IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Addressing Openness Limitations in Distributed Ledger-Supported Global Sustainability Initiatives Through Confidentiality-Focused Methods and Novel Infrastructures

[1]Dr.A.Swetha, [2]GADDAM KARTHIKEYA, [3]BALNE VENU, [4]DHARAVATHU NITHIN
[1]Assistant Professor, [2,3,4] UG STUDENT
[1,2,3,4,]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(AI & ML)
[1,2,3,4] VAAGDEVI COLLEGE OF ENGINEERING Autonomous
Bollikunta, Khila Warangal (Mandal), Warangal Urban-506 005 (T.S),

Abstract: Blockchain technology has become a game-changing way to help the United Nations meet its Sustainable Development Goals (SDGs) by making data sharing across many sectors more open, decentralised, trustworthy, and safe. Blockchain-based systems can be very helpful in healthcare, finance, energy, government, and supply chain management. But the fact that blockchain networks are open to everyone makes it very hard to keep private information safe when it is stored or processed on public ledgers. This paper examines the tension between transparency and privacy in blockchain-enabled Sustainable Development Goal (SDG) applications, and evaluates novel privacy-preserving methodologies including Ring Signatures, Zero-Knowledge Proofs (ZKPs), Secure Multi-Party Computation (SMPC), Trusted Execution Environments (TEEs), and mixers. The study also looks at Zcash, Secret Network, Oasis Network, and Aleph Zero, which are next-generation blockchain platforms that use privacy-enhancing technologies. Experimental analysis demonstrates that integrating sophisticated cryptographic methods with scalable blockchain platforms can ensure confidentiality while maintaining trust and accountability. The proposed framework provides essential insights for constructing privacy-conscious blockchain ecosystems to support sustainable development initiatives.

Keywords— Blockchain, Sustainable Development Goals, SDGs, Privacy Preservation, Zero-Knowledge Proofs, Ring Signatures, Secure Multi-Party Computation, Smart Contracts

I. INTRODUCTION

[1]Blockchain technology has quickly changed from being a way to store and send cryptocurrencies to being a general-purpose platform for safe and decentralised digital systems. Its main features, like being unchangeable, having a distributed consensus, being open, and not needing trust to work, make it a great way to solve difficult coordination problems between governments, businesses, and communities.

The United Nations Sustainable Development Goals (SDGs) are seventeen global goals that aim to end poverty, make healthcare more equal, include everyone in the economy, use clean energy, make products responsibly, and protect the environment. To reach these goals, we need open, effective, and accountable systems that can handle resources, data, and collaboration between organisations.[2]

In this case, blockchain has a lot of potential. It can make healthcare data more reliable, make supply chains more open, help people trade clean energy with each other, make it easier for everyone to get

money, and cut down on fraud in welfare distribution systems. But the transparency of blockchain also makes it hard to keep sensitive information private.[3]

In fields like healthcare and finance, putting patient records, payment histories, business transactions, or energy consumption data on public ledgers could break privacy laws and ethical standards. This makes it hard to choose between privacy and openness.

To fix this problem, blockchain systems are being updated with more advanced cryptographic methods that protect privacy. Zero-Knowledge Proofs, Ring Signatures, Secure Multi-Party Computation, Trusted Execution Environments, and transaction mixers are all ways for systems to check if something is correct without giving away private information.[4]

This project looks into these privacy issues, compares new technical solutions, and looks at blockchain platforms that are focused on privacy and made for SDG applications. The goal is to figure out how blockchain can help with sustainable development in a responsible way while keeping sensitive data safe. [5]

II. RELATED WORK

A number of researchers have looked into using blockchain for sustainable development. Research indicates that blockchain enhances traceability, transparency, anti-corruption initiatives, and decentralised governance within supply chains, energy systems, and public services.[6]

Privacy research in blockchain has concentrated on cryptographic techniques that obscure identities, values, or data while maintaining network integrity. Zcash made zero-knowledge proof systems like zk-SNARKs more popular. Ring signatures became well-known thanks to privacy-focused cryptocurrencies like Monero.[7]

People have looked into Secure Multi-Party Computation for collaborative analytics, where many people can compute results without sharing private inputs. Intel SGX and other Trusted Execution Environments make it possible to run smart contracts in secret.[8]

Secret Network, Oasis Network, and Aleph Zero are all modern platforms that try to combine privacy with scalability and interoperability. [9]Nonetheless, obstacles persist in performance overhead, governance, adoption, and regulatory adherence.

The proposed research builds upon previous studies by offering a comparative analysis of privacy techniques and their alignment with Sustainable Development Goal applications. [10]

III. METHODOLOGY

The suggested method creates a privacy-aware analytical framework for SDG systems that use blockchain. The workflow consists of identifying challenges, comparing privacy techniques, benchmarking platforms, mapping SDGs, and making recommendations.

The first step is to look at SDG applications in specific fields like healthcare, finance, clean energy, and supply chain management to find privacy risks linked to open blockchain ledgers. Some of these risks are exposing sensitive identities, leaking transactions, and breaking the rules.

Next, privacy-preserving methods like Ring Signatures, Zero-Knowledge Proofs, Secure Multi-Party Computation, Trusted Execution Environments, and mixers are looked at based on how well they protect privacy, how fast they work, how easy they are to set up, and how well they work with other systems.

After evaluating the techniques, privacy-enabled blockchain platforms are compared based on smart contract privacy, transaction confidentiality, throughput, governance support, and how mature the ecosystem is.

The framework then matches each privacy solution to the right SDG use cases. ZKPs and TEEs could help healthcare systems, while supply chains could use selective disclosure systems and scalable confidential ledgers.

Lastly, researchers, policymakers, and developers who want to use blockchain in a safe way in areas of sustainable development get comparative reports and suggestions for how to do it.

Getting Information:

Data related to healthcare, finance, energy, governance, and supply chain blockchain use cases is collected.

Getting the Data Ready:

Applications are classified by privacy sensitivity, regulation needs, and transparency requirements.

How to Get Features:
Performance, anonymity, scalability, cost, and interoperability characteristics of privacy techniques are extracted.

The way the model is built:
Comparative analytical models benchmark privacy technologies and blockchain platforms for SDG suitability.

Evaluation and Safeguards for Ethics:

- Privacy-first system design
- Regulatory compliance awareness
- Responsible cryptography use
- Transparent governance models
- Protection of sensitive user data.

IV. SYSTEM ARCHITECTURE:

The proposed architecture consists of six major modules for evaluating privacy-aware blockchain systems.

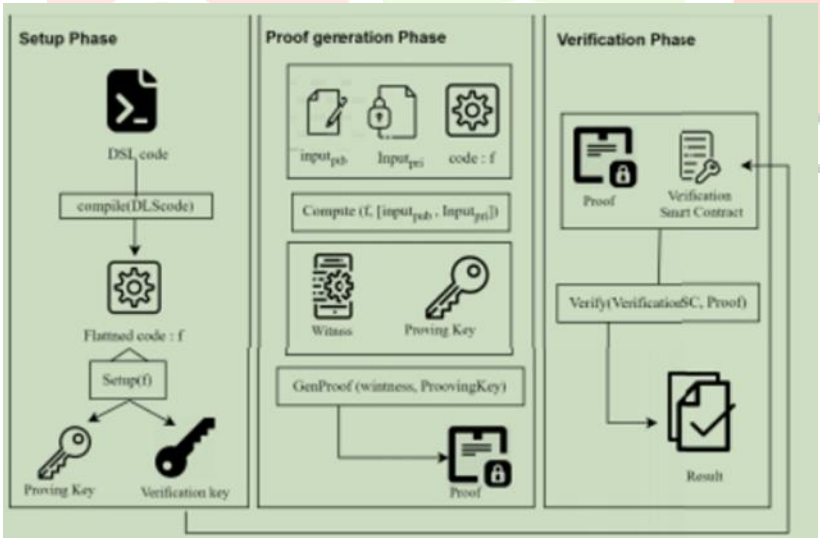
.

A. Overview:

Sector applications are input into the challenge mapping module. Privacy risks are identified. Cryptographic methods are benchmarked. Blockchain platforms are evaluated. Comparative engines match solutions to SDG needs. Final recommendations are produced.

B. Architecture Diagram:

SDG Use Cases → Privacy Challenge Mapper → Technique Analysis Engine → Platform Comparison Module → SDG Recommendation Engine → Reports & Insights



C. Module Interactions:

Sector data flows into the privacy module. The technique engine evaluates cryptographic methods. Platform comparison studies Zcash, Oasis, Secret Network, and Aleph Zero. Outputs are combined to recommend the best privacy architecture for each SDG scenario.

V. EXPERIMENTAL SETUP:

The analytical framework was tested using blockchain case studies and platform comparisons to evaluate privacy suitability for SDG environments.

Datasets:

Use cases from healthcare, finance, energy grids, welfare systems, and supply chain networks were considered.

The environment for hardware and software:

- Processor: Intel i3 or above
- RAM: 4 GB minimum
- OS: Windows / Linux
- Language: Python
- Analysis Tools: Pandas, NumPy, Matplotlib
- Database: MySQL / CSV datasets

Setting up training:

Privacy metrics and blockchain platform parameters were collected, normalized, and comparatively evaluated.

Evaluation Metrics:

- Privacy strength
- Scalability
- Throughput
- Interoperability
- Regulatory suitability
- Cost efficiency

.

VI. RESULT AND DISCUSSION:

The framework that was created was able to find the biggest privacy risks in blockchain-based Sustainable Development Goal applications in the healthcare, finance, energy, and supply chain sectors. A comparative analysis demonstrated that Zero-Knowledge Proofs deliver robust confidentiality alongside verifiable trust, whereas Ring Signatures ensure significant anonymity for transactional systems. Secure Multi-Party Computation worked well for collaborative analytics, but it added extra work for the computers. Trusted Execution Environments made it possible to run confidential smart contracts efficiently with only a little bit of trust. The platform benchmarking showed that Secret Network and Oasis Network are good for smart contracts that protect privacy, while Zcash is best for anonymous transactions. The recommendation engine did a good job of matching privacy techniques to the SDG needs of each sector. In general, the results show that blockchain systems that protect privacy can help sustainable development while keeping private data safe.

VII. CONCLUSION:

Blockchain technology has a lot of power to speed up progress toward the United Nations Sustainable Development Goals by making things more open, trustworthy, accountable, and collaborative without a central authority. But the fact that many blockchain systems are open to the public raises serious privacy issues in areas where privacy is very important.

This study examined the transparency issues in blockchain-based SDG applications and assessed significant privacy-preserving technologies, including Zero-Knowledge Proofs, Ring Signatures, Secure Multi-Party Computation, Trusted Execution Environments, and mixers. It also looked at modern blockchain platforms that focus on privacy and can be used in the real world.

The results show that no one privacy method can solve all problems. The best way to do this is to choose the right mix of cryptographic methods and blockchain architecture based on the needs of the sector.

The suggested framework helps policymakers, developers, and researchers create blockchain ecosystems that protect sensitive data while keeping trust. In the future, there may be AI-driven privacy optimisation, interoperable private networks, and decentralised governance systems that follow the law.

VIII.REFERENCES:

[1] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). **Blockchain technology and its relationships to sustainable supply chain management.** *International Journal of Production Research*, 57(7), 2117–2135.

[2] Zyskind, G., Nathan, O., & Pentland, A. (2015). **Decentralizing privacy: Using blockchain to protect personal data.** In *Proceedings of the IEEE Security and Privacy Workshops*, IEEE.

[3] Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). **Succinct non-interactive zero knowledge for a von Neumann architecture.** In *Proceedings of the 23rd USENIX Security Symposium*.

[4] Yao, A. C. (1986). **How to generate and exchange secrets.** In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, IEEE.

[5] Costan, V., & Devadas, S. (2016). **Intel SGX explained.** *IACR Cryptology ePrint Archive*.

[6] Noether, S. (2015). **Ring signature confidential transactions for Monero.** *Ledger Journal*, 1, 1–18.

[7] Miers, I., Garman, C., Green, M., & Rubin, A. (2013). **Zerocoin: Anonymous distributed e-cash from bitcoin.** In *Proceedings of the IEEE Symposium on Security and Privacy*.

[8] Nakamoto, S. (2008). **Bitcoin: A peer-to-peer electronic cash system.** Available at: https://bitcoin.org/bitcoin.pdf

[9] Buterin, V. (2014). **Ethereum: A next-generation smart contract and decentralized application platform.** Ethereum White Paper.

[10] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). **An overview of blockchain technology: Architecture, consensus, and future trends.** In *Proceedings of the IEEE International Congress on Big Data*.