# A Review of SDN and Blockchain for Enhanced QoS and Security in P2P Multimedia Networks

Given Name Surname
*Department. name of organization*
*University name*
*City, Country*
{email address or ORCID}

Given Name Surname
*Department. name of organization*
*University name*
*City, Country*
{email address or ORCID}

***Abstract:*** **A single node in a "peer-to-peer (P2P)" network functions has both a producer and a consumer by sharing resources including bandwidth, storage, and processing power. Despite their proven scalability and resilience, they face numerous managements, resource synchronization, and security challenges because they are inherently decentralized and can withstand failures in a global context (resilience) as well as failures in individual nodes (scalability). Considering the P2P architecture's propensity for unwanted access, possible data breaches, and attack weaknesses, security continues to be a major concern. Security is important, but teamwork is also required to ensure efficiency and consistency using techniques like Distributed Hash Tables (DHT). Combining blockchain technology with Software-Defined Networking (SDN) is one possible strategy to overcome these issues. Few studies have looked into combining the two for P2P applications, despite the fact that both strategies have been portrayed as comprehensively helpful across domains like cloud computing, secure video streaming, and the Internet of Things. The recent research on SDN-blockchain systems in P2P multimedia networks to enhance security and quality of service is the main objectives of this review (2022–2025). In recent years, "software-defined networking (SDN)" and Blockchain technology have emerged as different solutions to overcome the limitations of traditional P2P frameworks. Separate Research is also being done on block chain's potential for secure video streaming. With features like smart contracts and cryptographic verification, Decentralized technology provides a decentralized, immutable ledger that improves security, trust, and transparency. No thorough study has yet to integrate SDN and Blockchain specifically to address the particular difficulties of P2P streaming systems, despite the fact that previous research has examined the two technologies independently for general IoT or resource management. Blockchain increases tamper-resistance, transparency, and trust in distributed scenarios, SDN also provides centralized programming and visibility for network resource management. The potential of SDN and blockchain applications in cloud computing and the Internet of Things is demonstrated by earlier studies.**

***Keywords: SDN (software defined networking), Blockchain, P2P (Peer to Peer networking), Iot networks, Vanet.***

## 1. Introduction

P2P (peer-to-peer) multimedia streaming is important because it offers improved scalability by offloading delivery to users, reduces costs for content providers by leveraging user bandwidth, and provides better resilience to traffic spikes compared to traditional server-based models. This decentralized approach enhances the overall user experience by improving performance through faster distribution and lower latency, making it more cost-effective and efficient for distributing large volumes of video content [1, 2]. In a p2p network, scalability is one of the most important one, each user becomes a small distributor, allowing a streaming platform to scale to millions of viewers without proportionally increasing central server capacity. Cost reduction and resilience also important for p2p network. Cost reduction is also significantly reducing their dependence on costly content delivery networks and infrastructure [6]. Peers efficiently can exchange content segments, minimizing content and optimizing network utilization which can benefits both users and also content providers [3]. In (P2P) have some obstacles due to their varying bandwidth and uptime. Potential security flaws, the difficulty of finding compatible peers, maintaining quality consistency in the face of peer turnover, and the effect of Internet Service Provider (ISP) filtering and limitations on P2P traffic are further concerns [4, 5]. Blockchain implementation employ cryptographic techniques to protect the integrity and secrecy of transaction data that is locally held on several nodes in a peer-to-peer network [7].Since blockchain systems function has a peer-to-peer (P2P) network where nodes lack mutual trust, the first transaction needs to be finished in front of every node in the network [8]. In a peer to peer network, every node has two keys of different kinds. A public key is used for other nodes to encrypt their message, while the private key is used to decrypt the received message [9]. Peer and network related challenges are the other obstacles of P2P networks. Peers behind firewalls or network addresses translator are frequently inaccessible. This increases complexity and delay [10]. Peer turnover and uptime is also a challenge in this, the system has continuously discovered new supplying

peers, because, peers enters and exit the networks at erratic rates, which can interfere with streaming. A distributed software-defined networking (DSDN) architecture with a blockchain backbone will allow reliable, scalable, and secure P2P video streaming [43]; however, high service quality can be difficult to sustain in a dynamic network where users' capabilities and varying network conditions frequently update. P2P networking with Blockchain and SDN (Software Defined Networking) provide network management and control in which the data plane and control plane are separated. The laptop, on the other hand, stores data and transactions in a decentralized, secure, and unchangeable ledger [11, 12, 21–23].Network-based communication and structures that utilize the newest technology developments are used into blockchain and highlight the need to optimize the network [49]. Blockchain can also provide solutions on a network level to challenges such as: DDoS attacks; detecting and preventing intrusions; and securing routing protocols of SDN [54]. Together, both SDN and blockchain create invaluable solutions for complex network infrastructures like the next generation networks to improve decentralized control and apply verification policies using smart contracts to applications like a network of things (or IoT). By understanding and implementing the modular frameworks, we can develop a viable IoT-Edge-Cloud platform can successfully allocate resources and scale to handle multiple applications [37].Flexible and adaptable 6G TestBeds with a focus on Digital Twin applications are needed to support new and changing industrial and real-time requirements. Software-defined networks (SDNs) allow for automation and a dynamic configuration perspective from a single interface. Compared to traditional networks, SDNs provide enhanced network flexibility, agility, and centralized management.

In research paper [56] Blockchain and P2P networking for multimedia streaming is a fusion of two decentralized technologies to create more efficient, secure and fair content delivery system [13]. P2P networks are useful for file sharing, content distribution, and other purposes. Since P2P networks don't have a single point of failure, they are more resilient than traditional client-server networks [14]. It removes the need for a control server or authority, allowing users to stream and share content directly through the networks. After the P2P controller receives the request, the file classifier and routed of the controller [38] will send the file information to the user using a strategy similar to ONU. After extracting the package's filename, the P2P controller will request user authentication. The purpose of this study is to deliberately review SDN and blockchain for improved security and quality of service in peer-to-peer multimedia networks. We examine pertinent research from 2022–2025, concentrating on different scheduling strategies and the critical factors affecting their efficacy. The following describes this investigation's main objectives.

- Improves the quality of audio and video through reduced lag and buffering. It also prevents user data from being hacked or manipulated.
- Software Defined Networking (SDN) allows for centralized management and control of the network without needing a central authority to trusted dynamics between users. Smart contracts in blockchain can automate rules and agreements between users.
- Combining SDN and blockchain enhances both the performance and security of P2P multimedia networks.
- It is useful for ensuring user identity, data security, and transparent transactions.

### 1.1 Research gap

In this section, we have described about the overall problem statement;

- Scalability Limitations: While P2P is naturally scalable, maintaining efficient communication and resource allocation in large, dynamic networks is challenging.
- Consensus Mechanism Challenges: Energy-intensive consensus methods like Proof of Work (PoW) increase computational and power costs.
- Cloud Security Challenges: Cloud computing still faces privacy, compliance, compatibility, control, and reliability issues that the proposed system does not fully solve.
- Complexity of Integration: Establishing and maintaining the virtual communication layer between SDN and blockchain adds architectural complexity.
- Generalizability Issues: Effectiveness may vary depending on IoT device heterogeneity, network conditions, and application contexts.

### 1.2 Objectives

The main objectives of this research are shown in below,

- In this paper, first, we have reviewed about P2P (Peer to Peer) and how it works on several industries.
- At second, we have noticed about SDN (Software defined networks) in p2p streaming and how it enhanced the quality of streaming.
- At thirdly, we have reviewed about Blockchain in P2P streaming and its security of p2p networks.
- To look into how latency, scalability, and privacy concerns might be resolved by combining SDN and Blockchain.
- To ascertain the traditional P2P multimedia networks' QoS and security limitations.
- To evaluate current SDN and blockchain-based methods for safe and effective P2P multimedia streaming.
- To suggest a conceptual paradigm for improved multimedia delivery that combines SDN and Blockchain.

## 2. Background/Technical foundation

### 2.1 p2p multimedia streaming

Peer-to-peer (P2P) video streaming struggles to meet its goals of low latency, better QoS (Quality of Service), and scalability because of the decentralized and dynamic nature of peer networks [28,29,39,40]. Some solutions include physical-topology-aware overlay networks for reduced data transfer latency, adaptive algorithms for neighbor selection and buffering, Scalable Video Coding (SVC) to adapt quality to peer capabilities, and P2P video integration with cloud services or edge computing for hybrid approaches that offer stability and flexibility [18, and 42, 53]. Difficulties Latency refers to Network congestion, ineffective routing, and sluggish peer discovery can all have an impact on the duration of the data's journey from the source to the recipient. When live streaming, the term Quality of Service (QoS) presents particular challenges [77].The effectiveness of the streaming service may be impacted by problems with monitoring systems that check bandwidth, such as errors or malfunctions. Lower QoS can also result from abrupt changes in network traffic or unpredictable peer behavior [41], which explains it could be challenging to ensure a steady and excellent viewing experience in P2P networks because of peer heterogeneity, varying network conditions, and low dependability. Blockchain technology has the potential to improve cellular networks' trust in addition to their security. Blockchain-based systems' transparency makes it possible to keep tamper-evident records of every network transaction. Exchanges [19, 63]. Maintaining effective communication and resource allocation in a large and dynamic P2P network can be difficult, particularly when it comes to live streaming, even though P2P by nature offers strong scalability by utilizing a large number of peers. Swarm effectively combines the affordability of a decentralized P2P network with the resilience of a traditional CDN. P2P systems can also be thought of as [73], streaming applications that use event detection techniques to locate a new peer in the network. Its main goal is to minimize traffic costs while offering users dependable streaming quality [75]. Using a summary of the most recent developments in P2P trade, the different P2P energy operational algorithms were trading along their features, standards, and scope in detail [32, 33, 35, 44, 45, and 68]. Prior research has created strategies for content replication incentives and hybrid “content delivery networks-P2P (CDN-P2P)” networks in the context of P2P video streaming [30, 34]. These provided increases in throughput and a slight decrease in streaming latency for multimedia. By introducing FRING [36], the initial geographically oriented P2P overlay network that provides blockchain systems with dependable and quick broadcasting. Through the efficiency of broadcast message delivery and convergence time, FRING improves the overall throughput of blockchain systems, albeit at the expense of some robustness. Evaluations and efficiency demonstrate that FRING is incredibly secure, resilient, and efficient.

### 2.2 Software Defined networking

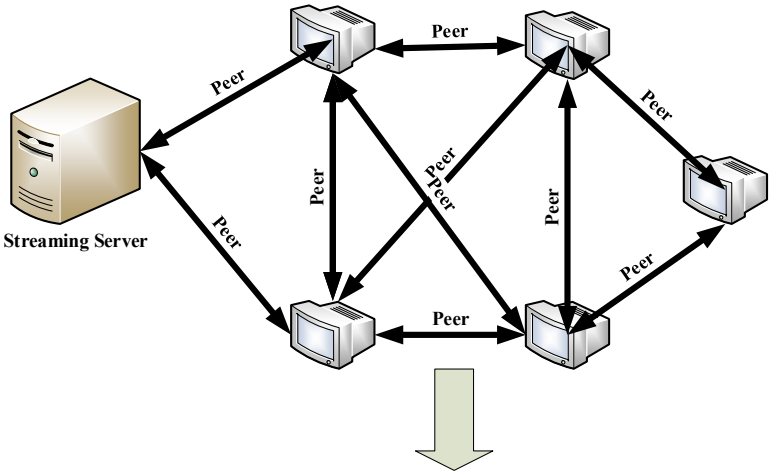
SDN can be used to manage peer-to-peer (P2P) networks, like a central controller that controls the flow of data. Alternatively, SDN controllers can be built with P2P-like control architecture to get around the problems of scalability and availability that come with having one central SDN controller. The first method aims to improve P2P networks through central control, while the latter shares the control plane role amongst several interconnected SDN controllers [20]. By controlling data flows and protocols, a software-defined networking (SDN) controller will serve as the sole point of contact for managing and keeping an eye on the P2P network. By making wise choices, the controller can reroute traffic, minimize congestion, and maximize network resources. When the utility can see the topology, it has an advantage. Software-Defined Networking (SDN) has

a lot to offer peer-to-peer (P2P) networks. Improved traffic control, scalability, and resource management are among the advantages, along with simpler operations and programmatic flexibility that can be adjusted to P2P environment changes. A number of ingression combinations are investigated in a typical SDN scenario. The ingress-egress pair represents a predetermined source and destination that traffic can walk through. The traffic that can be routed as a tunnel between the ingress-egress pair is represented by each video connection request in this case. The SDN controller performs routing in order to enhance "Quality of Service (QoS)". [80] The QSroute network design deploys several programmable functional modules on the SDN controller by utilizing the benefits of SDN centralized control. [76, 79] SDN makes P2P the investigation of the utilization of peer-to-peer network applications over an SDN-based network has explored the bandwidth and latency concerns [78]. The results indicated data distribution and sharing were more efficient when control was centralized and network features were turned into software. This enabled more intelligent traffic routing, automatic policy enforcement, and faster service deployment. The deep learning (DL) and machine learning (ML) models in two datasets with an SDNIoT focus. The efficient multiclass classification of network attacks in IoT networks; it combines an LSTM-based architecture [57, 58]. The P2P nature of the blockchain eliminates a single point of failure, preserves data security and integrity, and opens the door for the SDN controller to use blockchain features. In a cluster domain, it keeps IoT devices connected P2P [24, 25, 46].Despite assuming on SDN's efficacy in IoT contexts, the suggested solutions rely on a centralized architecture-based SDN approach. Although this strategy encourages network management, it severely restricts the infrastructure's scalability and resiliency [26]. Network programmability, a concept unique to SDN, exhibits strong performance in terms of scalability, flexibility, and programmability [27].

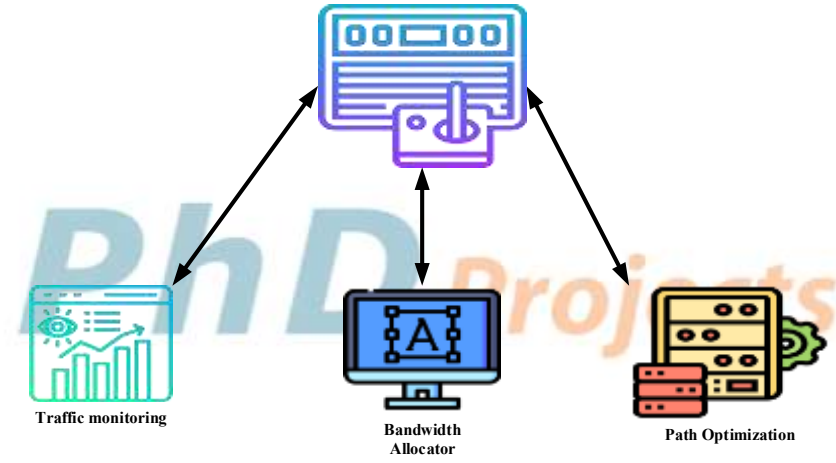
### 2.3 Blockchain in networking

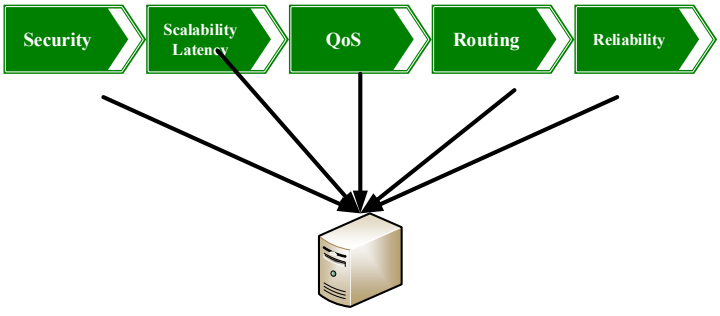
Blockchain, a decentralized technology that enables transactions to be recorded on a distributed, shared ledger without the need for middlemen, relies on peer-to-peer (P2P) networks. In the peer-to-peer (P2P) network of a blockchain, each and every node has a copy of the entire ledger and connects directly to confirm transactions by consensus. This distributed and collaborative approach ensures data security, transparency, and integrity while also making the system resistant to manipulation and limited points of error. P2P networks distribute data among a network of connected devices (nodes), doing away with central authorities in contrast to conventional client-server models. Each node in the P2P network keeps an up-to-date, complete copy of the transaction ledger on the blockchain. Including user accounts and balances. Sufficient redundancy guarantees the operational stability of blockchain nodes [50, 52]. DDS enables data sharing among parties in Dataspace 4.0 without the need for centralized control enhancing aspects, like data security, privacy, collaboration, and economic opportunities [66]. In figure 1, we have explained how p2p, SDN and Blockchain works given that all devices in the blockchain network are trusted; every transaction of data will require consensus approval to take place. In IoT networks, devices can create an authenticated connection to blockchain applications by generating a shared key amongst entities [55]. Each transaction block must first receive a majority agreement in the network, providing valid constraints for nodes to achieve consensus to add new transactions to the blockchain.

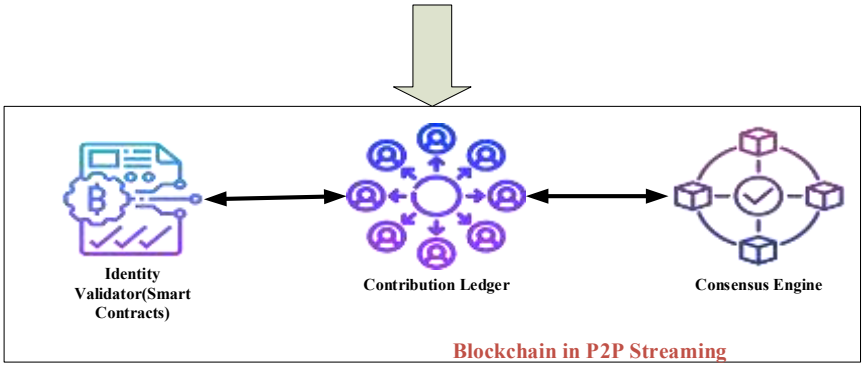
P2P Streaming




SDN in P2P Streaming




Blockchain in P2P Streaming

Figure 1: P2P, SDN and Blockchain in streaming.

## 3. Literature Review

### 3.1 SDN in P2P Streaming

In this section, we have reviewed about SDN in P2P streaming and how the SDN contributions takes place in P2P streaming. We have categorized this review as three sections such as SDN in P2P Streaming, Blockchain in P2P Streaming and SDN & Blockchain in other contexts. At first, we reviewed SDN in P2P live video Streaming [71], in this section; the author has proposed a unique method for effective bandwidth control for peer-to-peer applications that makes use of the Random Forest algorithm [70]. This method calculates and forecasts the bandwidth consumption of various applications. By offering programmability modules for system manipulation, software-defined networking enables administration flexibility and control. To create a functional network in SDN, network monitoring is crucial. Every issue that has arisen needs to be tracked and managed [15]. Data forwarding is handled by the information plane, which is the lowest layer of the SDN architecture. On the other hand, the SDN system's central component is the control plane. It has the ability to dynamically update forwarding rules, manage network resources, and create agile and flexible configuration [64]. To identify and lessen security threats on SDN planes, various techniques and systems have been studied. Peer-to-peer (P2P) networks of microcontrollers allow rapid sharing of the information between industrial robots and enable a real time change in the manufacturing processes because Centralized control, programmability, and flexibility are made possible by the separation of the control and data planes. However, communication problems between these various planes also create vulnerabilities. However there are also limitations in this approach as the computational cost can be lower because the decision trees are not balanced. In the scenario where Random Forest is applied, the unification costs of ensemble techniques which were ignored from the theoretical cost analysis because they are negligible to become very considerable and make up the bulk of the total cost.

### 3.2 Blockchain in P2P Streaming

In this section, we gathered about BlockChain in P2P Streaming and how it works and performance in streaming [48]. The Author proposes. The combination of Network function virtualization and software-defined networking show promise as a defense against IoT cyberattacks. 6G technology was included in the suggested solution to provide higher security and faster connectivity. The scalability of the suggested secure blockchain [61, and 62] communication method is tested by analyzing different dataset sizes based on node-to-node transactions. On edge computing, the proposed VNFSDN was put into practice. The results show that VNFSDN is a viable strategy for improving the performance and scalability of network security [16]. The proposed VNFSDN exhibits a lower reaction and packet loss rate, in addition to other advantages. The results may not apply to all scenarios, though, due to the constraints of the proposed work, which include the fact that each scenario was carried out in a particular setting and context. One example of a centralized P2P network is a blockchain network, where all peers are anonymous, and energy-efficient consensus methods, like "proof of work (POW)," are utilized to maintain the network [74]. Besides, VNFSDN will not fit every case of network security and performance problems due to other factors to think about such as costs, scalability, or ease of deployment.Blockchain architecture contains transactions that are created and shared by every system in the network. The blockchain, based on its type, provides there is a consensus process on each network node. Before the previous chain is added, a process such as "Proof of Work (PoW)," "Proof of Stake (PoS)," or "Proof of Authority (PoA)" is added to the chain [60] to verify and validate the transactions in that block.

### 3.3 SDN + Blockchain in Other Contexts

In this section, we have reviewed about, How SDN and Blockchain contributed in other contexts. The author introduces architecture for improved the name for DistB-SDCloud provides cloud security for intelligent IIoT applications. The distributed BC technique used in the suggested architecture ensures security features and guarantees of confidentiality, privacy, and integrity while offering flexibility and scalability. It enables users to upgrade resources quickly, in contrast to outdated hardware-based computer systems that took a long time to do

so. Among the services provided by cloud computing are "Software as a Service (SaaS)," "Platform as a Service (PaaS)," and "Infrastructure as a Service (IaaS)."In essence, this is a network-dependent application where sensor devices are used to accomplish most of the work; the architecture generates a hash value to secure the data sent through the structure. IoT sensor data can be converted from the sensor level to the SDN environment with the help of an SDN-intelligent gateway [47]. It is becoming more and more important to secure and manage the massive volumes of data generated by IoT devices as they are incorporated into more and more services and daily activities. SDN has become a viable way to control the network traffic produced by Internet of Things devices [59, 65, and 67]. In order to improve the security of SDN-based IIoT architecture; this study makes use of blockchain and CNN-based IDS as complimentary elements. As centralized technologies offers a secure and reliability for data sharing and managing reliability trust, SDN's programmability, centralized controller and holistic view of the network make it a crucial component for securing IIoT [69]. SDN is a proper control mechanism of all filtered data after filtering the data and BC [17]. Additionally, the SDN environment and the BC approach are connected via a virtual communication layer. It combines two cutting-edge technologies, SDN and BC [51], to optimize cloud computing infrastructure security and efficiency. Among the most popular topics of IoT research are privacy and security. Cloud computing does however; face a number of security risks, issues, and difficulties, such as privacy, compliance, compatibility, control, and reliability issues.

## 4. Taxonomy

In this section, we have given the diagrammatic structure for P2P (Peer to Peer) networks, SDN (Software defined networking) and Blockchain. This diagram shows the technologies used in p2p networks, how SDN performed in p2p and Blockchain in p2p, and then both were integrating in p2p streaming networks. The security, quality of service, and coordination of typical P2P networks are inadequate, even though they are resilient and scalable. SDN-based approaches improve traffic control and resource allocation, but they create a central control bottleneck and lack peer-level trust. Taxonomy of p2p Networks is presented figure 2, which explained through a diagrammatic view of how the technologies were used in SDN, P2P and Blockchain. Although blockchain-based solutions have high overhead, latency, and scalability issues for real-time streaming, they ensure decentralized trust, transparency, and resistance to tampering. Blockchain and SDN integration combines the security of blockchain with the programmability of SDN to enhance QoS and fortify protection in P2P multimedia networks.

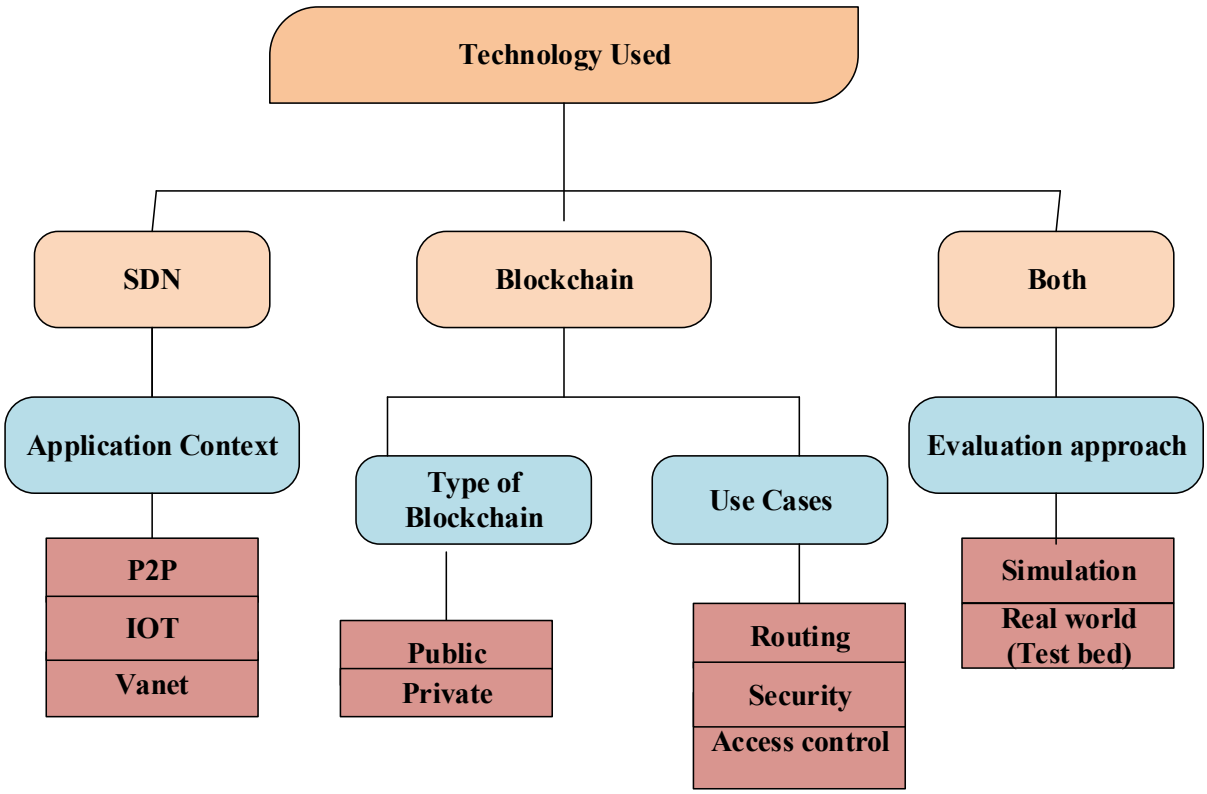



Figure 2: Taxonomy of p2p Networks

## 5. Comparative analysis

In this section, we have given the comparative analysis table for P2P Streaming. In table 1, described about the usage of p2p, SDN and Blockchain contributions and limitations. The Traditional P2P networks provide scalability and resilience but suffer from weak security, poor QoS, and inefficient coordination. SDN-based approaches improve traffic management and resource allocation but create a central control bottleneck and lack peer-level trust. Blockchain-based solutions ensure decentralized trust, transparency, and tamper resistance, yet face challenges of latency, high overhead and limited scalability for real-time streaming.

**Table: 1** The comparative Analysis of P2P, SDN and Blockchain from existing research.

| YEAR | USAGE | MAIN CONTRIBUTIONS | LIMITATIONS |
|---|---|---|---|
| Khacef, K., et al., (2024) | Blockchain | • SecuSca: new blockchain system architecture.<br>• Designed for P2P streaming. | • Each node needs storage space to maintain streaming privacy.<br>• SecuSca architecture avoids replicating blocks across the entire network. |
| Yu, C., et | | • Security of cryptocurrencies is analyzed from multiple perspectives using the | • Security is unclear and protocol is different.<br>• Some cryptocurrency protocols |

| | | | |
|---|---|---|---|
| al.,(2022) | Blockchain | proposed framework<br>• Blockchain technology platforms' technical assistance is taken into account. | are not open source, so protocol differences can't be compared. |
| Dua, A. (2023). | Peer to Peer | • Analog communication, basic voice services.<br>• Digital communication, GMSK modulation, SMS introduced.<br>• Higher data rates, QPSK modulation, support multimedia.<br>• High-speed internet, OFDM modulation, IP-based services.<br>• Ultra-low latency, massive IoT support, QAM & advanced | • The level of security have not improved.<br>• Complete decentralization not achieved. |
| Latif, S. A., (2022) | SDN(Software-Defined Networks) | • Personalized decentralized-based SDN controller architecture for IoT networks.<br>• Secure energy-sensitive SDN cluster structure and Supports file transfer among IoT devices. | • Negative impact on IoT network communication.<br>• Energy optimization is affected.<br>• Consensus protocol adds computational complications. |
| Ibrahim, R. F., (2022) | Blockchain | • Track malicious IoT device IPs.<br>• Store IPs in blockchain.<br>• Prevent malicious connections. | • Centralized systems face scalability limitations.<br>• Decentralized systems offer limited scalability. |
| Alsamhi, S. H., (2024) | Blockchain | • Novel framework integrates FL, blockchain, P2P networks, semantic webs, and decentralized file systems combine to create a coherent DDS environment.<br>• Ensures privacy, security, accessibility, and interoperability in data management. | • Use cutting-edge tools: edge computing, distributed ledgers, semantic web.<br>• DDS development and deployment can be complex.<br>• Complexity poses implementation challenges. |
| Al Ghamdi, M. A. (2022). | Blockchain and SDN(Software-Defined Networks) | • Sdn-Blockchain Classifier outperforms baseline in energy is used and end-to-end latency.<br>• SDN-Blockchain IoT framework offers better performance.<br>• Outperforms traditional blockchain. | • Plan to develop architecture's functionality.<br>• Implement suggested architecture.<br>• Target large-scale, real-world scenarios in future research. |

phdprojectsorg@gmail.com
+91 98946 59122

| | | | |
|---|---|---|---|
| Zhao, S., (2023) | Peer to Peer | • Group signature and secret sharing scheme permits permission control and data access in IoT multi-device settings.<br>• IoT environment ensures high communication efficiency. | • Scheme not demonstrated.<br>• Scheme remains unclear and hard to understand. |
| Peng, S., (2023) | Blockchain and SDN(Software-Defined Networks) | • SDN-based IIoT system proposed.<br>• Combines benefits of SDN and IIoT.<br>• Improves flexibility and scalability.<br>• Addresses security concerns. | • Use balancing methods to improve classification metrics.<br>• Explore alternative algorithms for better performance.<br>• Implement multi-controllers to prevent system bottlenecks. |
| Pakpahan, A. F., (2024) | SDN(Software-Defined Networks) | • Proposed architecture integrates advanced P2P-FL.<br>• Uses an enhanced and dedicated P2P transceiver.<br>• Optimizes network resources. | • Develop practical hardware and software solutions.<br>• Demonstrate real-world potential.<br>• Address security challenges.<br>• Improve scalability.<br>. |
| Farahani, R. (2024) | SDN(Software-Defined Networks) | • Make use of edge computing tools.<br>• Proposed a hybrid P2P-CDN framework for live video streaming.<br>• Improve Quality of Experience (QoE) | • System does not use edge-supported methods.<br>• System doesn't utilize peers computational resources.<br>. |
| Nakakaze, O., (2024) | SDN(Software-Defined Networks) | • Introduce a new concept for industrial retrofitting.<br>• Develop a prototype implementation.<br>• Use lightweight web technologies.<br>• Deploy at the edge for efficiency.<br>. | • Communication over WiFi can be erratic.<br>• Caused by capacity issues.<br>• Problem occurs when root node connects to external network. |
| Bellaj, B., (2022) | Peer to Peer | • Model the peer selection process as a reinforcement learning problem.<br>• Apply Multi-Armed Bandits (MABs) framework.<br>• Continuously evaluate peers' performance.<br>• Identify the fastest peer for downloading | • Negative integration observed between variance and the number of peers.<br>• Data remains ambiguous.<br>• Suggests solution may scale effectively with more peers.<br>• Variance relationship needs further investigation. |

phdprojectsorg@gmail.com
+91 98946 59122

| | | | |
|---|---|---|---|
| Rodríguez-Sela, F., (2025) | Blockchain | • Decentralized P2P networks used for computing tasks.<br>• Provide enhanced security.<br>• Ensure greater transparency. | • Adversarial behavior in the real world could exhibit more intricate and dynamic patterns. |
| Wei, D., (2024) | Peer to Peer | • Peers create distributed content-sharing framework.<br>• Swarm system introduced.<br>• Conventional CDN capabilities integrated. | • Cost-effective challenges.<br>• Bandwidth challenges.<br>• Bandwidth is variable.<br>• Bandwidth is inadequately available |
| Makris, A., (2022) | SDN(Software-Defined Networks) | • Improved resource management protects the network.<br>• Ensures no compromise on QoS.<br>• Software-defined networking is one of the latest technologies.<br>• A centralized view of network resources is offered by SDN. | • QSroute balances measures according to relative importance.<br>• Considers specific requirements.<br>• Trade-offs adds complexity to protocol design. |
| Almakdi, S., (2023) | SDN(Software-Defined Networks) | • 5G + SDN improve scalability and effectiveness.<br>• SDN increases 5G reliability.<br>• Achieved by separating control plane from data plane. | • Lower system overhead while maintaining efficacy. Identify real-world traffic backdrops.<br>• Improve overall performance.<br>• Enhance system generalization. |
| Aldabbas, H. (2023) | SDN(Software-Defined Networks) | • DN controller creates new guidelines for every communication.<br>• P2P protocols deployed in the system.<br>• Enable fast content propagation.<br>• Operate over a layered architecture. | • High computational cost in input space.<br>• Increased complexity in input space.<br>• Neglect of nodes and child nodes.<br>• Leads to an unbalanced strategy. |
| Samadi, R., (2023) | SDN(Software-Defined Networks) | • SDN architecture forms clusters.<br>• Discovers transmission routes.<br>• Manages network topology changes from node mobility. | • No packet-controlling mechanism considered.<br>• Clustering causes high overhead.<br>• Leads to increased energy consumption. |

| | | | |
|---|---|---|---|
| Wang, Z., (2024) | SDN(Software-Defined Networks) | • Developed IFRA-GLB algorithm.<br>• Based on intelligent fuzzy reinforcement learning.<br>• Ensures stable video conferencing connections.<br>• Operates under latency and bandwidth constraints. | • Future studies can advance SDN-based video conferencing.<br>• Aim for more reliable communication.<br>• Provide greater efficiency.<br>• Ensure enhanced security. |

### 5.1 Research challenges

In this section, we discussed about the challenges.

- **Computational and scalability issue:** A significant challenge arises from the aggregation of predictions across multiple trees, which, while often overlooked in theory, can dominate the computational cost in practice. Scalability becomes an issue as storage needs increase exponentially with tree depth, placing a heavy burden on system resources. The unification cost of ensemble methods, which is typically considered to be negligible, becomes substantial in cases where Random Forests are highly successful. One significant drawback of unbalanced trees is that while they lower processing costs for individuals, they lose this advantage for large ensembles. Memory consumption is a drawback, especially in cases where the trees are deeper, restricting the applicability of the method in resource-constrained environments. Even though the model is theoretically efficient, the practical performance of the method suffers as prediction aggregation and memory cost have clear ramifications on all its efficiency. In practice, these limitations affect the viability and the efficiency of the utilization of our technology and thus should be dealt in a reasonable manner.
- **The problem of generalizing:** This problem pertains to network effectiveness in many contexts since the results of each study may vary depending on the particular circumstances in which each experiment was carried out. One problem is that the findings could not be applied to every real-world situation. This may not be the best solution for every network security or performance problem, despite its advantages. Cost, scalability, and ease of deployment are some of the most important factors to take into account while selecting the optimal approach. Depending on the situation, it can actually need major changes in its current form to attain optimal efficiency in larger or more complex deployments.

- **Further complicating Effects and Growing Demand:** The sudden increase in demand for cloud computing services, together with other contemporary trends like the Industrial Internet of Things (IIoT), has made things more difficult. Cloud infrastructures that are dependable, scalable, and secure are in high demand due to the market's oversupply of linked devices and clients. Last but not least, despite significant advancements, cloud computing still has significant security issues, especially when it comes to user control, privacy, data protection, regulatory compliance, system interoperability, and general dependability. These issues have a major influence on how widely and securely cloud services are accessible in IIoT environments. Many recommendations have been proposed by researchers as ways to address these security concerns, but many of the proposed solutions are often inadequate and/or lack situational specificity, therefore, an adequate solution that provides extensive protection in large-scale and dynamic environments remains elusive.

### 5.2 Future Research

This section will describe the findings and the opportunities for future research; these opportunities include:

- In the future, studies should aim at developing and running lightweight consensus protocols in the SDN control plane that can work on “Delegated Proof-of-Stake (DPoS)”, “Practical Byzantine Fault Tolerance (PBFT)”, etc.
- Secure and fast routing decisions would be possible without affecting network responsiveness.

- Making use of consortium blockchain: While allowing for regulated participation, private and consortium blockchain designs offer superior scalability and consensus. Future research should examine their application in multimedia networks where maintaining quality of service and protecting sensitive data require regulated participation and fast response times.
- Intelligence-Enhanced SDN Controllers: Adaptive network management has improved in intelligence and skill because SDN controllers employ AI and machine learning. AI-powered SDN control protocols that can detect abnormalities, predict traffic, learn from traffic, and re-optimize routing routes in real-time human activities should be the main focus of future research. These protocols will improve the quality of service and security. Researchers can test different control methods, simulate demanding multimedia streaming workload models, and assess performance metrics for individual models across a range of networks.
- Hybrid Edge-Cloud testbed. Again, within these testbed, it will become easier to explore by experimenting with decentralized and distributed elements across the cloud and edge.

## 6. Conclusion

The two technologies - the decentralized, immutable ledger capabilities of blockchain for authentication, data integrity, and trust, and the centralized control of software-defined networking (SDN) to provide effective traffic management - work together to significantly enhance QoS and security in P2P multimedia networks. While blockchains can serve as a simple and tamper-proof authority, SDNs focus their attention on dynamic flow control and performance concerns, such as management of congestion. Cited avenues for further research from this study included controller vulnerability issues, integration, standardization and regulatory/legal implications, but combining the two technologies has the potential to create a more robust, scalable and secure system. By removing the reliance on a centralized server, the blockchain paradigm builds user trust and ensures their data remains immutable or trustworthy. These two separate entities come together with an intelligent, adaptable, and secure network environment. However, both blockchain technology and SDN are still developing; together they can serve as a potential ideal methodology for multimedia broadcasting and sharing in a decentralized and P2P environment. This will enhance the blockchain technology for discovery, distribution, and communication for P2P-P2P multimedia networks. Peers represent both clients and servers in P2P multimedia networks, giving users decentralized, scalable, reliable systems and effective resource use. However, Quality-of-Service (QoS) management in delay-sensitive content delivery, resource sharing, and data search processes is continuously hampered by peers that prioritize their own interests. Distributed Hash Tables (DHT), mesh-based overlays, network coding techniques to improve resource efficiency and data accessibility, and application support for file sharing, multimedia distribution, and streaming are the three primary components of the system that solve these issues. The SDN and blockchain platforms require improvements in their scalability and latency performance to enable support for live streaming video applications. However, we will not be able to measure the efficacy of any mechanisms using P2P network data. The development of new technologies depends on establishing proper governance systems. In order to reduce operating costs and power consumption in large network systems, scientists must continue to explore novel techniques. By utilizing SDN and blockchain technologies, this study seeks to provide real-time video streaming with enhanced scalability and operational efficiency.

## Reference

1. Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., & Ullah, S. S. (2023). A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*, *11*, 10995-11015.
2. Gupta, N., Maashi, M. S., Tanwar, S., Badotra, S., Aljebreen, M., & Bharany, S. (2022). A comparative study of software defined networking controllers using mininet. *Electronics*, *11*(17), 2715.
3. Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient secure routing mechanisms for the low-powered IoT network: A literature review. *Electronics*, *12*(3), 482.
4. Yadav, A. K., Singh, K., Amin, A. H., Almutairi, L., Alsenani, T. R., & Ahmadian, A. (2023). A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Computer Communications*, *201*, 102-115.

5. Rahman, A., Montieri, A., Kundu, D., Karim, M. R., Islam, M. J., Umme, S., ... & Pescapé, A. (2022). On the integration of blockchain and sdn: Overview, applications, and future perspectives. *Journal of Network and Systems Management*, *30*(4), 73.
6. Siddiqui, S., Hameed, S., Shah, S. A., Ahmad, I., Aneiba, A., Draheim, D., & Dustdar, S. (2022). Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects. *Ieee Access*, *10*, 70850-70901.
7. Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., ... & Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access*, *10*, 96538-96555.
8. Zuo, Y., Guo, J., Gao, N., Zhu, Y., Jin, S., & Li, X. (2023). A survey of blockchain and artificial intelligence for 6G wireless communications. *IEEE Communications Surveys & Tutorials*, *25*(4), 2494-2528.
9. Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and blockchain: a comprehensive survey on security, integration strategies, applications and future research directions. *Big Data and Cognitive Computing*, *8*(12), 174.
10. Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A review of security issues when integrating IoT with cloud computing and blockchain. *IEEE Access*.
11. Velasquez, W., Moreira-Moreira, G. Z., & Alvarez-Alvarado, M. S. (2024). Smart grids empowered by software-defined network: A comprehensive review of advancements and challenges. *IEEE Access*, *12*, 63400-63416.
12. Chen, C., & Quan, S. (2022). A summary of security techniques-based Blockchain in IoV. *Security and Communication Networks*, *2022*(1), 8689651.
13. Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-preserving and security in SDN-based IoT: A survey. *IEEE Access*, *11*, 44772-44786.
14. Yang, H., Pan, H., & Ma, L. (2023). A review on software defined content delivery network: a novel combination of CDN and SDN. *IEEE Access*, *11*, 43822-43843.
15. Aldabbas, H. (2023). Efficient bandwidth allocation in SDN-based peer-to-peer data streaming using machine learning algorithm. *The Journal of Supercomputing*, *79*(6), 6802-6824.
16. Razaque, A., Yoo, J., Bektemyssova, G., Alshammari, M., Chinibayeva, T. T., Amanzholova, S., ... & Umutkulov, D. (2023). Efficient internet-of-things cyberattack depletion using blockchain-enabled software-defined networking and 6G network technology. *Sensors*, *23*(24), 9690.
17. Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, *9*(2), 411-421.
18. Pakpahan, A. F., & Hwang, I. S. (2024). Peer-to-peer federated learning on software-defined optical access network. *IEEE Access*, *12*, 84435-84451.
19. Song, L., Hu, X., Zhang, G., Spachos, P., Plataniotis, K. N., & Wu, H. (2022). Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal*, *9*(20), 20352-20381.
20. Rani, S., Babbar, H., Srivastava, G., Gadekallu, T. R., & Dhiman, G. (2022). Security framework for internet-of-things-based software-defined networks using blockchain. *IEEE Internet of Things Journal*, *10*(7), 6074-6081.
21. Hassan, H. A., Hemdan, E. E., El-Shafai, W., Shokair, M., & El-Samie, F. E. A. (2023). Intrusion detection systems for the internet of thing: a survey study. *Wireless Personal Communications*, *128*(4), 2753-2778.
22. Gupta, A., & Lakhwani, K. (2025). Enhancing blockchain quality-of-service: a comparative analysis and novel smart contract mechanism. *Discover Applied Sciences*, *7*(8), 1-26.
23. Hirsi, A., Alhartomi, M. A., Audah, L., Salh, A., bin Mad Sahar, N., Ahmed, S., ... & Farah, A. (2025). Comprehensive analysis of ddos anomaly detection in software-defined networks. *IEEE Access*.
24. Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A., ... & Maiwada, U. D. (2024). Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. *IEEE access*, *12*, 51630-51649.
25. Latif, S. A., Wen, F. B. X., Iwendi, C., Wang, L. L. F., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer communications*, *181*, 274-283.
26. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, 103414.
27. Fu, H., Sun, M., He, B., Li, J., & Zhu, X. (2022). A survey of traffic shaping technology in internet of things. *IEEE Access*, *11*, 3794-3809.

28. Hernández-Oregón, G., Rivero-Angeles, M. E., Chimal-Eguía, J. C., & Coyac-Torres, J. E. (2023). Performance Analysis of P2P Networks with Light Communication Links: The Static Managed Case. *Applied Sciences*, *13*(13), 7906.
29. Hristov-Kalamov, N., Fernández-Ruiz, R., Álvarez-Marquina, A., Guillén-García, J., Gallardo-Cava, R., & Palacios-Alonso, D. (2025). Composable Privacy-Preserving Framework for Stakes-Based Online Peer-to-Peer Applications. *Cryptography*, *9*(3), 48.
30. Ali, A., Ullah, I., Ahmed, A., Noor, W., Sajid, A., & Khan, I. U. (2022). Behavior dissection of NGWN live audio and video streaming users with enhanced and efficient modelling. *Wireless Communications and Mobile Computing*, *2022*(1), 7564543.
31. Farooq, M. S., Riaz, S., & Alvi, A. (2023). Security and privacy issues in software-defined networking (SDN): A systematic literature review. *Electronics*, *12*(14), 3077.
32. Baig, M. J. A., Iqbal, M. T., Jamil, M., & Khan, J. (2022). A low-cost, open-source peer-to-peer energy trading system for a remote community using the internet-of-things, blockchain, and hypertext transfer protocol. *Energies*, *15*(13), 4862.
33. Eltamaly, A. M., & Ahmed, M. A. (2023). Performance evaluation of communication infrastructure for peer-to-peer energy trading in community microgrids. *Energies*, *16*(13), 5116.
34. Viswanadh, K. S., Gureja, A., Walchatwar, N., Agrawal, R., Sinha, S., Chaudhari, S., ... & Hussain, A. (2024). Engineering end-to-end remote labs using IoT-based retrofitting. *IEEE Access*.
35. Akhter, A. S., Arnob, T. Z., Noor, E. B., Hizal, S., & Pathan, A. S. K. (2022). An edge-supported blockchain-based secure authentication method and a cryptocurrency-based billing system for P2P charging of electric vehicles. *Entropy*, *24*(11), 1644.
36. Qiu, H., Ji, T., Zhao, S., Chen, X., Qi, J., Cui, H., & Wang, S. (2022). A geography-based p2p overlay network for fast and robust blockchain systems. *IEEE Transactions on Services Computing*, *16*(3), 1572-1588.
37. Crespo-Aguado, M., Lozano, R., Hernandez-Gobertti, F., Molner, N., & Gomez-Barquero, D. (2024). Flexible Hyper-Distributed IoT–Edge–Cloud Platform for Real-Time Digital Twin Applications on 6G-Intended Testbeds for Logistics and Industry. *Future Internet*, *16*(11), 431.
38. Tang, Y., You, J., Qin, P., Fu, Y., & Wang, W. (2022). Cloud-edge collaboration based peer to peer services redirection strategy for passive optical network. *IET Communications*, *16*(8), 902-914.
39. Chen, N., & Yang, Y. (2023). The role of influencers in live streaming e-commerce: influencer trust, attachment, and consumer purchase intention. *Journal of Theoretical and Applied Electronic Commerce Research*, *18*(3), 1601-1618.
40. Chen, J., & Fujita, S. (2025). Adaptive Multi-Hop P2P Video Communication: A Super Node-Based Architecture for Conversation-Aware Streaming. *Information*, *16*(8), 643.
41. Kalan, R., & Dulger, I. (2024). A survey on QoE management schemes for HTTP adaptive video streaming: challenges, solutions, and opportunities. *IEEE Access*.
42. Al-Habashna, A. A., & Wainer, G. A. (2022). Application of Device-to-Device Communication in Video Streaming for 5G Wireless Networks. In *Advances in Computing, Informatics, Networking and Cybersecurity: A Book Honoring Professor Mohammad S. Obaidat's Significant Scientific Contributions* (pp. 345-371). Cham: Springer International Publishing.
43. Alshiky, A. M., Khemakhem, M. A., Eassa, F., & Alzahrani, A. (2025). Comparative Analysis of SDN and Blockchain Integration in P2P Streaming Networks for Secure and Reliable Communication. *Electronics*, *14*(17), 3558.
44. Kumari, A., Chintukumar Sukharamwala, U., Tanwar, S., Raboaca, M. S., Alqahtani, F., Tolba, A., ... & Mihaltan, T. C. (2022). Blockchain-based peer-to-peer transactive energy management scheme for smart grid system. *Sensors*, *22*(13), 4826.
45. Zafar, B., & Ben Slama, S. (2022). Energy internet opportunities in distributed peer-to-peer energy trading reveal by blockchain for future smart grid 2.0. *Sensors*, *22*(21), 8397.
46. Firouzi, R., & Rahmani, R. (2022). A distributed SDN controller for distributed IoT. *IEEE Access*, *10*, 42873-42882.
47. Al Jameel, M., Kanakis, T., Turner, S., Al-Sherbaz, A., & Bhaya, W. S. (2022). A reinforcement learning-based routing for real-time multimedia traffic transmission over software-defined networking. *Electronics*, *11*(15), 2441.
48. Miao, Q., Lin, H., Hu, J., & Wang, X. (2022). An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things. *Digital Communications and Networks*, *8*(5), 636-643.
49. Antwi, R., Gadze, J. D., Tchao, E. T., Sikora, A., Nunoo-Mensah, H., Agbemenu, A. S., ... & Keelson, E. (2022). A survey on network optimization techniques for blockchain systems. *Algorithms*, *15*(6), 193.
50. Roopa, V., & Pradhan, H. S. (2025). Exploring blockchain and artificial intelligence for next generation wireless networks. *Journal of Communications and Networks*.

51. Algarni, S., Eassa, F., Almarhabi, K., Algarni, A., & Albeshri, A. (2022). BCNBI: A blockchain-based security framework for northbound interface in software-defined networking. *Electronics*, *11*(7), 996.
52. Alhusayni, A., Thayananthan, V., Albeshri, A., & Alghamdi, S. (2023). Decentralized multi-layered architecture to strengthen the security in the internet of things environment using blockchain technology. *Electronics*, *12*(20), 4314.
53. Geng, J., & Fujita, S. (2024). Enhancing crowd-sourced video sharing through P2P-assisted HTTP video streaming. *Electronics*, *13*(7), 1270.
54. Khorasany, M., Gazafroudi, A. S., Razzaghi, R., Morstyn, T., & Shafie-khah, M. (2022). A framework for participation of prosumers in peer-to-peer energy trading and flexibility markets. *Applied energy*, *314*, 118907.
55. Moosavi, N., & Taherdoost, H. (2023). Blockchain technology application in security: A systematic review. *Blockchains*, *1*(2), 58-72.
56. Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2023). Peer-to-peer user identity verification time optimization in IoT Blockchain network. *Sensors*, *23*(4), 2106.
57. Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, *14*(1), 41.
58. Serag, R. H., Abdalzaher, M. S., Elsayed, H. A. E. A., Sobh, M., Krichen, M., & Salim, M. M. (2024). Machine-learning-based traffic classification in software-defined networks. *Electronics*, *13*(6), 1108.
59. Jmal, R., Ghabri, W., Guesmi, R., Alshammari, B. M., Alshammari, A. S., & Alsaif, H. (2023). Distributed blockchain-SDN secure IoT system based on ANN to mitigate DDoS attacks. *Applied Sciences*, *13*(8), 4953.
60. Ibrahim, R. F., Abu Al-Haija, Q., & Ahmad, A. (2022). DDoS attack prevention for internet of thing devices using ethereum blockchain technology. *Sensors*, *22*(18), 6806.
61. Khacef, K., Benbernou, S., Ouziri, M., & Younas, M. (2024). A dynamic sharding model aware security and scalability in blockchain. *Information Systems Frontiers*, *26*(6), 2323-2336.
62. Yu, C., Yang, W., Xie, F., & He, J. (2022). Technology and security analysis of cryptocurrency based on blockchain. *Complexity*, *2022*(1), 5835457.
63. Dua, A. (2023). Leveraging AI-enabled 6G-driven IoT for sustainable smart cities.
64. Febro, A., Xiao, H., Spring, J., & Christianson, B. (2022). Synchronizing DDoS defense at network edge with P4, SDN, and Blockchain. *Computer Networks*, *216*, 109267..
65. Rahman, M. M. (2025). Blockchain-Assisted QoS-Aware Routing for Software-Defined Wide Area Network. *Electronics*, *14*(10), 1949.
66. Alsamhi, S. H., Hawbani, A., Kumar, S., Timilsina, M., Al-Qatf, M., Haque, R., ... & Curry, E. (2024). Empowering dataspace 4.0: Unveiling promise of decentralized data-sharing. *IEEE Access*, *12*, 112637-112658.
67. Al Ghamdi, M. A. (2022). An optimized and secure energy-efficient blockchain-based framework in IoT. *IEEE Access*, *10*, 133682-133697.
68. Zhao, S., Zeng, Z., Peng, J., & Yu, F. (2023). Achieving a secure and traceable high-definition multimedia data trading scheme based on blockchain. *Mathematics*, *11*(10), 2224.
69. Peng, S., Bao, W., Liu, H., Xiao, X., Shang, J., Han, L., ... & Xu, Y. (2023). A peer-to-peer file storage and sharing system based on consortium blockchain. *Future Generation Computer Systems*, *141*, 197-204.
70. Núñez-Gómez, C., Carrión, C., Caminero, B., & Delicado, F. M. (2023). S-HIDRA: A blockchain and SDN domain-based architecture to orchestrate fog computing environments. *Computer Networks*, *221*, 109512.
71. Farahani, R., Timmerer, C., & Hellwagner, H. (2024). Towards low-latency and energy-efficient hybrid P2P-CDN live video streaming. *ArXiv preprint arXiv:2403.16985*.
72. Nakakaze, O., Koren, I., Brillowski, F., & Klamma, R. (2024). Adaptive retrofitting for industrial machines: utilizing webassembly and peer-to-peer connectivity on the edge. *World Wide Web*, *27*(1), 7.
73. Bellaj, B., Ouaddah, A., Bertin, E., Crespi, N., Mezrioui, A., & Bellaj, K. (2022). Btrust: A new blockchain-based trust management protocol for resource sharing. *Journal of Network and Systems Management*, *30*(4), 64.
74. Rodríguez-Sela, F., & Bordel, B. (2025). Towards Trustworthy Energy Efficient P2P Networks: A New Method for Validating Computing Results in Decentralized Networks. *Computers*, *14*(6), 216.
75. Wei, D., Zhang, J., Li, H., Xue, Z., Peng, Y., Pang, X., ... & Li, J. (2024). Swarm: Cost-Efficient Video Content Distribution with a Peer-to-Peer System. *ArXiv preprint arXiv:2401.15839*.
76. Makris, A., Kontopoulos, I., Psomakelis, E., Xyalis, S. N., Theodoropoulos, T., & Tserpes, K. (2022). Performance analysis of storage systems in edge computing infrastructures. *Applied Sciences*, *12*(17), 8923.

77. Almakdi, S., Aqdus, A., Amin, R., & Alshehri, M. S. (2023). An intelligent load balancing technique for software defined networking based 5G using machine learning models. *IEEE Access*, *11*, 105082-105104.
78. Guler, E. (2024). CITE-PSO: Cross-ISP Traffic Engineering Enhanced by Particle Swarm Optimization in Blockchain Enabled SDONs. *IEEE Access*, *12*, 27611-27632.
79. Samadi, R., Nazari, A., & Seitz, J. (2023). Intelligent energy-aware routing protocol in mobile IoT networks based on SDN. *IEEE transactions on green communications and networking*, *7*(4), 2093-2103.
80. Wang, Z., Jin, Z., Yang, Z., Zhao, W., & Mir, M. (2024). An intelligent fuzzy reinforcement learning-based routing algorithm with guaranteed latency and bandwidth in SDN: Application of video conferencing services. *Egyptian Informatics Journal*, *27*, 100524.