Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability

Youness Bentayeb[1], Kenza Chaoui[2], Hassan Badir[3]
IDS Research Team, ENSAT, UAE, Tanger, Morocco[1, 2]
Department of Computer Science, ENSAT, UAE, Tanger, Morocco[3]

***Abstract*—The integration of blockchain and edge computing presents a transformative potential to enhance security, computing efficiency, and data privacy across diverse industries. This paper begins with an overview of blockchain and edge computing, establishing the foundational technologies for this synergy. It explores the key benefits of their integration, such as improved data security through blockchain's decentralized nature and reduced latency via edge computing's localized data processing. Methodologically, the paper employs a systematic analysis of existing technologies and challenges, emphasizing issues such as scalability, managing decentralized networks, and ensuring independence from cloud infrastructure. A detailed Ethereum-based case study demonstrates the feasibility and practical implications of deploying blockchain in edge computing environments, supported by a comparative analysis and an algorithmic approach to integration. The conclusion synthesizes the findings, addressing unresolved challenges and proposing future research directions to optimize performance and ensure the seamless convergence of these technologies.**

***Keywords*—Blockchain; edge computing; security; computing efficiency; data privacy**

I. INTRODUCTION

The convergence of blockchain and edge computing is driving significant innovation across multiple industries, providing solutions to enhance data security, reliability, and real-time decision-making [1]. Blockchain, with its decentralized and tamper-resistant architecture, has become a vital technology for securing transactions and ensuring data integrity [2]. Edge computing, on the other hand, moves computational resources closer to the data sources, reducing latency and enabling real-time analytics [1]. Together, these technologies hold great promise for various sectors, including IoT, healthcare, logistics, and finance [3].

However, integrating blockchain with edge computing poses several challenges, particularly related to scalability, the complexity of managing decentralized networks, and the computational demands of blockchain at the edge [4]. Yang et al. [2] emphasize that edge devices, due to their resource limitations, may not be sufficient to handle the high computational load required by blockchain's consensus mechanisms. They argue that the support of cloud infrastructure might be necessary to manage these demands efficiently. This viewpoint is reinforced by Nawaz et al. [6], who propose a hybrid edge-cloud architecture where computationally intensive tasks, such as smart contract execution and data storage, are offloaded to cloud servers while edge devices manage time-sensitive operations.

In the context of critical communication networks, Narouwa et al. [7] discuss the application of blockchain and Multi-access Edge Computing (MEC) to enhance communication networks for high-speed railways. Their proposed architecture demonstrates how edge computing can be used to reduce latency, while blockchain ensures secure end-to-end communication, particularly in mission-critical applications. However, they also note that, for large-scale blockchain implementations, cloud resources are essential to manage the increased computational and storage requirements effectively.

Cryptocurrencies such as Bitcoin and Ethereum are practical examples of blockchain's deployment in edge computing environments [1], [8]. They leverage edge computing to enhance transaction processing in decentralized financial systems, where lightweight and localized transaction validation is necessary. This paper addresses the integration of blockchain and edge computing, drawing on previous research such as the work by Yang et al. [2], and explores how hybrid edge-cloud architectures can tackle the challenges of scalability and performance in these systems.

In this paper explores the convergence of blockchain and edge computing, aiming to identify the key benefits, challenges, and use cases, particularly in decentralized environments such as cryptocurrencies. Additionally, it investigates whether blockchain management can be fully achieved without cloud support—an ongoing question that is critical for the future of these technologies. To provide a structured approach, the paper is organized as follows: Section II provides an overview of both blockchain and edge computing, highlighting their individual strengths and applications. Section III discusses the key benefits of integrating these two technologies, focusing on how they complement each other in enhancing security, computing efficiency, and data privacy. Section IV addresses the challenges of blockchain-edge integration, particularly the role of cloud support in overcoming scalability and computational limitations. Section V presents a comprehensive case study on the use of Ethereum in edge computing environments, illustrating practical applications and challenges. Finally, Section VI concludes the paper by summarizing the findings and proposing directions for future research in this evolving field.

II. OVERVIEW

A. Overview of Blockchain

Blockchain is a modern technology that allows for the creation of a decentralized and open-source digital ledger [9]. Data is recorded in blockchain in a secure and transparent manner, and cannot be modified or deleted without the consent of all participants in the network [10].

Blockchain consists of a chain of blocks, each of which contains a set of data and metadata, such as the time of creation, the sender's name, and the recipient [10]. Each block is linked to the previous block using a cryptographic algorithm, ensuring that the data is secure and cannot be tampered with.

Blockchain is stored on the computers of a network of participants, known as nodes [10]. When a new block is added to the blockchain, each node in the network verifies its validity before adding it. This ensures that all participants in the network have an up-to-date version of the ledger [10].

Blockchain consists of four main components:

- Block: A small unit of data that is stored in blockchain. Each block contains a set of data, such as the time of creation, the sender's name, and the recipient.
- Node: A computer that is connected to the blockchain network. Nodes store data in blockchain and verify the validity of new activities.
- Chain: A sequential order of blocks. Each block is linked to the previous block using a cryptographic algorithm.
- Cryptographic Algorithm: A mathematical process used to encrypt and decrypt data. Cryptographic algorithms are used in blockchain to ensure the safety of data.

Blockchain works through a process called blockchain mining. Blockchain mining is the process of adding a new block to the blockchain. To do this, nodes solve a complex mathematical equation. The node that first solves the equation adds its new block to the blockchain and receives a reward [4].

The validity of each new block is verified by all nodes in the network. If a new block is not verified, it will not be added to the blockchain [4], [11].

There are three main types of blockchain:

- Public blockchain: A blockchain that is accessible by anyone. Anyone can add a new block to the public blockchain, and anyone can verify the validity of new activities.
- Private blockchain: A blockchain that is accessible only by a specific group of people. Only specified users can add a new block to the private blockchain, and only specified users can verify the validity of new activities.
- Hybrid blockchain: A combination of public and private blockchain. Authorized people can access the hybrid blockchain.

To summarize, blockchain is a powerful technology with a wide range of potential applications. It is important to understand the basics of blockchain, including its components, how it works, and its types, in order to appreciate its full potential.

B. Overview of Edge Computing

Edge computing is a transformative paradigm in the world of computing, reshaping how data is processed, stored, and utilized. Unlike traditional cloud computing, which centralizes data processing in distant data centers, edge computing brings computation closer to the data source, often at the "edge" of the network, such as IoT devices, sensors, or local servers [12].

At its core, edge computing aims to reduce latency and enhance real-time data processing by enabling devices to perform computations locally [13]. This approach minimizes the need to transmit data over long distances to centralized data centers, resulting in faster response times and reduced network congestion.

Key elements of edge computing include:

- Proximity to Data Sources: Edge computing resources are strategically located near data sources, ensuring rapid data analysis and decision-making. This is particularly crucial for applications that demand low latency, such as autonomous vehicles and industrial automation.
- Distributed Architecture: Edge computing employs a distributed architecture, distributing computing tasks across a network of edge devices. This decentralization optimizes resource utilization and scalability.
- Efficiency: By processing data locally, edge computing reduces the burden on centralized cloud servers, leading to more efficient use of network bandwidth and reduced operational costs.
- Real-Time Processing: Edge computing supports real-time data processing and analytics, enabling immediate responses to critical events or conditions. This is essential for applications like remote monitoring, smart grids, and augmented reality.
- Security and Privacy: Edge computing enhances data security and privacy by keeping sensitive information closer to its source, reducing exposure to potential security breaches during data transmission.

Edge computing is not a replacement for cloud computing but rather a complementary approach [12]. Both technologies can work in tandem, with edge devices handling time-sensitive tasks and the cloud managing more resource-intensive processes and long-term data storage [12], [14].

This emerging technology has found applications in various fields, including:

- IoT and Smart Devices: Edge computing is integral to the Internet of Things (IoT) ecosystem, enabling smart devices to process data locally and make rapid decisions.
- Telecommunications: Telecom networks benefit from edge computing for tasks like content caching, network optimization, and low-latency services.

- Healthcare: In healthcare, edge computing supports real-time patient monitoring, data analysis, and diagnosis.
- Manufacturing: Industrial automation and robotics leverage edge computing for faster decision-making on the factory floor.
- Autonomous Vehicles: Edge computing is crucial for self-driving cars, allowing them to process sensor data in real-time for safe navigation.

Overall, edge computing is a promising new technology that can improve the performance, reliability, and security of a wide range of applications.

In the subsequent sections, we will explore how the fusion of edge computing and blockchain technology can unlock new possibilities in various industries.

III. Integration of Blockchain and Edge Computing: Key Benefits

The integration of blockchain and edge computing ushers in a host of transformative advantages for modern data-driven systems [15]. First and foremost, data security experiences a significant boost [17]. Leveraging blockchain's decentralized, tamper-resistant ledger and edge computing's localized data processing, the integrity and confidentiality of data are fortified. Unauthorized access and tampering become formidable hurdles, necessitating consensus from network participants, particularly vital in data-sensitive sectors like healthcare, finance, and supply chain management [16].

Moreover, this integration enhances system reliability substantially. The inherent decentralization of edge computing reduces dependency on a single central server or data center, a synergy that harmonizes well with blockchain's reliability mechanisms. Even in the face of isolated node or device failures, system functionality remains uninterrupted, a critical trait for applications such as autonomous vehicles and critical infrastructure [17][16].

Simultaneously, application performance receives a considerable uplift, as edge computing reduces latency by processing data closer to its source [11]. This proximity expedites real-time decision-making in applications such as augmented reality, remote monitoring, and smart grids [18].

Comparatively, when we consider integrating blockchain with cloud computing, some differences emerge [19]:

- Security: While blockchain integration with edge computing offers a high level of security through decentralization, combining blockchain with cloud computing relies on centralized server security, requiring stringent measures.
- Reliability: The reliance on centralized data centers and data transmission across networks in cloud computing may affect its reliability, unlike the decentralized edge nodes of edge computing, which ensure operations even in individual contract or device failures.
- Application Performance: Edge computing's local data processing significantly improves application performance, reducing latency. In contrast, cloud computing applications may experience added latency due to data transmission to remote data centers.
- Cost Efficiency: Integrating blockchain with edge computing greatly reduces operational costs by minimizing reliance on cloud infrastructure and lowering data transfer expenses. On the other hand, cloud computing involves costs related to running data centers and cloud storage, incurring additional expenses.

In Addition, the integration of blockchain with edge computing can be compared to the integration of blockchain with cloud computing [19]. The following table summarizes the key differences between these two approaches:

TABLE I. Comparison of Blockchain Integration Approaches

Feature	Blockchain and Edge Computing	Blockchain and Cloud Computing
Data Security	Enhanced [6]	Reduced [9]
System Reliability	Enhanced [2]	Reduced [8]
Application Performance	Enhanced [5]	Unaffected [20]
Cost-Efficiency	Enhanced [2]	Unaffected [8]
Suitable use cases	Data-sensitive applications, applications requiring real-time processing, applications with high security requirements [20]	Applications that require a lot of computing power, applications that need to store large amounts of data [20]

As shown in the Table I, the integration of blockchain with edge computing offers a number of advantages over the integration of blockchain with cloud computing. Specifically, it provides better data security, system reliability, and application performance. Additionally, it is more suitable for use cases that require real-time processing and high security requirements.

Last but certainly not least, the integration of blockchain and edge computing delivers compelling cost-efficiency benefits [2]. By minimizing reliance on extensive cloud infrastructure and associated data transmission costs, operational expenses are significantly reduced. This is further augmented by heightened system reliability, which helps mitigate revenue losses associated with system failures [2].

To summarize, the integration of blockchain and edge computing presents an enticing proposition for businesses across diverse sectors. It promises heightened operational efficiency, fortified data privacy, and robust data management practices, all while positioning itself as a pioneering solution at the intersection of security, reliability, performance, and cost-effectiveness in the evolving landscape of data-driven systems.

IV. Challenges and Cloud Independence in Blockchain-Edge Integration

A. Challenges in Integrating Blockchain and Edge Computing

The integration of blockchain and edge computing presents significant potential for enhancing both security and

performance in modern data systems [6]. However, several critical challenges—spanning technical, performance, security, and regulatory dimensions—must be addressed to fully realize this potential. One of the foremost technical challenges is scalability. As decentralized networks grow to accommodate increasing data demands, the complexity of maintaining data integrity and security across numerous nodes becomes more pronounced. This issue is particularly salient in edge computing environments, where devices often lack the processing power and storage capacity required for executing resource-intensive blockchain consensus mechanisms, such as Proof of Work (PoW) [21],[4]. Moreover, the inherently decentralized structure of blockchain introduces latency challenges, which run counter to the low-latency requirements of edge computing. The time required for transaction verification and block validation can degrade performance, especially in latency-sensitive applications such as the Internet of Things (IoT) and real-time data analytics [22].

Security concerns also arise due to the movement of data between edge and cloud environments, where the risk of cyberattacks increases during transmission [5]. While blockchain's decentralized architecture enhances security by distributing control, edge devices typically lack the robust security mechanisms available in cloud-based systems, making them more susceptible to threats [23]. Managing identity and access in decentralized systems further complicates this challenge. Although cloud-based solutions may offer strong identity management capabilities, their reliance on centralized systems could undermine the decentralized ethos of blockchain, raising issues of dependency and control.

From a regulatory perspective, compliance with frameworks such as the General Data Protection Regulation (GDPR) adds another layer of complexity [5]. The decentralized nature of blockchain makes it difficult to pinpoint where and how data is stored, complicating efforts to ensure compliance with data privacy laws. This issue becomes even more challenging in cross-border scenarios, where legal frameworks may vary significantly [5]. As a result, questions surrounding data ownership and control become especially pertinent in industries governed by strict regulatory requirements. Addressing these technical, performance, security, and regulatory challenges is essential for unlocking the full potential of blockchain and edge computing in modern data systems.

Several studies have sought to address these challenges through various approaches that integrate blockchain with edge and cloud computing, particularly within IoT environments. Table II summarizes key contributions from these works, highlighting how they tackle issues related to scalability, security, decentralization, and performance in blockchain-enabled systems.

TABLE II. KEY CONTRIBUTIONS IN BLOCKCHAIN AND EDGE COMPUTING INTEGRATION

Ref.	Key Contributions	Layered Architecture	Cryptocurrency Involvement	Blockchain Decentralization	IoT Applications	Cloud of Things	Cloud Computing	Journal
[5]	Exploring the Integration of Edge Computing and Blockchain to Enhance IoT Systems and Address Key Challenges in Security and Efficiency	✓	✗	✓	✓	✓	✓	ScienceDirect
[1]	Surveying the Integration of Blockchain and Edge Computing to Enhance Resource Utilization and Security in IoT Applications	✗	✗	✗	✓	✓	✓	ScienceDirect
[6]	EdgeBoT as a Smart Contracts-Based Platform to Enhance Data Ownership and Privacy in IoT Through Blockchain Technology	✗	✗	✓	✓	✓	✓	Sensors

[25]	Proposing a Scalable and Secure Cloud Architecture to Enhance IoT Integration with Cryptographic Techniques for Improved Multi-User Access and Data Security	✓	✗	✓	✓	✗	✓	IEEE Access
[4]	The Convergence of Blockchain and Edge of Things Exploring Opportunities, Applications, and Security Challenges in the BEoT Paradigm	✗	✗	✗	✗	✗	✓	IEEE IoTJ
[26]	The Potential of Blockchain Technology in Integrated IoT Networks for Scalable Intelligent Transportation Systems in India	✗	✗	✗	✓	✗	✓	ScienceDirect
[3]	Advancements in Edge Computing: Integrating AI and Blockchain for Enhanced Performance in Maritime and Aerial Systems	✗	✗	✓	✓	✓	✓	IEEE Access
[16]	A Blockchain-Assisted Handover Authentication Scheme for Intelligent Telehealth Systems in Multi-Server Edge Computing Environments	✗	✓	✗	✓	✗	✓	ScienceDirect
[27]	A Novel Trust-Aware Blockchain-Based Framework for Enhancing Privacy and Security in Decentralized IoT Applications	✗	✗	✗	✓	✓	✓	Electronics
[28]	Analyzing the Integration of Blockchain in IoT and Healthcare: Enhancing Data Security and Management Strategies	✗	✗	✗	✓	✗	✓	ScienceDirect

[18]	Integrating Blockchain and Federated Learning for Enhanced Security and Privacy in Smart Healthcare with a Novel Conceptual Framework	✗	✓	✗	✓	✗	✓	IEEE Internet of Things Journal
[13]	The Evolution of Mobile Cloud Computing and Edge Computing for Enhanced Mobile Applications and Open Research Challenges	✗	✗	✓	✓	✗	✓	Springer
[29]	Analyzing Security Challenges and Solutions for Data Privacy in Cloud-IoT Environments with Insights into Emerging Technologies	✗	✗	✗	✗	✗	✓	Springer
[7]	Proposing a Unified Control Framework for Enhancing Railway Communications Through Integration of Advanced Technologies in the Era of 5G and Future 6G	✗	✗	✗	✗	✗	✓	IEEE Access
[30]	Proposing a Blockchain-Based Cloud Integrated IoT Application for Enhanced Security and Intruder Detection in Challenging Environments	✗	✓	✓	✗	✗	✓	Springer
[31]	Integrating Blockchain and Edge Computing to Create a Secure, Scalable Architecture for Data Processing in Industry 4.0 Applications	✗	✗	✓	✗	✗	✓	Springer

Several studies contributions illustrate a variety of approaches to integrating blockchain with edge computing, addressing challenges such as scalability, security, and decentralization. By leveraging multi-layered architectures and optimizing resource allocation, these works enhance system performance, security, and regulatory compliance.

Based on the studies presented in Table II, it is evident that while various approaches have been proposed to tackle challenges like scalability, security, and performance, the role of cloud computing remains a consistent element across all studies. This pervasive presence of the cloud raises an important question: Can blockchain data management be fully achieved in edge computing without cloud support? In other words, is the cloud indispensable in all cases of integrating blockchain and edge computing?

B. Blockchain-Edge Computing Integration and Cloud Support

The integration of blockchain with edge computing has

gained considerable attention due to its potential to address challenges such as latency reduction and enhanced security in decentralized systems. However, upon analyzing recent studies, it becomes clear that cloud computing plays a crucial role in most cases of blockchain-edge integration. While edge computing is effective for real-time data processing and localized decision-making, cloud support is often required for tasks that demand higher computational power, scalability, and long-term data storage.

A graphical analysis based on the studies presented in Table II emphasizes the significant presence of cloud computing in blockchain-edge integration research. As demonstrated in Fig. 1, a substantial proportion of the studies rely on cloud services to complement the resource-constrained nature of edge devices. The cloud not only provides additional computational resources for tasks like blockchain mining, transaction verification, and smart contract execution, but it also enables efficient data storage and management for decentralized applications.

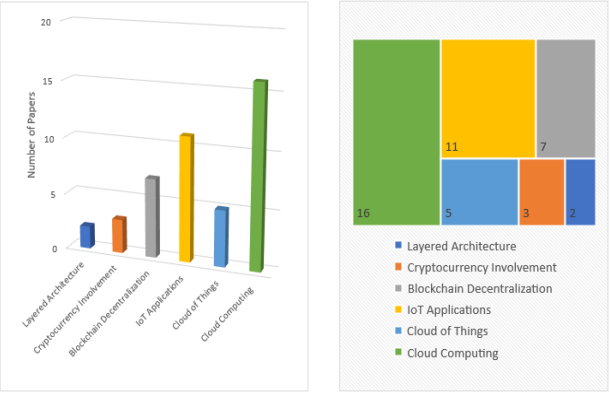

Fig. 1. Prevalence of cloud support in blockchain-edge computing integration studies.

As illustrated in Fig. 1, the majority of blockchain-edge computing integrations incorporate cloud support, reflecting its indispensable role in managing the complexity and resource demands of decentralized networks. For example, studies by Tri et al. [5] and Yang et al. [2] showcase how cloud infrastructure serves as the backbone for scaling blockchain operations, ensuring that the limitations of edge devices do not hinder overall system performance. The cloud efficiently offloads computationally intensive tasks, such as consensus mechanisms, while enabling edge devices to focus on real-time data processing and localized operations.

Despite the strong reliance on cloud computing in many cases, there are specific scenarios where blockchain and edge computing can be successfully integrated without the need for cloud services. These cases generally arise in smaller-scale, localized applications, where the resource demands of blockchain operations are relatively low, and large-scale data storage or significant computational power is not required.

1) Localized IoT networks: In small, self-contained IoT environments—such as smart homes or small industrial setups—blockchain can be integrated with edge devices to manage secure transactions and ensure data integrity without the need for cloud support. In these scenarios, lightweight consensus mechanisms like Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) can be efficiently handled by edge devices, thus eliminating the need for external cloud resources [32].

2) Decentralized autonomous systems: Some decentralized systems, such as autonomous drones or vehicular networks, can operate blockchain-based frameworks using only edge computing. These systems typically rely on localized blockchain networks, where each node (e.g., a drone or vehicle) has sufficient computational power to process transactions and validate blocks, avoiding the latency and delays introduced by cloud-based solutions [20].

3) Data sovereignty and privacy-centric applications: In highly sensitive environments, such as healthcare or military applications, where data sovereignty and privacy are paramount, blockchain and edge computing can be combined to maintain strict control over data without transmitting it to cloud servers. These use cases focus on local data processing and handling, ensuring privacy and removing reliance on external cloud providers [5].

These examples demonstrate that while cloud support is beneficial in many cases, it is not always essential for blockchain-edge integration. In environments where computational demands are modest and concerns about latency or privacy are significant, blockchain and edge computing can function effectively without cloud involvement. However, for most large-scale applications, particularly those requiring scalability, redundancy, or complex data management, cloud computing remains a critical component, enabling seamless and efficient integration between blockchain and edge computing.

V. Ethereum in Edge Computing: A Comprehensive Case Study

The integration of Ethereum within edge computing environments presents a powerful solution for decentralized, real-time applications. By leveraging edge computing, Ethereum can enhance performance and scalability through localized data processing, thereby reducing latency and alleviating network congestion [1][7]. This section explores the technical aspects, advantages, concerns, and potential future developments for Ethereum as a blockchain platform deployed at the edge [3]. Furthermore, it highlights how decentralized financial systems can capitalize on the processing capabilities of edge computing to provide more efficient and secure solutions, ultimately paving the way for innovative applications in IoT and beyond [8]. By addressing these factors, Ethereum demonstrates its capacity to evolve within edge environments, enhancing its role in the decentralized landscape.

A. Technical Advantages of Ethereum in Edge Computing

Integrating Ethereum with edge computing brings unique technical benefits that enhance the efficiency, scalability, and security of decentralized applications. Ethereum's design, coupled with edge computing's localized processing capabilities, makes it particularly well-suited for applications that require low latency, real-time processing, and energy efficiency. Key technical advantages include:

1) Real-Time processing and reduced latency:

a) Localized transaction validation: By handling transactions closer to the data source, edge devices can validate and process Ethereum transactions locally, which greatly reduces latency compared to centralized blockchain processing [19]. This is especially valuable for applications in IoT and smart city infrastructure where rapid decision-making is critical.

b) Enhanced decentralized applications (dApps): Real-time data processing at the edge allows decentralized applications to operate with faster response times, improving user experience in applications like financial trading, supply chain management, and decentralized exchanges (DEXs) that rely on immediate updates [2].

c) Smart contract execution at the edge: Ethereum's capability to execute smart contracts can be enhanced in edge environments, where real-time contract execution reduces the time required for transactions to finalize. This brings significant improvements for IoT applications that rely on automated responses based on data analytics.

2) Energy efficiency through Proof-of-Stake (PoS):

a) Reduced resource consumption: Ethereum's shift from Proof-of-Work (PoW) to Proof-of-Stake (PoS) consensus drastically lowers the computational and energy demands on devices participating in the network [3], [2]. This reduction is crucial for edge devices, which typically have limited resources compared to traditional data centers.

b) Compatibility with resource-constrained edge devices: PoS allows edge devices to contribute to the network without requiring the intensive hardware needed for PoW mining, making it feasible for smaller, more energy-efficient devices to play an active role in transaction validation and block creation within the Ethereum network [2].

c) Support for sustainability goals: By using PoS, Ethereum aligns well with the sustainability objectives of many IoT and smart infrastructure projects, where energy consumption is a key concern [2][5].

3) Scalability with layer two solutions:

a) Layer 2 offloading: Ethereum's Layer 2 scaling solutions, such as rollups and zk-Rollups, enable transactions to be processed off-chain while still anchored to the main Ethereum blockchain for security. This alleviates congestion on the main network, making it easier for edge devices to handle high transaction volumes without compromising performance [6].

b) Improved throughput: By batching multiple transactions off-chain, Layer 2 solutions significantly improve throughput, making Ethereum capable of handling more transactions per second (TPS) without overwhelming edge devices [16]. This is particularly useful in IoT ecosystems, where numerous small transactions are generated by devices.

c) Interoperability with other blockchains: Many Layer 2 solutions on Ethereum are designed with interoperability in mind, allowing edge devices in one network to interact with other blockchain ecosystems. This cross-chain compatibility fosters greater flexibility for decentralized applications, particularly in settings like supply chain networks and logistics [2][8].

4) Security benefits of decentralized processing:

a) Enhanced data security: The decentralized nature of Ethereum, combined with edge computing, strengthens data security by processing and storing data closer to the source. This decentralized architecture reduces the risk of centralized points of failure and data breaches, which is especially beneficial for sensitive applications such as healthcare and finance [28].

b) Zero-Knowledge proofs (zk-SNARKs) for privacy: Ethereum's zk-SNARK technology enables data verification without revealing sensitive information, supporting privacy in edge applications where personal or confidential data may be processed [15]. This ensures that data privacy is maintained while still benefiting from Ethereum's secure transaction model.

c) Tamper-Resistant IoT networks: By deploying Ethereum nodes on edge devices, IoT networks gain resilience against tampering and unauthorized access, as data must undergo consensus verification before being accepted. This adds a strong layer of security to edge-based IoT environments [22].

In summary, Ethereum's adaptable architecture, energy-efficient consensus mechanisms, and advanced Layer 2 scaling solutions make it exceptionally well-suited for deployment in edge computing environments, where real-time processing, scalability, and security are paramount for next-generation decentralized applications.

B. Comparison of Ethereum with Other Cryptocurrencies in Edge Environments

Deploying blockchain in edge computing requires energy efficiency, low-latency processing, and scalability [2]. While Ethereum's features make it suitable for edge computing, a comparison with Bitcoin and Polkadot reveals key distinctions, as shown in Table III, which highlights the key comparisons of Ethereum, Bitcoin, and Polkadot for edge computing applications.

TABLE III. KEY COMPARISONS OF ETHEREUM, BITCOIN, AND POLKADOT FOR EDGE COMPUTING APPLICATIONS

Feature	Ethereum	Bitcoin	Polkadot
Consensus Mechanism	Proof-of-Stake (PoS)	Proof-of-Work (PoW)	Nominated Proof-of-Stake (NPoS)
Energy Efficiency	High, low-power PoS [1]	Low, resource-intensive [2]	Moderate, optimized for PoS [3]
Smart Contract Support	Extensive (EVM)	Limited scripting [4]	Multi-chain smart contracts
Layer 2 Scaling	Robust (Rollups) [5]	Limited	Cross-chain scalability (parachains)
Latency Sensitivity	Optimized for real-time dApps [6]	Slower confirmations [7]	Optimized for cross-chain processing

Ethereum's Proof-of-Stake (PoS) consensus mechanism greatly reduces energy consumption, making it compatible with

edge device constraints, where power and resources are often limited. Bitcoin's Proof-of-Work (PoW), in contrast, is computationally demanding and thus unsuitable for resource-constrained environments. Polkadot's Nominated Proof-of-Stake (NPoS) model is similarly efficient and well-suited for multi-chain edge networks, where various blockchains need to operate seamlessly.

C. Proposed Algorithm for Ethereum-Based Transactions in Edge Environments

Some studies have introduced algorithms to optimize blockchain integration in edge computing, focusing on reducing latency and managing data consistency. Common approaches include distributed consensus mechanisms [1], off-chain scaling solutions like Plasma and state channels [2], and layered architectures that rely on cloud support for intensive processing [3]. While effective, these methods often depend on centralized infrastructures, potentially limiting decentralization.

Our proposed algorithm presents a decentralized transaction validation framework tailored for Ethereum-based systems in edge environments. By utilizing local consensus among edge nodes and Layer 2 scaling, the algorithm minimizes cloud dependency, enabling autonomous, secure transaction processing directly at the edge.

Algorithm 1: Decentralized Transaction Validation at the Edge Using Ethereum

Objective: Efficiently process transactions on Ethereum using edge devices while maintaining security and minimizing latency.

Input: Transaction data (Tx), Node ID (Edge Node), Blockchain state (S)

Output: Validated transaction and updated blockchain state (S')

1. Edge device (Node) receives a transaction request (Tx).
2. Node verifies transaction data (Tx) using Ethereum's cryptographic validation method [5].
3. If the transaction is valid:
    1. Node checks its local blockchain state (S) to ensure consistency.
    2. Transaction is added to a local temporary block.
4. The temporary block is broadcasted to nearby nodes in the edge network for additional validation (Consensus) [6].
5. Upon achieving consensus among edge devices, the validated block is appended to the blockchain.
6. If Layer 2 rollup is enabled, the batch of transactions is compressed and sent to the main Ethereum chain for final settlement [7].
7. **Output:** Updated blockchain state (S') is stored across all edge nodes.

This algorithm utilizes the proximity of edge devices for transaction validation, minimizing reliance on centralized servers or cloud infrastructures. By incorporating Layer 2 scaling solutions, such as rollups, the algorithm offloads part of the computational workload to off-chain solutions, optimizing resource use in constrained edge devices. Consensus mechanisms within the edge network ensure data consistency before broadcasting the validated block to the larger Ethereum blockchain, balancing security and speed [2].

D. Regulatory and Privacy Concerns

While the technical feasibility of deploying Ethereum in edge environments is promising, regulatory challenges must also be addressed. Ethereum's decentralized nature complicates data privacy and ownership, particularly when considering laws like the General Data Protection Regulation (GDPR) in Europe. Key regulatory issues include:

- Data Privacy: Since Ethereum transactions are publicly visible, storing sensitive data (e.g., personal or medical information) on the blockchain may violate privacy regulations. Solutions like Zero-Knowledge Proofs (zk-SNARKs), which allow verification of transactions without revealing sensitive information, could mitigate this issue [9].
- Cross-Jurisdictional Compliance: With edge devices deployed globally, ensuring compliance with different legal frameworks across borders poses a significant challenge [11].
- Data Sovereignty: Edge environments often operate in localized settings, and the transmission of data to global blockchains raises concerns about who controls and owns that data [11].

E. Future Research Directions

The integration of Ethereum within edge computing environments presents promising opportunities, yet several key challenges in efficiency, security, and scalability remain to be addressed. Future research directions that may significantly advance this field include the following:

1) Hybrid architectures: Investigating hybrid architectures that combine both edge and cloud resources could enhance the performance of Ethereum-based applications in edge environments. A proposed approach involves handling time-sensitive, low-latency tasks, such as initial transaction validations, at the edge, while offloading computationally intensive tasks (e.g., complex smart contract execution and large-scale data analysis) to the cloud. This distribution strategy optimizes the limited resources of edge devices while leveraging cloud computational power to handle more demanding tasks, leading to more efficient operations across edge-cloud ecosystems [24].

2) Improved consensus mechanisms: To promote scalability and energy efficiency in edge environments, developing lightweight consensus protocols tailored for edge computing is essential. Traditional consensus algorithms, such as Proof of Work (PoW), are highly resource-intensive and unsuitable for resource-constrained edge devices. Future research should explore alternative protocols, such as Proof of Authority (PoA) or adapted Byzantine Fault Tolerance (BFT) models, which could reduce computational overhead and energy requirements while maintaining security. Such protocols would enable resource-constrained edge devices to

participate effectively in Ethereum networks without compromising network performance [13].

3) Security enhancements: Enhancing security for Ethereum-edge networks is critical, given the vulnerabilities of edge devices to cyber threats. Research into advanced cryptographic techniques, including secure multiparty computation and zero-knowledge proofs, may strengthen data privacy and integrity within decentralized edge networks. Additionally, exploring post-quantum cryptographic methods is crucial for ensuring resilience against potential future threats from quantum computing, ultimately securing Ethereum-edge networks for long-term operation [2].

4) Decentralized data storage solutions: The adoption of decentralized storage solutions offers a pathway to securely manage and distribute data across edge environments. Technologies such as the InterPlanetary File System (IPFS) provide secure, distributed data storage without centralized dependencies. Integrating IPFS with Ethereum could enable edge networks to store data with higher redundancy and fault tolerance, even in disconnected or remote environments [1]. This is particularly advantageous for Internet of Things (IoT) ecosystems, where data generated by edge devices requires secure, decentralized storage and accessibility [2].

Expanding research in these areas could substantially enhance the efficiency, scalability, and security of Ethereum applications within edge computing environments. By addressing these challenges, researchers can contribute to building a robust foundation for decentralized applications capable of operating reliably across distributed edge-cloud ecosystems.

VI. Conclusion

The integration of blockchain and edge computing presents a transformative opportunity to improve data security, computing efficiency, and data privacy across various industries, particularly in IoT environments where real-time data processing and secure transactions are crucial. This paper has explored the foundational principles of these two technologies, examined their synergies, and highlighted the significant benefits of their convergence. By leveraging blockchain's decentralized, tamper-resistant structure alongside edge computing's ability to process data locally, this integration promises substantial advancements in performance, reducing latency and enhancing security in decentralized networks. Furthermore, the Ethereum-based case study offered practical insights into how blockchain can be deployed in edge environments, illustrating both its feasibility and the challenges that arise in ensuring efficiency and scalability.

The contributions of this research lie in its systematic analysis of the integration of blockchain and edge computing, with a particular focus on the practical implications of their convergence. The study provides valuable perspectives on the ways these technologies can enhance security through blockchain's immutability and edge computing's localized data processing, while also addressing the challenges related to computational demands, scalability, and managing decentralized networks. The Ethereum case study served as a critical example of the potential applications in edge environments, but it also underscored the importance of addressing challenges like computational load, network management, and the reliance on cloud infrastructure for certain tasks. This paper contributes to the ongoing dialogue in the field by identifying these key challenges and providing a foundation for future studies focused on optimizing these systems.

Despite the promising potential of blockchain and edge computing, this research is not without its limitations. The case study was limited to Ethereum, and while it provided useful insights, it may not fully represent the diverse array of blockchain platforms with differing consensus mechanisms or resource requirements. Additionally, the study focused primarily on the computational aspects of blockchain at the edge, leaving out considerations around hardware diversity in edge devices, which could impact the integration's performance across different environments. While the hybrid edge-cloud architecture discussed in this paper provides a practical solution, the potential challenges of security, privacy, and the added complexity of cloud dependencies need further investigation, particularly when considering large-scale deployments.

Looking ahead, future research should address several critical areas to optimize the integration of blockchain and edge computing. First, there is a need for the development of lightweight consensus mechanisms that can reduce the computational burden on edge devices, ensuring that blockchain systems remain secure and decentralized while being efficient enough to operate in resource-constrained environments. Second, scalable architectures that can support the growing demands of decentralized edge computing systems should be explored. These architectures should balance the need for real-time processing with the constraints of limited edge resources, while also maintaining the integrity of the blockchain. Finally, further exploration of data privacy solutions is essential, particularly in decentralized systems. Techniques such as zero-knowledge proofs and advanced encryption methods could help ensure privacy without sacrificing performance, enabling secure blockchain operations in edge environments. Addressing these areas will be key to advancing the integration of blockchain and edge computing, enabling the development of secure, efficient, and scalable decentralized systems for future data-driven applications.

References

[1] Xue, H., Chen, D., Zhang, N., Dai, H.-N., & Yu, K. (2022). Integration of blockchain and edge computing in Internet of Things: A survey. arXiv. https://arxiv.org/abs/2205.13160.

[2] Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. IEEE Communications Surveys & Tutorials, 21(2), 1508-1532. https://doi.org/10.1109/COMST.2019.2894727

[3] A. Alanhdi and L. Toka, "A Survey on Integrating Edge Computing With AI and Blockchain in Maritime Domain, Aerial Systems, IoT, and Industry 4.0," in IEEE Access, vol. 12, pp. 28684-28709, 2024, doi: 10.1109/ACCESS.2024.3367118.

[4] Gadekallu, T. R., Pham, Q.-V., Nguyen, D. C., Maddikunta, P. K. R., Deepa, N., B, P., Pathirana, P. N., Zhao, J., & Hwang, W.-J. (2021). Blockchain for edge of things: Applications, opportunities, and challenges. arXiv. https://arxiv.org/abs/2110.05022.

[5] Tri Nguyen, Huong Nguyen, Tuan Nguyen Gia, Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security,

and applications, Journal of Network and Computer Applications, Volume 226, 2024, 103884, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2024.103884.

[6] Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Nguyen Gia, T., Bashir, A.K., Kan, H., & Westerlund, T. (2020). Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. *Sensors*, 20(14), 3965. https://doi.org/10.3390/s20143965

[7] Narouwa, M., Mendiboure, L., Badis, H., Maaloul, S., Berbineau, M., & Langar, R. (2024). Enabling Network Technologies For Flexible Railway Connectivity. *IEEE Access*, 12, 151532-151547. https://doi.org/10.1109/ACCESS.2024.3479879.

[8] W. Jaafar, K. Jean Romeo Beyara, I. Aouini, J. Ben Abderrazak and H. Yanikomeroglu, "On the Deployment of Blockchain in Edge Computing Wireless Networks," 2022 IEEE 11th International Conference on Cloud Networking (CloudNet), Paris, France, 2022, pp. 168-176, doi: 10.1109/CloudNet55617.2022.9978739.

[9] Bentayeb, Youness & Badir, Hassan & En-Nahnahi, Noureddine. (2023). Blockchain-Based Cloud Computing: Model-Driven Engineering Approach. 10.1007/978-3-031-26384-2_55.

[10] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf

[11] B. C. Girish Kumar, P. Nand and V. Bali, "Opportunities and Challenges of Blockchain Technology for Tourism Industry in Future Smart Society," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2022, pp. 318-323, doi: 10.1109/CCiCT56684.2022.00065.

[12] Yu, W., et al.: A survey on the edge computing for the Internet of Things. IEEE Access 6, 6900–6919 (2018).

[13] Dimou, A., Iliopoulos, C., Polytidou, E., Dhurandher, S.K., Papadimitriou, G., Nicopolitidis, P. (2022). A Comprehensive Review on Edge Computing: Focusing on Mobile Users. In: Nicopolitidis, P., Misra, S., Yang, L.T., Zeigler, B., Ning, Z. (eds) Advances in Computing, Informatics, Networking and Cybersecurity. Lecture Notes in Networks and Systems, vol 289. Springer, Cham. https://doi.org/10.1007/978-3-030-87049-2_30

[14] K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," in IEEE Access, vol. 8, pp. 85714-85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[15] L. Fotia, F. C. Delicato and G. Fortino, "Integrating Blockchain and Edge Computing in Internet of Things: Brief Review and Open Issues," 2021 International Conference on Cyber-Physical Social Intelligence (ICCSI), Beijing, China, 2021, pp. 1-6, doi: 10.1109/ICCSI53130.2021.9736164.

[16] Wenming Wang, Haiping Huang, Lingyan Xue, Qi Li, Reza Malekian, Youzhi Zhang, Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment, Journal of Systems Architecture, Volume 115, 2021, 102024, ISSN 1383-7621.

[17] A. C. Baktir, A. Ozgovde and C. Ersoy, "How Can Edge Computing Benefit From Software-Defined Networking: A Survey, Use Cases, and Future Directions," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2359-2391, Fourthquarter 2017, doi: 10.1109/COMST.2017.2717482.

[18] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani and X. Wei, "Blockchain Meets Federated Learning in Healthcare: A Systematic Review With Challenges and Opportunities," in IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14418-14437, 15 Aug.15, 2023, doi: 10.1109/JIOT.2023.3263598.

[19] T. R. Gadekallu et al., "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," in IEEE Internet of Things Journal, vol. 9, no. 2, pp. 964-988, 15 Jan.15, 2022, doi: 10.1109/JIOT.2021.3119639.

[20] Gao, Q., Xiao, J., Cao, Y., Deng, S., Ouyang, C., & Feng, Z. (2023). Blockchain-based collaborative edge computing: Efficiency, incentive and trust. Journal of Cloud Computing, 12(1), 72. https://doi.org/10.1186/s13677-023-00452-4.

[21] Oliveira, Miguel, Sumit Chauhan, Filipe Pereira, Carlos Felgueiras, and David Carvalho. 2023. "Blockchain Protocols and Edge Computing Targeting Industry 5.0 Needs" Sensors 23, no. 22: 9174. https://doi.org/10.3390/s23229174

[22] Yuanxing Yin, Xinyu Wang, Huan Wang, Baoli Lu, Application of edge computing and IoT technology in supply chain finance, Alexandria Engineering Journal, Volume 108, 2024, Pages 754-763, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2024.09.016.

[23] Bentayeb, Youness & Badir, Hassan. (2024). Blockchain-Based Cloud Computing: A Comparative Study of BoC, CoB, and MBC. 255-260. 10.1007/978-3-031-52388-5_24.

[24] Andriulo, F.C.; Fiore, M.; Mongiello, M.; Traversa, E.; Zizzo, V. Edge Computing and Cloud Computing for Internet of Things: A Review. Informatics 2024, 11, 71. https://doi.org/10.3390/informatics11040071

[25] R. R. Irshad *et al*., "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," in *IEEE Access*, vol. 11, pp. 105479-105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[26] Arya Kharche, Sanskar Badholia, Ram Krishna Upadhyay, Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India, Blockchain: Research and Applications, Volume 5, Issue 2, 2024, 100188, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2024.100188.

[27] Al Hwaitat, Ahmad K., Mohammed Amin Almaiah, Aitizaz Ali, Shaha Al-Otaibi, Rima Shishakly, Abdalwali Lutfi, and Mahmaod Alrawad. 2023. "A New Blockchain-Based Authentication Framework for Secure IoT Networks" *Electronics* 12, no. 17: 3618. https://doi.org/10.3390/electronics12173618

[28] Endale Mitiku Adere, Blockchain in healthcare and IoT: A systematic literature review, Array, Volume 14, 2022, 100139, ISSN 2590-0056, https://doi.org/10.1016/j.array.2022.100139.

[29] Pathak, M., Mishra, K.N. & Singh, S.P. Securing data and preserving privacy in cloud IoT-based technologies an analysis of assessing threats and developing effective safeguard. *Artif Intell Rev* **57**, 269 (2024). https://doi.org/10.1007/s10462-024-10908-x

[30] Rupa, Ch & Srivastava, Gautam & Gadekallu, Thippa & Reddy, Praveen & Bhattacharya, Sweta. (2021). A Blockchain Based Cloud Integrated IoT Architecture Using a Hybrid Design. 10.1007/978-3-030-67540-0_36.

[31] Sittón-Candanedo, I. (2020). RETRACTED CHAPTER: A New Approach: Edge Computing and Blockchain for Industry 4.0. In: Herrera-Viedma, E., Vale, Z., Nielsen, P., Martin Del Rey, A., Casado Vara, R. (eds) Distributed Computing and Artificial Intelligence, 16th International Conference, Special Sessions. DCAI 2019. Advances in Intelligent Systems and Computing, vol 1004. Springer, Cham. https://doi.org/10.1007/978-3-030-23946-6_25

[32] Bo Gan, Yaojie Wang, Qiwu Wu, Yang Zhou, Lingzhi Jiang, EIoT-PBFT: A multi-stage consensus algorithm for IoT edge computing based on PBFT, Microprocessors and Microsystems, Volume 95, 2022, 104713, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2022.104713.