https://doi.org/10.55343/CogSust.60

BluBSIoT: Advancing Sustainability through Peer-to-Peer Cross-Ledgering in Social Internet of Things

Chandra Priya J[1*], Dhinesh Balasubramanian[2]
0000-0003-3891-0950, 0000-0003-2687-9095,
Department of Computer Science and Engineering, Department of Mechanical Engineering,
Mepco Schenk Engineering College
Sivakasi, India
jchandrapriya@gmail.com, dhineshbala91@gmail.com

Abstract
The global emphasis on sustainability has stimulated the demand for state-of-the-art solutions that drive the green and blue economy. However, the exponentially growing data analysis remains constrained, leading to a substantial disparity between data supply and demand. This discrepancy primarily arises from data being isolated, inaccessible, and infrequently shared due to concerns regarding data governance and privacy breaches. To tackle these challenges, we propose the integration of Peer-to-Peer (P2P) cross-ledgering within the Social Internet of Things (SIoT) framework as a promising approach to advance cognitive sustainability through improved information sharing and storage. The P2P network configured at the base facilitates a decentralized and secure exchange of information among diverse stakeholders involved in promoting sustainability. By leveraging the immutability and authorized accessibility of blockchain, consortia nodes evaluate and segregate data suitable for on-chain, off-chain, or one-to-one transactions. This ensures the safeguarding of sensitive data while enabling seamless collaboration and sharing. The integration of ledger systems enables interoperability across multiple platforms, fostering smooth information exchange between entities engaged in green and blue economy initiatives.

Keywords
Green economy, Cognitive science, Social Internet of Things, Blockchain, Sustainability

1. Introduction

1.1. Blockchain Technology for secure storage and communication

A blockchain can be viewed as a distributed smart database. Rather than holding the data in a centralized architecture, this digital ledger is distributed among all the network users. A further point is its immutable back traversal of all transactions ever transpired by the network entities (*Priya et al., 2022*). It is by no means an exaggeration to state that the blockchain is vastly complex to hack, with no central authority to cause faults to bankrupt the system. The consensus process uses a pre-set verification algorithm that automatically facilitates data transmission, verification, and storing on a blockchain. This process brings out the property of immutability as the cryptographically locked block of transactions threaded together to form a chain. Bitcoin cryptocurrency has been the initial application of blockchain, but then cryptocurrencies become just one of the technology's use cases (*Upadhyay, et al., 2021*). Additional support for its usability comes from Ethereum blockchains, which use functions to facilitate automatedly triggered smart contracts. In light of these properties, blockchain collaborations can be attained viable by self-executing code eradicating the intermediaries to mediate concerning transacting parties (*Njualem, 2022*). These deductions imply that trustless environments can use this technology where the users can trust the authenticity of records of a distributed ledger. Incentivization and tokenization are not vital elements of blockchain. Regardless of the same peer-to-peer (P2P) methodology, different blockchain platforms retain the resemblance of the essentials and tend to open their framework based on the infrastructure or motive of the use case.

1.2 IoT network of smart green and blue devices

Internet of Things (IoT) sensors and devices have been used for remote monitoring. These methods generate considerable interest in resource management that reaches an optimum stature with minimal resource cost and maximal profits by monitoring diverse environmental parameters of blue and green resources (*Daoud et al., 2022*). The data acquired from IoT sensors and devices can be used for immediate notification for action and long-term observation, and analysis with generalization (*Zahoor, Mir, 2018*). A secluded IoT platform for meticulous resource management and environmental monitoring was proposed in existing literature (*Haertel et al., 2022*) with distinctive approaches of multiple views for various high-level scenarios. The deployment and evaluation of various platforms with sensors and devices were studied. Evidence of implementations in research (Qasabeh et al., 2022), (Rayes, Salam, 2022) suggests the lack of infrastructure from some

https://doi.org/10.55343/CogSust.60

perspectives. The absence of a standardized protocol that incorporates appropriate privacy-preserving mechanisms has impeded the secure sharing of sensitive blue and green economic data. This deficiency undermines the ability of stakeholders to effectively collaborate and develop insights that could lead to innovative and sustainable solutions for complex economic and environmental challenges. Developing a robust and privacy-preserving data-sharing protocol is essential for ensuring sensitive data's confidentiality, integrity, and availability, thereby enhancing data-driven decision-making processes.

Data analysts demand comprehensive insights into the data management processes that precede data arrival in their systems (*Gastón, 2017*). Prior data management uncertainties, such as using strict data cleaning methodologies or malicious alterations, create scepticism about the accuracy of analytical results. In addition, conventional security approaches impose significant energy consumption and processing overheads on IoT devices (*Ashir et al., 2022*). The central server-based security frameworks that underpin these approaches are costly and inefficient, as summarized in *Table 1*. As such, alternative security solutions that are lightweight, distributed, and energy-efficient are necessary to enhance the security of IoT devices and mitigate the risks associated with centralization (*Effah, Bai, Quayson, 2022*).

Table 1. Literature summary in socialization contexts

	Reputation	Socialization	Timeliness	Context Awareness	Social Trust
Fu et al. (2022)	Yes	No	No	Yes	Yes
Nitti et al. (2015)	Yes	Yes	Yes	No	No
Mabodi et al. (2020)	Yes	No	Yes	No	Yes

1.3 Social Internet of Things

The point of convergence of social networking with IoT leads to an extended IoT paradigm referred to as the Social Internet of Things (SIoT) (*Rayes, Salam, 2022*). The smart objects are socially interconnected in a network to subject the material things to a virtual dimensionality cognitive function. The deployed things can smartly interact on social networks to reach social loops for intelligent information to publish to benefit a community group of users and actuate gestures. The deployed network autonomously navigates on efficient object discovery. It is a primary concern on the level of reliability in establishing contacts to share information within the range of socially interconnected things (*Chauhan et al., 2022*). Socialized things contribute to offering scalable networking while increasing the degree of trustworthiness, as illustrated in *Fig. 1*. However, it can be observed from our present-day scenario that ever-increasing demand far and wide is for decentralized trust-enforcing strategies in various social networking contexts. SIoT can revolutionize precision agriculture by enabling the collection of data on crop conditions and environmental factors (*Polas et al., 2022*).

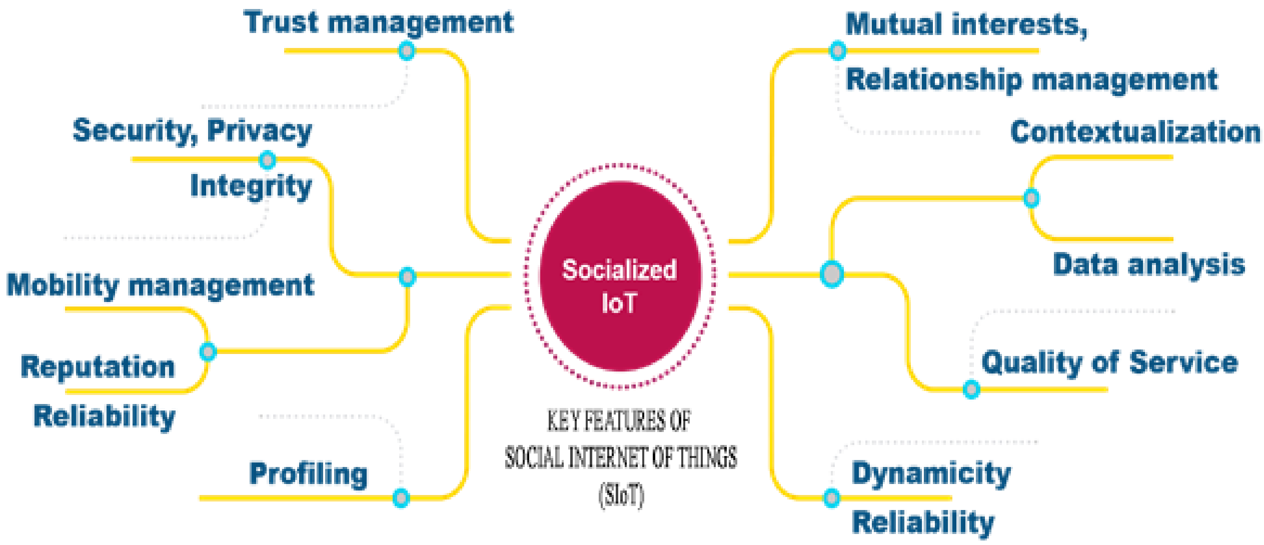

Fig. 1 Characteristics of SIoT

https://doi.org/10.55343/CogSust.60

With smarter green resource management, farmers can achieve scientific crop cultivation. Automation, intelligence, and remote surveillance can revolutionize modern precision farming practices to enhance productivity and efficiency. Various factors are crucial for achieving optimal green resource management in precision agriculture, including atmospheric monitoring, soil analysis, and pest control. By leveraging SIoT, we can transform agriculture and pave the way for a more sustainable future which is summarized in *Table 2*:

Table 2. Literature summary

	Reputation	Social	Timeliness	Context Awareness	Social Trust
Wang et al. (2022)	Yes	No	No	No	Yes
Bao et al. (2013)	Yes	No	No	No	Yes
Chen et al. (2015)	Yes	No	No	No	Yes
Datta et al. (2015)	Yes	No	Yes	Yes	Yes
Xu et al. (2014)	Yes	No	No	Yes	Yes
Gai et al. (2022)	Yes	Yes	No	Yes	Yes

1.4 Consortium group of nodes

A private permissioned Blockchain is a type of network that imposes restrictions on who can access, edit, and verify data on the blockchain (*Heidari et al., 2022*). In the case of a network that involves multiple organizations, it is referred to as a Blockchain consortium. The mechanism of the consortium assumes that the participants are known, registered, and verified within the consortium. The underlying algorithm is designed to validate the ledger once a considerable amount of node responses is signed, eliminating the energy costs associated with hashing protocols (*Singh et al., 2021*). Business networks usually support this consensus mechanism. We plan to utilize a blockchain incorporating the interoperable consortium consensus to minimize processing time and associated costs.

1.5 Cross-ledgering of Blockchains

Cross-ledger denotes the number of approaches that attempt to establish distributed ledgers or blockchains (*Abdelmaboud et al., 2022*). A wide spectrum of diverse blockchains is expected to continue operating in parallel. It is necessary to interconnect such diverse blockchains securely and efficiently to guarantee a universal, unified, and non-segregated realm for distributed ledgers. The primary motivation of cross-ledger is to have multiple interconnected ledgers that exploit transaction locality to achieve scalability, while different ledgers can be designed to offer different functionality (*Sekarlangit, Wardhani, 2021*). The core problem of cross-ledgering is to deploy ledgering without influencing the functionality of other correlated blockchains.

2. Green and blue resources' sustainability

Despite the tremendous volumes of data being generated, a significant challenge lies in finding a secure, privacy-preserving, and globally accessible solution that can unlock the potential of the emerging blue and green economy. Integrating SIoT and decentralized technologies presents a unique opportunity to address the sustainability issues associated with green and blue resources. By connecting and monitoring various devices and sensors, IoT enables real-time data collection and analysis, providing valuable insights into resource consumption, waste management, energy efficiency, and ecosystem preservation. P2P offers scalable storage and computational capabilities, allowing for efficient data processing and collaborative decision-making across stakeholders. The ongoing research and development efforts in this field aim to design and implement robust frameworks that ensure the collected data's security and privacy while enabling seamless sharing and collaboration among stakeholders globally. The pursuit of a safe, privacy-preserving, and borderless solution for unlocking the potential of the green and blue economy is an ongoing endeavour. By harnessing the power of IoT and blockchain, researchers and developers are actively exploring ways to achieve sustainable resource management and promote environmental conservation on a global scale. The outcome of these efforts holds excellent promise for shaping a more sustainable and resilient future for our planet.

https://doi.org/10.55343/CogSust.60

3. Problem analysis

Problem 1 – Energy depletion and excessive expenditure: Blockchain technology's environmental and sustainability ramifications have not been adequately analyzed, particularly concerning its energy consumption. Obtaining more precise and comprehensive information on current and future energy usage related to a blockchain is urgent and requires more exacting methodologies and alternative situations. Developing nations require careful monitoring and sustainability assessments to alleviate detrimental environmental effects. There is a considerable cost in uploading data to blockchain platforms to tackle environmental and ocean data inadequacies. The reason is that most people and fishers are not smart, technologically savvy and without smartphones. There are inadequate standards and frameworks for organizing blockchain activities toward environmental protection and blue resources management.

Problem 2 – On-transit data disclosure: Public data availability to all the entities across a network. Massive data upload onto the blockchain creates a bottleneck in scaling the storage system. Although many studies and research claim that blockchain is safe in every aspect, some studies show that it is still hard to ensure complete privacy, which may create more opportunities for hackers.

Problem 3 – Interoperability between the blockchains implemented within the same context: Currently, most blockchain networks operate independently. The biggest challenge to interoperability is the existence of many blockchain networks that differ in parameters, such as consensus models, transaction schemes, and smart contract functionality.

Problem 4: Once written into the blockchain, data cannot be changed. However, there are situations where data has to be modified by its owner, which cannot be feasible. Because blockchains are deemed immutable, correcting inaccurate or fraudulent data can be onerous. Any inaccurate data input into the blockchain record would be highly costly for the supply chain. This is directly related to human error. Despite the accuracy of data and information flow, the logistics process is still vulnerable to human error, which could cause an increase in rejection rates of process outcomes.

4. Methodology: Secured information storage

Utilizing the Deep Belief Network (DBN) as a generative model of the Deep Neural Network (DNN) technique involves structuring it as a stacked Restricted Boltzmann Machine (RBM) and Sigmoid Belief Network (SBN). The customized DBN comprises three cascaded RBMs with three hidden layers {h1, h2, h3}. An input vector {X=h0} and the hidden layer h1 are connected to a generative stochastic Artificial Neural Network (ANN) known as RBMI. During the first layer training, the DBN is treated as a single-layer RBM and is trained using the constructive divergence technique. During the second layer training, the DBN has two layers, where the upper layer is assumed to be RBM2 and the lower layer is assumed to be a Sigmoid belief network with weight W1 frozen (*Fig. 2*):

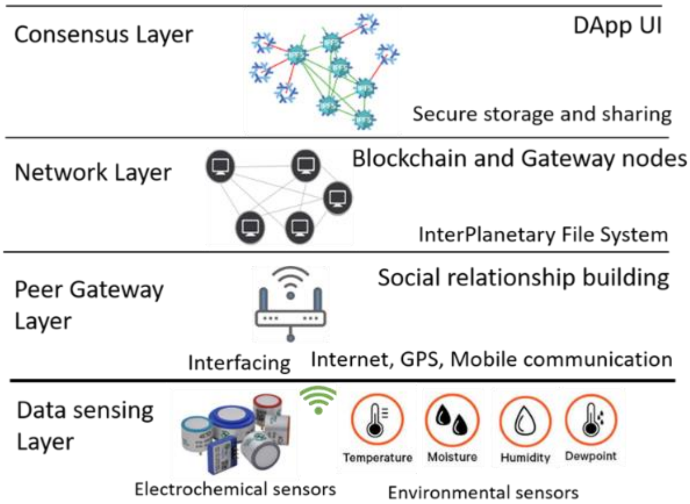

Fig. 2 BluBSIoT: Layered Architecture

https://doi.org/10.55343/CogSust.60

Similarly, during the third layer training, the top layer is treated as RBM3 and the other two as SBN with weights W1 and W2 frozen. The mathematical process of DBN is represented by Eq. (1):

$$P(X,h^1,h^2,\dots,h^n) = P(X|h^1)P(h^1|h^2)\dots P(h^{(n-2)}|h^{(n-1)})P(h^{(n-1)},h^n) \quad \text{(Eq. 1)}$$

The probability $P(h^{(n-1)},h^n)$ of (1) is defined with RBM utilizing (Eq. 2) and (Eq. 3):

$$P(h^i|h^{i+1}) = \prod_j P\left(h_j^i|h^{(i+1)}\right) \quad \text{(Eq. 2)}$$

$$P\left(h_j^i|h^{(i+1)}\right) = \sigma\left(b_j^i + \sum_k^{i+1} W_{kj}^i\, h_k^{i+1}\right) \quad \text{(Eq. 3)}$$

The Greedy trained manner was utilized for training RBMs of DBN. The RBM generates features and recreates inputs (*Wang et al., 2021*). Thus, the contrastive divergence method has been utilized for training the RBM. The utilized Gibbs Sampling-based contrastive divergence technique is as follows.

- Initiation of the parameters.
- Define the activation probability of hidden layers utilizing (Eq. 4):

$$P\left(h_j|X\right) = \sigma\left(b_j + \sum_{i=1}^{m} W_{ij}\, X_i\right) \quad \text{(Eq. 4)}$$

- Define the activation probability of the input layer utilizing (Eq. 5):

$$P(X_i|h) = \sigma\left(a_j + \sum_{j=1}^{n} W_{ij}\, h_j\right) \quad \text{(Eq. 5)}$$

- Upgrade the edge weight utilizing (Eq. 6):

$$Wij = Wij + \alpha\left(P\left(h_j|X\right) - P(X_i|h)\right) \quad \text{(Eq. 6)}$$

At this point, α refers to the rate of learning. Afterwards, trained the initial RBM, the edge weights are frozen. Then, it can be trained in the succeeding RBM resulting in similar contrastive divergence phases. However, the resultant preceding trained RBM was utilized as the input of the succeeding RBM. Afterwards, after the practical training of stacked RBM, the DBN feature was removed in the topmost hidden layers. As data shared on the blockchain is tamper-evident and accessible to those that have the proper permission to see it, the consortium should consider what type of data should be on-chain, what data need to be accessed by whom, for how long and for what purpose, and what data should be limited to one-to-one transactions as depicted in Fig.3:

https://doi.org/10.55343/CogSust.60

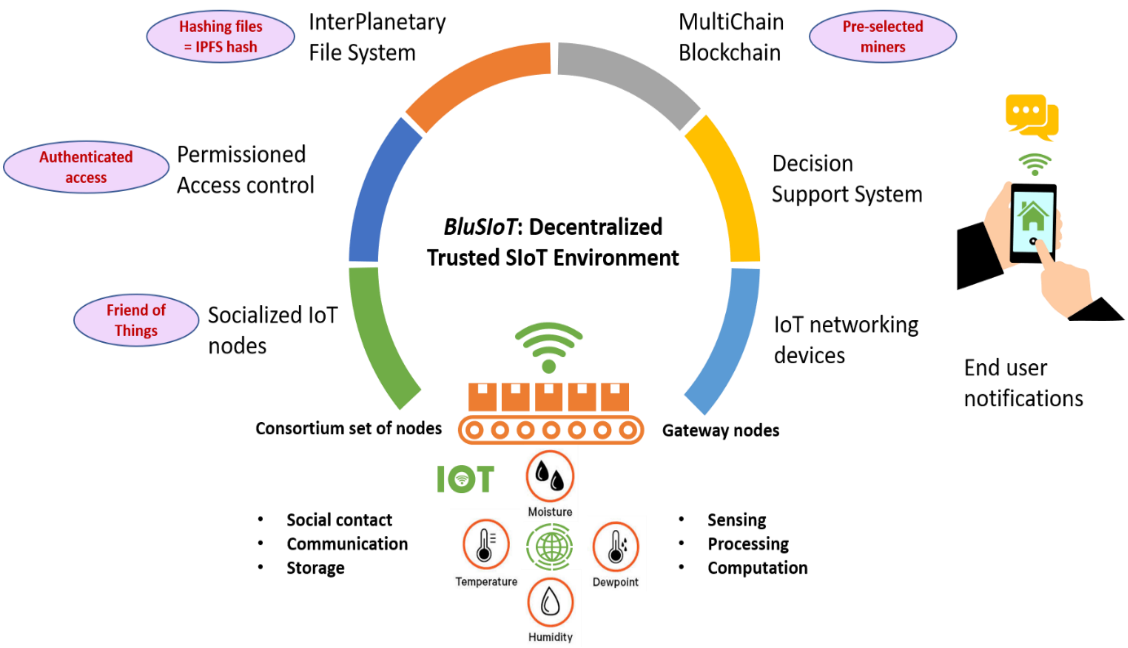

Fig.3 BluBSIoT: Environmental Aspects
Source: Own edition

5. Integrating SIS into green and blue resources for sustainability SWOT analysis

Our system uses blockchain technology, smart contracts, and tokens to enable safe and secure data sharing, guaranteeing control and auditability while protecting privacy. The technology allows organizations and individuals to set pricing and trade data without losing control of their data assets. Smart contracts allow data owners to program the conditions of access, which are then executed with precision. This gives data owners and buyers transparency, security and guarantees of payment and use. This framework is a safe, borderless data-sharing system that unlocks sharing and access to data, allowing consumers and authorized society to benefit from the green and blue economy. It allows for building data services. The system allows people to unlock the data's value without necessarily unlocking it itself. It is a substrate to finally realize the potential of an open permission-less data economy while still preserving privacy. BluBSIoT is a decentralized data exchange protocol to unlock data for decision-making. Through blockchain technology, smart contracts, and tokens, the frameworks connect data providers and consumers, allowing data to be shared while guaranteeing traceability, transparency, and trust for all stakeholders involved. It allows data owners to give value to and control their data assets without being locked into any marketplace by bringing together decentralized blockchain technology, a data-sharing framework, and an ecosystem for data and related services in a blue and green economy that touches every single person, locality and device, giving power back to data owners, enabling people to reap value from data to better the agriculture world.

https://doi.org/10.55343/CogSust.60

Our framework sets standards and demonstrates how to share data safely and securely without compromising privacy or ownership. The work involves ground for a series of private and public partnerships from the research, insurance, retail and healthcare sectors to deploy their Proof-of-Concept solutions on the blockchain-enabled data-sharing platform. Sharing is enabled without exposing the data or taking a copy, thereby retaining privacy, ensuring regulatory compliance, and freeing up data to advance data analytics and solve problems for the economy and society through decision-making capabilities. The various inter-ledger approaches are compared in this paper in terms of the following features: i) whether they support the transfer of value or the exchange of value, ii) the interconnection trust mechanism, iii) complexity, iv) scalability, and v) transaction cost. Approaches that perform the exchange of value across two or more chains rely on the consensus mechanisms of the chains that are involved, which provides decentralized trust, thus avoiding the need for a single trusted entity which is tabulated in *Fig. 4*:

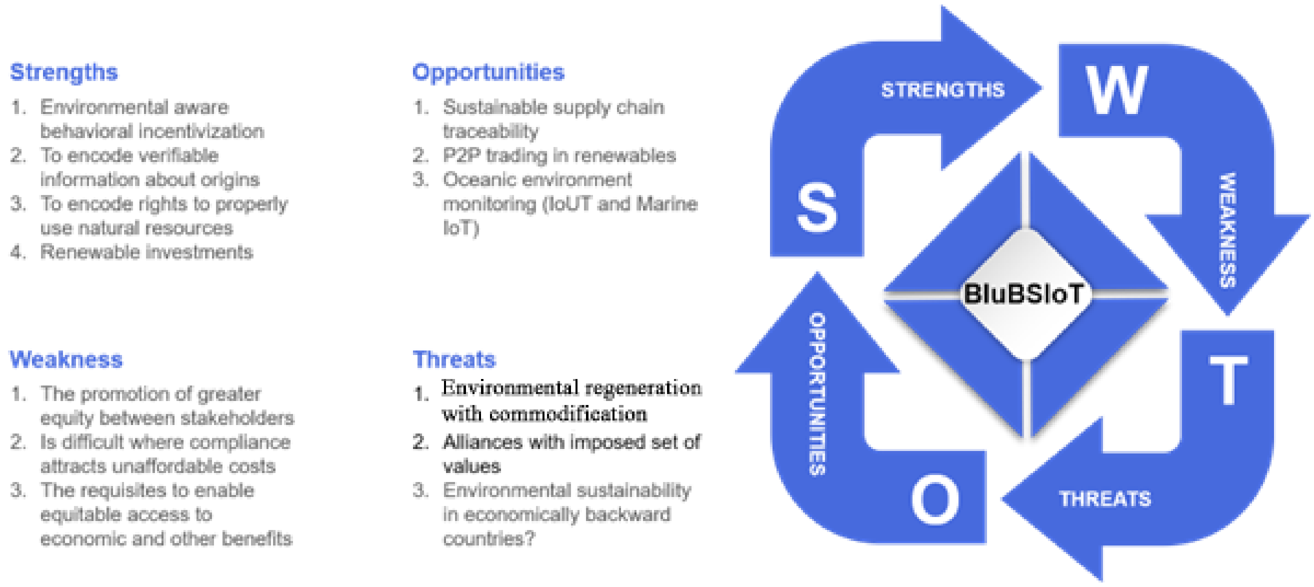

Fig. 4 SWOT Analysis of BluBSIoT
Source: Own edition

The interconnected trust mechanism defines where the immutable state of the transactions across chains is recorded; this is related to the mechanism which ensures the trusted execution of these transactions without relying on a single trusted entity. The complexity of the inter-ledger approach is determined by the amount of data (transactions) from each interconnected chain that the approach needs to process to ensure the trusted commitment of transactions across chains. Scalability refers to the total number of transactions a solution can support per unit of time and how the incremental cost for supporting additional transactions depends on the total number of transactions per unit of time. Finally, the transaction cost refers to the aggregate cost of all transactions, which depends on the percentage of transactions inside the main chain or inside the sidechains and the transactions across the two.

6. Framework for implementations

The hardware components designed for IoT applications consist of two devices: a Raspberry Pi and a Photon IoT microcontroller. The system's usability is boosted by the inclusion of an Android smartphone, featuring a Snapdragon

https://doi.org/10.55343/CogSust.60

900 MHz processor and 1 GB of memory, which provides a versatile interface for real-time monitoring and display of data acquired by the electrochemical and environmental sensors, as well as for system control using a mobile app (*Table 3*):

Table 3. Development Environment

Component	Devices	Specifications
	Raspberry Pi	Processor: ARM Cortex-A7 900 MHz Memory: 1 GB
Hardware	Photon IoT	Processor: ARM Cortex-M3 120 MHz Memory: 1 MB flash, 128 KB RAM
User interface	Smart Phone	Android device Processor: Snapdragon 900 MHz Memory: 1 GB
Connectivity standard	Wi-Fi module	Wi-Fi router with SoC m processor
Library and framework	Python API libraries	
Resources	Electrochemical and environmental sensors	

The smartphone leverages Wi-Fi connectivity to transmit commands to the Raspberry Pi and Photon IoT devices, enabling remote system control and providing seamless connectivity. The Wi-Fi module is linked to a Wi-Fi router with an integrated SoC (System on a Chip) processor to ensure consistent and reliable connectivity. The development framework incorporates Python API libraries for software development. The DApp is built upon a MultiChain framework that provides a range of features and functionalities for creating distributed applications. The Savoir library is employed to facilitate the information flow from the decentralized application to the storage area to streamline the development process (*Table 4.*):

Table 4. Blockchain Development Environment

Component	Specifications
Processor configuration	Pre-selected miner: Intel Core i7, 4 cores @ 1.30 GHz; Peers: Intel Core i5, 2 cores @ 3.4 MHz
Memory configuration	Pre-selected miner: 32 GB RAM; Peers: 8 GB RAM
Operating systems	Windows 10, 64-bit
DApp framework	MultiChain V 2.0
Library support	Savoir library

The plot in *Fig. 5* depicts the correlation between propagation delay and maximum transmission unit with an experimental environment that holds channel bandwidth set at 250 kHz and transmission power at 18 dBm. It is observed that BluBSIoT has a comparatively low linear relationship in comparison with the standard IoT network. This suggests that the P2P cross-ledgering SIoT framework can achieve efficient transmission of data with reduced delay, which is crucial for ensuring that information is shared and stocked effectively for promoting sustainability in the green and blue economy.

https://doi.org/10.55343/CogSust.60

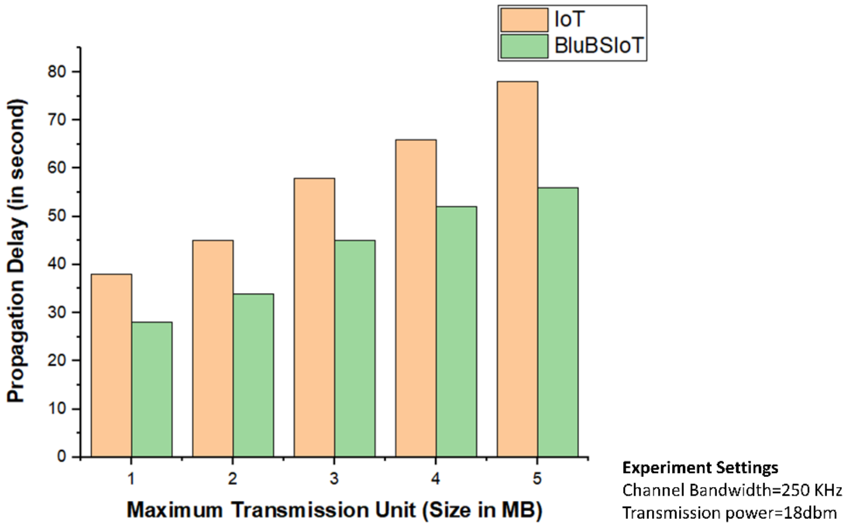

Fig.5 Impact analysis of delay in Transmission

In blockchain-based IoT applications, it is essential to consider the correlation between the number of nodes in the network and the average block time in milliseconds. The block time is the time to validate and add a new block to the blockchain. As per observation, the increase in the number of nodes in the network leads to an increase in the average block time. This is because each node has to validate and confirm the transactions before adding the block to the blockchain, and the validation process becomes time-consuming with an increase in the number of nodes. As a result, this can cause slower transaction processing and reduced efficiency. Therefore, it is vital to maintain a balance between the number of nodes and the average block time to ensure optimal performance in blockchain and IoT applications (*Fig. 6*):

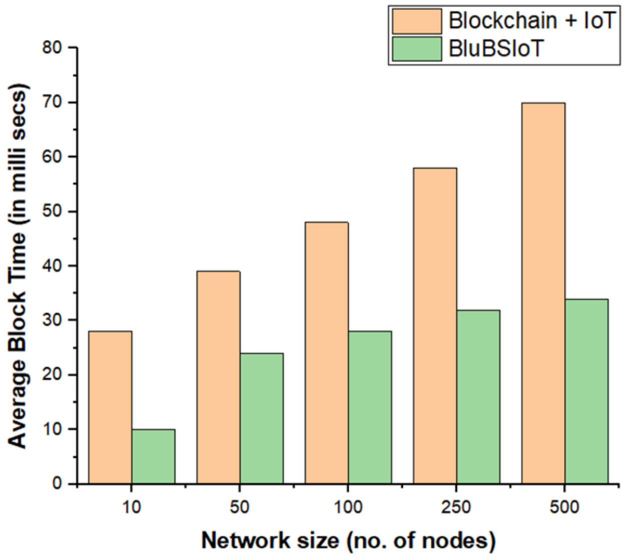

Fig.6 Impact analysis of block time to the size of the network

7. Conclusion

In the context of the Sustainable Development Goals (SDGs), BluBSIoT can be used to support progress towards several of the goals, including,

Goal 9: Industry, Innovation and Infrastructure – BluBSIoT can improve supply chain management, reduce fraud and corruption, and increase efficiency and transparency in industry and infrastructure.

Goal 16: Peace, Justice and Strong Institutions – BluBSIoT can help to create more secure and transparent governance systems, reduce corruption, and improve access to justice and accountability.

Goal 17: Partnerships for the Goals – BluBSIoT can facilitate more effective and secure partnerships between governments, businesses, and civil society organizations, by providing a shared, secure platform for collaboration.

In conclusion, BluBSIoT has the potential to enhance secured information storage and contribute to Sustainable Development Goals. By addressing issues related to interoperability, scalability, privacy, and stakeholder engagement, blockchain systems can be developed to support sustainable development and contribute to the decade of action towards achieving the SDGs.

References

Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, 11(4), 630. DOI: https://doi.org/grkk64

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4), 2347-2376. DOI: https://doi.org/cmxz

Ashir, D. M. N. A., Ahad, M. T., Talukder, M., & Rahman, T. (2022). Internet of Things (IoT) based smart agriculture aiming to achieve sustainable goals. *arXiv preprint arXiv:2206.06300*. DOI: https://doi.org/kgj2

Bao, F., Chen, R., & Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In *2013 IEEE eleventh international symposium on autonomous decentralized systems (ISADS)* (pp. 1-7). IEEE. DOI: https://doi.org/kgk3

Chauhan, S., Singh, R., Gehlot, A., Akram, S. V., Twala, B., & Priyadarshi, N. (2022). Digitalization of Supply Chain Management with Industry 4.0 Enabling Technologies: A Sustainable Perspective. *Processes*, 11(1), 96. DOI: https://doi.org/kgj4

Chen, R., Bao, F., & Guo, J. (2015). Trust-based service management for social internet of things systems. *IEEE transactions on dependable and secure computing*, 13(6), 684-696. DOI: https://doi.org/f9c6kq

Daoud, W. B., Mchergui, A., Moulahi, T., & Alabdulatif, A. (2022). Cloud-IoT resource management based on artificial intelligence for energy reduction. *Wireless Communications and Mobile Computing*, DOI: https://doi.org/kgjq

Datta, S. K., Da Costa, R. P. F., & Bonnet, C. (2015, December). Resource discovery in Internet of Things: Current trends and future standardization aspects. In *2015 IEEE 2nd world forum on internet of things (WF-IoT)* (pp. 542-547). IEEE. DOI: https://doi.org/kgk4

Effah, D., Bai, C., & Quayson, M. (2022). Artificial Intelligence and Innovation to Reduce the Impact of Extreme Weather Events on Sustainable Production. *arXiv preprint arXiv:2210.08962*. DOI: https://doi.org/kgj5

Fu, M., Sun, S., Gao, H., Wang, D., Tong, X., Liu, Q., & Liang, Q. (2021). Improving Person Reidentification Using a Self-Focusing Network in Internet of Things. *IEEE Internet of Things Journal*, 9(12), 9342-9353. DOI: https://doi.org/kgj8

Gai, X. (2022). Intelligent advertising design strategy based on internet of things technology. *Wireless Communications and Mobile Computing*, Article ID 5163330, 13 pages. DOI: https://doi.org/kgk5

Gastón, H. C. (2017). MQTT Essentials-A Lightweight IoT Protocol: The preferred IoT publish subscribe lightweight messaging protocol. *Birmingham, UK: Packt Publishing* Ltd. p280. ISBN 9781787285149

Haertel, F., Camargo, L., Lopes, J., Pernas, A., Mota, F., Barbosa, J., & Yamin, A. (2022). Helix Project: Exploring the Social Internet of Things (SIoT) in Care of Blind People. *Journal of the Brazilian Computer Society*, 28(1), 26-37. DOI: https://doi.org/kgjs

Heidari, A., Jabraeil Jamali, M. A., Jafari Navimipour, N., & Akbarpour, S. (2022). Deep Q-Learning technique for offloading offline/online computation in blockchain-enabled green IoT-Edge scenarios. *Applied Sciences*, 12(16), 8232. DOI: https://doi.org/kgjz

Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. *The journal of supercomputing*, 76, 7081-7106. DOI: https://doi.org/ggjxjr

Nitti, M., Atzori, L., & Cvijikj, I. P. (2014). Friendship selection in the social internet of things: challenges and possible strategies. *IEEE Internet of things journal*, 2(3), 240-247. DOI: https://doi.org/kgj7

Njualem, L. A. (2022). Leveraging Blockchain Technology in Supply Chain Sustainability: A Provenance Perspective. *Sustainability*, 14(17), 10533. DOI: https://doi.org/gq4c7p

Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Karim, R., & Tabash, M. I. (2022). Blockchain Technology as a Game Changer for Green Innovation: Green Entrepreneurship as a Roadmap to Green Economic Sustainability in Peru. *Journal of Open Innovation: Technology, Market, and Complexity,* 8(2), 62. DOI: https://doi.org/kgj3

Priya, J. C., Choudhury, T., Khanna, A., & Preethi, R. (2022). Blockchain-based transfer learning for health screening with digital anthropometry from body images. *Network Modeling Analysis in Health Informatics and Bioinformatics*, 11(1), 23. DOI: https://doi.org/kgjp

Qasabeh, Z. T., Naderlou, L., Ismayilova, N., & Feyziyev, A. (2022). A Review SIoT (Social Internet of Things): Techniques, Applications, Challenges and Trends. *Azerbaijan Journal of High Performance Computing*, 5(2), pp. 236-253 DOI: https://doi.org/kgjv

Rayes, A., & Salam, S. (2022). IoT protocol stack: a layered view. In Internet of Things From Hype to Reality: The Road to Digitization (pp. 97-152). *Cham: Springer International Publishing*. DOI: https://doi.org/kgjw

Sekarlangit, L. D., & Wardhani, R. (2021). The effect of the characteristics and activities of the board of directors on sustainable development goal (SDG) disclosures: Empirical evidence from Southeast Asia. *Sustainability*, 13(14), 8007. DOI: https://doi.org/kgj6

Singh, G. G., Oduber, M., Cisneros-Montemayor, A. M., & Ridderstaat, J. (2021). Aiding ocean development planning with SDG relationships in Small Island Developing States. *Nature Sustainability*, 4(7), 573-582. DOI: https://doi.org/gjmxk8

Upadhyay, A., Mukhuty, S., Kumar, V., & Kazancoglu, Y. (2021). Blockchain technology and the circular economy: Implications for sustainability and social responsibility. *Journal of Cleaner Production*, 293, 126130. DOI: https://doi.org/gpwm3c

Wang, X., Garg, S., Lin, H., Hu, J., Kaddoum, G., Piran, M. J., & Hossain, M. S. (2021). Toward accurate anomaly detection in Industrial Internet of Things using hierarchical federated learning. *IEEE Internet of Things Journal*, 9(10), 7110-7119. DOI: https://doi.org/gk8sx5

Zahoor, S., & Mir, R. N. (2018). Virtualization and IoT resource management: A survey. *International Journal of Computer Networks and Applications*, 5(4), 43-51. DOI: https://doi.org/kgjr