Blockchain Over Named Data Networking Architecture: A Review

Mohammed Alsamman[1](✉), Suhaidi Hassan[1], Fathey Mohammed[2], and Yousef Fazea[3]

[1] School of Computing, Universiti Utara Malaysia, Sintok, 06010 Bukit Kayu Hitam, Kedah, Malaysia
alsamman@uum.edu.my
[2] Sunway Business School, Sunway University, 47500 Subang Jaya, Selangor, Malaysia
[3] Computer and Information Technology, Marshall University, 1 John Marshall Drive, Huntington, WV 25755, USA

Abstract. With infinite apps and online services, future Internet architecture will face new challenges and consequences, such as scalability, dependability, suitable mobility, and security. Internet use has changed spectacularly from one-way communication to content distribution, as much content is generated every minute. Blockchain and Named Data Networking (NDN) are two cutting-edge technologies on the verge of revolutionizing how we use the Internet. Blockchain is a decentralized ledger technology allowing users to store and share data securely. On the other hand, NDN is a new way of networking that focuses on content instead of location. Combining blockchain and NDN can create a safer, more efficient, and more decentralized internet. Blockchain can provide tamper-proof data records, and NDN can deliver content to users efficiently and securely. This paper emphasizes the importance of research in the field of blockchain over Named Data networks. It highlights the advantages of combining blockchain with NDN and discusses the difficulties and open research questions related to the use of blockchain over NDN. Also, the potential impact of blockchain over NDN on the future of the Internet as it can create a safer, more efficient, and more decentralized Internet.

Keywords: Blockchain · Content Distribution · Content-Centric Network · Future Internet

1 Introduction

Blockchain technology is currently one of the most popular technologies [1], as seen in Fig. 1, which shows the market size of blockchain technology globally. The widespread recognition of blockchain technology as a technological revolution generates enormous attention and publicity. The history of all transactions is kept in the distributed digital ledger, which comprises blocks of encrypted, signed transactions [2]. By providing copies of documents to each participant, the Blockchain concept avoids the need for centralized authority. Unlike traditional transactions, data control stays in the hands of

N. H. Zakaria et al. (Eds.): ICOCI 2023, CCIS 2001, pp. 367–379, 2024.
https://doi.org/10.1007/978-981-99-9589-9_28

a central authority, which is also in charge of verifying the customers' credentials. The conventional source manages and administers data and ensures that it cannot be changed or erased. Contrarily, the blockchain concept employs. However, decentralized control eliminates the dangers present in the conventional paradigm.

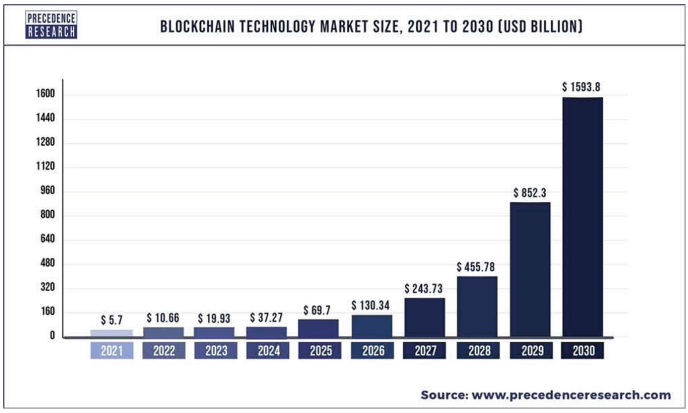

Fig. 1. Blockchain Technology Market [1].

Blockchain technology has several uses in various industries, including crypto currency, the Internet of Things, healthcare, and distributed cloud storage. Every transaction in a blockchain network generates a hash dependent on the current and the prior transaction. Even minor changes in the transaction generate a whole new hash. The P2P network of nodes receives the broadcast of the transaction after that. The network nodes examine the hash to confirm that the transactions have not been altered. This network uses well-known techniques to authenticate the transaction. After confirmation, the transaction is combined with other transactions to create a new ledger data block. Similar to how the Internet evolved, the blockchain paradigm's rapid expansion has become pivotal. While decentralized approaches eliminate the single point of failure problem by allowing each node to calculate ratings and share them with other nodes independently, this requires the trustworthiness of the individual nodes to perform the computations and provide reputation values that cannot be found in today's network architectural (TCP/IP) [2].

The Named Data Networking (NDN) architecture was developed to address the challenges of tracking and delivering the ever-increasing amount of content produced and delivered online. Unlike the current TCP/IP architecture, which focuses on the location of data, NDN focuses on the content itself. This allows for more efficient and scalable content delivery, and improved security and privacy. In NDN, data is named using a hierarchical naming scheme that makes it easy to find and retrieve. Data can be stored locally or in the cache of nearby nodes. The physical address of the host node is not required for communication in NDN, as the names of the data themselves are sufficient to identify the desired content. This eliminates the need for DNS, which is a major bottleneck in the current Internet architecture. The NDN architecture is designed to be backward-compatible with the existing Internet, making it a straightforward and scalable upgrade path [3].

The original Internet design is elegant and powerful due to its hourglass architecture. The narrow waist of the hourglass represents the core network layer, which implements the essential features necessary for global interconnectedness. This small size has been essential to the development of the Internet, as it has freed higher- and lower-layer technologies from unnecessary limitations. The NDN design also has a narrow waist, but it differs from the IP architecture in a fundamental way [3]. The use of data names in NDN allows for more efficient and scalable content delivery, as well as improved security and privacy. Data names are hierarchical, making finding and retrieving content easy. They are also self-describing, which means they contain information about the content, such as its type, size, and last modified date. Routers can use this information to make more informed decisions about how to route data packets [4].

Integrating blockchain technology with NDN has recently gained much attention in the research community. Scholars have highlighted the potential benefits of this integration, such as improved security, privacy, and scalability. NDN can also fulfill the needs of blockchain applications by providing a secure and efficient way to store and transfer data. This study focuses on integrating NDN and blockchain technology and discusses the potential benefits of this integration [5, 6].

The use of blockchain over NDN will be examined in this paper. The document layout is as follows: We'll present the Methodology in Sect. 2 and the Background review in Sect. 3. A review of the latest studies of blockchain over NDN will be covered in Sect. 4. The discussions on the value of blockchain over NDN will be covered in Sect. 5. Open challenges will be presented in Sect. 6 and Sect. 7 will conclude the paper.

2 Methodology

The narrative review method is used in this study to give readers enough background information to comprehend the research issue and emphasize the value of new knowledge. IEEE, ACM, Springer, and Elsevier are just a few of the research databases that the researchers use. Papers are initially chosen based on the broad keyword" Named Data Networks" and filtered to exclude duplicates and irrelevant ones. Additionally, particular keywords like" Blockchain over Named Data Network," Named Data Networks," and" Blockchain" are utilized to narrow down the articles that have been gathered. With 45% of the total publications from the IEEE database, the papers are mostly from 2021 to 2023. The remaining papers are sourced from various conferences and journals, with distribution percentages of 4%, 14%, 14%, 9%, and 14% for ACM, Springer, MDPI, Elsevier, and other conferences and journals, respectively. The study adopts a qualitative approach and conducts a narrative investigation. Qualitative research allows researchers to obtain comprehensive data in their natural settings, offering the opportunity for data interpretation given the interpretative nature of the study. Figure 2 illustrates the distribution of articles from different resources.

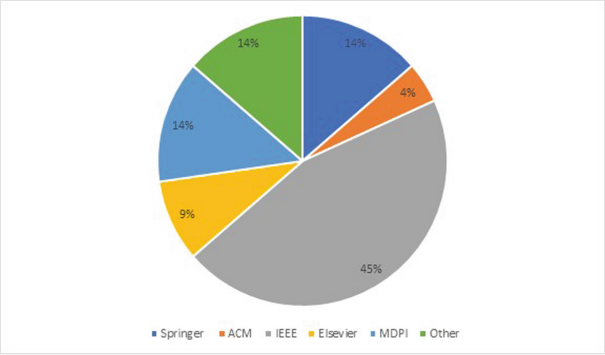

Fig. 2. Articles from different resources.

3 Background First Section

Blockchain and named data networking (NDN) are two emerging technologies that have the potential to revolutionize the way we interact with the Internet. Blockchain is a distributed ledger technology that can securely record and share data, while NDN is a new networking paradigm focusing on content rather than location. In this section, we will provide a background on blockchain and NDN. We will then discuss the potential benefits of combining these two technologies [6].

3.1 NDN Forwarding Plane

NDN architectural design proposes two packet types: interest packets and data packets. NDN users can access the data by subscribing to an Interest packet, which requests a content object and returns it as a Data packet; both packets contain the name of the content object. The Forwarding Information Base (FIB), the Pending Interest Table (PIT), and the Content Store are the three significant Data structures that an NDN router must maintain (CS) [3].

The FIB of an NDN router is often similar to the FIB of an IP router, with the architectural difference that it holds name prefixes rather than IP address prefixes. By doing this, the name prefixes may be sent to various interfaces. Each PIT section keeps a record of the Interest's name, arriving interface(s), and forwarding interface(s) that it has been passed to (like a history table), when a router receives an interest packet, it first checks the Content Store (CS) to see whether there is any matching Data. The CS provides short-term in-network storage (caching) of the incoming Data packet. The interface from which the Interest is coming receives the data immediately [7].

On the other hand, if the name matches, the interest will proceed to look up the PIT entries. Suppose the name already appears in the PIT. In that case, it may be a duplicate Interest that has to be discarded or a retransmitted Interest from the same customer sent via a different outgoing interface (or an Interest from an alternate consumer requesting the same Data). This causes the PIT to check the nonce of the Interest and update the existing PIT record with the number of incoming interfaces. This effectively creates a

multicast tree for users requesting the same Data simultaneously. If the Interest name does not already exist in the PIT, it is added to the PIT and sent to the FIB, where the forwarding plane module will handle it.

When a Data packet comes at this stage, the PIT is checked using the packet's name. The router delivers the Data packet to the interface(s) from which the Interest arrived and deletes the PIT entrance if there is a match in the PIT entrance. Data packets then frequently follow the interests' backward routes. The Data packet is discarded or cached in the CS if no match is detected. Every Interest has an associated lifespan that the consumer determines; if an Interest is unsatisfied before its lifetime expires, a PIT item is removed. Nevertheless, an NDN router may keep a Data packet in the CS due to the signature's uniqueness and the dependability of the caching strategy. Even so, future interests can be satisfied using the data packets stored in the CS [8].

3.2 Blockchain Framework

Most modern blockchain systems use a common framework that was first established in Bitcoin and Ethereum and may be organized generally into four levels [9] as follow:

Application Layer: By utilizing smart contracts, the decentralized applications of blockchain technology, such as supply chain management, identity management, and notarial services, have grown to include the application layer, which is used for cryptocurrency transfers.

Data Layer: A blockchain framework's data layer contains structures for consensus, data transfer, and ledger maintenance. Blocks are connected via hash references; however, block architectures may vary.

Consensus Layer: The shared ledger is created via a process followed by the consensus layer in blockchain nodes, with copies on each node. Consistency requires agreement on how transactions should be executed in order. For quicker processing, transactions are organized into blocks, and the block sequence is chosen instead. The PoW consensus, used by many blockchain systems, is infamous for its lengthy transaction times and lack of transactional finality because of ledger forking. Researchers are looking into novel consensus methods to get over these restrictions and support a range of blockchain technology use cases.

Transport Layer: The blockchain network's transport layer defines how transactions are recorded to the ledger and how blockchain data is propagated. Public blockchains like Bitcoin and Ethereum use a P2P overlay to transfer data items to all nodes from a single source. The transport layer of the blockchain network controls how transactions are recorded and propagated.

4 Blockchain over Named Data Networks

Most research on Named Data Networks and Blockchain technology has been done independently. Table 1 shows recent years that adopted Blockchain over NDN in various fields, including security and privacy, networks, the Internet of Things, mobility, and

others. TCP/IP was the primary platform for the blockchain's creation. When a node sends data over TCP/IP to several nodes, it must first package that data in a packet and send it to each node separately, which results in extra data transfer. NDN uses in-network caching, which can help to enhance the entire broadcast of a blockchain application.

NDN's data-centric methodology makes it possible to synchronize blocks on a blockchain effectively and distribute records. Data in NDN is gathered from the complete network rather than from a single node or location. Since there is no concept of a light node or a full node with blockchain technology via NDN, all nodes are treated equally. This resolves a critical security flaw in existing distributed ledger systems where the light node depends on the entire node to receive and deliver data, leaving it vulnerable to the full nodes' malevolent behavior [10].

The studies in [10–12] investigate how different blockchains, including public, private, and consortium blockchains, can distribute data across NDN. Anyone with internet connectivity can become a certified node on a public blockchain, which is open and unrestricted and welcomes new nodes. A new node relay pressure metric is used for routing decisions in a green global routing system (GGNRP) to reduce power consumption and forwarding time [11]. Using a blockchain-based key management system for safe key distribution and verification is also suggested. While several organizations run consortium blockchains, private blockchains are used only by particular enterprises or organizations.

With the potential to expand NDN application ecosystems, a new blockchain platform proposed in [12] uses named data networking (NDN) rather than the conventional internet protocol (IP) to build blockchain platforms. The suggested framework [13], which uses NDN and IPFS for data management and has three layers—the data layer, the blockchain layer, and the application layer—offers superior privacy protection, scalability, and efficiency than existing federated learning frameworks. The blockchain is used to store the aggregated data and to ensure its integrity. The framework has several advantages over traditional federated learning frameworks. First, it provides better privacy protection for the raw data. Second, it is more scalable and can support many edge devices. Third, it is more efficient, as it does not require transferring large amounts of data to the cloud server.

A new certificate ledger system called CLedger. CLedger is a distributed system that uses named data networking (NDN) to store and manage certificates [14]. As NDN is naming data instead of nodes, this makes it possible to store and manage certificates in a distributed manner without having to worry about the identity of the nodes that store the certificates [14].

In addition, researchers in [15] proposed an XRP-NDN Overlay as a solution for improving the communication efficiency of consensus-validation-based blockchains like the XRP Ledger. It does this by using a Named Data Networking (NDN) overlay network. This allows for more efficient routing, as data can be routed directly to the destination, without having to go through a central server. In [9] it is suggested to use blockchain technology and hierarchical identity-based cryptography (HIBC) to construct anonymous identities and independently verify the validity of data in named data networking (NDN).

Table 1. Blockchain over Named Data Network related works

Ref	Year	Area	Contribution
[11]	2021	Security	Present a routing scheme based on node relaying pressure and blockchain-based key management scheme
[12]	2023	Routing	Present new protocols for propagating blockchain data using NDN features
[13]	2022	Routing	Proposed framework consists of three layers and used NDN to name the aggregated data
[14]	2023	Security	Design of CLedger, a secure distributed certificate ledger
[15]	2023	Routing	Proposed an XRP-NDN Overlay to enhance the effectiveness of communication across consensus - validation-based blockchains
[9]	2022	Security	Presents hierarchical identity-based cryptography (HIBC) and blockchain-based security method for NDN
[16]	2023	Security	Proposed efficient and secure auditing of data transmission behavior for NDN IIoT networks
[17]	2023	Security	Proposed a NACDA approach for data verification in NDN, which improved the considerable delays brought on by the extremely dynamic nature of vehicle networks
[18]	2023	Security	Proposed a decentralized data authentication mechanism based on blockchain technology
[19]	2023	Trust	Build mechanics trust between vehicles using NDN to route data efficiently, and blockchain to record transactions securely
[20]	2022	Security	proposed a system called BIoVN, to secure IoV over NDN
[21]	2023	Routing	Present a new data dissemination protocol called A-C is based on the NDN forwarding
[6]	2022	Routing	Proposed a deployment of named data networking (NDN) at the network layer of the blockchain to provide differentiated QoS assurance
[22]	2023	Routing	Proposed a framework called AFFIRM for generating, validating, storing, and retrieving mobility data in Web3 applications
[23]	2022	Trust	Present a trust management system is to allow well-behaved peers to gain a good reputation
[24]	2021	Security	Proposes a novel encryption-based data access control scheme for Named Data Networking (NDN) using Role-Based Encryption (RBE)
[25]	2023	Trust	Proposes a proof-of-trust-based data authentication system for blockchains in NDN
[26]	2022	Routing	Proposed access control system based on NFT enables NDN routers to forward ciphertext data
[27]	2022	Routing	This paper proposes integrating blockchain and NDN to improve document content storage

(*continued*)

Table 1. (*continued*)

Ref	Year	Area	Contribution
[28]	2023	Security	Proposed a CCN-based secure content delivery scheme for V2G networks
[29]	2022	Security	Proposes a security architecture for NDN based on a consortium blockchain and bootstrapping procedures

The authors [16] In the Industrial Internet of Things (IIoT), the study provides a simple transmission behavior audit scheme for Named Data Networking (NDN). The blockchain-based system makes it possible to audit data transmission behavior in NDN networks safely and effectively. It consists of three basic parts: a lightweight auditor for gathering and submitting records to the blockchain, a blockchain-based audit system for managing records, and a data packet for carrying audit records. The findings show that NDN networks can effectively detect malicious activities and have high throughput and low latency.

IN [17] proposed Naming-Based Access Control and Decentralized Authorization (NACDA) system addresses challenges in data verification in dynamic vehicular net works by enabling secure and flexible data sharing on the Named Data Network (NDN) using Identity-Based Encryption with Wildcard Key Derivation (WKD-IBE) and blockchain. A new mechanism has been proposed in [18] to provide a decentralized data authentication mechanism based on blockchain technology that is both efficient and straightforward.

A new framework proposed in [19] uses VSNs to build trust between vehicles, NDN to route data efficiently, and blockchain to record transactions securely. The framework is designed to be P2P, meaning that vehicles can trade energy directly with each other without needing central authority. While in [20] the authors proposed another system called BIoVN, which is a combination of blockchain technology and named data networking (NDN) for the Internet of Vehicles (IoV). The purpose of this system is to improve the security of vehicular communications over NDN.

The authors in [21] introduce the Named Data Networking (NDN) and Erasure Coding (EC)-based A-C data distribution protocol. The protocol uses a two-layer NDN-based publication-subscription mechanism to maximize bandwidth efficiency and speed up data dissemination. It focuses on the prompt distribution of blocks and transactions in blockchain systems, which is crucial for consensus, effectiveness, and security. The A-C protocol improves data transmission efficiency and security in blockchain systems, reduces data redundancy, and addresses shortcomings of flooding-based gossip protocols.

A deployment of named data networking (NDN) at the network layer of the blockchain to provide differentiated QoS assurance is proposed in [6]. It discussed the use of window sliding and forwarding strategies to speed up packet processing and meet the delay requirements of delay-sensitive packets. Also, a blockchain framework called AFFIRM for generating, validating, storing, and retrieving mobility data in Web3 applications. This framework enables nearby devices to self-organize as a fog network

and collaboratively train machine learning algorithms locally to securely generate, validate, store, and retrieve mobility data via consensus leveraging Information Centric Networking as the underlying architecture [22].

Author in [24] proposes a novel encryption-based data access control scheme for Named Data Networking (NDN) using Role-Based Encryption (RBE). The scheme ensures efficient data access control over hierarchical content, making it suitable for large-scale content-centric applications like Netflix. The study [25] proposes a proof-of-trust-based data authentication system for blockchains. The technique collects votes from a group of nodes to distribute and store items in the cache memory. The suggested system provides a fresh data authentication option for the upcoming Internet environment while attempting to address difficulties with tainted cache memory. In [26] smart contracts are used to distribute AttributeNFT and AccessNFT, a proposed access control system based on Non-Fungible Token (NFT) that enables NDN routers to forward ciphertext data packets only to authorized users, assuring data security and secure distribution. To increase document content distribution, security, and network speed, research in [27] suggests fusing blockchain technology with Named Data Networks (NDN).

Three key contributions are made in the paper's proposal for a CCN-based Three key contributions are made in the paper's proposal for a CCN-based secure content delivery scheme for V2G networks: in-network caching for quick content delivery; a contract theory-based incentive scheme to entice vehicle participation, and the proof of authority consensus algorithm for secure content delivery and network trust [28]. Authors in [29] Used a symmetric-key-based authenticated encryption technique and a one-way hash chain for source authentication, this article suggests a security architecture for NDN that is based on a consortium blockchain and bootstrapping procedures. In [30] proposed CPA detection and prevention mechanism includes a threshold-based content caching system, a blockchain system for privacy, and an extension of NDN to push-based content dissemination.

5 Discussion

With the goal of replacing TCP/IP at the network layer, adopting blockchain technology over NDN offers special benefits and applications that will benefit both the blockchain community and established online services. [5]. By focusing on network-level connectivity and adopting "data-driven authenticity" to assure the security of the data's source, blockchain over NDN prioritizes data over location and ensures real decentralization.

Researchers are interested in how specific technologies are emerging. Data retrieval is efficient using NDN, and data security is ensured via blockchain. Some scholars believe using blockchain technology for the current IP would be unwise. Instead, using blockchain technology over NDN may lead to more effective performance [6, 11]. NDN, a hypothetical future Internet architecture, can support blockchain technology, offering a dependable way to maintain databases without central authority. Blockchain over NDN fixes IP network problems and provides a decentralized system, making connecting nodes and synchronizing data simpler. Trust models can be centralized or decentralized; a prior method involved a central credit authority to collect and disseminate reputation values, but this method still entailed communication costs [15].

Decentralized approaches eliminate the single point of failure problem by allowing each node to calculate ratings and share them with other nodes independently, but this requires the trustworthiness of the individual nodes to perform the computations and provide reputation values. While Encryption is incorporated into NDN to provide data security and authentication, and trust management enables good peers to build up a positive reputation while identifying and excluding bad peers from transactions [13, 25].

The decentralized nature of P2P networks needs a dispersed strategy in contrast to online reputation models. Blockchain over NDN can provide a decentralized system that is more efficient and simpler to implement. By using blockchain technology over NDN, it is possible to reduce the transmission cost, eliminate redundant network traffic, clear up congestion, and boost network efficiency.

Blockchain over-Named Data Network (NDN) provides several advantages and addresses specific data networking needs. Here are some of the reasons why blockchain is seen as useful in conjunction with data networking [5, 6, 9, 11–30]:

Enhanced Security: Blockchain provides a decentralized, tamper-resistant framework to secure data transactions and data distribution. Integrating blockchain into NDN strengthens data integrity and authentication reducing the risk of unauthorized access and manipulation.

Data Ownership and Control: Blockchain's smart contracts allow for fine-grained data ownership and control. In NDN, where data is accessed based on the name, blockchain can help to secure and transparently manage data ownership, enabling content creators to take control of their intellectual property.

Trust and Transparency: Blockchain's distributed ledger provides an unalterable record of data exchanges and transactions. Integration into NDN increases trust and transparency by allowing for verifiable, auditable, and transparent delivery and sharing of data. This is especially important in supply chain management and decentralized applications, where participant trust is essential.

Resilience and Data Availability: NDN's in-network caching capability, combined with the blockchain's decentralized nature, can improve the availability and resilience of data. Blockchain over NDN can utilize distributed storage and caching capabilities, ensuring that content remains available even during network disruption or failure.

Better Consensus and Governance: Blockchain introduces consensus mechanisms allowing decentralized decision-making and governance. When integrated with NDN, blockchain can be used to implement consensus protocols to facilitate agreement on the content distribution policies, the allocation of network resources, and participation rules in the NDN ecosystem.

6 Open Research Challenges

The review highlights the possible advantages and drawbacks of employing blockchain technology in the context of Named Data Networking (NDN), emphasizing the need for additional research into security and content caching issues as well as unsolved privacy-related concerns [5, 25, 28]. It also highlights the need for real-time fairness among

network miners, emphasizing the unfairness that results when the miner nearest to the producer receives a newly created block earlier than other miners and the need to foster network miner dynamics [5, 6].

Performance Optimization: Future research should concentrate on creating effective consensus mechanisms and algorithms to integrate blockchain with NDN, to reduce overhead and maintain security guarantees by investigating solutions like sharing off-chain transactions, and optimized consensus protocols to improve scalability and transaction throughput.

Privacy-Preserving Techniques: The highlighted text suggests that researching privacy-preserving methods in Blockchain over NDN can aid in creating mechanisms that safeguard data privacy while utilizing the blockchain's transparency. These methods include zero-knowledge proofs, secure multi-party computation, and differential privacy.

Interoperability and Standardization: Future research can concentrate on creating interoperability frameworks and standards to allow seamless integration with current network infrastructures and protocols as blockchain integration with NDN advances. This entails determining standardized data formats for blockchain-based NDN and looking into ways to connect various blockchain systems.

Security and Trust Model Design: By establishing new cryptographic methods and consensus mechanisms, more research is required to produce secure and reliable models for integrating blockchain with NDN, solving issues such as secure content naming, identity management, and combating Sybil attacks.

Real-World Use Cases and Applications: Future research should concentrate on identifying and examining real-world use cases and applications, such as IoT, content distribution networks, supply chain management, decentralized finance, and healthcare, where Blockchain over NDN can offer significant benefits to assess feasibility, performance, and impact.

7 Conclusion

Blockchain technology is a new concept in NDN that is quickly gaining footing. Blockchain technology over IP still has several significant issues, such as a lack of hierarchical access efficiency. These issues have been resolved by adopting blockchain technology over NDN, which provides a decentralized system and streamlines the design. This article outlined the research examining the application of blockchain technology in NDN. Over NDN, we discussed some of the difficulties with blockchain technology.

The investigation revealed that with an increased number of articles each year, blockchain technology in NDN is receiving increased attention. The survey report demonstrates that the search for Blockchain technology over NDN is still in its infancy, encouraging the NDN research community to devote serious attention to the issue. This study will clear the way for scholars interested in learning more about leveraging blockchain technology over NDN.

References

1. Precedence Research. Blockchain Technology Market Size to Hit USD, 593.8 Bn By 2030 (2021). https://www.precedenceresearch.com/blockchain-technology-market. Accessed 25 Oct 2022
2. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564 (2017). https://doi.org/10.1109/BigDataCongress.2017.85
3. Jacobson, V., et al.: Named Data Networking (NDN) Project 2012–2013 Annual Report (2013)
4. Askar, N., et al.: Forwarding strategies for named data networking based IOT: requirements, taxonomy, and open research challenges. IEEE Access (2023)
5. Asaf, K., Rehman, R.A., Kim, B.-S.: Blockchain technology in named data networks: a detailed survey. J. Netw. Comput. Appl. **171**, 102840 (2020). https://doi.org/10.1016/j.jnca.102840
6. Shang, J., Huo, R., Wang, S., Huang, T.: An NDN-enabled differentiated routing strategy for blockchain. In: 2022 IEEE 2nd International Conference on Computer Communication and Artificial Intelligence (CCAI), pp. 96–101 (2022). https://doi.org/10.1109/CCAI55564.2022.9807743
7. Abrar, A., Arif, A.S.C.M., Zaini, K.M.: A systematic analysis and review on producer mobility management in named data networks: research background and challenges. Alex. Eng. J. **69**, 785–808 (2023)
8. Alsamman, M., Hassan, S., Arif, S.: Deficit weighted round robin shaping mechanism for transport control in named data networking. J. Adv. Res. Dyn. Control Syst. **11**(8 Special Issue), 1115–1125 (2019)
9. Thai, Q.T., Ko, N., Byun, S.H., Kim, S.-M.: Design and implementation of NDN-based Ethereum blockchain. J. Netw. Comput. Appl. **200**, 103329 (2022). https://doi.org/10.1016/j.jnca.2021.103329
10. Yi, D., Huo, R., Wang, S., Huang, T.: An NDN-enabled data transfer strategy for blockchain network layer. In: Journal of Physics: Conference Series, vol. 2026, no. 1, p. 012001 (2021). https://doi.org/10.1088/1742-6596/2026/1/012001
11. Liu, H., Zhu, R., Wang, J., Xu, W.: Blockchain-based key management and green routing scheme for vehicular named data networking. Secur. Commun. Netw. **2021**, 1–13 (2021). https://doi.org/10.1155/2021/3717702
12. Li, B., Ma, M.: An advanced hierarchical identity-based security mechanism by blockchain in named data networking. J. Netw. Syst. Manag. **31**(1), 13 (2023)
13. Shen, T., Cui, Z., Tian, S., Bai, F., Zhang, C.A.: Network-elastic scalable blockchain for privacy-preserving federated learning in cloud-edge collaboration industrial internet of things. In: Proceedings of the 2022 7th International Conference on Cloud Computing and Internet of Things, pp. 17–25 (2022)
14. Yu, T., et al.: CLedger: a secure distributed certificate ledger via named data network. IEEE ICC (2023)
15. Trestioreanu, L., Shbair, W.M., de Cristo, F.S., State, R.: XRP-NDN overlay: improving the communication efficiency of consensus-validation based blockchains with an NDN overlay. In: 2023 IEEE/IFIP Network Operations and Management Symposium, NOMS 2023, pp. 1–5. IEEE (2023). arXiv:2301.10209
16. He, Y., Ma, Y., Hu, Q., Zhou, Z., Xiao, K., Wang, C.: Lightweight transmission behavior audit scheme for NDN industrial internet identity resolution and transmission based on blockchain. Electronics **12**(11), 2538 (2023)

17. Li, M., Xue, J., Wang, Y., Ma, R., Huo, W.: NACDA: naming-based access control and decentralized authorization for secure many-to-many data sharing. Electronics **12**(7), 1651 (2023)
18. Benmoussa, A., Kerrache, C.A., Calafate, C.T., Lagraa, N.: NDN-BDA: a blockchain-based decentralized data authentication mechanism for vehicular named data networking. Future Internet **15**(5), 167 (2023)
19. Komala, C.R., Dhanalakshmi, M., Gayathri, R., Aruna, R., GR, T.: VANET backbone in data networking and block-chain. J. Pharm. Negative Results 1539–1553 (2023)
20. Sabir, Z., Amine, A.: BIoVN: a novel blockchain-based system for securing internet of vehicles over NDN using bioinspired HoneyGuide. In: Maleh, Y., Tawalbeh, Lo.'ai, Motahhir, S., Hafid, A.S. (eds.) Advances in Blockchain Technology for Cyber Physical Systems. IT, pp. 177–192. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-93646-4_8
21. Wang, R., Njilla, L., Yu, S.: AC: an NDN-based blockchain network with erasure coding. In: 2023 International Conference on Computing, Networking and Communications (ICNC), pp. 591–595. IEEE (2023)
22. Khan, J.A., Ozbay, K.: AFFIRM: privacy-by-design blockchain for mobility data in Web3 using information centric fog networks with collaborative learning. In: 2023 International Conference on Computing, Networking and Communications (ICNC), pp. 456–462. IEEE (2023)
23. Sun, Y., Chen, S., Fang, Y., Xu, W., Luo, Q., Rui, L.: A trusted IoT communication architecture based on blockchain and named data network. In: Journal of Physics: Conference Series, vol. 2224, no. 1, p. 012091 (2022). https://doi.org/10.1088/1742-6596/2224/1/012091
24. Sultan, N.H., Varadharajan, V., Kumar, C., Camtepe, S., Nepal, S.: A secure access and accountability framework for provisioning services in named data networks. In: 2021 40th International Symposium on Reliable Distributed Systems (SRDS), Chicago, IL, USA, pp. 164–175 (2021). https://doi.org/10.1109/SRDS53918.2021.00025
25. Rosli, A., Hassan, S., Omar, M.H.: Data authentication mechanism using blockchain's proof-of-trust mechanism in named data networking. In: AIP Conference Proceedings, vol. 2608, no. 1. AIP Publishing (2023)
26. Zhao, H., Zhang, X., Li, R.: NFT-based access control in named data networks, pp. 139–146 (2022). https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00025
27. Kang, P., Wenzhong, Y., Ding, T.: Blockchain document forwarding and proof method based on NDN network. IEEE Access **10**, 75312–75322 (2022)
28. Miglani, A., Kumar, N.: Blockchain-based co-operative caching for secure content delivery in CCN-enabled V2G networks. IEEE Trans. Veh. Technol. **72**(4), 5274–5289 (2023). https://doi.org/10.1109/TVT.2022.3227291
29. Park, C.-S., Park, W.S., Woo, S.: Security bootstrapping for securing data plane and control plane in named data networking. IEEE Trans. Netw. Serv. Manag. https://doi.org/10.1109/TNSM.(2022).3232359
30. Magsi, A.H., Yovita, L.V., Ghulam, A., Muhammad, G., Ali, Z.: A content poisoning attack detection and prevention system in vehicular named data networking. Sustainability **15**(14), 10931 (2023)