Blockchain-Based Decentralised Threat Intelligence Validation System

Sushant Virghla, Sumit Sharma*, Udisha Singh, Prasanna Dwivedi

Department of Computer Science and Engineering, GL Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India

sushantvirghla@gmail.com, asyncsunlight@gmail.com, udishasingh865@gmail.com, prasannadwivedi12@gmail.com

ABSTRACT

This paper presents the design and implementation of a blockchain-based, decentralised threat intelligence validation system built on the Solana blockchain. The system addresses the fundamental challenge of enabling trustworthy cybersecurity intelligence sharing among organisations without relying on a central authority. By combining Solana's high-throughput blockchain with a token-based economic incentive model using the DTNC SPL token, the system establishes a stake-based validation mechanism that ensures data integrity, discourages malicious behaviour, and rewards accurate contributions. A hybrid storage architecture retains cryptographic hashes on-chain while keeping full report data off-chain, significantly reducing operational costs while preserving verifiability. Smart contracts developed using Python Seahorse automate the entire validation and reward lifecycle. Upon validation, the consensus-verified data is passed to a downstream AI pipeline for contextual threat intelligence analysis. The results demonstrate that decentralised, economically incentivised threat intelligence sharing is both technically feasible and practically viable using current blockchain technology.

Keywords: *Solana, blockchain, threat intelligence, smart contracts, SPL token, decentralised validation, cybersecurity, Proof of History*

1. Introduction

The choice of blockchain architecture is significant for any decentralised platform, and not every chain is suited for real-world high-frequency applications [7]. Solana is an advanced blockchain platform that enables the simultaneous execution of decentralised applications and cryptocurrency transactions [8]. Launched in 2020, Solana achieves high speed through a combination of Proof of Stake and a unique Proof of History consensus mechanism. This cryptographic innovation essentially acts as a decentralised clock, allowing validators to process transactions in parallel rather than sequentially [12]. The result is a network that can accommodate thousands of transactions per second, and tips remain well within a cent of each other [10, 11, 12]. These attributes make it a truly practical solution for situations where users are constantly submitting and validating data, which many older, well-established blockchains won't support without becoming prohibitively expensive or slow [7, 11].

Solana smart contracts enable you to write self-executing agreements that run automatically without intermediaries [8, 9]. Because of this scheme, they autonomously execute the entire validation and reward pipeline — keeping track of validator stakes, determining when majority consensus is achieved (and therefore rewards can be distributed), and distributing tokens without any human involvement to coordinate. These contracts are clear, unchangeable logic once deployed and thus differ in meaningful ways from traditional platforms where these decisions take place behind closed doors.

The token economy is based on the SPL standard, which is similar to the Ethereum ERC-20 standard. The SPL standard specifies how tokens are created, transferred, and managed on the Solana blockchain. All fungible and non-fungible tokens on the Solana blockchain are SPL tokens by default. The system's utility token, DTNC, is built on the SPL standard to ensure seamless integration with the wider Solana ecosystem. The metadata for the token is managed as is standard with the Solana blockchain. The total supply is managed through minting. Validators stake the utility token when endorsing reports. This has economic value as collateral

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

for the accuracy of the judgment. Validators earn the utility token as a reward for correct validation. Validators are subject to token slashing as a penalty for negligent or malicious behaviour [8].

2. Related Work

Decentralised systems and advanced computational methodologies have garnered significant scholarly attention across diverse application areas [1], including blockchain-based Internet of Things (IoT) networks and artificial intelligence evaluation systems. These approaches leverage distributed architectures to mitigate fundamental issues concerning network dependability, data sovereignty, and system trust.

2.1. Decentralised Networks and Blockchain Technologies

Various works have investigated the combination of blockchain technology and IoT systems to increase security, transparency, and fault tolerance. An Optimised Link State Routing (OLSR) protocol-based private blockchain-IoT solution illustrates how decentralising the network layer can eliminate Single-Point-of-Failure (SPoF) threats that affect infrastructure-dependent wireless networks, with experimental results demonstrating auto-recovery capabilities following network failures [2]. This solution extends blockchain connections across multiple ad hoc hops, offering adaptability for diverse IoT deployment scenarios.

Blockchain technology serves as a foundational building block of decentralised networks, existing as an open database where validated information cannot be altered, alleviating growing concerns around security, verifiability, and transparency [3]. By removing single points of failure, blockchain facilitates applications in sectors that require direct information flow and network security, including logistics, manufacturing quality assurance, and equipment maintenance transparency. [5]

Furthermore, blockchain technology has been used in supply chain management, where an architecture combining blockchain and IoT devices enables end-to-end traceability across multi-echelon suppliers, leveraging the Solana blockchain for its speed and cost-effectiveness, with IoT devices tracking environmental factors such as temperature, humidity, and location [4]. The verifiability of a blockchain addresses the disadvantages of centralised approaches by using smart contracts for supply chain business logic, thereby enhancing verification and dependability in provenance verification.

In addition, when applied to other fields, blockchain technology has shown substantial potential in the energy sector. In a vehicle-to-grid power trading model, for example, smart contracts are used in a decentralized system where peer-to-peer transactions are made possible between vehicles, thus creating a decentralized power trading system with information equivalence and openness in a system where reverse auctions are integrated with dynamic pricing to deal with the randomness and uncertainty in electric vehicle transactions, thus showing how a complex system of transactions can be made possible with increased profits for sellers and buyers with lower costs for buyers [6].

3. Research Methodology

3.1. System Architecture

The system is built on a six-layer blockchain architecture deployed on top of Solana's high-performance blockchain platform, as illustrated in Fig. 1.

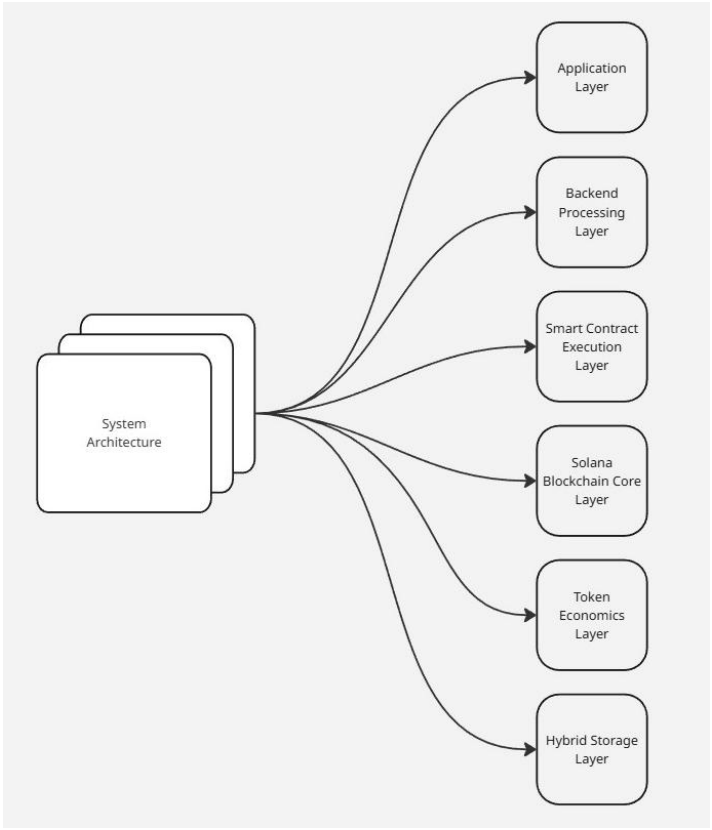

Figure 1: System Architecture

The **Application Layer** is where users interact with the web interface and submit cybersecurity threat reports using Solana wallets [8]. Submitted information then travels through the **Backend Processing Layer,** where Node.js servers encrypt and store full reports in local databases before they are prepared for blockchain deployment. From there, only the strictly necessary information proceeds to the **Smart Contract Execution Layer,** developed using the Python Seahorse framework, which provides an accessible development environment while maintaining the security and performance of Rust-compiled code running on Solana's virtual machine as per Figure 1. [9].

The core of the system resides in the **Solana Blockchain Core Layer**, where Proof of History (PoH) enables cryptographic timestamping, Tower BFT provides consensus finality, and the Sealevel runtime supports parallel transaction processing at rates exceeding thousands of transactions per second with sub-second finality [11, 12]. Running in parallel are two supporting layers: the **Token Economics Layer**, which manages DTNC SPL token staking requiring a minimum three-validator consensus, automatic reward distribution, and penalty enforcement for misvalidated entries; and the **Hybrid Storage Layer**, which stores only cryptographic hashes and essential metadata on-chain while retaining full report content off-chain, achieving over 95% cost savings compared to full on-chain storage.

Once consensus is reached in the validation process, the verified blockchain data is transmitted via API endpoints to a FAISS vector database for use by the RAG-based AI system in the context of threat intelligence queries, thus marking the integration point between blockchain-verified trust and AI-based intelligence analysis.

3.2. System Workflow

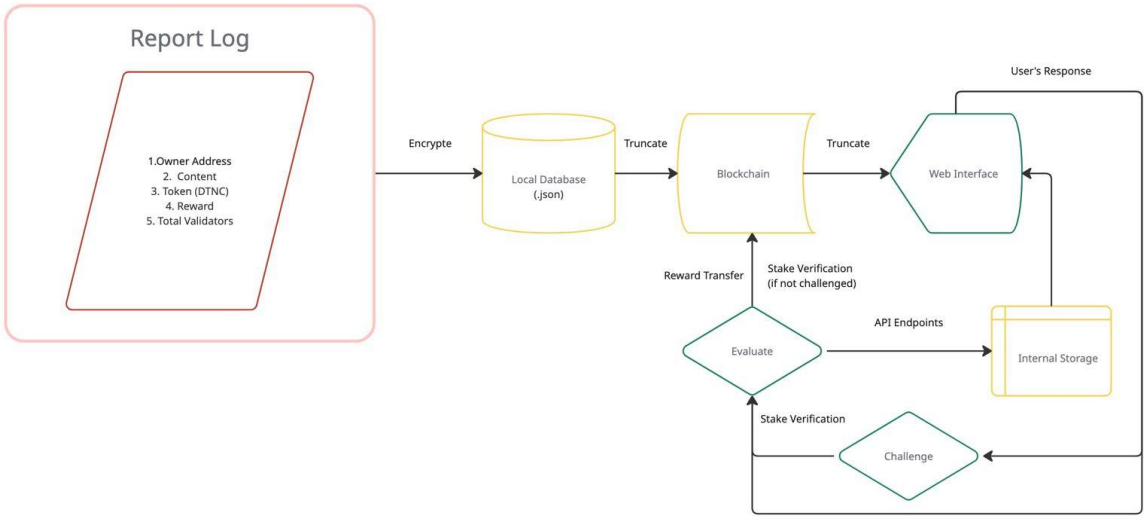

Figure 2: System Workflow

Fig. 2 shows the system workflow of the proposed model. A Report Log is the data submitted by the user through the system web interface and contains five core fields: the owner wallet address, report content, token address, reward amount, and the required number of validators. The owner's wallet address identifies the submitting user on-chain. The content field contains the reported threat intelligence. The token address for this field defaults to DTNC for personal users but can be a custom SPL token address for enterprise users [4, 7]. Once validation is successful, the user is rewarded with a specified token. There must be a minimum validator threshold to fulfil the system's validation needs before a report can be verified [13].

After a report has been submitted, it is encrypted and stored in a local database. This offers flexibility and redundancy until it is committed to the Solana blockchain. The information in this database is then truncated to its essential elements before being sent to the blockchain through a smart contract. This prevents the high costs associated with storing an entire report on the blockchain. The truncated information on the blockchain contains pointers to the full information in the local database [14, 15]. Once committed to the blockchain, other users can view this report through a forum-style interface to comment on it, like it, and validate it. The user can also edit it if they are the original submitter.

Validation is carried out through a stake verification process in which validators stake DTNC tokens against their endorsement decision [13, 16]. Incorrect validations trigger the re-evaluation mechanism, which allows any user with superior or more accurate information to challenge a validated report by reinitiating the staking process and receiving the same reward upon successful re-validation [17]. Validated report content is subsequently forwarded to the system's vector database through API endpoints, where it becomes part of the knowledge base used by the integrated AI model [18].

3.3. Smart Contract Development Framework

The system's smart contracts are developed using Python Seahorse on Solana Playground [9]. Seahorse enables developers to write Solana programs in Python rather than Rust, substantially reducing development time while maintaining the runtime guarantees of the underlying Anchor framework. The transpiled code is compiled into BPF bytecode that executes directly on the Solana Virtual Machine, preserving the performance and memory safety properties of Rust without requiring developers to write in it directly.

3.4. Blockchain Data Structure and Token Architecture

Every report stored on the blockchain contains five fundamental elements: the wallet address of the submitting user, the report content, the token address, the reward amount, and the required number of validators for verification. DTNC is an SPL token created specifically for this platform. Given the cost constraints of on-chain storage, the system maintains complete reports in a traditional database while storing only essential references and cryptographic hashes on the blockchain, ensuring verifiability without incurring unnecessary expense. [8, 9, 12]

3.5. Report Submission and Processing Workflow

When a report is submitted through the system website, it is initially transmitted to the Node.js backend. The backend encrypts and stores all report data in a local database. A separate process then retrieves this data, truncates it to the strictly necessary fields, and transmits it to the Solana blockchain. The reports become viewable by other users in a forum-style interface where they can comment, like, edit (restricted to the original submitter), and validate submissions.

3.6. Stake Verification and Validation Mechanism

To become a validator, a user needs to stake DTNC tokens. This way, the validator will definitely assume financial risk proportional to the endorsement [13, 16]. At least three validators must endorse a report before it can be considered verified [13]. The smart contract tracks staking amounts, validator identities, and timestamps throughout this process [6, 4]. A validator reads the submitted report, makes an independent judgment on its accuracy, and deposits their stake alongside that decision. Once the three validators agree, the smart contract will automatically reward all participants in the validation process, and the process will be carried out independently without any human intervention [6, 17].

After the report has been verified, other participants, in case they have better information or have spotted errors, can contest the decision by repeating the staking process. If the validator in question secures sufficient agreement from other validators, the report will be updated in the system database and the vector database [18]. This establishes a continuous improvement cycle in which information accuracy progressively increases over time [1, 17].

3.7. Reward and Penalty Mechanism

Rewards are transferred automatically once the minimum validator requirement is met, and re-evaluators receive the same reward as the original validators [13, 17]. All reward transfers are executed automatically by a Python script integrated with the smart contract layer. If a report is found to be incorrectly validated, any user can challenge and re-evaluate it through the stake verification process [14, 16]. On a finding of wrong validation, DTNC tokens are slashed from the offending validator's account as a financial penalty [13]. This punishment mechanism is designed to be strong enough to deter users from validating reports they have not genuinely read or from colluding to endorse inaccurate information [17].

4. Results and Discussion

Table 1: System Performance Metrics

Metric	Observed Value
Transaction Cost	$0.01 [10, 11]
Consensus Validators	Minimum 3
Blockchain TPS	Thousands per second [12]
Storage Reduction	95%

The system was tested with respect to operational performance metrics on blockchain transaction efficiency and validation mechanisms. Experimental deployment on the Solana DevNet showed transaction costs as low as $0.01 per operation [10]. Due to Solana's high-throughput architecture, report submission and blockchain confirmation typically occurred in less than a second as per Table 1 [11, 12]. For the validator consensus process between independent validators, at least three separate validators were required to approve any given report. In actual use, consensus was reached within a handful of seconds across the network, resulting in up to 16 updates per second. Using cryptographic hashes on the blockchain and storing the full report data in a separate, off-chain database could reduce the storage needed on the blockchain. That design also minimises operational costs while retaining the ability to verify stored threat intelligence.

5. Conclusions

This work demonstrates that decentralised threat intelligence sharing can be both cryptographically verifiable and economically viable without sacrificing real-time responsiveness, showing that the fundamental tension between organisational privacy and collaborative transparency is an engineering problem rather than an inherent limitation. The hybrid storage approach uses blockchain solely for trust establishment while keeping all data off-chain, directly addressing the long-standing cost barrier that has historically blocked blockchain adoption in data-intensive applications [14, 15]. This architectural pattern extends well beyond cybersecurity and serves as a replicable blueprint for healthcare record validation, academic credential verification, supply chain transparency, and scientific data collaboration where the integrity of verification matters more than on-chain data availability [4]. The stake-based DTNC token economy converts validator reputation into measurable financial risk, building a self-regulating quality control mechanism that naturally discourages malicious or careless behaviour without relying on a central moderating authority [13, 16]. Equally critical is the re-evaluation mechanism, which provides a rare self-correcting capability in otherwise immutable ledger technology, ensuring that knowledge can be revised and challenged over time without compromising the original validation record and addressing one of the persistent criticisms of blockchain systems where inaccurate data, once committed, cannot be corrected [16, 17].By empirically leveraging both the Proof of History consensus mechanism and token-based game theory, this system challenges the conventional blockchain trilemma, in which decentralisation, scalability, and security are treated as mutually exclusive properties [7, 12]. The confirmed sub-cent transaction costs combined with sub-second block finality validate that blockchain-based systems can outperform centralised alternatives across multiple dimensions when the appropriate infrastructure is selected for the application at hand [10, 11]. The seamless interoperability between the blockchain validation layer and the downstream AI processing pipeline further sets a technical precedent for systems in which blockchain serves solely as a trust infrastructure. At the same time, AI handles intelligent processing on top [1, 18]. In conclusion, the precise implementation of Python Seahorse for smart contract development sets a valuable benchmark, significantly reducing the technical hurdles for domain experts to engage directly in the creation of blockchain applications [9]. This advancement has the potential to foster innovation across sectors that rely on less trust and coordination among stakeholders who share objectives yet compete in other areas [3].

Acknowledgements

The authors would like to acknowledge the Department of Computer Science and Engineering at GL Bajaj Institute of Technology and Management for providing academic support during the development of this research work.

Funding source

No funding was received for this study. The research was conducted using publicly available open-source technologies and resources.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] A. Nash, "Decentralized Intelligence Network (DIN)," arXiv, arXiv:2407.02461, Jul. 2024. doi: 10.48550/arXiv.2407.02461

[2] X. Chen, S. Tian, K. Nguyen, and H. Sekiya, "Decentralizing Private Blockchain-IoT Network with OLSR," Future Internet, vol. 13, no. 7, p. 168, 2021. doi: 10.3390/fi13070168

[3] I. Kremenova and M. Gajdos, "Decentralized Networks: The Future Internet," Mobile Netw. Appl., vol. 24, pp. 2016–2023, 2019. doi: 10.1007/s11036-018-01211-5

[4] M. Ashraf and C. Heavey, "A Prototype of Supply Chain Traceability Using Solana as Blockchain and IoT," Procedia Comput. Sci., vol. 217, pp. 948–959, 2023. doi: 10.1016/j.procs.2022.12.292

[5] J. Marx and M. Cheong, "Decentralised Social Media: Scoping Review and Future Research Directions," in Proc. Australasian Conf. Inf. Syst. (ACIS), 2023. [Online]. Available: https://aisel.aisnet.org/acis2023/58/

[6] H. Liu, Y. Zhang, S. Zheng, and Y. Li, "Electric Vehicle Power Trading Mechanism Based on Blockchain and Smart Contract in V2G Network," IEEE Access, vol. 7, pp. 160546–160558, 2019. doi: 10.1109/ACCESS.2019.2951057

[7] H. Song, Y. Wei, Z. Qu, and W. Wang, "Unveiling Decentralization: A Comprehensive Review of Technologies, Comparison, Challenges in Bitcoin, Ethereum, and Solana Blockchain," arXiv, arXiv:2404.04841, Apr. 2024. doi: 10.48550/arXiv.2404.04841

[8] Solana Labs, “Solana Documentation,” Available: https://docs.solana.com.

[9] Seahorse Development Team, “Seahorse — Write Solana Programs in Python,” Available: https://docs.seahorse.dev.

[10] Solana Labs, “Solana Transaction Fees,” Available: https://docs.solana.com/transaction_fees

[11] S. Alizadeh and M. Khabbazian, “Solana’s transaction network: Analysis, insights, and comparison,” EPJ Data Science, vol. 14, no. 1, p. 48, Jul. 2025. [Online]. Available: https://doi.org/10.1140/epjds/s13688-025-00561-x

[12] A. Yakovenko, “Solana: A New Architecture for a High Performance Blockchain,” Solana Foundation, Whitepaper, Nov. 2017. [Online]. Available: https://solana.com/solana-whitepaper.pdf

[13] K. Sharma , M. Makino, G. Shrivastava, B. Agarwa “Forensic investigations and risk management in mobile and wireless communications.” IGI Global; 2019.

[14] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration," it – Inf. Technol., vol. 60, no. 5-6, pp. 283–291, 2018. doi: 10.1515/itit-2018-0019

[15] Ö. Karaduman et al., "Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review," *Appl. Sci.*, vol. 15, no. 6, p. 3225, 2025. doi: 10.3390/app15063225

[16] D. Chatziamanetoglou and K. Rantos, "Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus," Secur. Commun. Netw., vol. 2023, Art. no. 3303122, 2023. doi: 10.1155/2023/3303122

[17] M. Khari, G. Shrivastava, S. Gupta, & R. Gupta, (2017). Role of cyber security in today's scenario. In *Detecting and Mitigating Robotic Cyber Security Risks,* IGI Global

(pp. 177-191), 2017.

[18] Y. Gao et al., "Retrieval-Augmented Generation for Large Language Models: A Survey," arXiv, arXiv:2312.10997, 2023. doi: 10.48550/arXiv.2312.10997