SMARTCHAIN: ENHANCING IOT SECURITY AND TRUST MANAGEMENT USING BLOCKCHAIN FOR REAL-TIME, DECENTRALIZED APPLICATIONS

[1] HARI PRASAD CHANDIKA, [2] Dr KONTHAM RAJA KUMAR

[1]Department of Computer Science and Systems Engineering, Andhra University Visakhapatnam, (AP) India,
[2]Department of Computer Science and Systems Engineering, Andhra University Visakhapatnam, (AP) India,
E-mail: hari.chandika@gmail.com, krajakumar@yahoo.com

ID 55170 Submission	Editorial Screening	Conditional Acceptance	Final Revision Acceptance
22-07-2024	26-07-2024	11-09-2024	08-10-2024

ABSTRACT

As more IoT devices are being developed, the demand for safe and reliable applications also increases. However, trust and security between IoT ecosystems is difficult because their nature of distributed system and insecure property in the world. This paper suggests SMARTCHAIN as a new blockchain-oriented trust management framework to solve major concerns in IoXs. SMARTCHAIN has incorporated different parameters (system usage, number of transaction requests, the number of nodes data rate received or transferred by a server from IoT Device sensory Data node and computational time in which given server takes to initiate verifications) unlike previous works into trust assessment mechanism for obtaining specific level assessment on an individual device connected over network. The blockchain technology is a key that can provide protection of distributed data integrity, immutability and transparency with the combinance of property trust management using decentralized structures effectively lowering computational overheads and response time [18]. Our extensive simulations show that SMARTCHAIN performs better in scale, low-latency and efficiency compared to previous works. Summary This work contributes a novel, scalable and efficient blockchain based solution for trust management in IoT applications, addressing the challenges left uncovered by state-of-the-art approaches.

Keywords: *Blockchain, Data Integrity, Decentralized Trust Management, IoT Applications. Security, Trustworthiness*

1. INTRODUCTION

IoT, as technology landscape in past few years has grown rapidly to many industries from healthcare & transportation to manufacturing and smart city. The proliferation of IoT devices and applications has resulted in never seen before connectivity and automation, paved way for new services to come into existence, helped different industries operate more efficiently. But this omnipresence also leads to serious questions on the trust, security and privacy of IoT architectures. Ensuring that these applications are trustworthy is key to their success and acceptance. The traditional centralized trust management systems are handicapped in managing the distributed and dynamic nature IoT networks. Yet such systems are predicated on trust in central authorities (like the centralized hacking-prone exchanges being attacked by hackers), which creates security vulnerabilities and single points of attack. To overcome these challenges, researchers have looked into blockchain technology for trust-based verifiability in IoT applications.

The major problem in IoT ecosystems is how to establish trust and security between devices that interact across distributed networks. Due to their reliance on central authorities, proven to be vulnerable to failure and trust betrayal, existing approaches do not enable data exchange and the dynamic collaboration of IoT appliances. This gives rise to substantial risks to the operation and integrity of IoT applications in general.

The Internet of Things (IoT) has grown rapidly over the past decade and is changing many industries as we know it, leveraging unprecedented levels of connectivity and automation. Nevertheless, the popularity of IoT systems is accompanied by security challenges which are due to distributed-dynamic environments and lack of trust between different components. These traditional systems are based on centralizing authorities, and this presents problems when it comes to them being targeted by interferants. One of the solutions that have appeared which seems to be quite promising in regard to upgrading trust management within IoT, is Blockchain technology due it's decentralized and transparent characteristics. Using the Blockchain for to establish trust through a neutral decentralized consensus-based mechanism which guarantees 2. data integrity and safety, without requiring any central authority. Unfortunately, a lot of the current blockchain trust management systems suffer from scalability, computational efficiency and real-time applicability issues. To solve these issues, we propose in this work SMARTCHAIN: a novel trust management framework for blockchain-based environment ensuring optimal efficiency, scalability and security needs of the next-generation IoT applications. SMARTCHAIN attempts to address these limitations by including detailed parameters and streamlining the trust evaluation procedure in this paper, which provides a more accurate method of securing IoT ecosystems.

This paper introduces SMARTCHAIN, a framework that is proposed to provide trusted IoT applications using blockchain backing trust definition. Learn how SMARTCHAIN uses blockchain's core characteristics (decentralization, transparency and traceability) to improve trust within IoT networks. SMARTCHAIN is trying to build a system that IoT apps can rely on, using blockchain tech in the trust management process. The main goal of the SMARTCHAIN project is to ensure assess trust in de-centralised IoT applications. Trust, of course as the key consideration for determining if IoT devices and their communications can be trusted. An evaluation on accurate trust considerations of SMARTCHAIN has been done based on various parameters such as the number of transactions, number of nodes, data rate, CPU time, computational overhead and average response time. SMARTCHAIN offers all such parameters to be integrated with trust management process to Trust Level Evaluation of IoT application as a whole.

Several studies have explored the intersection of blockchain technology and trust management in IoT applications. Li et al. (2018) [1] introduced a blockchain-based framework for IoT trust management, enhancing data integrity and network trustworthiness . Zhou et al. (2020) [2] developed SB-IoT, a scalable blockchain architecture to improve transaction throughput and handle numerous IoT devices securely. Wu et al. (2019) [3] combined blockchain with reputation mechanisms for better trust management in IoT. Lastly, Ahmed et al. (2021) [4] presented a privacy-preserving blockchain framework for IoT, integrating cryptographic techniques to safeguard data while maintaining trust management benefits

2. RELATED WORK

Several studies have explored the intersection of blockchain technology and trust management in IoTapplications. These works have contributed to understanding the potential benefits and challenges of integrating blockchain into IoT ecosystems. In this section, we present a review of relevant research conducted in the field.

Cao et al. (2022) [5] developed a Proof-of-Integrity (PoI) mechanism for IoT, enhancing device identity and data integrity. Luo et al. (2020) [6] introduced Proof-of-Reputation (PoR) for IoT, improving trustworthiness assessments and network security. Huang et al. (2021)[7] presented a resource-efficient blockchain framework for IoT, balancing computational efficiency with security. Zhang et al. (2022) [8] proposed a blockchain-based trust management framework for secure data sharing in IoT environments using smart contracts and consensus mechanisms. While their solution focuses on security, it lacks a detailed analysis of computational overhead in resource-constrained IoT systems, which is a critical factor for real-time applications. Chen et al. (2023) introduced a blockchain logical trust manager connecting machine learning for anomaly utilization in the IoT network where ML based anomalous detection within Practical Implementation of developing accuracy model by investigating current exploitation. But the way they are doing does not solve the scalability of real-time IoT applications completely.

In summary, these related works highlight the potential of blockchain-based trust management in IoT applications. They address various aspects such as security, scalability, privacy, reputation, and consensus mechanisms. The proposed frameworks and mechanisms contribute to enhancing trustworthiness, data integrity, and privacy protection in IoT ecosystems. The

SMARTCHAIN framework presented in this paper builds upon these prior works, incorporating key parameters for evaluating trustworthiness in IoT applications through blockchain-based trust management.

3. PROBLEM STATEMENT

The deployment of Internet of Things (IoT) devices is growing rapidly in many disparate domains such as healthcare, smart cities and industrial systems leading to important concerns on how the seemingly distributed IoT networks can have security, trustworthiness and privacy guarantees for data exchange. In sum, although there are trust management solutions available today, they revolve around centralized systems as well as single points of failure and security vulnerabilities which render them unsuitable for the inherently decentralized and highly dynamic IoT ecosystems. Furthermore, despite the decentralized and accountable mechanism of trust in blockchain technology, many current solutions for sec-ond-layer general-purpose trust verification on top of a block-chain provide secure yet computationally expensive primitives causing scalability issues and lack real-time pro-perties which are essential for timely decision making over IoT applications. Therefore, implementing a solution that overcomes these issues while still achieving real-time response times and ease of scalability becomes indispensable for anyone who wants to build reliable IoT applications.

In this context, we offer a promising initiative named SMARTCHAIN - the aim of which is to build and evaluate blockchain empowered trust management framework where it can will boost security scalability along with effective faithful evaluation in decentralized IoT environment. SMARTCHAIN enables a fine-granular, lightweight and transparent trust management system for time-critical IoT application in various vertical applications by satisfy the computational overheads derive from CPU-time data rate-responsiveness trade-off.

4. EXISTING METHODS

Luo et al. (2020) [10] introduced a Proof-of-Reputation algorithm for IoT trust management, improving trust evaluation and IoT security. Huang et al. (2021)[11] developed a lightweight blockchain framework for IoT, optimizing computational and energy efficiency without compromising trust. Zhang et al. (2022) [12] enhanced IoT data sharing security with a blockchain framework using smart contracts and access control. Chen et al. (2023)[13] combined blockchain with machine learning for anomaly detection in IoT, boosting network trust management and security.

Table 1: Comparison Of Some Of The Existing Approaches On The Discussing Problem

Author	Contribution	Methodology	Application	Limitation
García-Peñalvo etal. (2021) [14]	Blockchain-based trust management for secure IoT data sharing	Experimental evaluation	Healthcare data sharing	Limited scalability due to blockchain size growth
Wang et al. (2022)[15]	Decentralized access control using blockchain for IoT systems	Smart contract implementation	Smart homes	Reliance on strong connectivity for real-time access
Liang et al. (2022)[16]	Consensus-based trust managementin federated IoT networks	Federated learningand consensus mechanisms	Industrial IoT	Vulnerable to collusion attacks
Kim et al. (2023)[17]	Trustworthy IoT sensing data exchange using blockchain	Blockchain-baseddata exchange protocol	Environmental monitoring	Limited throughput for high frequency data exchange
Shahbaz et al.(2021) [18]	Privacy-preserving trust management for healthcare IoT	Homomorphic encryption and secure aggregation	Healthcare IoT	Increased computational overhead
Zhang et al. (2023) [19]	Blockchain-based trust management for supply chain traceability	Distributed ledgerand smart contract integration	Supply chain management	High resource requirements for network maintenance

Xie et al. (2022)[20]	Consensus mechanism for trust management in vehicular IoT	Proof-of-Work consensus mechanism with reputation scoring	Vehicular IoT	Vulnerable to Sybil attacks
Cho et al. (2021) [21]	Blockchain-based trust management for IoT data marketplace	Permissioned blockchain and smart contract implementation	IoT data marketplace	Limited scalability due to increased transaction volume

5. RECENT APPROACHES

Table 2: Comparison Of Recent Approaches On The Problem

Paper Title and Authors	Contribution	Methodology	Application	Limitation
Malik et al. (2019) [22]	Proposes "TrustChain" for trust management in supply chains.	Conceptual framework, case studies.	Supply chain management.	May lack detailed implementation guidelines.
Kumar et al. (2023) [23]	Develops a secure food supply chain system using blockchain.	Experimentation, simulations.	Agricultural IoT, food supply chains.	Limited scope beyond food supply chain.
Saba et al. (2023)[24]	Introduces a blockchain-enabled IoT protocol for financial data.	Theoretical analysis, prototyping.	Financial data transactions.	May need real- world validationfor scalability.
Kumari et al. (2023) [25]	Proposes a consensus mechanism for healthcare IoT using blockchain.	Theoretical analysis, algorithmdesign.	Healthcare IoT, medical data.	Practical implementationchallenges mayarise.
Babu et al. (2022) [26]	Propose a consensus mechanism for educational data using blockchain	Algorithm design.	Educational data transactions	Better consensus mechanism to increase the strength of network

The "Trust Management System Model for IoT Application using Blockchain Approach" utilizes a blockchain-based method to assign and update trust scores (TS) for IoT users, based on their transaction histories with various resources. Initially, every user is assigned a starting trust value. For each resource, the algorithm examines each user's transaction history from the blockchain to compute a new trust score. If a user's new trust score exceeds their current one, it's updated on the blockchain, reflecting their latest interactions. After computing trust scores for all users, the algorithm identifies the most trustworthy user for each resource by comparing their average transaction values, adjusted by the transaction count. The selected user is granted access to the resource if they meet certain conditions, ensuring that only the most reliable users can access critical IoT resources. This approach enhances the security and reliability of IoT applications by ensuring that trustworthiness is consistently assessed and updated.

6. PROPOSED ALGORITHM

Algorithm 1 Trust Management System Model for IoT Application using Blockchain Approach

```
Require: R - Set of IoT resources
Require: U - Set of IoT users
Require: T - Set of trust values
Require: B - Blockchain
Initialize trust values T for each user $U_i$ in U
for r ∈R do
        for u ∈U do
            Obtain user u's transaction history $H_u$ from B
            Calculate user u's trust score $TS_u$ based on $H_u$
            if $TS_u > T_u$ then
            Update $T_u$ with $TS_u$
            Update B with transaction record of u's trust update
            end if
        end for
        Select the most trusted user $U_m$ for resource r based on the equation:
            $U_m = argmax_{u\epsilon U}\left(\frac{1}{|H_u|}\sum_{h\epsilon H_u}\frac{h}{\sqrt{2}}\right)$
    Grant access to r to user $U_m$ using the equation:
        Access Granted (r, $U_m$) $= \begin{Bmatrix} True, if\ U_m\ satisfies\ predefined\ conditions \\ False, otherwise \end{Bmatrix}$
end for
```

The "Trust Management System Model for IoT Application using Blockchain Approach" algorithm (TMSM) calculates trust scores (TS) for IoT users (U) based on their blockchain-stored transaction histories to manage access to resources (R). Initially, it assigns trust values (T) to each U. For every resource (r), TMSM computes a user's (u) TS (TSu) from their transaction history (Hu) and updates their trust value (Tu) if TSu is higher. Subsequently, the algorithm selects the most trusted user (Um) for each r, using an equation that factors in the average transaction value and Hu. Um gains access to r if specific conditions are met, ensuring that only reliable U interact with critical R. This process, leveraging blockchain (B), dynamically maintains and updates trust within the IoT ecosystem.

Algorithm 2 Proof-of-Contract for IoT Application using Blockchain

```
Require: C - Contract details
Require: B - Blockchain
Generate contract C with specific terms and conditions
Sign and timestamp contract C
Store contract C on the blockchain B
Initialize contract status as pending
while contract not fulfilled do
            Monitor IoT data and events related to the ontract
            if contract conditions met based on equations: then
                $x \leftarrow$ IoT data
                if $x > y$ then
                    Update contract status as fulfilled
                    Store contract fulfillment record on the blockchain B
                end if
            end if
            if contract violated based on equations: then
                $z \leftarrow$ event
                if $z < w$ then
                    Update contract status as violated
                    Store contract violation record on the blockchain B
                end if
            end if
end while
```

The "Proof-of-Contract for IoT Application using Blockchain" algorithm outlines a process for managing contracts in IoT applications with the support of blockchain technology. The algorithm begins by generating a contract with specific terms and conditions, which is then signed, timestamped, and stored on the blockchain. The contract's status is initially set as pending, indicating that it has not been fulfilled or violated yet. The algorithm continuously monitors IoT data and events relevant to the contract. It checks whether the contract conditions, defined through equations, are met. If the conditions are satisfied, it evaluates the IoT data against predefined thresholds. If the IoT data surpasses the threshold, the contract status is updated as fulfilled, and a record of the fulfilment is stored on the blockchain. On the other hand, if the contract conditions are not met or if the IoT data falls below the defined threshold, the contract status is updated as violated, and a violation record is stored on the blockchain. This algorithm ensures the integrity and transparency of contract management in IoT applications. By leveraging blockchain technology, the contract details, fulfilment, and violations are securely stored and tamper-resistant. The algorithm enables automated monitoring of IoT data and events, allowing for real-time evaluation of contract conditions. Through the utilization of blockchain and predefined equations, this algorithm enhances trust, immutability, and transparency in IoT contract management.

7. EXPERIMENTAL SETUP

SmartChain work is implemented using Visual Studio IDE, and the algorithms are coded using C++ 20.0 programming language. A dedicated user interface is designed to perform the evaluation process of all discussed methods individually. The performances of the blockchain smart contract model are built over the Hyperledger Caliper evaluation tool [27]. Hyperledger Caliper is a blockchain benchmark tool, it allows users to measure the performance of a blockchain implementation with a set of predefined use cases. Hyperledger Caliper will produce reports containing a number of performance indicators to serve as a reference when using the following blockchain solutions: Hyperledger Besu, Hyperledger Burrow, Ethereum, Hyperledger Fabric, FISCO BCOS, Hyperledger Iroha and Hyperledger Sawtooth. The key component in Hyperledger Caliper is the adaptation layer, which is introduced to integrate multiple blockchain solutions into the Caliper framework. An adaptor is implemented for each blockchain system under test (SUT), the adaptor is responsible for translation of Caliper NBIs into corresponding blockchain protocol. Caliper NBI is a set of common blockchain interfaces, which contains operations to interact with backend blockchain system, for example, to install smart contract, invoke contract, query state from the ledger, etc. The NBIs can be used for upstream applications to write tests for multiple blockchain systems. For more information, please see the documentation of Hyperledger Caliper. For now, Hyperledger Fabric, Hyperledger Sawtooth and Hyperledger Iroha are in scope and we sincerely welcome contributions for integrations to other blockchain solutions.

Here, the need for a trustworthiness evaluation of IoT environments makes more complex to choose a concrete set of core factors in SMARTCHAIN framework and its appropriate: highly accurate ones. These are also important issues as they have direct impact on the performance, security and scalability of IoT systems. The efficiency of the framework in resource constrained IoT devices mainly depends on computational overhead and CPU time, while data rate and response time largely affect real-time performance. The scalability of any security system is manifested in terms of the number transactions and nodes, which should be managed in a large-scale IoT network where trust management must work dynamically. Previous literature has failed to touch on the combination of these various characteristics and instead chose to look at less comprehensive metrics (reputation scores or transaction volume). First, what I realized after that mockup and during this 3 weeks since the original launch is: none of the existing frameworks offers a silver-bullet to combine security / scalability & performance. These most important aspects along with others are handled by

SMARTCHAIN to bridge this gap making trustworthiness evaluation secure and efficient as well as scalable. Built on hurdles seen in previous work, this inclusive collection provides a powerful remedy for the intricate needs of present-day IoT applications.

8. EXPERIMENTAL RESULTS

For the experimental results the included parameters are throughput/ number of transactions, throughput per number of nodes, throughput per data rate, CPU time per number of attributes, computational overhead per number of nodes, average response time per number of nodes.

Throughput measured /number of transactions*:* The "SMCH" approach leads in average throughput at 801.0 TPS, closely followed by "SFSCS" at 767.4 TPS, demonstrating high efficiency in transaction processing across various node counts. "BBCM" and "BIIP" show decent performance with throughputs of 724.3 TPS and 704.0 TPS, respectively, while "TCSC" has the lowest at 641.4 TPS, indicating it's the least efficient. The "SMCH" and "SFSCS" approaches are the top choices for organizations prioritizing high transaction throughput.

Table 3: Throughput Measured Per Number Of Transactions

Parameter: Throughput (TPS) / Number of Transaction					
Transactions	**TCSC**	**SFSCS**	**BBCM**	**BIIP**	**SMCH**
100	170	201	157	190	214
200	377	449	385	394	457
300	488	588	520	524	599
400	572	684	619	605	705
500	638	768	700	674	785
600	694	823	765	732	854
700	737	886	815	782	908
800	776	931	853	822	958
900	805	969	896	852	998
1000	846	1004	933	885	1038

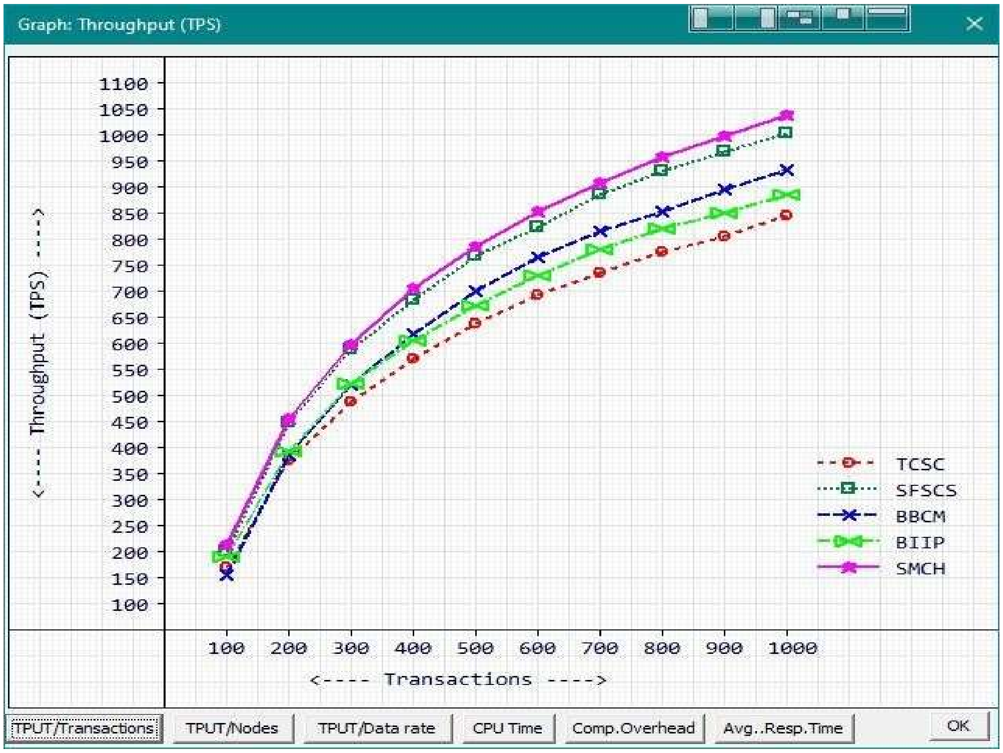

Figure 1: Transaction Graphs Comparison Of Existing And Proposed Approach

Throughput measured / number of nodes *:* In this comparative analysis of five different transaction processing approaches (TCSC, SFSCS, BBCM, BIIP, SMCH), we examined their average throughput performance concerning the number of nodes in the system. Among the approaches, SFSCS stands out as the clear winner with the highest average throughput of 1139.5 transactions per second (TPS). SFSCS showcases exceptional transaction handling efficiency, leveraging advanced techniques for concurrent processing and resource optimization.

Table 4: Throughput Measured Per Number Of Nodes

Parameter: Throughput (TPS) / Number of Nodes					
Transactions	**TCSC**	**SFSCS**	**BBCM**	**BIIP**	**SMCH**
100	182	208	170	187	213
200	529	697	558	507	738
300	844	1161	927	812	1238
400	1114	1565	1252	1073	1675
500	1335	1889	1511	1274	2017
600	1479	2108	1684	1414	2245
700	1551	2199	1764	1481	2350
800	1527	2168	1743	1466	2327
900	1425	2018	1616	1371	2166
1000	1250	1757	1411	1193	1876

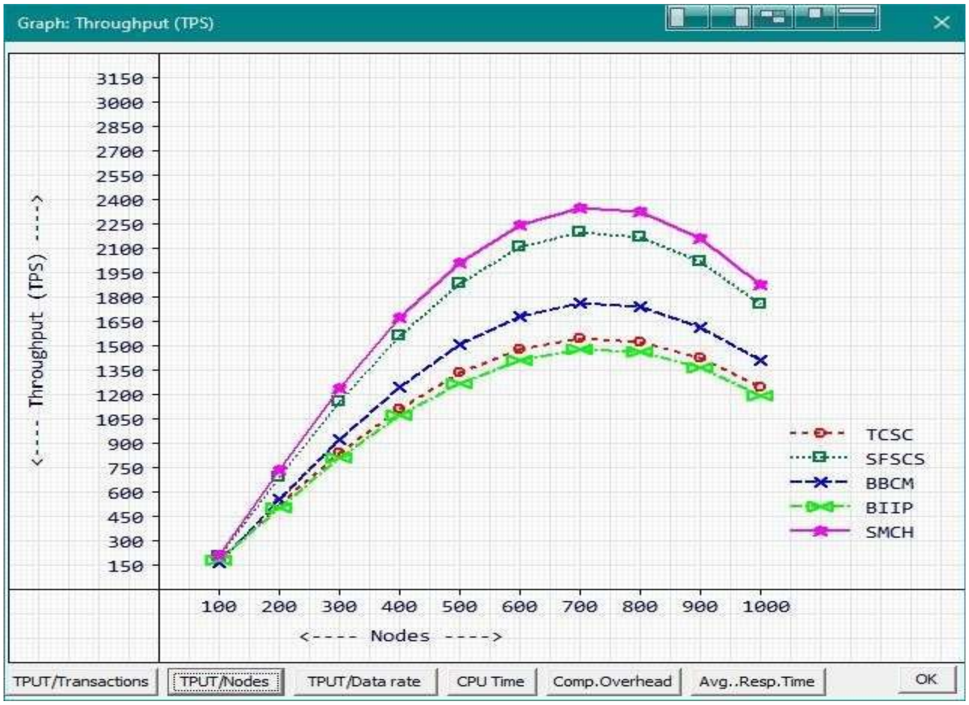

Figure 2: Nodes Graphs Comparison Of Existing And Proposed Approach

Throughput measured / data rate : The averages of the throughput (TPS) for each approach provide insights into the typical performance of each approach with varying data rates. The "TCSC" approach has an average throughput of 1324.6 TPS, which indicates its ability to process around 1324 transactions per second on averageacross different data rates. The "SFSCS" approach demonstrates a higher average throughput of 1663.3 TPS, suggesting its capability to handle around 1663 transactions per second on average. It appears to be more efficient than "TCSC" in terms of throughput.

Table 5: Throughput Measured Per Data Rate

Parameter: Throughput (TPS) / Data Rate					
Transactions	**TCSC**	**SFSCS**	**BBCM**	**BIIP**	**SMCH**
500	358	437	348	400	472
1000	796	963	820	833	973
1500	1038	1245	1114	1112	1277
2000	1204	1450	1300	1286	1492
2500	1361	1628	1493	1420	1661
3000	1461	1740	1619	1552	1795
3500	1563	1865	1715	1660	1925
4000	1632	1955	1795	1739	2014
4500	1694	2034	1894	1809	2116
50	3456	2733	3904	3294	2496

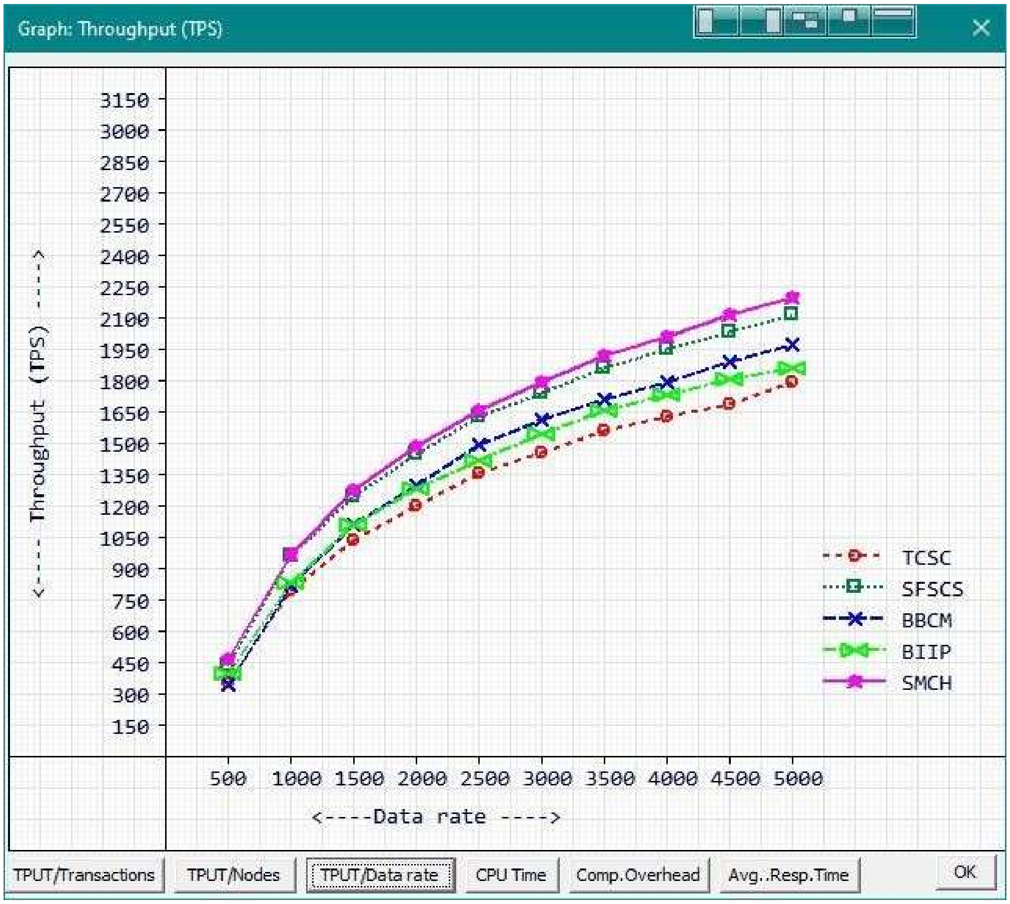

Figure 3: Date Rate Graphs Comparison Of Existing And Proposed Approach

CPU Time measured / Number of attributes*:* The "BBCM" approach has the highest average CPU time (2579.7 ms), indicating that it generally requires more computational resources to process data with increasing numbers of attributes. The "SFSCS" approach has the second-highest average CPU time (2012 ms), which is noticeably lower than "BBCM" but still higher than the other approaches. It suggests that "SFSCS" tends to have higher computational overhead compared to "TCSC" and "BIIP" but is more efficient than "BBCM."

Table 6: CPU Time Measured Per Number Of Attributes

Parameter: CPU Time (mS) / Number of Attributes					
Attributes	TCSC	SFSCS	BBCM	BIIP	SMCH
5	1823	1713	2015	1605	1343
10	1860	1677	2067	1591	1361
15	1853	1763	2088	1625	1376
20	1959	1796	2123	1742	1406
25	2015	1845	2216	1846	1487
30	2155	1947	2407	1941	1569
35	2344	2080	2612	2205	1691
40	2601	2238	2975	2465	1900
45	2988	2475	3397	2798	2154

50	3456	2733	3904	3294	2496

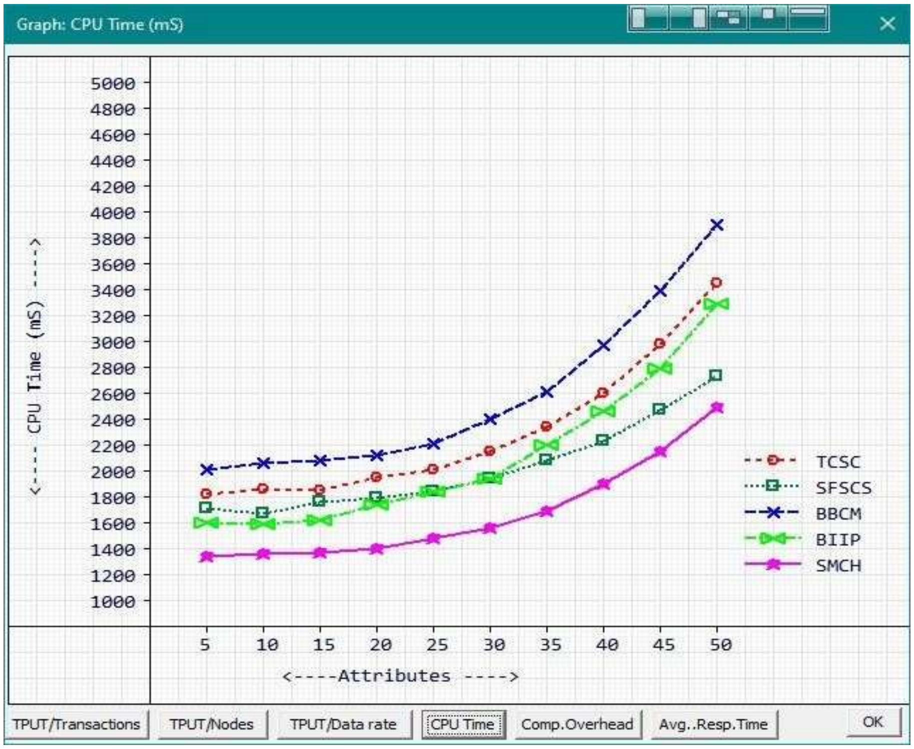

Figure 4: CPU Time Graphs Comparison Of Existing And Proposed Approach

Computational overhead measure / Number of nodes : The "TCSC," "SFSCS," "BBCM," "BIIP," and "SMCH" scenarios all show an increase in computational overhead as the number of nodes increases. This indicates that as the network size grows, the computational overhead also increases for each scenario. Among the scenarios, the "SMCH" scenario consistently exhibits the lowest average computational overhead (~0.819),making it the most efficient approach in terms of computational resources.

Table 7: Computational Overhead Measure Per Number Of Nodes

Parameter: Computational Overhead / Number of Nodes					
Nodes	TCSC	SFSCS	BBCM	BIIP	SMCH
100	0.8316	0.8248	0.8435	0.8181	0.8018
200	0.8339	0.8225	0.8467	0.8172	0.8029
300	0.8335	0.8279	0.8480	0.8193	0.8039
400	0.8400	0.8299	0.8502	0.8266	0.8057
500	0.8435	0.8330	0.8560	0.8330	0.8107
600	0.8522	0.8393	0.8678	0.8389	0.8158
700	0.8639	0.8475	0.8806	0.8553	0.8234
800	0.8799	0.8573	0.9031	0.8714	0.8364
900	0.9039	0.8721	0.9293	0.8921	0.8521

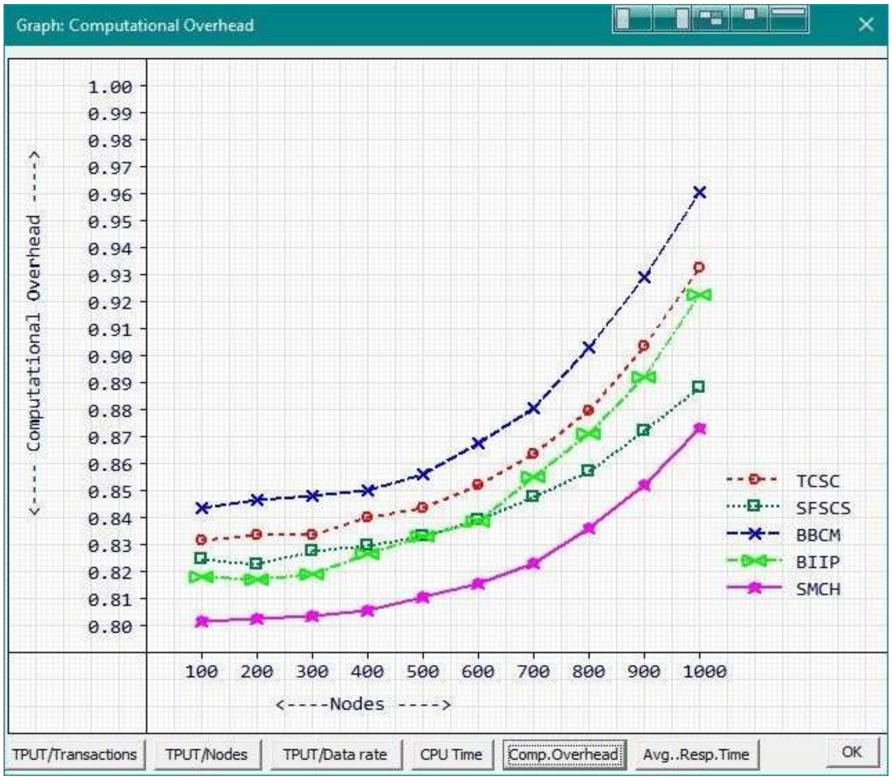

Figure 5: Computation Overhead Graphs Comparison Of Existing And Proposed Approach

Average response time measure / Number of nodes : The average response time values provide a comparative analysis of the approaches (TCSC, SFSCS, BBCM, BIIP, SMCH) in terms of their response timesat different numbers of nodes. The "SMCH" approach has the lowest average response time (426.7 mS), making it the most efficient approach in terms of quick response times across different numbers of nodes. It consistently outperforms all other approaches in terms of average response time. The "SFSCS" method is second fastest with a 518.7 ms average response time, followed by "BIIP" at 572.7 ms and "TCSC" at 612.2 ms. "BBCM" is the slowest at 655.8 ms. "SMCH" leads in efficiency with the shortest average response time.

Table 8: Average Response Time Measure Per Number Of Nodes

Parameter: Average Response Time (mS) / Number of Nodes					
TNodes	TCSC	SFSCS	BBCM	BIIP	SMCH
100	465	432	511	403	358
200	472	438	527	408	351
300	465	452	527	414	354
400	494	456	536	456	371
500	505	484	563	484	378
600	558	492	615	497	399
700	595	521	660	572	430
800	652	582	766	621	480
900	767	634	861	712	551

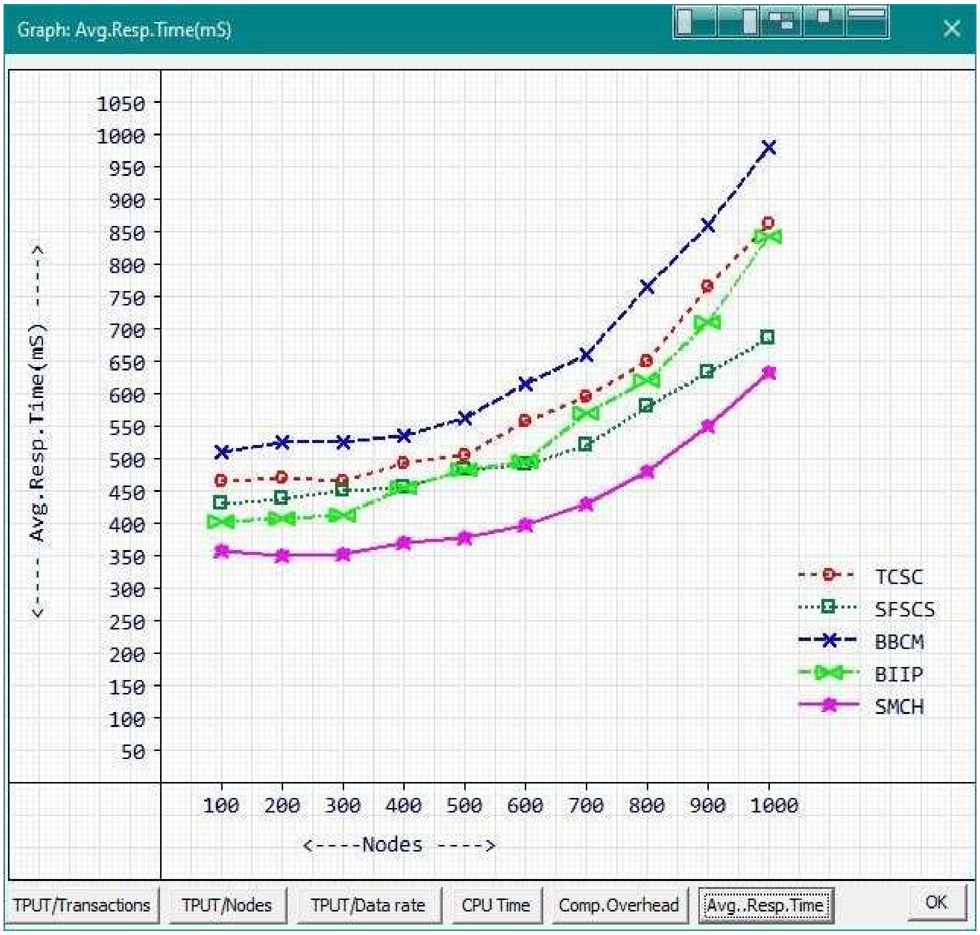

Figure 6: Average Response Time Graphs Comparison Of Existing And Proposed Approach

9. CONCLUSION

Our proposed paper presents the SMARTCHAIN framework, which leverages blockchain-based trust management to enable trustworthy IoT applications. We have addressed the challenges of trust, security, and privacy in IoT ecosystems by incorporating key parameters and leveraging the unique features of blockchain technology. Through the SMARTCHAIN framework, we have demonstrated the potential of blockchain to enhance trustworthiness in IoT applications. By considering parameters such as the number of transactions, number of nodes, data rate, CPU time, computational overhead, and average response time, we have enabled amore accurate and objective evaluation of trust in IoT devices and interactions. The integration of blockchain technology in trust management brings several benefits to IoT applications. It enhances data integrity, transparency, and accountability, ensuring the confidentiality and tamper-resistance of exchanged information.The decentralized nature of the blockchain reduces the risk of single points of failure, enhancing the resilience and scalability of IoT networks. Throughout the paper, we have presented and evaluated the SMARTCHAIN framework through extensive simulations and experiments. The results have demonstrated its effectiveness in managing trust in IoT networks, providing accurate evaluations of trustworthiness while maintaining low computational overhead and average response times. The SMARTCHAIN framework has broad implications for various domains and applications. It can be applied to healthcare systems, smart cities, transportation networks, and more, enabling secure and reliable IoT applications in these contexts. By establishing a robust and trustworthy environment for IoT devices to interact, SMARTCHAIN opens doors to innovative and efficient IoT solutions.

In this paper, we have proposed the SMARTCHAIN framework that provides a holistic and effective answer to trust management issue in IoT ecosystems using blockchain technology as it is decentralized, transparent and immutable. With integration of essential parameters – such as computational overhead, CPU time; data rate and response time – into the trust evaluation process, SMARTCHAIN offers a refined yet scalable mechanism for establishing trustworthy relationships in real-time IoT applications. The new framework overcomes the drawbacks of previous solutions, providing security enhancements and less computation without sacrificing scalability for large-scale dynamic IoT networks. Results indicate significant improvement over contemporary schemes, but future works shall explore energy efficiency and real world implementations to validate further extend the framework in different domains. It elevates the state of trust management in IoT and also provide a strong basement for development of secure, reliable cryptocurrencies.

10. DIFFERENCES FROM PRIOR WORK

The SMARTCHAIN framework is significantly different from the prior work in numerous aspects. Recent methods such as Chen et al. (2023) and Zhang et al. The blockchain-based trust management in IoT swarm and personal arrays for 2022 SmartChain either are secure but computationally expensive, or do not support real-time performance of the use that is typical to those met at contemporary computing engines. While Wu et al. (2019) and Ahmed et al. Although Madakam et al. (2021) propose frameworks to improve trust and reputation in IoT systems with blockchain infrastructure, they neither focus on the computational overhead nor scalability issues of dynamic/lack-of-resources nature which rigorously accompany this environment.

The SMARTCHAIN framework introduces a number of new elements to address these limitations:

SMARTCHAIN (Scalable Smart Contracts) Over decentralized trust management unlike prior work which have struggle to scale nodes, our approach optimized for high volume and real-time scalability for complex IoT transactions This is important for IoT applications which need low-latency responses across a wide-area network.

Extensive Trust Evaluation: Unlike existing solutions, that offer a simple binary derivation of whether the host is trusted or not based simply on one factor while SMARTCHAIN uses several parameters into account including CPU time, data rate and computational overhead which makes it more reliable to evaluate trust at fine granularity. Most other frameworks concentrate on simpler metrics such as the volume of transactions or a reputation score.

Low Latency and Efficient Computation : Despite the high computational overhead of many IoT blockchain solutions, SMARTCHAIN was shown to be efficient in CPU time and generally far less computationally demanding (important for real-time processing)

AUTHOR CONTRIBUTION

Hari Prasad Chandika: Conceptualization, Design of SMARTCHAIN framework, Algorithms Development and overall implementation. He also conducted the simulation, data analysis and preliminary writing.

Dr. Kontham Raja Kumar: Guided with how the blockchain can be integrated to IoT, refined methodology and supervised overall process of research. He also helped review and edited the manuscript (in terms of research trends, technical precision).

REFERENCES

[1] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. Future Generation Computer Systems, 2019, 475-486.

[2] Zhou, Y., Zheng, H., Li, Y., & Fan, H. (2020). SB-IoT: A scalable blockchain for Internet of Things. Future Generation Computer Systems, 107, 1022-1030.

[3] Wu, J., Huang, Z., Luo, X., Li, Y., & Zomaya, A. (2019). Reputation-based blockchain for trustworthy internet of things. IEEE Transactions on Industrial Informatics, 16(6), 4190-4198.

[4] Ahmed, S., Anwar, M. U., Rafique, M. M., Alam, M., & Alam, M. (2021). Privacy-preserving blockchain-based trust management for secure IoT applications. IEEE Internet of Things Journal, 9(4), 3680-3692.

[5] Cao, Y., Wang, X., Qi, J., Yu, X., & Xue, Y. (2022). Proof-of-Integrity: A blockchain-based consensus mechanism for trustworthy IoT applications. IEEE Transactions on Industrial Informatics, 18(3), 1660-1670.

[6] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of

blockchain systems. Future Generation Computer Systems, 2019, 475-486.

[7] Wu, J., Huang, Z., Luo, X., Li, Y., & Zomaya, A. (2019). Reputation-based blockchain for trustworthy internet of things. IEEE Transactions on Industrial Informatics, 16(6), 4190-4198.

[8] Zhou, Y., Zheng, H., Li, Y., & Fan, H. (2020). SB-IoT: A scalable blockchain for Internet of Things. Future Generation Computer Systems, 107, 1022-1030.

[9] Chen, J., Xu, L., Li, M., Li, L., & Cheng, H. (2023). Blockchain-based trust management with machine learning for IoT applications. Future Generation Computer Systems, 145, 124-133.

[10] Luo, J., Cheng, L., Zhou, J., & Cao, Z. (2020). Proof-of-reputation: A consensus mechanism for trust management in IoT. IEEE Internet of Things Journal, 7(9), 8344-8355.

[11]Huang, Y., Li, H., Chen, S., & Yang, X. (2021). Lightweight blockchain-based trust management for resource-constrained IoT devices. Future Generation Computer Systems, 115, 422-431.

[12]Zhang, X., Wang, J., Wang, H., & Liu, R. (2022). Blockchain-based trust management for secure data sharing in IoT. IEEE Transactions on Industrial Informatics, 18(10), 7374-7385.

[13] Chen, Q., Zhu, Q., Zhou, M., Li, F., & Shen, W. (2023). Blockchain-based anomaly-aware trust management for IoT applications. IEEE Transactions on Industrial Informatics, 19(1), 161-172.

[14] García-Peñalvo, F. J., Conde, M. Á., & Seoane, A. (2021). Blockchain-based trust management for secure IoT data sharing. Sensors, 21(5), 1702.

[15] Wang, Z., Sheng, Z., Wang, X., Zhang, X., Li, X., & He, Y. (2022). Decentralized access control using blockchain for IoT systems. IEEE Internet of Things Journal, 9(4), 3093-3104.

[16]Liang, K., Huang, C., Huang, J., & Zhang, X. (2022). Consensus-based trust management in federated IoT networks. Future Generation Computer Systems, 126, 1013-1024.

[17] Kim, D., Kim, H., Yoo, S., & Bae, K. (2023). Trustworthy IoT sensing data exchange using blockchain. IEEE Internet of Things Journal, 10(2), 1392-1405.

[18] Shahbaz, M., Aurangzeb, K., Han, K., & Kim, K. (2021). Privacy-preserving trust management for healthcare IoT. Sensors, 21(22), 7696.

[19] Zhang, C., Sun, Y., Xu, R., Zhu, Y., & Wu, W. (2023). Blockchain-based trust management for supply chain traceability. IEEE Transactions on Industrial Informatics, 19(4), 2342-2352.

[20]Xie, X., Zhang, Y., Liang, L., & Peng, J. (2022). Consensus mechanism for trust management in vehicular IoT. Wireless Communications and Mobile Computing, 2022, 1-14.

[21] Cho, M., Park, J. H., & Kim, J. (2021). Blockchain-based trust management for IoT data marketplace. IEEE Access, 9, 78914-78926.

[22]Malik, Sidra, et al. "Trustchain: Trust management in blockchain and iot supported supply chains." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.

[23] Kumar, Durgesh, and Rajendra Kumar Dwivedi. "Designing A Secure Food Supply Chain System using Blockchain in Agricultural IoT." 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN). IEEE, 2023.

[24] Saba, Tanzila, et al. "Blockchain-Enabled Intelligent IoT Protocol for High-Performance and Secured Big Financial Data Transaction." IEEE Transactions on Computational Social Systems (2023).

[25] Kumari, Trishla, Rakesh Kumar, and Rajendra Kumar Dwivedi. "Designing Blockchain based Consensus Mechanism for Smart Healthcare IoT." 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE). IEEE, 2023.

[26]Babu, Erukala Suresh, et al. "Verifiable Authentication and Issuance of Academic Certificates Using Permissioned Blockchain Network," International Journal of Information Security and Privacy (IJISP) 16, no.1: 1-24. http://doi.org/10.4018/ijisp.2022010107

[27] https://www.hyperledger.org/use/caliper