in a clustering-based wireless sensor network clustered using fuzzy rules [59].

Table 2 displays a summary of existing literature on different routing approaches.

Table 2. A summary of existing literature on different routing approaches.

Routing approach	Framework	Specific methodology	Performance
Static	Static routing [6]	Static configuration	Good performance in newly initiated call blocking
Dynamic	Optimized dynamic routing [3]	K-means clustering, ant-colony optimization	Good computation time, efficiency, delay
Centralized	QoS routing [46]	Prioritize flows based on QoS	Better balance in channel resource load
Distributed	Trusted distributed routing [48]	AODV, fuzzy logic reactive protocol for trust	Stable and secure routing with low false positive rate
Hierarchical	Inter-AS QoS [49]	Inter-autonomous system routing with QoS	50% less traffic than non-hierarchy architecture
Single-path	Load balancing [50]	Evaluate load balancing under different K-values	Load balancing is comparable to that of multi-path
Multi-path	On-demand-multipath QoS [51]	Multipath AODV with link stability prediction	Good QoS metrics under any speed
	Environment fusion [52]	Consider environment and residual energy	Sustainable message sending in drastic environments
Source	Dynamic source routing [54]	On-demand route discovery and maintenance	Low routing overhead even under high mobility
	Power-aware source [55]	Control transmission power based on residual energy	High network lifetime
Table-based	EABRT-TOPSIS [56]	Backup routing table for AODV	Good performance metrics than AODV, AOMDV
	Link stability-based routing [57]	Flow table update using stable routing	Has better packet delivery rate than Dijkstra
Data aggregation	Energy efficient routing [58]	Q-learning with energy efficient data aggregation	Improves wireless network lifetime
	ASLPP-RR [59]	Clustering, aggregation-based routing using fuzzy rules	Low packet loss rate, high residual energy



(a)

(b)

Figure 4. Two types of blockchain architectures. (a) Linear (single-path) blockchain. (b) Graph (multi-path) blockchain.

5. A SUMMARY OF BLOCKCHAIN SYSTEM

A concatenation of connected blocks or transactions consists of the peer-to-peer ledger acknowledged as a blockchain.

5.1. Architecture

Every unique block within a linear (single-path) blockchain, which consists of a header element and body element, is connected to its previous block (unless the genesis block) employing the previous block's hash signature, and the transactions within a body element are broken down into a Merkle tree layout [15].

A graph (multi-path) blockchain is consisting of a concatenation of connected transactions, where one transaction can certify the validity of numerous other prevailing transactions. These transactions don't contain header elements and body elements; therefore, Merkle trees are not employed [14].

These two types of blockchains are pictorially displayed in Figure 4.

5.2. Transactions

A utilizer is capable of launching a blockchain transaction, which is after that communicated to the group of nodes within the network and encoded employing the sender's privileged key. An unanimity operation will fire up once each utilizer employs the accessible key to substantiate the transaction. Block validators frequently involve consensus/unanimity by adding the transaction at the core of a block, which is after that communicated around the peer-to-peer network and participated in by each utilizer in the P2P ledger network after block substantiation [60].

5.3. Consensus/Unanimity

Blockchain consensus employs widespread agreement to make and substantiate the latest blocks, assuring the faithfulness of the peer-to-peer ledger system.

In vote-based unanimity, concerning information is dispatched and obtained within the presence of the group of nodes as they work in harmony to substantiate blocks. The most popular vote-based unanimity process employs byzantine fault-resistance unanimity, wherein a leader adds transactions at the core of a block, communicates it, and utilizers recommunicate it to substantiate the block given via the parent, which is indistinguishable as different [18]. Supposing each utilizer got indistinguishable replicas of the latest block via over a majority (2/3) of the network's utilizers, the block is anticipated to be added to the peer-to-peer ledger.

Proof-based unanimity requires utilizers to furnish compelling testimony in view of reason that they are anticipated to be recompensed for adding the latest block to the peer-to-peer ledger. The most trendy proof-based unanimity process is termed proof-of-work, entailing a utilizer to deplete energy by resolving a complicated concern for the sake of assuring its reliability [60].

5.4. Cryptography

To assure the faithfulness of transactions in a peer-to-peer ledger, a hash function is employed to furnish a preset-size hash signature with sparse collisions of signatures [61]. Employing a digital signature, public key cryptography possesses a concealed and revealed key duo and is employed to substantiate transactions. For the sake of reinforcing the secrecy of immutable data, it could additionally be employed to cryptograph blockchain transactions [62].

Privacy-enhancing proofs are employed to substantiate transactions' accuracy by covertly protecting the identities of transactions, reinforcing secrecy, and prohibiting the communication of non-public material [63]. Post-quantum cryptography employs efficient cryptographic processes that are protected from ambushes from quantum data engines, including but not limited to Kyber, SIKE, and similar things [17].

6. BLOCKCHAIN-BASED ROUTING

6.1. Concept

Derived from this study, the blockchain-based routing concept can be divided into the subsequent 5 divisions.

- C1 -- Storage of routing decisions and updates securely in blockchain with high integrity, transparency, and faithfulness, improving these features in routing and preventing routing attacks.
- C2 -- Automating routing decisions by implementing routing techniques using blockchain with/without SCs to generate routes using a routing technique.
- C3 -- Employing blockchain for authentication for secure routing.
- C4 – Blockchain-aided reputation-based routing.
- C5 -- Blockchain-based onion routing.

This identified blockchain-based routing concept can be pictorially displayed using Figure 5.

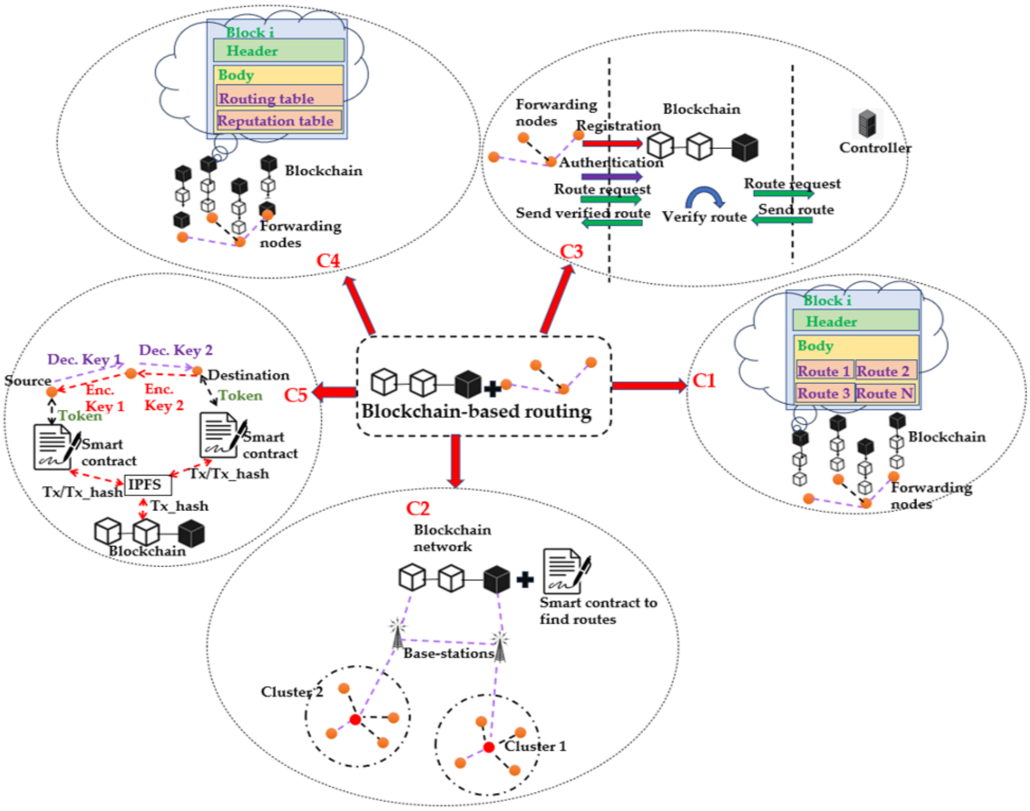


Figure 5. High-level blockchain-based routing concept.

6.2. Review of Current Blockchain-based routing frameworks

6.2.1. Blockchain-based probabilistic routing

For an IoT network, a secure probabilistic routing protocol is presented by predicting the delivery of messages using a probabilistic approach and leveraging blockchain for the security and privacy of routing [64]. This single-path and dynamic routing scheme has outperformed traditional routing techniques like PRoPHET and epidemic routing.

6.2.2. Blockchain and query-based routing

ISRchain is a routing framework for secure routing between inter-domains where the routes stored in the blockchain are verified using SCs with a path validation algorithm by querying for routing using Broader Gateway Protocol (BGP) [20]. ISRchain has deployed RAFT consensus in a consortium blockchain and has resulted in efficient route verification for interdomain routing in the case studies of the BHARTI Airtel prefix hijack and Google route leak. Similarly, DRRS-BC is a decentralized network route registration system using blockchain where the routes are authenticated, and BGP routers can query the ownership routes by querying the blockchain [65]. In DRRS-BC, SBFT consensus is deployed, and it solves identity and behavior authentication and also has been shown to be resistant against prefix and subprefix hijacking attacks, satisfying the security demands of route registration.

6.2.3. Blockchain and optimization-based routing

A blockchain-based framework utilizes blockchain for lightweight authentication and to store a list of malicious nodes to aid in route correction after routes are computed using a genetic algorithm in a software-defined IoT network [66]. In the study [66], a graph blockchain is deployed so that it has resulted in lower gas consumption, and it results in optimized route calculations shown by the residual energy of the network. For joined tasks of dynamic routing and spectrum allocation, integer linear programming has been employed to reduce spectrum utilization where a heuristic algorithm of the blockchain is employed to select the largest load for spectrum allocation [67]. This decentralized and dynamic routing scheme has resulted in a 99.7% spectrum utilization rate with a bandwidth blocking rate of zero, as the proposed system is designed to reduce spectrum usage. Particle swarm optimization has been proposed to perform priority-based routing while utilizing blockchain for assessing the sensitivity level of the encrypted packets, which has resulted in better routing QoS parameters [68]. In the study [68], zone-based authentication with BLAKE-3 hashing, guard nodes, and environment-aware clustering with deep reinforcement learning are utilized in a mobile ad hoc network for secure priority-driven routing, and it has used a zone-based blockchain consensus scheme. Similarly, in [69], a modified version of particle swarm optimization is employed to select optimum paths for routing while blockchain is integrated to ensure secure communication among the unmanned aerial vehicles. In the study [69], it has outperformed the GNSS path selection approach in terms of average channel path loss under insecure scenarios. On the other hand, improved bee colony optimization has been employed to select cluster heads by considering multiple constraints in flying ad hoc networks, such as energy, blockchain transactions, etc., which uses a proof-of-witness-based blockchain consensus approach for mining using the cluster head, which is also responsible for routing packets in the network [70]. This routing approach is hierarchical and uses an optimal cluster head for mining, and it has resulted in a 90% packet delivery ratio, low latency, resistance against 51% attacks, and high throughput.

6.2.4. Blockchain and machine learning-based routing

Reinforcement learning has been employed to select trusted and efficient nodes from a given network dynamically, while blockchain is employed to store routing information in an immutable manner [71]. This scheme has good performance in terms of delay, even in a network that has half of the nodes as malicious nodes in a sensor network. A routing framework known as ENIR in an edge network of an IoT uses Deep Reinforcement Learning (DRL) to learn knowledge from the network based on network demands and conditions for routing optimization, in which blockchain is employed for secure sharing of routing optimizations and knowledge [72]. In ENIR, decentralized routing in the IoT network has resulted in better link utilization and transmission delay. Another work proposes to use off-chain routing in a blockchain-based IoT network that leverages DRL to learn a routing policy as a means to maximize transaction efficiencies [73]. In this off-chain routing technique in IoT, only 1/10th of resources are needed in comparison to the original teacher model. Proof of authority consensus is employed to authenticate transmissions, while a deep neural network selects groups for proofing, prioritizing the characteristics of each node, and the Markov decision process is leveraged to select the next hop for routing to effectively forward packets in the presence of malicious nodes in the study [74]. In this framework, a consortium blockchain is deployed in a wireless sensor network and has resulted in a better routing performance under a scenario in which the majority of nodes are malicious. In decentralized military sensor networks, a generative adversarial network is employed for intrusion detection by monitoring routing transactions, while blockchain is integrated to ensure the trustworthiness of data forwarded in routing by authenticating and validating the routing [75]. They have utilized a custom consensus approach in a public blockchain, and it has resulted in secure routing.

6.2.5. Blockchain and fuzzy logic-based routing

Fuzzy logic has been employed to compute the quality of the neighbor nodes in an energy-efficient routing framework that leverages blockchain to reduce identical data transfers and use load parameters, such as transmission count, remaining energy, etc., when computing routes for inter-cluster routing [76]. This framework has been validated in an industrial IoT network and has resulted in improved network lifetime and a high packet delivery ratio.

6.2.6. Blockchain-based quality of service routing

A proof-of-work-based and side-chain-based blockchain is proposed to improve the security of routing in SDNs, while Q learning has been employed to optimize blockchain parameters to maintain routing QoS parameters like delay, energy consumption, and throughput in a VANET [21]. Thus, the study [21] has resulted in high throughput and reduced attacks by 99% in an SDVN. TRAQR is a framework that utilizes the Ethereum blockchain and SCs to store and transmit different trust information in a multi-domain SDN to make sure that QoS parameters are satisfied in routing [77]. In TRAQR, it ensures that QoS compliance is achieved in an untrusted environment. QoSChain is a QoS-based routing framework that integrates SDN with blockchain to provide QoS between autonomous systems, which masks confidential information while minimizing messages processed by the controllers [78]. QoSChain utilizes proof of authority consensus for multipath routing.

6.2.7. Blockchain-based onion routing

A blockchain- and token-based approach has been employed in an internet of military vehicle networks to secure anonymity and privacy known as B-IoMV by anonymous device-to-device communication using onion routing [79]. In B-IoMV, the decentralized routing approach has resulted in better latency and network bandwidth utilization. In [25], long-short-term memory is employed to detect harmful messages, and non-harmful messages are forwarded using onion routing associated with blockchain by using tokens and time-to-live fields to validate the messages, which has shown better performance than conventional onion routing in industrial internet of things networks. A similar work uses artificial intelligence and onion routing in an internet of underwater vehicle network, where encrypted data is routed using onion routing with the aid of encryption and validated by tokens utilizing blockchain [80]. This routing scheme has resulted in good accuracy, decryption time, and good scalability.

6.2.8. Blockchain-based source routing

In source routing, the sensitive network topology can be leaked among the participating nodes. For the sake of preventing network topology leakage, blockchain has been employed as a solution to gather and distribute routing information in source routing using a secure approach in unmanned aerial system mesh networks [81]. This dynamic and decentralized routing framework can prevent sensitive topology disclosure thanks to the security features of the blockchain. VEIN is a source routing approach employed in payment channel networks built using blockchains to improve transactions. It has a dynamic and multipath routing approach that preserves the decentralized features of blockchains while achieving a high transaction success ratio [82]. SoRBlock is a traffic management framework that leverages blockchain technology for inter-domain routing while utilizing source routing within each domain in multi-controller software-defined networks [83]. SoRBlock's routing has resulted in low path setup times and fewer control messages in SDN.

6.2.9. Blockchain as a trusted shared memory for routing

Some have used blockchain as a shared memory to store the active paths in real-time as transactions in the blockchain network when transmitting a packet from a source terminal to a sink terminal, where the ownership of network terminals is changed during the routing process. In this scheme, routes are determined by balancing load and reducing interference while having a mechanism for getting rid of the malicious nodes [84]. This routing scheme has been proposed for a wireless sensor network, and it has resulted in reduced risk and high confidence in routing. Similarly, in another framework, network equipment is treated as coins, where ownership can switch between source and sink while transactions are retained in the blockchain, providing further security for routing in the selected paths [85]. This scheme is also proposed for a wireless sensor network in an IoT for blockchain-based decentralized routing for improved security and traffic load balance. Likewise, in [86], blockchain is employed as a shared memory to enable clustering and routing using meta-heuristic approaches (Chimp and Horse optimization) with the aid of a fitness function to select routes where the sensor nodes are treated as coins. This blockchain-based routing scheme for wireless sensor networks is dynamic, hierarchical, and aggregation-based.

6.2.10. Blockchain and authentication-based secure routing

Blockchain has been tested as a framework for authenticating and adding network nodes to the blockchain to link with networks or clusters, where the state of a node from one network to another can be different, and an authenticated node is available to all networks to be employed in routing, making it secure [87]. In this study [87], blockchain-based routing is proposed for an IoT network, and it has resulted in fast computations and low power consumption. In a wireless sensor network, a private blockchain has been employed to authenticate sensor nodes, while a public blockchain is employed to authenticate cluster heads, which also leverages a trust value allocation system to reduce the effect of malicious nodes [88]. In this work, it resulted in high trust and throughput owing to the hybrid use of public and private blockchains. Another similar work, while using blockchain authentication, also uses node registration using a certificate authority that is verified with the aid of SHA-256 as a means to hinder the engagement of malevolent equipment in the routing process [23]. This study has utilized proof of authority consensus in the blockchain in a wireless sensor network, and it has resulted in high packet delivery and improved network lifetime.

6.2.11. Blockchain and reputation/trust-based secure routing

For multi-domain software-defined IoT networks controlled by multiple controllers, a secure crossing domain routing framework that avoids black hole attacks by using blockchains in controllers is presented in [89], which uses a reputation-based mechanism for enhancing routing reliability. In this study, permissioned blockchain is utilized with PBFT consensus in an SDN to result in trusted controller communication and routing. Similarly, SCs have been employed to provide the topologies of each controller as a means to build a global reputation for crossing-domain routing with multiple controllers in an IoT unmanned aerial vehicle network [22]. In this study [22], also, a permissioned blockchain with PBFT consensus is deployed in IoT for decentralized routing that has resulted in enhanced accuracy. A trust-based secure routing framework for wireless sensor networks leverages blockchain to authenticate aggregators and sensor nodes using private and public blockchains, where the trust values of sensor nodes are calculated and employed for secure routing [24]. In this study [24], a hybrid consensus approach of PoW and PoA is utilized owing to the use of public and private blockchains, and it has resulted in a high packet delivery ratio in the wireless sensor network. Blockchain and SCs have been employed to create alerts on nodes that attempt to manipulate low-power lossy network set-up data to elevate the security and effectiveness of routing in an IoT low-power lossy network [90]. In this BBR scheme, it can detect and alert routing attacks in the IoT using a private blockchain. The consensus of blockchain technology has been employed to validate the routing actions of nodes and to set the reputation of each node such that malicious nodes can be isolated from routing in mobile ad hoc networks where the routing algorithm selects the shortest and most reputed path [91]. In this study [91], the blockchain-based routing has been proposed for a MANET, and it has resulted in a 12% improvement in packet delivery. A two-level insider attack detection system, with the first level calculating trust separately and the second level employing a consortium blockchain that has road-side units as block validators, compiles trust values for automobile nodes in a vehicular network such that routing can occur based on trust scores, preventing insider attacks [92]. This scheme leverages a consortium blockchain with PBFT consensus that has shown to be relatively scalable and capable of mitigating insider attacks in a VANET scenario.

6.2.12. Blockchain-based contractual routing

BCR is a framework that uses self-executing contracts-based contractual routing for forwarding a packet starting from a given source equipment to a given destination equipment without a centralized authority, where a source node requests routes from the destination nodes using SCs. Furthermore, BCR has been resistant to blackhole and greyhole attacks [93]. BCR has been proposed for IoT networks, and it uses a DPoS consensus for implementing decentralized routing, and it has resulted in 5 times lower overhead compared to AODV. In a smart agriculture IoT network with distributed nodes in a blockchain, SCs are used to find a path to a given destination or base-station. In the preceding scheme, due to the use of blockchain, redundant data transmissions are avoided, and energy consumption is improved [94]. This scheme has resulted in low energy consumption and high throughput in the routing scenario.

6.2.13. Blockchain-based distance vector routing

A blockchain-based distance vector routing approach known as Q-AODV is an improved queued version of the well-known AODV routing protocol that integrates with blockchain technology. In Q-AODV, a cluster is generated using the source node with the aid of self-executing contracts, and paths are detected afterwards and attached to the blockchain [95]. Q-AODV has resulted in high stability compared to AODV and DSR. Another similar work known as AODV-MQS improves AODV by proposing a multi-path quality of service secure routing by integrating with blockchain and SCs to filter the devices that satisfy QoS constraints and to find out the main path and a standby path [96]. In AODV-MQS, multipath routing is improved by using blockchain to result in better routing in unsafe environments. EE-AODV, also known as the energy-efficient AODV, leverages blockchain technology to select cluster heads in a wireless sensor network using energy, distance, and packet delivery capability to route packets from the cluster head to the base-station in an energy-efficient manner [97]. EE-AODV has been proposed for a wireless sensor network by deploying a private blockchain and has been energy efficient and resulted in a better performance compared to ALEACH.

6.2.14. Blockchain-based path vector routing

A bi-directional hierarchical blockchain is employed to detect fake BGP prefixes before spreading to develop trust between autonomous systems that use BGP for secure routing, preventing BGP attacks known as RouteChain [98]. In RouteChain, the clique blockchain consensus approach is utilized for hierarchical routing in autonomous systems to effectively curtail BGP attacks. Similarly, ROAchain uses blockchain for route origin authorization for BGP, where the route origin authorization repository is stored securely in the blockchain as a means to authenticate the route origin, including a novel consensus algorithm to ensure secure routing [99]. Thus, in ROAchain, a custom consensus is utilized for hierarchical routing, and the solution has been scalable and secure.

6.2.15. Blockchain-based link state routing

For content-centric networks, blockchain has been employed to create a routing table for a link-state routing approach to forward packets with the help of content identifiers, which has resulted in a high fault tolerance [100]. This routing approach is dynamic, decentralized, fault-tolerant, and improves manageable content. The optimized Link State Routing (OLSR) protocol has been employed to form an ad hoc network in an IoT network, where the private Ethereum blockchain has been integrated to provide services and collect data. OLSR integrated with blockchain has shown superior performance in automatic fault recovery under link failures [101].

7. REVIEW SCRUTINIZATION

7.1. Scrutinization of distinct units

Table 3 displays the scrutinization of blockchain-based routing frameworks, touching on routing technique and approach, BC concept, BC consensus, BC type, network-related parameters, performance, and proposed year.

Table 3. Scrutinization of blockchain-based routing frameworks.

Routing technique	Framework	Blockchain concept	Blockchain Architecture	Blockchain consensus	Blockchain type	Routing approach	Network architecture	Network type	Performance	Pub. year
Probabilistic	Probabilistic [64]	C1	Linear	PoW, PoS	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT	Outperforms PRoPHET	2020
Query-based	ISRchain [20]	C3	Linear	Raft	Consortium	Dynamic, Decentralized, single-path, table-based	Distributed	Generic	Efficient route verification	2020
	DRRS-BC [65]	C3	Linear	SBFT	Generic	Dynamic, Decentralized, single-path, table-based	Distributed	Generic	Solve identity and behavior authentication	2021
Optimization-based	Genetic al. [66]	C3	Graph	PoW	Public	Dynamic, Centralized, single-path, table-based	Centralized	IoT	Low gas consumption	2021
	Dynamic [67]	C1	Linear	PoW	Public	Dynamic, Decentralized, single-path, table-based	Decentralized	Generic	99.7% spectrum utilization rate	2023
	Bi-Fitness [68]	C1	Linear	Zone-based	Public	Dynamic, Decentralized, single-path, table-based	Decentralized	MANET	Good performance in terms of QoS	2021
	UAV [69]	C1	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	UAV	Provide better security than others	2021
	Clustering [70]	C1	Linear	AI-PoWCA	Public	Dynamic, hierarchical, single-path, table-based	Hierarchical	FANET	90% PDR, low latency, high throughput	2021
Machine learning	RL [71]	C1	Linear	PoAu	Public	Dynamic, decentralized, single-path, table-based	Decentralized	Sensor	Good delay performance under malicious nodes	2019
	ENIR [72]	C1	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT	Better link utilization, transmission delay	2023
	Off-chain [73]	C1	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT	Need only 1/10th of resources	2022
	DNN [74]	C3	Linear	PoAu	Consortium	Dynamic, Decentralized, single-path, table-based	Decentralized	WSN	Better than other under majority malicious nodes	2022

Routing technique	Framework	Blockchain concept	Blockchain Architecture	Blockchain consensus	Blockchain type	Routing approach	Network architectture	Network type	Performance	Pub. year
	Military [75]	C1	Linear	Custom	Public	Dynamic, Decentralized, single-path, table-based	Decentralized	Sensor	Better secured routing	2021
Fuzzy logic	Energy [76]	C1	Linear	Generic	Generic	Dynamic, hierarchical , single-path, table-based	Hierarchical	IIoT	Improved network lifetime, high PDR	2022
QoS	QoS-SDVN [21]	C1	Linear	PoW	Public	Dynamic, Centralized, single-path, table-based	Centralized	SDVN	High throughput, reduces attacks by 99%, delay	2022
	TRAQR [77]	C1	Linear	PoW	Private	Dynamic, Decentralized, single-path, table-based	Centralized	SDN	QoS compliance in untrusted environments	2021
	QoSChain [78]	C1	Linear	PoAu	Public	Dynamic, Decentralized, multi-path, table-based	Centralized	SDN	Reduces setup time, messages exchanged	2021
Onion	B-IoMV [79]	C5	Linear + Graph	PoW	Public	Dynamic, Decentralized, single-path, table-based	Decentralized	IoMV	Better latency, network bandwidth utilization	2022
	Onion-IIoT [25]	C5	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	IIoT	Better throughput, decryption time	2022
	Onion-IoUV [80]	C5	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	IoUV	Good accuracy, decryption time, scalability	2022
Source	Air-borne [81]	C1	Linear	Generic	Public	Dynamic, Decentralized, single-path, source	Decentralized	UAS	Avoid sensitive topology disclosure	2019
	VEIN [82]	C1	Linear	Generic	Generic	Dynamic, Decentralized, multi-path, source	Decentralized	PCN	34% increment in transaction success	2021
	SoRBlock [83]	C2	Linear	Generic	Public	Dynamic, hierarchical , single-path, source	Centralized	SDN	Low path setup times, control messages	2023
BC as shared memory	SM-WSN [84]	C1	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	WSN	Reduced risk, high confidence in routing	2021
	WSN-IoT [85]	C1	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	WSN	Improved security, traffic load balance	2019
	SM [86]	C1	Linear	Generic	Generic	Dynamic, hierarchical , single-path, aggregation	Decentralized	WSN	Improved network lifetime	2023
Authentication-based	BSI [87]	C3	Linear	Generic	Generic	Dynamic, Decentralized, single-	Decentralized	IoT	Fast computations,	2022

Routing technique	Framework	Blockchain concept	Blockchain Architecture	Blockchain consensus	Blockchain type	Routing approach	Network architectture	Network type	Performance	Pub. year
						path, table-based			low power consumption	
	Auth-WSN [88]	C3	Linear	Generic	Public + Private	Dynamic, hierarchical, single-path, table-based	Decentralized	WSN	High trust resulting high throughput	2021
	Auth-WSN [23]	C3	Linear	PoAu	Generic	Dynamic, hierarchical, single-path, table-based	Decentralized	WSN	Improved PDR and network lifetime	2022
Reputation-based	SR-SDN [89]	C4	Linear	PBFT	Permissioned	Dynamic, Decentralized, single-path, table-based	Centralized	SDN	Trusted controller communication, routing	2022
	SR-UAV [22]	C4	Linear	PBFT	Permissioned	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT	Enhanced accuracy, precision, recall, etc.	2023
	SR-WSN [24]	C4	Linear	PoW + PoA	Private + Public	Dynamic, hierarchical, single-path, aggregation	Decentralized	WSN	High packet delivery ratio	2022
	LLN [90]	C4	Linear	Generic	Private	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT-LLN	Detects and alerts routing attacks	2020
	SR-MANET [91]	C4	Linear	PoW	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	MANET	12% improvement in packet delivery	2020
	Trust-man [92]	C4	Linear	PBFT	Consortium	Dynamic, Decentralized, single-path, table-based	Decentralized	VANET	Scalable, mitigates insider attacks	2021
BC-based contractual	Con-IoT [93]	C2	Linear	DPoS	Public	Dynamic, Decentralized, single-path, table-based	Decentralized	IoT	5 times lower overhead with respect to AODV	2018
	Agri-contract [94]	C2	Linear	Generic	Generic	Dynamic, hierarchical, single-path, aggregation	Decentralized	IoT	Efficient, low energy, high throughput	2020
Distance vector	Q-AODV [95]	C2	Linear	Generic	Generic	Dynamic, Decentralized, single-path, table-based	Decentralized	Adhoc	High stability than AODV, DSR	2020
	AODV-MQS [96]	C2	Linear	Generic	Generic	Dynamic, Decentralized, multi-path, table-based	Decentralized	Adhoc	Better routing in unsafe environments	2021
	EE-AODV [97]	C2	Linear	PoW	Private	Dynamic, hierarchical, single-path, table-based	Decentralized	WSN	Energy efficient, better than ALEACH	2023
Path vector	RouteChain [98]	C1	Hierarchical	Clique	Generic	Dynamic, hierarchical, single-	Hierarchical	Auto. system	Effectively curtail BGP attack	2022

Routing technique	Frame-work	Block-chain concept	Blockchain Architec-ture	Block-chain consen-sus	Blockchain type	Routing approach	Network architect-ture	Network type	Performance	Pub. year
						path, table-based				
Link state	ROAchain [99]	C3	Linear	Custom	Generic	Dynamic, Decentralized, single-path, table-based	Hierarchical	Auto. system	Consistent, scalable, and secure	2020
	Link-CCN [100]	C2	Linear	PoW	Public	Dynamic, Decentralized, single-path, table-based	Decentrali-zed	CCN	Improves fault tolerance, manageable content	2021
	OLSR [101]	C1	Linear	PoW	Private	Dynamic, Decentralized, single-path, table-based	Decentrali-zed	IoT	Automatic failure recovery	2021

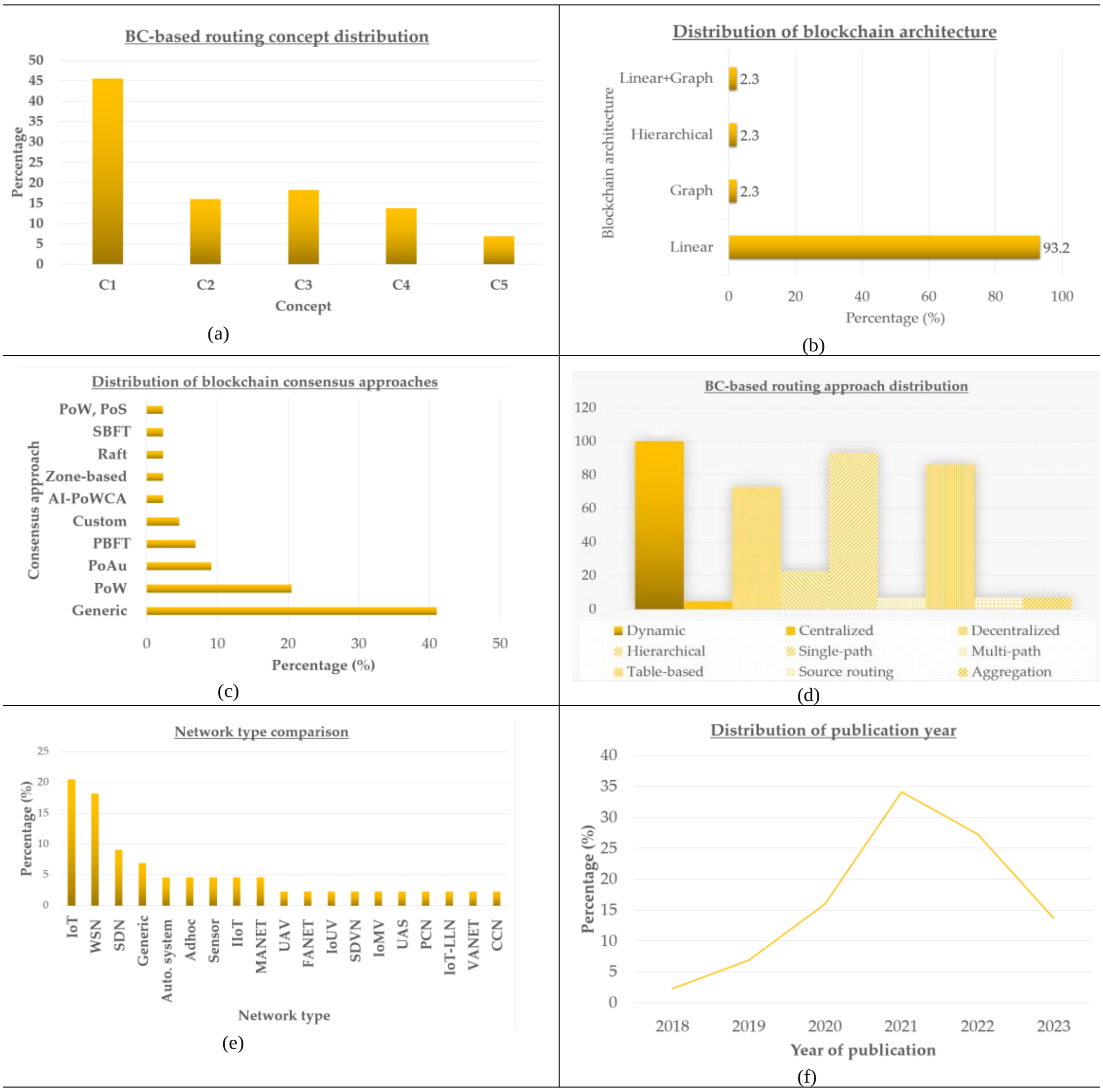


Figure 6. Overall scrutinization (a) BC-based routing concept (b) BC architecture (c) BC unanimity (d) BC-based routing approach (e) Network classification (f) Year of publication.

7.2. Overall scrutinization

Figure 6 pictorially displays the proportional allocation of numerous characteristics of BC-based routing frameworks.

As displayed within Figure 6a, the highest (45.5%) of blockchain-based routing frameworks are based on concept C1, subsequent to C3 (18.2%), C2 (16%), C4 (13.7%), and C5 (6.9%). Next, 93.2% of frameworks have exploited linear blockchain architecture, while graph, hierarchical, and linear and graph combinations each have the least percentage of 2.3%, as displayed within Figure 6b. Moreover, the majority of blockchain-based routing frameworks do not define an unanimity method; apart from that, others define an unanimity approach: PoW (20.5%) is commanding, subsequent to PoAu (9.1%), PBFT (6.9%), custom unanimity (4.6%), and others, as displayed within Figure 6c. Furthermore, as displayed within Figure 6d, all BC-based routing frameworks are dynamic, while 72.8% have a decentralized routing approach, 22.8% have a hierarchical routing approach, 4.6% exploit a centralized routing approach, 93.2% are single-path routing, 6.9% are multi-path routing, and 86.4% are table based, while source routing and aggregation-based routing exploitation are 6.9%. Moreover, in the BC-based routing frameworks scrutinized, the highest percentage (20.5%) are exploited in IoT networks, subsequent to WSN (18.2%), SDN (9.1%), generic networks (6.9%), and others, as displayed within Figure 6e. Finally, as displayed within Figure 6f, the blockchain-based routing concept has elevated publication content starting from 2018 and has reached the apex of publications by 2021, and the volume has been decaying ever since, as displayed within Figure 6f.

We can critically evaluate the performance of reviewed blockchain-based routing frameworks, as given in Table 4.

Table 4. Performance evaluation comparison to identify strengths and weaknesses.

Parameter	Strength	Weakness
Route verification	Efficient [20]	
Authentication	High [65]	
Gas consumption	Low [66]	
Spectrum utilization rate	High [67]	
Quality of service	High [68], [77]	
Security	High [69], [75], [21], [81], [85], [88], [99]	
Packet delivery ratio	90% [70], High [76], [23], [24]	Low in low rounds [88], Medium [89], Low under low attacks [91], [96], Low [93]
Latency	Low [70], [71], [72], [21], [79]	High [95]
Throughput	High [70], [21], [25]	Low in low rounds [88]
Link utilization	Good [72]	
Transaction throughput	High [74]	
Network lifetime	High [76], [86], [23], [94]	
Setup time	Low [78], [84]	
Cost	Low [73]	High [79], [100]
Decryption time	Low [25]	
Scalability	High [80], [82], [92], [99]	Low [84], [97], [100]
Energy consumption	Low [86], [87], [24], [97]	
Reputation		Medium [89]
Trust	High [82], High [22]	
Routing attacks	Detect [90], [98]	Fair resistance only [93]
Block mining time		High [91], [92]
Overhead	Low [93]	High in safe environments [96]
Stability	High [95]	
Consensus time		High for PoET [98]
Fault tolerance	High [100], [101]	

As analyzed in Table 4, it should be noted that efficient route verification, high authentication, low gas consumption, high spectrum utilization rate, high quality of service, high security, good link utilization, high transaction throughput, high network lifetime, low setup time, low decryption time, high trust, high stability, and high fault tolerance can be clearly recognized as performance strengths of the blockchain-based routing frameworks discussed. On the other hand, it is also very clear that medium reputation, high block mining time, and high consensus time are performance limitations of the blockchain-based routing frameworks reviewed. Alternatively, there exist some performance metrics that have shown signs of both limitations and strengths. First is the packet delivery ratio, which has been comparatively higher under unsafe environments, while it is lower at safe environments or at lower rounds. In most frameworks, the latency has been low, while it has been observed to be higher in the study [95] due to nodes moving faster, resulting in more re-searching operations. The cost is observed to be high in a higher number of frameworks, except in study [75] due to the utilization of proof of authority consensus and deep learning. On the other hand, in most frameworks, the throughput has been high, except in study [88], which has been low under low rounds. Scalability performance is highly subjective and debatable, as similar proportions of studies have reported high and low scalabilities alternatively. For instance, in study [80], it has been reported low owing to the fact of using IPFS and the use of AI to classify data. In contrast, the study [100] reports low scalability owing to the utilization of proof-of-work in the proposed system. Blockchain-based routing systems are capable of detecting routing attacks, despite some studies, such as [93], only showing a fair performance in detection. Finally, in blockchain-based routing, the routing overhead is typically lower under unsafe environments despite it having a tendency to be high in safe environments.

One of the gaps of the review is that most of the blockchain-based routing frameworks have been validated in simulation environments and lack empirical results except for the studies ISRchain [20], Onion-IIoT [25], and RouteChain [98]. In ISRchain, two case studies, BHARTI airtel prefix hijack and Google route leak, are used for real-world internet source allocation simulations. Furthermore, in Onion-IIoT, empirical results for routing are used, while in RouteChain, the 2008 YouTube Hijacking case study is considered. Moreover, the debatable performance evaluations need further assessments.

Now, let us compare the conception of blockchain-based routing reviewed in this study with traditional routing, as shown in Table 5.

Table 5. Comparison of blockchain-based routing with traditional routing

Blockchain-based routing conception	**Performance of blockchain-based routing**	**Performance of traditional routing**
C1	High security, good performance under malicious nodes	Low security, good performance in safe environments, low failure recovery
C2	Energy efficient, low overhead	Higher overhead
C3	Better authentication and route verification	Poor authentication
C4	Good packet delivery, trusted communication	Lower trust
C5	Better throughput and bandwidth utilization in blockchain-based onion routing	Inferior routing metrics in conventional onion routing

As evident from Table 5, overall, the blockchain-based routing results in higher security, good routing performance under unsafe environments in non-onion routing, higher trust, good authentication, and superior routing performance in blockchain-based onion routing, compared to traditional routing.

Now, based on the review, we can provide directions for application domains for each blockchain-based routing technique and concept, as shown in Table 6.

As evident from Table 6, it is clear that for all of the blockchain conceptions identified in this review, IoT is utilized as an application domain; thus, it can be recommended for all BBR concepts identified. The next most frequently utilized application domains are WSNs, followed by SDN. Thus, Table 6 can be utilized as a guideline in selecting application domains for each blockchain-based routing technique and blockchain-based routing concept.

Table 6. Application domain recommendation for blockchain-based routing techniques and concepts

Blockchain-based routing technique or concept	Application domains
C1	IoT, WSN, SDN
C2	IoT, Ad hoc, WSN
C3	IoT, WSN
C4	IoT, SDN, WSN, Ad hoc
C5	IoT
Probabilistic	IoT
Optimization-based	IoT, Ad hoc, UAV
Machine learning	WSN, IoT
Fuzzy logic	IIoT
QoS	SDN
Onion	IoT
Source	UAS, PCN, SDN
BC as shared memory	WSN
Authentication-based	IoT, WSN
Reputation-based	IoT, WSN, Ad hoc
BC-based contractual	IoT
Distance vector	Ad hoc, WSN
Path vector	Autonomous systems
Link state	IoT, CCN

8. DISCUSSION

8.1. Possibilities

8.1.1. Prevention of routing attacks

Blockchains enable reputation-/trust-based routing, preventing or reducing possible routing attacks such as black hole attacks and grey hole attacks. They can enhance routing reliability by enabling reputation-based routing by computing and storing a reputation score for each node of the network. Moreover, SCs-based contractual routing can be employed to generate automatic alerts when network nodes attempt to behave maliciously and remove such nodes from the routing approach, while distributed consensus can be employed to validate routing actions. Furthermore, insider attacks can be detected using trust values, and blockchain can be employed to aggregate trust values to enable secure routing.

8.1.2. Caters a secure ledger for storing routing decisions and updates

Blockchains can provide a source of distributed ledgers for storing data, decisions, parameters, paths, etc. related to routing in a transparent and immutable manner. Moreover, the stored routes can be queried using querying techniques during verification. Furthermore, blockchains can be employed to prevent network topology leakage among participating nodes in source routing approaches. Most importantly, it can act as a trusted shared memory to store routing paths and parameters in real-time, where the ownership of the nodes can change during the routing process. Thus, the trustworthiness and integrity of routing can be improved by employing blockchain technology.

8.1.3. Robust routing authentication

In the routing process, node authentication is an important step in determining the authenticity of network nodes and preventing unauthorized malicious nodes from poisoning the routing process. Blockchains can be employed for automatic authentication of network nodes, where authenticated nodes can be inserted into the blockchain to be employed in subsequent routing processes. Different levels of authentication, such as individual nodes or routing cluster heads, can be realized to be used with the corresponding routing strategy. Blockchains allow decentralized authentication without requiring a trusted third party and rely on robust cryptographic or non-cryptographic techniques to achieve it.

8.1.4. Routing automation employing SCs

First, SCs can be employed to implement a routing approach to search for a path from a given source equipment to a destination equipment in an automated fashion, avoiding redundant data transmissions. Moreover, filtration strategies can be employed on SCs to filter devices, considering factors such as quality of service parameters in determining optimal routing paths. Furthermore, they can be employed to exchange trust information and topology information among network domains as a means to implement secure routing. Thus, network administrators can implement high-level routing policies inside the SCs of blockchains to execute automatically in determining optimum paths upon meeting a specified set of conditions, providing dynamic routing optimization.

8.1.5. High cohesion with onion routing

Onion routing is a privacy-preserving routing approach where the intermediate nodes are aware of only the previous and next nodes in the route, hiding the source and destination nodes of the route. Blockchain, along with tokens, have been frequently employed to implement onion routing, where tokens are used for validating encrypted messages sent through onion routing. Thus, by integrating blockchain with onion routing, a trustworthy, immutable, non-repudiable, and anonymous routing framework can be built, where the parameter "anonymous" is provided by the onion routing and other security parameters are offered by the blockchain. Therefore, privacy information such as network topology leakage to intermediate routers in secure blockchain-based routing can be prevented by integrating it with onion routing that uses multiple layers of encryption.

8.1.6. High integratability with artificial intelligence-aided routing

Artificial intelligence makes inferences from available data, helping in decision-making processes [102]. Artificial intelligence techniques like machine learning, fuzzy logic, meta-heuristics, etc. generate knowledge using given input data [103]. In the network routing domain, these techniques can generate routing paths or select cluster heads using network traffic information and topology. While generating routing paths using artificial intelligence, blockchain can aid in achieving that task by selecting routing loads, assessing the sensitivity of the packets, enabling secure communication of generated knowledge and optimizations, storing routing information securely, using consensus approaches for authentication, reducing identical data exchange, etc.

8.2. Impediments

8.2.1. Impediments in incentivizing packet forwarding

In blockchain-based routing frameworks, there is a lack of proper mechanisms to incentivize packet forwarding, despite the fact that it can be treated as a service rewarded with cryptocurrency. It is essential to have mechanisms for the nodes to prove that they have contributed to data forwarding so that they can be incentivized proportional to the workload of data forwarding. However, in the literature, there is a lack of standardized techniques for generating such forwarding proofs, and the generation of such proofs can be complex in highly dynamic network environments such as adhoc networks and device-to-device communication. It is laborious to implement monitoring mechanisms in order to create such forwarding proofs, despite the fact that some researchers have posited an algorithmic game theoretic approach for modeling incentives [104].

8.2.2. QoS degradation of routing

Despite the fact that there are efforts to improve the QoS of routing by leveraging blockchains such as TRAQR [77] and QoSChain [78] to store and exchange trust-related information in a secure mode, the amalgamation of blockchains for routing can challenge the maintenance of QoS in routing. QoS parameters like latency and throughput can be degraded thanks to additional blockchain processes such as distributed consensus and block validation that can incur additional latency in the routing approach, increasing the overall latency and decreasing the overall throughput.

8.2.3. Boosted migration cost

Conventional networks have used conventional routing approaches since the beginning of computer networks. That is because employing blockchain to enhance the trustworthiness of routing can demand additional computation resources, memory resources, and transmission resources in the network, which will escalate the overall financial cost. Thus, network users or administrators may be reluctant to integrate blockchain into the network as it can cause additional costs to the system.

8.2.4. Amplified route computation energy

Blockchains are well-known for high resource-consuming computations such as proof-of-work-based consensus, energy spent on cryptographic techniques, etc. [105]. Routing techniques already deplete node energy by message exchanging and performing computations to find optimum routing paths using either protocol, algorithmic, artificial intelligence, or optimization techniques [106]. When blockchain is integrated on top of these approaches for performing tasks such as secure route storage, automatic route computation, routing authentication, performing routing using a reputation- or trust-based score, etc., additional energy can be depleted from nodes. Due to the additional energy devouring blockchain computations, the energy in the nodes can be depleted, causing the nodes to switch to energy conservation approaches, thus reducing the overall performance of routing in energy-restricted networks such as wireless sensor networks and the internet of things.

8.2.5. Deficiency of scalability for the routing

It is a well-known fact that the complexity of routing escalates with network volume [107]. In blockchain-based routing, the computational and space complexity will be even higher with the expansion of network volume thanks to the additional processes involved in blockchains, such as block validation, block propagation [108], blockchain transactions, SCs implementation [109], etc. These processes can get slower and cause additional latency in large networks. Thus, it will be challenging for the blockchain-based routing systems to adhere to routing QoS requirements for packet forwarding when the network volume escalates.

9. CONCLUSION, PROPOSALS, AND FUTURE AVENUES

In this appraisal, we first appraised different classes of routing techniques like probabilistic routing, onion routing, etc. and then classified routing approaches based on their dynamic nature, network architecture, data forwarding, and protocol definition. Then, we gave a summary of the blockchain system, and later, we appraised blockchain-based routing, categorizing them based on the routing approach combined with the blockchain. Derived from this study, we established that blockchain-based routing in networks belongs to one of 5 divisions: providing secure storage for making routing decisions, automatic routing implementation using SCs, employing blockchain for authentication for secure routing, blockchain-based onion routing, and blockchain aided reputation-based routing. Then, we meticulously scrutinized the appraised frameworks to distinguish the trend in blockchain-based routing under different criteria with numerical percentage prevalence. Specifically, it was revealed that storage of routing decisions and updates securely in blockchain was the most utilized blockchain-based routing concept, linear blockchain being the most utilized blockchain type, proof-of-work being the most frequently utilized specific consensus type, and most routing approaches being dynamic, decentralized, single-path, and table-based. Finally, we communicated the possibilities and impediments of blockchain-based routing.

This survey delivers a convenient reference to the already existing field of study on blockchain-based routing, as it divides and meticulously scrutinizes them under various criteria. This will deliver a convenient guide for upcoming researchers to appraise more on this field by swiftly identifying trends, voids, possibilities, and impediments in blockchain-based routing.

Derived from the analyzed impediments, subsequent proposals can be proposed to overcome them.

- For the sake of overcoming the challenge of difficulties in incentivizing routing, researchers can make use of game theoretic approaches that have been recently proposed by researchers. Moreover, a token-based reward system can be employed where participants receive incentives in the form of cryptocurrency for successfully forwarding a packet. Moreover, consensus approaches like proof-of-stake can be employed for the participants to risk losing stake if engaged in malicious routing.
- For the sake of overcoming the challenges of QoS degradation in routing, several countermeasures can be proposed. First, the blockchain can be implemented as a layered architecture with a base layer handling critical consensus and security functions while having higher layers responsible for routing. Moreover, sharding strategies can be employed to divide the blockchain into interconnected subsets, where each shard can handle transactions autonomously, boosting the throughput. Furthermore, caching strategies can be employed to store frequently accessed data in a cache without frequently accessing the blockchain, reducing the overall latency.
- The migration cost from traditional routing to blockchain cannot be prevented; however, it can be minimized to a certain extent. Specifically, the migration cost involved in buying and installing new hardware and software resources to employ blockchain cannot be evaded. However, the operational cost involved in migration can be reduced by optimizing smart contracts to work efficiently, utilizing the least amount of resources, getting aid from off-chain storage for routing, employing low-cost routing approaches, etc.
- For the sake of reducing route computation energy in blockchain-based routing, energy-efficient consensus approaches like green consensus approaches can be employed. Moreover, dynamic routing strategies can be employed to adapt to network conditions dynamically by shifting to a low-energy

consumption mode under low network loads. Furthermore, energy-efficient hardware that is dedicated to tasks such as blockchain-based mining can be employed to boost energy conservation.

- One of the main solutions proposed to tackle the scalability issue in blockchain-based routing is to employ off-chain-based storage, where the hash digest of transactions stored off-chain is stored in the blockchain to tackle the demand for resources when the network volume escalates. Alternatively, multi-path (DAG) blockchain can be employed to scale well thanks to its parallel processing and computation capability compared to traditional blockchain.
- During review analysis, it was revealed that node mobility can increase the routing latency due to re-searching operations. This limitation can be overcome by using proactive routing that computes paths proactively even before link changes actually occur in the network. Moreover, the blockchain mining time can be effectively reduced by employing efficient consensus approaches or mining techniques that are different from traditional techniques. As it has been reported in many studies, the overall cost of the system tends to increase with the utilization of blockchain; cost-effective solutions such as off-chain storage and efficient consensus approaches such as PoA are recommended. However, the increase in cost can be traded-off with the gains in the routing security and trust.

In conventional routing, blockchain is not employed. Blockchain-based routing can revolutionize routing by ensuring that routing is trustworthy thanks to its inherent features of data modification resistivity, non-deniability, obscured individuality, optional secrecy using cryptographic techniques, etc. Upcoming research within blockchain-based routing can involve cross-asset routing that involves the forwarding of other digital assets other than packets with applications in gaming, art, etc. Additionally, upcoming blockchain-based routing can be implemented using quantum computations, catering robust security against quantum attacks. Furthermore, upcoming research can appraise more insight on how to improve the efficiency of consensus approaches and smart contracts that employ routing techniques. Furthermore, future work in this domain should definitely provide more focus towards real-world implementation and empirical validation of the blockchain-based routing frameworks, as this review identified that only a handful of studies have been validated in real-world case studies. Moreover, more research should be done in the future to reduce the high cost associated with blockchains in a blockchain-based routing scenario. Finally, quantum-resistant blockchain routing should be investigated in real-world or simulation scenarios to combat attacks from quantum computers without compromising gains in routing performance.

REFERENCES

[1] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, “Trust-based secure directed diffusion routing protocol in WSN,” *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 1405–1417, Nov. 2022.

[2] C. Seneviratne, P.A.D.S.N. Wijesekara, and H. Leung, “Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks,” *Sensors*, vol. 20, no. 2., p. 567, Jan. 2020.

[3] D.J.I.Z. Chen, and D.S. Smys, “Optimized dynamic routing in multimedia vehicular networks,” *J. Inf. Technol. Digit. World*, vol. 2, no. 3, pp. 174-182, Sep. 2020.

[4] K. Mershad, “SURFER: A secure SDN-based routing protocol for internet of vehicles,” *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7407-7422, Nov. 2020.

[5] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, “Optimized link state routing protocol for ad hoc networks,” in *Proc. IEEE Int. Multi Topic Conf.,* Lahore, Pakistan: IEEE, Dec. 2001, pp. 62-68.

[6] H.S. Chang, B.W. Kim, C.G. Lee, S.L. Min, Y. Choi, H.S. Yang, D.N. Kim, and C.S. Kim, “Performance comparison of static routing and dynamic routing in low-earth orbit satellite networks,” in *Proc. Veh. Technol. Conf.*, Atlanta, USA: IEEE, Apr. 1996, vol. 2, pp. 1240-1243.

[7] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, “An Optimization Framework for Data Collection in Software Defined Vehicular Networks,” *Sensors*, vol. 23, no. 3, p. 1600, Feb. 2023.

[8] Q. Guan, F. Ji, Y. Liu, H. Yu, and W. Chen, “Distance-vector-based opportunistic routing for underwater acoustic sensor networks,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3831-3839, Jan. 2019.

[9] N. Varyani, Z.L. Zhang, and D. Dai, “QROUTE: An efficient quality of service (QoS) routing scheme for software-defined overlay networks,” *IEEE Access*, vol. 8, no. 1, pp. 104109-104126, May 2020.

[10] H. Fatemidokht, M.K. Rafsanjani, B.B. Gupta, and C.H. Hsu, “Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. *22*, no. 7, pp. 4757-4769, Jan. 2021.

[11] L. Layuan, L. Chunlin, and Y. Peiyan, “Performance evaluation and simulations of routing protocols in ad hoc networks,” *Comput. Commun.*, vol. 30, no. 8, pp. 1890-1898, Jun. 2007.

[12] R. Arroyo-Valles, R. Alaiz-Rodriguez, A. Guerrero-Curieses, and J. Cid-Sueiro, “Q-probabilistic routing in wireless sensor networks,” in *Proc. 2007 3rd Int. Conf. Intell. Sensors Sensor Netw. Inf.*, Melbourne, Australia: IEEE, Dec. 2007, pp. 1-6.

[13] T.A. Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, and T.A. Alghamdi, “comparative analysis of blockchain architecture and its applications: Problems and recommendations,” *IEEE access*, vol. 7, pp. 176838-176869, Dec. 2019.

[14] S. Kably, M. Arioua, and N. Alaoui, “Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment,” *Comput. Mater. Continua*, vol. 71, no. 3, pp. 5271-5291, Jun. 2022.

[15] P.A.D.S.N. Wijesekara, “Load Balancing in Blockchain Networks: A Survey,” *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 13, no. 4, pp. 260-276, Jul. 2024.

[16] M. Raikwar, D. Gligoroski, and K. Kralevska, “SoK of used cryptography in blockchain,” *IEEE Access*, vol. 7, pp. 148550-148575, Oct. 2019.

[17] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, “IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques,” *Electronics*, vol. 10, no. 21, p. 2647, Oct. 2021.

[18] A. Baliga, “Understanding blockchain consensus models,” *Persistent*, vol. 4, no. 1, p. 14, Apr. 2017.

[19] P.A.D.S.N. Wijesekara, and S. Gunawardena, “A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges,” *Network*, vol. 3, no. 3, pp. 343-421, Aug. 2023.

[20] D. Chen, Y. Ba, H. Qiu, J. Zhu, and Q. Wang, “ISRchain: Achieving efficient interdomain secure routing with blockchain,” *Comput. Electr. Eng.*, vol. 83, p. 106584, May 2020.

[21] S. Choudhary, and S. Dorle, “A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc networks using machine learning-based blockchain routing,” *Concurrency Comput. Practice Experience*, vol. 34, no. 17, p. e6993, Aug. 2022.

[22] A. Aldaej, M. Atiquzzaman, T.A. Ahanger, and P.K. Shukla, “Multidomain blockchain-based intelligent routing in UAV-IoT networks,” *Comput. Commun.*, vol. 205, pp. 158-169, May 2023.

[23] U. Aziz, M.U. Gurmani, S. Awan, M.B.E. Sajid, S. Amjad, and N. Javaid, “A blockchain based secure authentication and routing mechanism for wireless sensor networks,” in *Proc. 15th Int. Conf. Innovative Mobile Internet Services Ubiquitous Comput. (IMIS-2021)*, Asan: Springer, 2022, pp. 87-95.

[24] S. Awan, N. Javaid, S. Ullah, A.U. Khan, A.M. Qamar, and J.G. Choi, “Blockchain based secure routing and trust management in wireless sensor networks,” *Sensors*, vol. 22, no. 2, p. 411, Jan. 2022.

[25] R. Gupta, N.K. Jadav, H. Mankodiya, M.D. Alshehri, S. Tanwar, and R. Sharma, “Blockchain and Onion-Routing-Based Secure Message Exchange System for Edge-Enabled IIoT,” *IEEE Trans. Indu. Informat.*, vol. 19, no. 2, pp. 1965-1976, Jul. 2022.

[26] L. Mastilak, P. Helebrandt, M. Galinski, and I. Kotuliak, “Secure inter-domain routing based on blockchain: A comprehensive survey,” *Sensors*, vol. 22, no. 4, p. 1437, Feb. 2022.

[27] P.A.D.S.N. Wijesekara, “Intrusion Detection Using Blockchain in Software-Defined Networking: A Literature Review,” *J. Eng. Sci. Technol. Rev.*, vol. 18, no. 1, pp. 57-79, Jan. 2025.

[28] Y. Mao, C. Zhou, Y. Ling, and J. Lloret, “An optimized probabilistic delay tolerant network (DTN) routing protocol based on scheduling mechanism for internet of things (IoT),” *Sensors*, vol. 19, no. 2, p. 243, Jan. 2019.

[29] D.V.A. Duong, and S. Yoon, “An efficient probabilistic routing algorithm based on limiting the number of replications,” in *Proc. 2019 Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, Jeju island, South Korea: IEEE, Oct. 2019, pp. 562-564.

[30] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, “Data Gathering Optimization in Hybrid Software Defined Vehicular Networks,” in *Proc. 20th Academic Sessions*, Matara, Sri Lanka: University of Ruhuna, Jun. 2023, p. 59.

[31] S. Jain, K.K. Pattanaik, and A. Shukla, “QWRP: Query-driven virtual wheel based routing protocol for wireless sensor networks with mobile sink,” *J. Netw. Comput. Appl.*, vol. 147, p. 102430, Dec. 2019.

[32] P. Maheshwari, A.K. Sharma, and K. Verma, “Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization,” *Ad Hoc Netw.*, vol. 110, p. 102317, Jan. 2021.

[33] A. Bhardwaj, and H. El-Ocla, “Multipath routing protocol using genetic algorithm in mobile ad hoc networks,” *IEEE Access*, vol. 8, pp. 177534-177548, Sep. 2020.

[34] L. Zhao, Z. Yin, K. Yu, X. Tang, L. Xu, Z. Guo, and P. Nehra, “A fuzzy logic-based intelligent multiattribute routing scheme for two-layered SDVNs,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 4189-4200, Aug. 2022.

[35] P.A.D.S.N. Wijesekara, and S. Gunawardena, “A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks,” *Telecom*, vol. 4, no. 3, pp. 393-458, Jul. 2023.

[36] S. AlQahtani, and A. Alotaibi, “A route stability-based multipath QoS routing protocol in cognitive radio ad hoc networks,” *Wireless Netw.*, vol. 25, pp. 2931-2951, Jul. 2019.

[37] Y.H. Robinson, E.G. Julie, K. Saravanan, R. Kumar, and L.H. Son, “FD-AOMDV: fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks,” *J. Ambient Intell. Humanized Comput*., vol. 10, pp. 4455-4472, Nov. 2019.

[38] Y.C. Hu, A. Perrig, and M. Sirbu, “SPV: Secure path vector routing for securing BGP,” in *Proc. 2004 Conf. Appl. Technol. Architectures Protocols Comput. Commun*., New York, USA: ACM, Aug. 2004, pp. 179-192.

[39] N. Feamster, J. Winick, and J. Rexford, “A model of BGP routing for network engineering,” *ACM SIGMETRICS Performance Evaluation Rev*., vol. 32, no. 1, pp. 331-342, Jun. 2004.

[40] R.L. Raghavendar, and C.R.K. Reddy, “Node activity based trust and reputation estimation approach for secure and QoS routing in MANET,” *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, p. 5340, Dec. 2019.

[41] L. Guaya-Delgado, E. Pallarès-Segarra, A.M. Mezher, and J. Forné, “A novel dynamic reputation-based source routing protocol for mobile ad hoc networks,” *EURASIP J. Wireless Commun. Netw*., vol. 2019, no. 1, pp. 1-16, Dec. 2019.

[42] P.A.D.S.N. Wijesekara, and S. Gunawardena, “A Comprehensive Survey on Knowledge-Defined Networking,” *Telecom*, vol. 4, no. 3, pp. 477-596, Aug. 2023.

[43] J. Yi, A. Adnane, S. David, and B. Parrein, “Multipath optimized link state routing for mobile ad hoc networks,” *Ad hoc Netw.*, vol. 9, no. 1, pp. 28-47, Jan. 2011.

[44] M.S. Haghighi, and Z. Aziminejad, “Highly anonymous mobility-tolerant location-based onion routing for VANETs,” *IEEE Internet Things J*., vol. 7, no. 4, pp. 2582-2590, Oct. 2019.

[45] C. Kuhn, D. Hofheinz, A. Rupp, and T. Strufe, “Onion routing with replies,” in *Proc. Adv. Cryptology–ASIACRYPT 2021: 27th Int. Conf. Theory Appl. Cryptology Inf. Security*, Singapore: Springer, Dec. 2021, pp. 573-604.

[46] M. Beshley, N. Kryvinska, H. Beshley, M. Medvetskyi, and L. Barolli, “Centralized QoS routing model for delay/loss sensitive flows at the SDN-IoT infrastructure,” *Comput. Mater. Continua*, vol. 69, no. 3, pp. 3727-3748, Dec. 2021.

[47] P.A.D.S.N. Wijesekara, W.M.A.K. Sangeeth, H.S.C. Perera, and N.D. Jayasundere, “Underwater Acoustic Digital Communication Channel for an UROV,” in *Proc. 5th Annual Research Symp. (ARS2018)*, Hapugala, Sri Lanka: University of Ruhuna, Jan. 2018, p. E17.

[48] A.R. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, “A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks,” *Peer-to-Peer Netw. Appl*., vol. 12, pp. 1076-1096, Sep. 2019.

[49] M. Karakus, and A. Durresi, “A scalable inter-as qos routing architecture in software defined network (sdn),” in *Proc. 2015 IEEE 29th Int. Conf. Adv. Inf. Netw. Appl*., Gwangju, South Korea: IEEE, Mar. 2015, pp. 148-154.

[50] Y. Ganjali, and A. Keshavarzian, “Load balancing in ad hoc networks: single-path routing vs. multi-path routing,” in *Proc. IEEE INFOCOM* 2004, Hong-Kong, China: IEEE, Mar. 2004, vol. 2, pp. 1120-1125.

[51] Z. Chen, W. Zhou, S. Wu, and L. Cheng, “An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET,” *IEEE Access*, vol. 8, pp. 44760-44773, Mar. 2020.

[52] X. Fu, G. Fortino, P. Pace, G. Aloi, and W. Li, “Environment-fusion multipath routing protocol for wireless sensor networks,” *Inform. Fusion*, vol. 53, pp. 4-19, Jan. 2020.

[53] P.A.D.S.N. Wijesekara, and Y.K. Wang, “A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka,” *COVID*, vol. 2, no. 6, pp. 793-826, Jun. 2022.

[54] D.B. Johnson, D.A. Maltz, and J. Broch, “DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks,” *Ad hoc Netw*., vol. 5, no. 1, pp. 139-172, Jan. 2001.

[55] M. Maleki, K. Dantu, and M. Pedram, “Power-aware source routing protocol for mobile ad hoc networks,” in *Proc 2002 Int. Symp. Low Power Electron. Design*, Monterey, USA: ACM, Aug. 2002, pp. 72-75.

[56] B.U. Prathyusha, and K.R. Babu, “EABRT-TOPSIS: An Enhanced AODV Routing Protocol with TOPSIS-based Backup Routing Table for Energy-Efficient Communication in CA-MANET,” *Int. J. Intell. Syst. Appl. Eng*., vol. 11, no. 3, pp. 1200-1210, 2023.

[57] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, “Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks,” in *Proc. 20th Academic Sessions*, Matara, Sri Lanka: University of Ruhuna, Jun. 2023, p. 60.

[58] W.K. Yun, and S.J. Yoo, “Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks,” *IEEE Access*, vol. 9, no. 1, pp. 10737-10750, Jan. 2021.

[59] M.V. Babu, J.A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, “An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network,” *Mobile Netw. Appl*., vol. 26, pp. 1059-1067, Jun. 2021.

[60] P.A.D.S.N. Wijesekara, “A Literature Review on Access Control in Networking Employing Blockchain,” *Indonesian J. Comput. Sci.*, vol. 13, no. 1, pp. 734-768, Feb. 2024.

[61] P.A.D.S.N. Wijesekara, “A Review on Deploying Blockchain Technology for Network Mobility Management,” *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 3, no. 1, pp. 1-33, Mar. 2024.

[62] P.A.D.S.N. Wijesekara, “A Review of Blockchain-Rooted Energy Administration in Networking,” *Indonesian J. Comput. Sci.*, vol. 13, no. 2, pp. 1607-1642, Apr. 2024.

[63] P.A.D.S.N. Wijesekara, “Blockchain and Artificial Intelligence for Big Data Analytics in Networking: Leading-edge Frameworks,” *J. Eng. Sci. Technol. Rev.*, vol. 17, no. 3, pp. 125-143, May 2024.

[64] P. Rani, A. Balyan, V. Jain, D. Sangwan, P.P. Singh, and J. Shokeen, “A probabilistic routing-based secure approach for opportunistic IoT network using blockchain*,”* in *Proc. 2020 IEEE 17th India Council Int. Conf. (INDICON)*, New Delhi, India: IEEE, Dec. 2020, pp. 1-7.

[65] H. Lu, Y. Tang, and Y. Sun, “DRRS-BC: Decentralized routing registration system based on blockchain,” *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 12, pp. 1868-1876, Jul. 2021.

[66] S. Abbas, N. Javaid, A. Almogren, S.M. Gulfam, A. Ahmed, and A. Radwan, “Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things,” *IEEE Access*, vol. 9, pp. 139739-139754, Oct. 2021.

[67] J. Ma, “Network dynamic routing and spectrum allocation algorithm based on blockchain technology,” *Int. J. Autonomous Adaptive Communi. Syst*., vol. 16, no. 1, pp. 17-30, Mar. 2023.

[68] A.R. Prasath, “Bi-Fitness Swarm Optimizer: Blockchain Assisted Secure Swarm Intelligence Routing Protocol for MANET,” *Indian J. Comput. Sci. Eng*., vol. 12, no. 5, pp. 1442-1458, Oct. 2021.

[69] M. Kayalvizhi, and S. Ramamoorthy, “Blockchain-based Secure Data Transmission for UAV Swarm using Modified Particle Swarm Optimization Path Planning Algorithm,” *Int. J. Adv. Comput. Sci. Appl*., vol. 12, no. 11, pp. 554-563, 2021.

[70] L. Zhao, M.B. Saif, A. Hawbani, G. Min, S. Peng, and N. Lin, “A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET,” *China Commun*., vol. 18, no. 7, pp. 103-116, Jul. 2021.

[71] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, “A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks,” *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019.

[72] Y. Guo, Y. Wang, and Q. Qian, “Intelligent edge network routing architecture with blockchain for the IoT,” *China Commun*., vol. 20, no. 11, pp. 151-163, May 2023.

[73] 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,” *IEEE J. Sel. Areas Commun*., vol. 40, no. 12, pp. 3615-3630, Oct. 2022.

[74] M. Ali, A. El-Moghith, A. Ibrahim, M.N. El-Derini, and S.M. Darwish, “Wireless Sensor Networks Routing Attacks Prevention with Blockchain and Deep Neural Network,” *Comput. Mater. Continua*., vol. 70, no. 3, pp. 6127-6140, Mar. 2022.

[75] S. Rajasoundaran, S.S. Kumar, M. Selvi, S. Ganapathy, R. Rakesh, and A. Kannan, “Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks,” *Wireless Netw*., vol. 27, no. 7, pp. 4513-4534, Oct. 2021.

[76] A. Mehbodniya, J.L. Webber, R. Rani, S.S. Ahmad, I. Wattar, L. Ali, and S.J. Nuagah, “Energy-aware routing protocol with fuzzy logic in industrial internet of things with blockchain technology,” *Wireless Commun. Mobile Comput*., vol. 2022, p.7665931, Jan. 2022.

[77] P. Podili, and K. Kataoka, “TRAQR: Trust aware End-to-End QoS routing in multi-domain SDN using Blockchain,” *J. Netw. Comput. Appl*., vol. 182, p. 103055, May 2021.

[78] M. Karakus, E. Guler, and S. Uludag, “Qoschain: Provisioning inter-as qos in software-defined networks with blockchain,” *IEEE Trans. Netw. Service Manag*., vol. 18, no. 2, pp. 1706-1717, Feb. 2021.

[79] R. Gupta, S. Tanwar, and N. Kumar, “B-IoMV: Blockchain-based onion routing protocol for D2D communication in an IoMV environment beyond 5G,” *Veh. Commun*., vol. 33, p. 100401, Jan. 2022.

[80] N.K. Jadav, A. Nair, R. Gupta, S. Tanwar, and A. Alabdulatif, “Blockchain-Assisted Onion Routing Protocol for Internet of Underwater Vehicle Communication,” *IEEE Internet Things Mag*., vol. 5, no. 4, pp. 30-35, Dec. 2022.

[81] Y. Liu, J. Wang, H. Song, J. Li, and J. Yuan, “Blockchain-based secure routing strategy for airborne mesh networks,” in *Proc. 2019 IEEE Int. Conf. Ind. Internet (ICII)*, Orlando, USA: IEEE, Nov. 2019, pp. 56-61.

[82] Q. Gong, C. Zhou, L. Qi, J. Li, J. Zhang, and J. Xu, “VEIN: High scalability routing algorithm for Blockchain-based payment channel networks,” in *Proc. 2021 IEEE 20th Int. Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, Shenyang, China: IEEE, Oct. 2021, pp. 43-50.

[83] M. KARAKUŞ, “Implementation of Blockchain-Assisted Source Routing for Traffic Management in Software-Defined Networks,” *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, vol. 11, no. 3, pp. 1250-1268, 2023.

[84] H. Lazrag, A. Chehri, R. Saadane, and M.D. Rahmani, “Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks,” *Concurrency Comput. Practice Experience*, vol. 33, no. 22, p. e6144, Nov. 2021.

[85] H. Lazrag, A. Chehri, R. Saadane, and M.D. Rahmani, “A blockchain-based approach for optimal and secure routing in wireless sensor networks and IoT,” in *Proc. 2019 15th Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS)*, Sorrento, Italy: IEEE, Nov. 2019, pp. 411-415.

[86] R.M. Bhavadharini, and S. Karthik, “Blockchain Enabled Metaheuristic Cluster Based Routing Model for Wireless Networks,” *Comput. Syst. Sci. Eng.*, vol. 44, no. 2, pp. 1233-1250, Jan. 2023.

[87] W. Jerbi, O. Cheikhrouhou, A. Guermazi, M. Baz, and H. Trabelsi, “BSI: Blockchain to secure routing protocol in Internet of Things,” *Concurrency Comput. Practice Experience*, vol. 34, no. 10, p. e6794, May 2022.

[88] S. Awan, M.B.E. Sajid, S. Amjad, U. Aziz, U. Gurmani, and N. Javaid, “Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks,” in *Proc. 15th Int. Conf. Innovative Mobile Internet Services Ubiquitous Comput. (IMIS-2021),* Asan: Springer, 2022, pp. 96-107.

[89] Z. Zeng, X. Zhang, and Z. Xia, “Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks,” *Wireless Commun. Mobile Comput*., vol. 2022, p.5693962, Feb. 2022.

[90] R. Sahay, G. Geethakumari, and B. Mitra, “A novel blockchain based framework to secure IoT-LLNs against routing attacks,” *Comput*., vol. 102, pp. 2445-2470, Nov. 2020.

[91] M.A.A. Careem, and A. Dutta, “Reputation based Routing in MANET using Blockchain,” in *Proc. 2020 Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangaluru, India: IEEE, Jan. 2020, pp. 1-6.

[92] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, “A scalable blockchain based trust management in VANET routing protocol,” *J. Parallel Distrib. Comput*., vol. 152, pp. 144-156, Jun. 2021.

[93] G. Ramezan, and C. Leung, “A blockchain-based contractual routing protocol for the internet of things using smart contracts,” *Wireless Commun. Mobile Comput*., vol. 2018, p. 4029591, Nov. 2018.

[94] S.H. Awan, S. Ahmed, A. Nawaz, S. Sulaiman, K. Zaman, M.Y Ali., Z. Najam, and S. Imran, “BlockChain with IoT, an emergent routing scheme for smart agriculture,” *Int. J. Adv. Comput. Sci. Appl*., vol. 11, no. 4, pp. 420-429, Jun. 2020.

[95] S. Yan, and Y. Chung, “Improved ad hoc on-demand distance vector routing (AODV) protocol based on blockchain node detection in ad hoc networks,” *Int. J. Internet Broadcast. Commun*., vol. 12, no. 3, pp. 46-55, Aug. 2020.

[96] C. Ran, S. Yan, L. Huang, and L. Zhang, “An improved AODV routing security algorithm based on blockchain technology in ad hoc network,” *EURASIP J. Wireless Commun. Netw*., vol. 2021, no. 1, p. 52, Mar. 2021.

[97] M. Faisal, and G. Husnain, “Blockchain Based Multi-hop Routing and Cost-Effective Decentralized Storage System for Wireless Sensor Networks,” *Wireless Personal Commun*., vol. 131, no. 4, pp. 3009-3025, Aug. 2023.

[98] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel, and D. Mohaisen, “RouteChain: Towards blockchain-based secure and efficient BGP routing,” *Comput. Netw*., vol. 217, p. 109362, Nov. 2022.

[99] G. He, W. Su, S. Gao, J. Yue, and S.K. Das, “ROAchain: Securing route origin authorization with blockchain for inter-domain routing,” *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1690-1705, Aug. 2020.

[100] S. Tokunaga, S. Ohzahata, and R. Yamamoto, “A Link State Routing Method for CCN with Blockchain,” in *Proc. 2021 Ninth Int. Symp. Comput. Netw. Workshops (CANDARW),* Matsue, Japan: IEEE, Nov. 2021, pp. 49-55.

[101] X. Chen, S. Tian, K. Nguyen, and H. Sekiya, “Decentralizing private blockchain-iot network with olsr,” *Future Internet*, vol. 13, no. 7, p. 168, Jun. 2021.

[102] P.A.D.S.N. Wijesekara, “Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving,” *Open Transp. J*., vol. 16, no. 1, p. e187444782208191, Oct. 2022.

[103] H.M.D.P.M. Herath, W.A.S.A. Weraniyagoda, R.T.M. Rajapaksha, P.A.D.S.N. Wijesekara, K.L.K. Sudheera, and P.H.J. Chong, “Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies,” *Sensors*, vol. 22, no. 18, p. 6966, Sep. 2022.

[104] C. Machado, and C.M. Westphall, “Blockchain incentivized data forwarding in MANETs: Strategies and challenges,” *Ad Hoc Netw*., vol. 110, p. 102321, Jan. 2021.

[105] P.A.D.S.N. Wijesekara, “Ethical Knowledge Sharing Leveraging Blockchain: An Overview,” *Sci. Eng. Technol*., vol. 4, no. 1, pp. 112-136, Apr. 2024.

[106] C. Pu, “Energy depletion attack against routing protocol in the Internet of Things,” in *Proc. 2019 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC),* Las Vegas, USA: IEEE, Jan. 2019, pp. 1-4.

[107] C.A. Santivanez, B. McDonald, I. Stavrakakis, and R. Ramanathan, “On the scalability of ad hoc routing protocols,” in *Proc. Twenty-First Annu. Joint Conf. IEEE Comput. Commun. Soc*., New York, USA: IEEE, Jun. 2002, pp. 1688-1697.

[108] P.A.D.S.N. Wijesekara, “Network Virtualization Utilizing Blockchain: A Review,” *J. Appl. Research Electric. Eng*., vol. 3, no. 2, pp. 136-158, Oct. 2024.

[109] A. Singh, R.M. Parizi, Q. Zhang, K.K.R. Choo, and A. Dehghantanha, “Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities,” *Comput. Security*, vol. *88*, p. 101654, Jan. 2020.

BIOGRAPHY OF AUTHORS

Patikiri Arachchige Don Shehan Nilmantha Wijesekara obtained his first-class hons. B.Sc. Engineering degree specialized in Electrical and Information Engineering in 2017 from the University of Ruhuna. He has received 6 academic awards for his bachelor's degree, including 2 gold medals and 1 scholarship. He has published his research works in reputed journals and holds an H-index of 12. He received a Ph.D. degree from the same university in computer networking. He has been recruited as a lecturer at the University of Ruhuna since 2018. His research interests include networking, machine learning, and blockchain.