Integrating Blockchain with IoT: A Survey on Secure and Power-efficient Blockchain Architecture

Serhii Kozlovskyi[1], Mykhailo Dombrovskyi[1]

[1] *West Ukrainian National University, 11 Lvivska Street, Ternopil, 46009, Ukraine*

Abstract

The exponential expansion of the Internet of Things (IoT) in various sectors underscores an urgent need for secure and efficient communication channels within its networks. Given the extensive yet resource-constrained nature of IoT devices, conventional security strategies are often inadequate, highlighting the necessity for novel solutions to ensure data integrity and privacy. Blockchain technology, distinguished by its decentralization, immutability, and transparency, emerges as a compelling candidate to mitigate these security vulnerabilities. This research is dedicated to identifying the optimal blockchain architecture for IoT environments, mindful of the specific resource limitations of IoT devices and networks. Through a thorough comparative analysis of different blockchain architectures – examining their scalability, security attributes, and resource efficiency – our study identifies a blockchain framework that markedly improves communication security within IoT ecosystems, while accommodating the unique constraints of IoT systems. The research discovers that a particular blockchain architecture, notable for its streamlined design and efficient consensus mechanism, is exceptionally well-suited to the rigorous demands of the IoT. This investigation not only contributes to the theoretical understanding of blockchain applications in IoT but also enriches the literature by offering a detailed comparison of blockchain architectures in the IoT context, thereby paving the way for future inquiries focused on optimizing these architectures for real-world IoT settings. Additionally, this paper outlines our examination of leading distributed ledger technologies (DLT) and their compatibility with the IoT domain, ensuring the study's objectives are clearly defined and addressed.

Keywords

DLT, IoT, blockchain, DAG, on-chain blockchain, off-chain blockchain, cross-chain blockchain

1. Introduction

The Internet of Things (IoT) has emerged as a transformative force in the digital landscape, seamlessly integrating physical devices with the Internet to revolutionize how we live, work, and interact with our environment. This integration has facilitated a new era of efficiency and innovation, enabling smart homes, healthcare monitoring, industrial automation, and more. The IoT's capacity to collect, analyze, and act on data in real time has unlocked unprecedented operational efficiencies and personalized user experiences, making it a critical component of modern business strategies and urban development.

The proliferation of IoT devices globally is a testament to the technology's impact and adoption across different sectors, with an upward trend that shows no signs of slowing. This rapid growth is illustrated in Fig. 1, which presents a comprehensive statistic illustrating the exponential increase in the number of IoT devices worldwide. The surge in IoT devices is fueled by the continuous advancements in technology, decreasing costs of IoT components, and the growing recognition of IoT's potential to enhance efficiency, productivity, and quality of life.

Despite the numerous benefits, the widespread adoption of IoT technologies is not without challenges. Security vulnerabilities, scalability issues, and resource constraints represent significant hurdles to the effective deployment of IoT solutions.

The First International Workshop of Young Scientists on Artificial Intelligence for Sustainable Development; May 10-11, 2024, Ternopil, Ukraine

koslovckiy@gmail.com (S. Kozlovskyi); m.dombrovskyi@wunu.edu.ua (M. Dombrovskyi)

0009-0000-5610-8158 (S. Kozlovskyi); 0000-0002-5582-5793 (M. Dombrovskyi)

CEUR Workshop Proceedings (CEUR-WS.org)

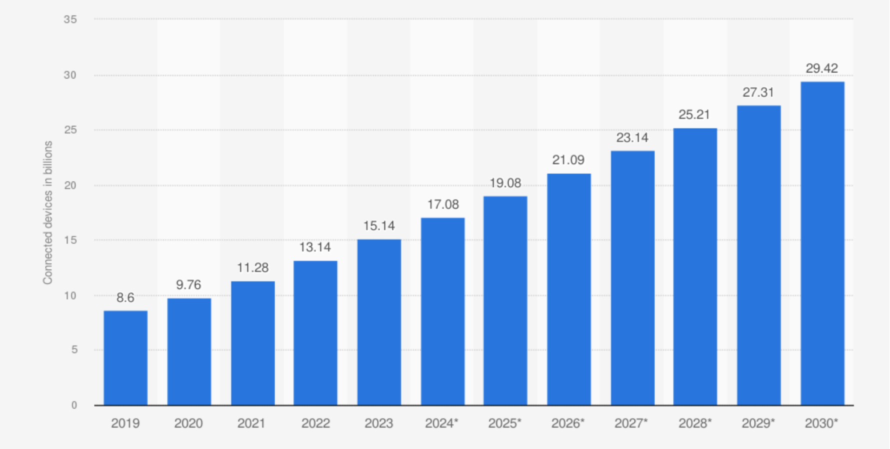

Figure 1: Number of Internet of Things (loT) connected devices worldwide from 2019 to 2023, with forecasts from 2024 to 2030 (in billions) [1].

The interconnected nature of IoT devices creates multiple potential points of entry for cyber threats, posing risks to data privacy and system integrity. Additionally, the vast amount of data generated by IoT devices requires robust processing and analysis capabilities, challenging the scalability of IoT networks. Furthermore, the limited computing power, storage capacity, and energy availability of many IoT devices complicate the implementation of comprehensive security measures. Table 1 outlines the essential requirements for an IoT network. As noted in a McKinsey report, deployment, interoperability, privacy considerations, cybersecurity, and change management represent challenges that must be addressed [10].

Table 1
IoT network requirements.

Requirement	Description
Power efficiency	Protocols must be designed to consume minimal power to extend the battery life of devices, which is crucial for IoT applications where devices are expected to operate for years on a single battery.
Range	The communication range must be appropriate for the application, ranging from short-range (e.g., Bluetooth, Zigbee) to long-range (e.g., LoRa, NB-IoT) communications.
Data rate	Depending on the application, the data rate can vary from low (for simple sensor data transmission) to high (for applications requiring the transfer of more significant amounts of data, like video surveillance).
Security	Strong security measures are vital to protect against unauthorized access and data breaches. This includes encryption, authentication, and data integrity checks.
Interoperability	Protocols should ensure interoperability among different devices and systems to enable seamless communication and integration.
Scalability	The network protocol must be able to scale from a few devices to thousands or even millions of devices without significant degradation in performance.
Cost-effectiveness	The cost of implementing and maintaining the network should be feasible for the intended application, including the cost of the devices themselves

	and any associated service fees.
Reliability	High reliability in delivering messages with minimal loss or errors, especially in environments with high interference or physical obstacles.
Latency	The protocol should support the required response times for the application, ranging from high-latency tolerant applications to real-time requirements.
Bandwidth Efficiency	Efficient use of bandwidth to accommodate the potentially large number of devices within the network, optimizing the data transmission to avoid congestion.

To address these challenges and harness the full potential of IoT, Distributed Ledger Technologies (DLT) emerge as a promising solution, offering a new paradigm for secure and efficient IoT communication. DLT offers highly desirable features such as decentralization, openness, immutability, transparency, traceability, security, and availability [2]. This study aims to identify the optimal blockchain architecture that meets IoT's unique requirements, such as minimal energy consumption, extensive range, and robust security, amidst its resource constraints. The primary objective is to establish a blockchain solution that not only enhances the security of IoT communications but also addresses scalability and interoperability challenges inherent in current technologies.

The subject of this research is the integration of blockchain technology within IoT networks, while the object is the IoT communication system itself. By exploring various blockchain architectures, this dissertation seeks to contribute novel insights into the design of a scalable, secure, and resource-efficient framework for IoT systems. This investigation is expected to offer significant scientific contributions by providing a detailed analysis of blockchain's potential to resolve the pressing security and scalability challenges faced by IoT networks, thereby unlocking new possibilities for its broader application and implementation.

2. Related works

The intersection of blockchain technology with the IoT is a burgeoning research area, promising to address the persistent challenges of security, scalability, and resource efficiency that hinder the full realization of IoT's potential. This literature review meticulously examines three pivotal articles, each contributing progressively to the discourse on blockchain's role in enhancing IoT ecosystems. By tracing the evolution from theoretical exploration to practical application, this review highlights the depth and breadth of current research while identifying areas that warrant further investigation.

The article "Blockchain-based IoT: A Survey" serves as a foundational entry point, offering a broad yet somewhat superficial overview of how blockchain technology could fortify IoT security. It outlines key blockchain principles – such as decentralization, immutability, and transparency – and theorizes their applicability in mitigating common IoT vulnerabilities, including data breaches, unauthorized access, and the risks associated with centralized control. While the survey is instrumental in delineating the potential intersections between blockchain and IoT, its primary limitation lies in its dated perspective and lack of empirical evidence, rendering it a preliminary, albeit essential, exploration of the subject matter.

Progressing from this theoretical base, "A Blockchain-based Approach for Secure IoT" delves into the specifics of a blockchain architecture designed to enhance IoT security. This article marks a significant leap forward by providing a detailed account of the architecture's components, its operational protocol, and its capability to tackle the nuanced challenges of IoT security and scalability. The strength of this research lies in its methodological rigor, presenting simulation results that demonstrate tangible improvements in data security, transaction throughput, and overall network resilience. However, it does not fully address the computational and energy constraints of IoT devices, which are critical considerations when deploying blockchain solutions in resource-limited environments.

The narrative advances with "Scalable and Secure IoT Architecture with Blockchain," which introduces an innovative, layered blockchain architecture specifically designed to address not only the security challenges but also the scalability and resource constraints inherent in IoT systems. This article is particularly noteworthy for its comprehensive approach, which separates data processing from security management, allowing for efficient handling of IoT-generated data while leveraging blockchain for critical security tasks. By proposing lightweight blockchain protocols that accommodate the limited resources of IoT devices, the research offers a balanced and pragmatic solution to the previously identified challenges. Real-world case studies further validate the architecture's effectiveness, providing a compelling argument for the practical implementation of blockchain in IoT networks.

3. Integration of blockchain and IoT

3.1. Blockchain as a solution

In exploring the integration of blockchain technology within IoT ecosystems, our research methodology elucidates the potential of blockchain to address the multifaceted challenges that plague IoT protocols and systems. This examination is rooted in the inherent characteristics of blockchain technology – its decentralization, immutability, and transparency – which collectively offer promising solutions to the pressing issues of security, scalability, privacy, data integrity, and regulatory compliance in IoT frameworks.

Blockchain's decentralized framework serves as a formidable defense against the prevalent security weaknesses in IoT devices, presenting a secure and trustworthy method for information sharing through a distributed peer-to-peer (P2P) system [3]. By removing central points of vulnerability, it distributes the risk of cyber threats throughout its network, markedly diminishing the effects of such attacks. Transactions within the blockchain are encrypted and sequentially linked, culminating in an unalterable ledger of all transactions (Fig. 2). This ledger's permanence guarantees that once information is logged, it cannot be changed without a network-wide agreement, thus preserving data integrity and preventing unauthorized alterations.

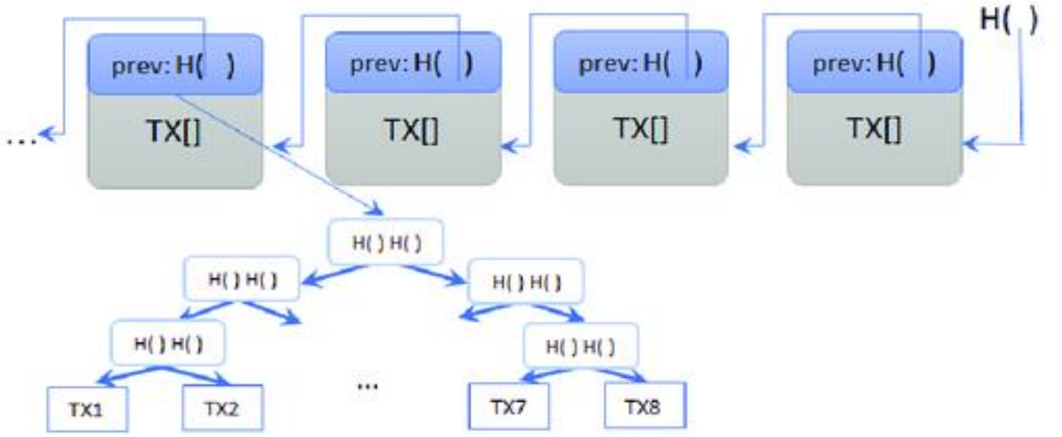

Figure 2: Blockchain structure [2].

Moreover, the functionality offered by blockchain technology can significantly benefit IoT by assisting in overcoming the regulatory and legal challenges that IoT projects encounter. The unalterable ledger ensures a trustworthy and unchangeable record of every transaction, which supports adherence to regulatory requirements and aids in settling legal disputes. Such clarity not only fosters trust among all parties involved but also streamlines regulatory reporting and the checking of compliance. This underlines how IoT can greatly benefit from the capabilities provided by blockchain, which in turn will contribute to the advancement of existing IoT technologies [5].

However, integrating blockchain with IoT systems presents significant challenges, especially concerning scalability and the resource limitations of IoT environments. These environments typically comprise numerous devices that produce large volumes of data needing swift processing. Conventional blockchain systems, where each node maintains the entire ledger and participates in consensus, struggle to handle the volume and speed of IoT transactions, leading to increased latency, which is impractical for real-time applications.

Additionally, many IoT devices, such as sensors and actuators, have limited computational power and energy resources, making it challenging to perform blockchain's intensive cryptographic operations and consensus algorithms. This can impair device performance and shorten their operational lifespan due to higher energy demands. Furthermore, integrating blockchain with IoT introduces serious security and privacy concerns. Although blockchain can enhance security by distributing data and removing single points of failure, it faces difficulties in enforcing uniform security policies and raises privacy issues due to its immutable ledger that permanently records data. Addressing these issues necessitates innovative blockchain architectures that may include lightweight protocols or hybrid models to optimize both performance and security.

In a practical example, IBM and Maersk launched TradeLens in 2018 intending to create the foundation for ecosystem leverage with a planned marketplace of innovative complementary services that can benefit actors in addition to a high level of network externalities and interdependency among the global supply chain actors in the shipping industry [4]. Despite the anticipated benefits such as reduced shipping times and costs, streamlined regulatory processes, and minimized fraud, TradeLens struggled to gain widespread adoption, mainly due to hesitation from other carriers to join a system dominated by Maersk. The limited participation from the broader industry restricted the necessary network effect, and the challenges of integrating blockchain technology across a complex global shipping industry resulted in insufficient scale and interoperability. These factors led to the decision to wind down TradeLens in late 2022 as it failed to become the industry standard it sought to establish.

3.2. Directed acyclic graph. An alternative to blockchain

Directed Acyclic Graph (DAG) technology emerges as a forward-thinking alternative to conventional blockchain, targeting the scalability and efficiency challenges blockchain encounters. Distinct from the blockchain's linear, block-connected structure, DAG employs a graph-like setup (Fig. 3), linking each transaction to multiple preceding ones. This structure facilitates parallel transaction processing, enhancing system capacity and speed.

The DAG model embeds transaction validation within the process of transaction addition, accelerating throughput and bolstering network security with growth. Without the traditional blockchain requirement for miners to validate and add transactions, DAG networks often feature lower, sometimes non-existent, transaction fees due to the self-validating nature of transactions. Moreover, DAGs surpass traditional blockchains in energy efficiency, sidestepping the computationally intensive puzzle-solving associated with block mining.

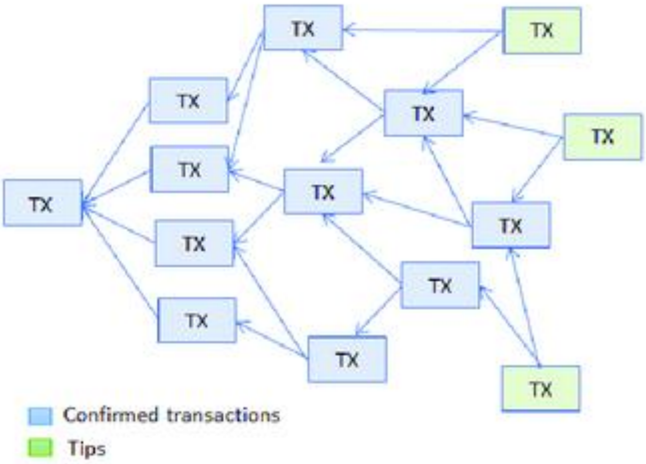

Figure 3: The structure of the directed acyclic graph [2].

However, DAG technology introduces its challenges:

- Security Concerns: Particularly in early stages or low-volume periods, DAG networks might be more vulnerable to attacks than blockchain networks, which benefit from extensive miner-contributed hash power.
- Network Adoption and Development Maturity: Being relatively newer, DAG faces hurdles in user adoption and ecosystem development, unlike more established blockchain platforms with robust communities and infrastructures.
- Complexity: The intricate structure and operational mechanisms of DAG networks can complicate understanding, adoption, and security assurance efforts, potentially impeding broader acceptance despite technical benefits.

Despite these challenges, DAG's potential to address key issues like scalability, transaction speed, and energy consumption presents a compelling option for efficiency- and sustainability-focused applications. As distributed ledger technology evolves, both DAG and blockchain will likely find unique applications, contributing to a diversified ecosystem of decentralized solutions.

In the Netherlands, the innovative company ElaadNL embarked on a project to develop smart charging stations for electric vehicles using IOTA's Tangle technology. The primary goal was to streamline energy consumption and transaction processes, allowing electric vehicles to autonomously pay for charging, thereby facilitating seamless energy and fund transfers without manual intervention. This system aimed to optimize power distribution, reduce operational costs, and enhance grid stability by dynamically adjusting charging rates based on real-time grid capacity and energy availability. By leveraging a decentralized, scalable, and zero-fee transaction platform, ElaadNL hoped to demonstrate the potential for significant improvements in national energy infrastructure.

The project, however, faced several technical and operational challenges. Integrating IOTA's Tangle with existing infrastructures required overcoming complexities related to ensuring transaction reliability, security, and data privacy. Additionally, the relatively untested nature of IOTA's technology raised concerns about scalability and potential network congestion as more devices connected to the system. These issues highlighted the need for continuous research and development to refine the technology, ensuring it could withstand the demands of modern energy systems and support the growing needs of smart urban ecosystems.

3.3. On-chain and off-chain approaches in blockchain architecture

In the exploration of blockchain technology's application within the IoT domain, understanding the distinctions between on-chain and off-chain transactions becomes pivotal. This differentiation is crucial for devising scalable, efficient solutions that can accommodate the unique characteristics and requirements of IoT systems.

Transactions executed on-chain are carried out directly on the blockchain, with their records preserved on the distributed ledger. This approach guarantees supreme security and clarity since every transaction is subjected to verification by network peers based on a consensus mechanism before its irreversible inclusion in the ledger. On-chain data, manifested as verified transactions structured in sequential blocks, and on-chain code necessitate validation and consensus by network peers [6]. Though these transactions capitalize on the blockchain's inherent attributes of security, immutability, and transparency, they encounter limitations like slower processing speeds and increased expenses, stemming from the intensive computational work needed for validation and the possible charges linked to recording transactions on the ledger.

Off-chain transactions occur outside the blockchain ledger or on an auxiliary layer, aiming to mitigate or bypass certain limitations inherent to on-chain processing. These transactions allow for quicker processing and minimal or zero fees by not requiring immediate consensus from the blockchain network. The objective for off-chaining data and computation is to reduce or overcome such limitations [6]. Following an agreement between the involved parties, the outcomes of these off-chain transactions can be aggregated and later logged onto the blockchain. This approach significantly lowers the amount of data that needs to be processed and stored directly on the blockchain. The distinctions between on-chain and off-chain blockchain transactions are depicted in Fig. 4.

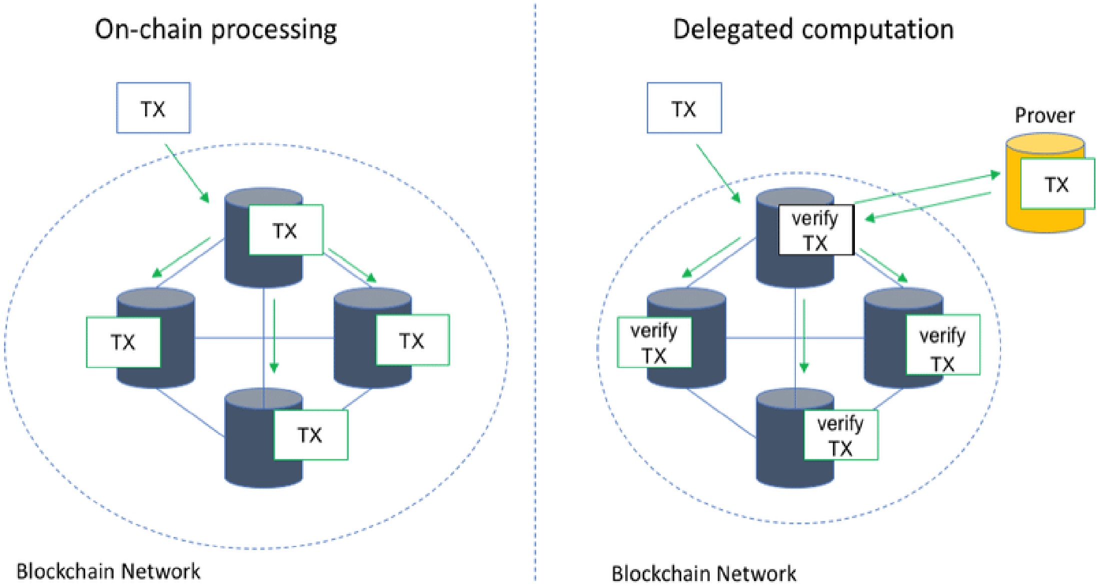

Figure 4: The operation principles of on-chain and off-chain blockchains [6].

The relevance of off-chain transactions to the IoT domain is particularly significant due to the volume, velocity, and variety of data generated by IoT devices. IoT environments often require the processing of vast numbers of transactions and interactions in real-time or near-real-time, which can strain the capabilities of purely on-chain solutions. Here, off-chain transactions offer a flexible and scalable alternative:

- Scalability and Efficiency: By handling transactions off-chain, IoT applications can achieve greater scalability, accommodating the high throughput of device communications and data exchanges without overwhelming the blockchain network.
- Cost Reduction: Off-chain transactions can mitigate the cost implications of recording every IoT device interaction on the blockchain, making it economically feasible to deploy blockchain solutions in IoT contexts.
- Energy Conservation: Given the resource constraints often associated with IoT devices, off-chain transactions provide a less energy-intensive method for facilitating interactions, aligning with the sustainability goals of many IoT applications.

- Latency Reduction: Off-chain methods can offer reduced latency in transaction processing, which is crucial for IoT applications that rely on timely data exchanges for operational efficiency and decision-making.

However, it is essential to balance the benefits of off-chain transactions with considerations of security, trust, and transparency. Mechanisms for ensuring the integrity and verifiability of off-chain transactions when they are eventually reconciled and recorded on the blockchain are vital. This may involve leveraging smart contracts or trusted execution environments to formalize off-chain interactions and their subsequent on-chain settlement.

In summary, the strategic use of off-chain transactions, alongside on-chain activities, can significantly enhance the applicability of blockchain technology in the IoT domain. This approach allows for a harmonious balance between leveraging blockchain's strengths and addressing the operational challenges posed by the vast and dynamic nature of IoT ecosystems.

3.4. Hybrid approach

Integrating Directed Acyclic Graph (DAG) technology with blockchain's privacy benefits offers a robust framework for the Internet of Things (IoT), marrying DAG's efficient data processing with blockchain's security and privacy. This synergy is pivotal in IoT, where the seamless exchange and secure handling of vast data volumes are essential.

DAG technology is a game-changer for IoT applications that demand rapid, scalable transaction processing. Its ability to process transactions in parallel, without the constraints of traditional blockchain structures, significantly enhances the flow of information across IoT devices. This efficiency is vital in environments like environmental monitoring or smart cities, where real-time data processing can lead to immediate and impactful decision-making.

However, the efficiency of data processing is only one side of the coin. The integration of blockchain solutions into this mix introduces a layer of privacy and security that is indispensable for IoT applications handling sensitive data. By utilizing privacy-preserving technologies such as zero-knowledge proofs (ZKPs) and homomorphic encryption, the system ensures that while data is efficiently processed and shared, it remains confidential and secure. ZKPs, for example, enable the system to validate transactions without revealing any underlying sensitive information, providing a balance between transparency and privacy.

Integrating blockchain with Directed Acyclic Graph (DAG) technologies form a hybrid system that capitalizes on the strengths of both to enhance scalability, security, and efficiency. This system is built around a blockchain layer that ensures security and immutability by handling user registration, identity verification, and digital asset issuance. Parallelly, a DAG layer facilitates high-throughput transactions, enabling faster processing by structuring each transaction to confirm previous ones. An interoperability protocol bridges these layers, allowing for seamless data transfer and maintaining consistency across the system. The DAG's unique consensus mechanism validates transactions within its layer, while a security and privacy module across both layers ensures data protection and privacy. The simplified architecture of this solution is depicted in Fig. 5.

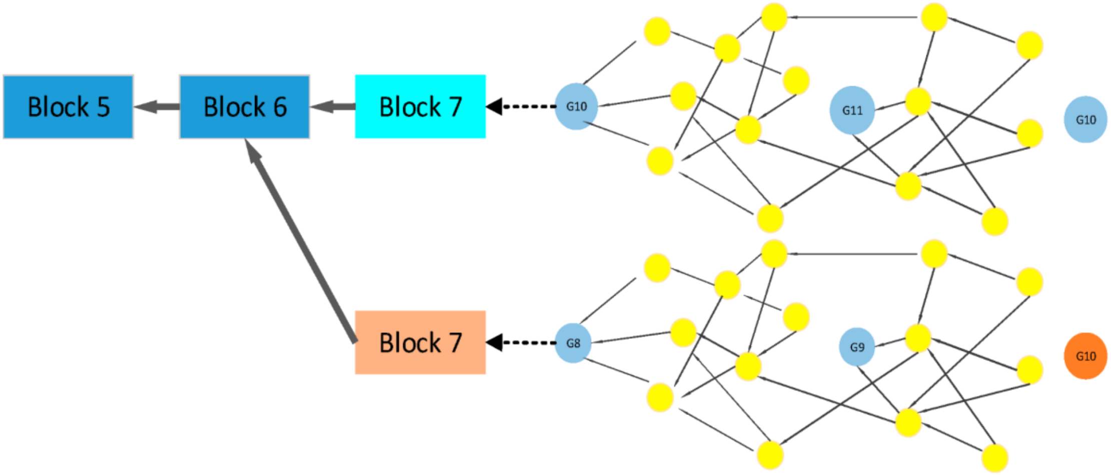

Figure 5: The basic structure of a combined blockchain and DAG approach [7].

By fusing DAG's transaction processing capabilities with blockchain's privacy and security strengths, a comprehensive solution emerges for IoT systems. This approach not only addresses the scalability and efficiency needs of the IoT but also ensures the highest standards of privacy and security [7]. As a result, IoT ecosystems become more agile, responsive, and trustworthy, capable of supporting a wide array of applications, from smart cities and healthcare monitoring to supply chain management, without compromising on performance or data integrity.

On the contrary, combining blockchain and Directed Acyclic Graph (DAG) networks for Internet of Things (IoT) applications presents several potential risks. First, the integration requires a complex connector to manage and translate transactions between the two different ledger technologies, which adds a layer of complexity and potential points of failure [11]. This could create bottlenecks, limiting overall system performance and potentially increasing the risk of errors and system failures. Second, the system results in data being stored on both DAG and Blockchain, which could lead to issues of data redundancy and increased storage needs [11]. Furthermore, this hybrid setup might amplify security vulnerabilities, as the interplay between blockchain's decentralized security mechanisms and DAG's less-proven security protocols could expose IoT devices to new attack vectors. Additionally, the energy consumption required to maintain such a system could negate one of the key advantages of DAGs, especially critical in power-sensitive IoT environments.

3.5. Cross-chain solutions

Cross-chain solutions, which facilitate interoperability between different blockchain networks, bring a transformative potential to the Internet of Things (IoT) by enabling seamless exchange of information and assets across diverse blockchain platforms, as shown in Fig. 6. This capability addresses crucial challenges associated with blockchain's integration into IoT ecosystems, notably enhancing interoperability, scalability, and the management of data and assets across the IoT landscape.

Cross-chain technology enhances the connectivity, interoperability, and scalability of IoT ecosystems. It enables seamless data and transaction exchanges across diverse blockchain networks. This integration allows for the development of expansive IoT solutions capable of efficiently handling vast amounts of data and scaling to meet the demands of different applications, ranging from smart infrastructure to healthcare. It introduces innovative approaches to asset and data management, including enhanced traceability in supply chains and efficient transactions in decentralized energy markets, while also increasing the security and privacy of IoT systems by leveraging the strengths of multiple blockchain networks.

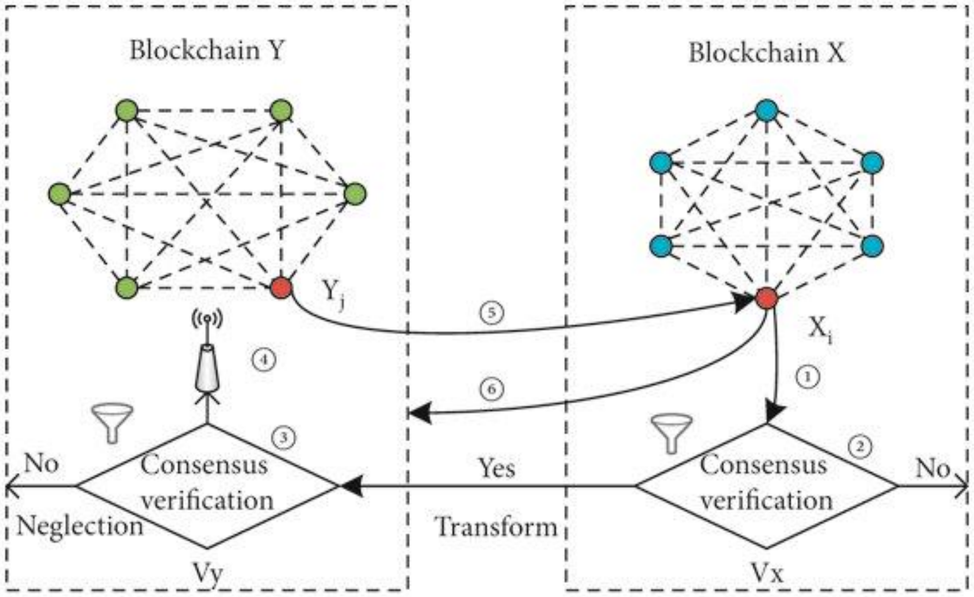

Figure 6: The operation principle of cross-chain blockchain [8].

To mitigate the high costs associated with multi-agent collaboration and protect individuals from attacks, a consortium blockchain serves as a control station via smart contracts [9]. This addition enhances the ability to choose the most fitting blockchain platform based on specific needs, like transaction speed, cost, or smart contract capabilities, giving developers and businesses the flexibility to customize IoT solutions for superior performance. Such customization ensures that IoT applications are not only effective and efficient but also economical, by utilizing the most appropriate blockchain features for their particular requirements.

However, realizing the full potential of cross-chain solutions in IoT is not without challenges. The complexity of integrating disparate blockchain platforms, potential security risks associated with cross-chain protocols, and the necessity for standardization to achieve true interoperability are significant hurdles that need to be addressed. Overcoming these challenges requires concerted effort and collaboration among blockchain developers, IoT solution providers, and industry stakeholders to ensure that cross-chain technology can be effectively and securely implemented.

4. Evaluation and discussion

In the IoT domain, the integration of distributed ledger technologies (DLT) presents several approaches to addressing key challenges such as security, privacy, scalability, and resource constraints. Directed Acyclic Graph (DAG), off-chain blockchain solutions, hybrid DAG and blockchain models, and cross-chain solutions each offer distinct advantages and potential limitations. Here's a comparative analysis of how IoT can benefit from each approach.

Directed Acyclic Graph (DAG)

Security & Privacy: DAG's structure inherently provides security through its linked transactions, but privacy can vary depending on the implementation. It doesn't naturally offer enhanced privacy features, so additional mechanisms may be needed.

Scalability: DAG excels in scalability due to its ability to process transactions in parallel, significantly reducing transaction confirmation times, which is ideal for high-volume IoT applications.

Resource Constraints: Its lightweight structure and efficiency in processing transactions make DAG particularly well-suited for IoT devices with limited computational resources.

Off-Chain Blockchain Solutions

Security & Privacy: Off-chain solutions enhance privacy by keeping transactions off the main ledger, reducing exposure. Security depends on the method of off-chain exchange and how securely the data is transferred and stored.

Scalability: By processing transactions off the main blockchain, these solutions greatly increase scalability and reduce network congestion, making them suitable for IoT applications with extensive transactional data.

Resource Constraints: Off-chain solutions can alleviate resource pressures on IoT devices by minimizing the need for on-chain transaction processing, thereby conserving energy and computational resources.

Hybrid DAG and Blockchain

Security & Privacy: A hybrid approach can leverage blockchain's robust security and privacy-enhancing features (like encryption and smart contracts) while utilizing DAG's structure for efficiency and scalability.

Scalability: This model benefits from DAG's scalable architecture for processing transactions and blockchain's structured approach for secure record-keeping, offering a balanced solution.

Resource Constraints: Hybrid models can be more resource-intensive than standalone DAG systems due to the added complexity of blockchain layers, potentially challenging for resource-limited IoT devices.

Cross-Chain Solutions

Security & Privacy: Cross-chain technologies can enhance security through diversified ledger systems, reducing the risk of systemic failures. Privacy can be improved by selectively sharing data across chains with specific privacy features.

Scalability: By enabling transactions and data to move across multiple blockchains, cross-chain solutions can address scalability by distributing the load, though at the cost of increased complexity.

Resource Constraints: These solutions might introduce additional resource overhead due to the need for interoperability mechanisms, potentially impacting IoT devices with limited capabilities.

Table 2
Comparison of various DLT solutions.

Feature	DAG	Off-chain blockchain	Hybrid DAG + Blockchain	Cross-chain Blockchain
Security	Inherent security through linked transactions.	Depends on secure data transfer and storage.	Leverages blockchain's security with DAG's efficiency.	Enhanced by diversified ledger systems.
Privacy	May require additional mechanisms for privacy.	Enhanced by keeping transactions off the main ledger.	Can integrate blockchain's privacy features.	Improved through selective data sharing across chains.
Scalability	High scalability due to parallel transaction processing.	Increased by handling transactions off the main chain.	Balances blockchain's secure structure with DAG's scalability.	Addressed by distributing the load across multiple blockchains.
Resource	Suitable for limited	Reduces	Potentially more	May introduce

constraints	resources due to its lightweight structure.	resource pressures by minimizing on-chain processing.	resource-intensive due to added complexity.	additional overhead due to interoperability mechanisms.
Suitable For	High-volume, real-time IoT applications.	IoT applications with extensive transactional data.	IoT systems need a balance of security, privacy, and scalability.	IoT ecosystems require integration across diverse blockchain platforms.

5. Conclusion

Considering the unique requirements of IoT ecosystems – particularly the need for scalability to handle vast numbers of devices and transactions, security and privacy to protect sensitive data, and efficiency to accommodate resource-constrained devices – the Directed Acyclic Graph (DAG) technology stands out as the most prominent approach.

DAG's inherent advantages in scalability and efficiency directly address the critical needs of IoT applications, ensuring that transactions can be processed rapidly and without unnecessary resource expenditure. While DAG alone may not offer the highest level of privacy, its compatibility with additional privacy-preserving mechanisms and security features can create a comprehensive solution tailored to IoT challenges. This approach provides a solid foundation for IoT systems, facilitating swift, secure, and scalable applications capable of thriving in diverse and demanding environments.

Choosing the most suitable DLT approach for IoT involves careful consideration of the specific application requirements and constraints. However, DAG’s unique combination of efficiency, scalability, and the potential for enhanced security and privacy through integration with other technologies offers a compelling framework for overcoming the core challenges faced by IoT ecosystems.

Future research should particularly focus on exploring privacy-preserving mechanisms within DAG architectures. This is vital for advancing IoT communication security and ensuring that IoT devices operate not only with optimal efficiency and scalability but also with the highest standards of privacy, which is increasingly critical in our interconnected digital world. This area holds the potential to significantly elevate the security posture of IoT networks, paving the way for more robust and trustable IoT applications.

References

[1]. Lionel Sujay Vailshery. “Number of IoT connected devices worldwide 2019-2023, with forecasts to 2030, 2023.” URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2]. Antal, Claudia & Cioara, Tudor & Anghel, Ionut & Antal, Marcel & Salomie, Ioan. “Distributed Ledger Technology Review and Decentralized Applications Development Guidelines” Future Internet (2021). doi: 10.3390/fi13030062

[3]. Riya Thakore, Rajkumar Vaghashiya, Chintan Patel and Nishant Doshi. “Blockchain-based IoT: A Survey” Technological Forecasting and Social Change (2022). doi: 10.1016/j.procs.2019.08.101.

[4]. Marin Jovanovic, Nikola Kostić, Ina M. Sebastian, Tomaz Sedej. “Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens” Procedia Computer Science (2023). doi: 10.1016/j.techfore.2022.121981.

[5]. Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz. “On blockchain and its integration with IoT. Challenges and opportunities”, Future Generation Computer Systems (2018). doi: 190. 10.1016/j.future.2018.05.046.

[6]. Eberhardt, Jacob & Tai, Stefan. “On or Off the Blockchain? Insights on Off-Chaining Computation and Data” Insights on Off-Chaining Computation and Data (2017). doi: 10.1007/978-3-319-67262-5_1.

[7]. Huang, Jie & Liu, Changsheng & Harding, Joseph. “Research on Blockchain Architecture and Operating Principles Based on H-DAG”, Symmetry (2023). doi: 10.3390/sym15071361.

[8]. Hu, Wei & Xia, Xue & Zhang, Yi. “Research on Multimicrogrid Transaction Model and Cross-Chain Transaction Mechanism Based on Blockchain.” Mathematical Problems in Engineering (2022). doi: 10.1155/2022/4535974.

[9]. Jiang, Yiming, Chenxu Wang, Yawei Wang, and Lang Gao. “A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management” Sensors (2019). doi: 10.3390/s19092042

[10]. Michael Chui, Mark Collins, Mark Patel. “The Internet of Things: Catching up to an accelerating opportunity” URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf

[11]. H. Hellani, L. Sliman, A. E. Samhat and E. Exposito. "Tangle the Blockchain:Towards Connecting Blockchain and DAG," IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (2021): 63-68