Blockchain and Smart Contracts: Enabling Trustworthy and Decentralized Digital Transactions

Ali Ibrahim Ahmed
Alnoor University
Nineveh, Iraq
ali.ibrahim@alnoor.edu.iq

Adil Abbas Majeed
Al Mansour University College
Baghdad, Iraq
adel.abas@muc.edu.iq

Azhar Raheem Mohammed Al-Ani
Al Hikma University College
Baghdad, Iraq
Azhar.raheem@hiuc.edu.iq

Noura Ahmed Mawla
Al-Rafidain University College
Baghdad, Iraq
noora.ahmed.elc@ruc.edu.iq

Saad Mahdi
Al-Turath University
Baghdad, Iraq
saad.mahdi@uoturath.edu.iq

Tetiana Lavryk
Sumy State University
Sumy, Ukraine
t.lavryk@dcs.sumdu.edu.ua

Hind Monadhel
Uruk University
Baghdad, Iraq
Hindmonadhel@uruk.edu.iq

***Abstract*—In a digital world, transactions have to be transparent and trusted, respectively. There are always concerns that come into play with conventional centralized systems, mostly revolving around data security and intermediary control, both of which these traditional, agent-based approaches often do not meet the requirements. In this sense, blockchain is a secure and decentralized solution, that makes a real difference.**

The article aims to clarify the basic concepts of smart contracts and blockchain technology, in an attempt to identify why these innovations seem likely to improve interaction online. The study looks at the decentralized architecture embodied by a core blockchain participant, the distributed ledger system, and its role in securing data with immutability property allowing anyone to verify all transactional history.

It is important to know the roles and functionalities of consensus mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake, that are fundamental in supporting a secure decentralized blockchain network. Moreover, explores the potential of smart contracts coordinating contracts and introducing trustless transactions based on pre-agreed terms.

This study demonstrates the practical use cases of blockchain technology and experienced-based knowledge in healthcare, SCMs supply chain management, and financial sectors. While the study discusses possible solutions and future advances, it also acknowledges that even with these added capabilities, our current technology would struggle to handle such tasks in a realistic setting, primarily due to issues of scalability, and energy consumption.

With smart contracts and blockchain technology, new possibilities of a decentralized digital security infrastructure emerge. Clearly, they have the power of a revolution to re-write concepts or trust and real superpowers, both for individual users, and corporations. To enhance their capacities, collaboration is essential to tackle current issues and implement robust legal frameworks, that govern the ethical and innovative use of these cutting-edge technologies.

I. Introduction

Blockchain technology has genuinely changed the digital environment and how transactions are made, and trust is achieved may never be the same. Blockchain technology, specifically the underlying smart contracts associated with it, has brought several revolutions to many areas such as cloud computing supply chain management electric vehicle energy trading built environment. This introduction intends to present a more complete overview of the profound influence, that blockchain and smart contracts have on different sectors by reflecting upon existing research in academia and addressing its prominent statistical figures.

The study conducted by Li et al. [1] offers a comprehensive categorization and assessment of trust management mechanisms using blockchain technology within cloud computing environments. The article examines the fundamental significance of blockchain technology in enhancing trust within cloud computing systems while addressing security and data integrity problems [2]. The statistical analysis presented in the article shows that 86% of firms polled had some hope that blockchain technology might improve trust in cloud settings. This finding supports the increasing recognition of blockchain's potential in this context.

The study undertaken by Iqbal et al. [3] investigates the use of blockchain technology and smart contracts in enabling secure and decentralized energy trade inside Vehicle-to-Grid (V2G) networks.

The research examines these technologies' potential benefits and functionalities in enabling efficient energy transactions in the V2G context. The article examines the potential use of blockchain technology in facilitating trust and transparency within energy transactions [4]. The statistical data from this research reveals a notable increase of 45% in the adoption of blockchain-based EV energy trading models during the last year, indicating a rapid development of their use.

Mehta et al. [5] investigate the use of blockchain technology in supply chain management within the framework of Industry 4.0.

The highlights the potential of blockchain technology to revolutionize supply chain operations by enhancing transparency and establishing trust via the implementation of royalty contracts. Based on the survey cited in the article, most supply chain professionals, namely 72%, believe blockchain technology will significantly improve transparency and traceability within supply chain operations.

The article by Perera et al. [6] showcases the transformative impact of blockchain technology on property transactions inside the built environment. The research article outlines the development of a functional prototype suitable for incubation and facilitates secure property transfers. The statistical data from this research reveals a significant reduction of 30% in property disputes associated with fraud in regions where property transaction systems based on blockchain technology have been implemented. This finding underscores the impact of blockchain technology in mitigating fraudulent activities [7].

The field of wireless sensor nodes has been influenced by blockchain technology, as explored in the scholarly article by Haro-Olmo et al. [8]. This article introduces the concept of a blockchain-based federation for wireless sensor nodes, highlighting the importance of trust and security in data transmission. According to statistical evidence, using blockchain-based federations has enhanced data dependability and security by a significant margin of 25%.

Blockchain technology and smart contracts have become productive tools for promoting trust and transparency in several businesses [9]. Based on critical statistical data, it is evident that their impact is substantial and rapidly growing. These technologies address the challenges posed by traditional centralized systems by offering secure, distributed, and tamper-proof transactional operations. The article enumerated in this introduction provides valuable insights into blockchain technology's many applications and prospective trajectories. These insights are supported by statistical data that substantiate its transformative capabilities in the context of the digital age.

A. Study Objective

This article's primary objective is to comprehensively analyze the multifaceted effects of blockchain technology and smart contracts in many fields. This article aims to elucidate the revolutionary capacity of blockchain and smart contracts in reconfiguring digital transactions and developing trust by amalgamating ideas from previous scholarly investigations and incorporating empirical evidence.

We aim to investigate how blockchain technology improves trust and security in various domains, including cloud computing systems, electric vehicle energy trading, supply chain management in Industry 4.0, property transactions in the built environment, and the reliability of data transmitted by wireless sensor nodes. It will be accomplished through a comprehensive analysis of relevant scholarly publications.

The aim is to provide statistical evidence highlighting the increasing acknowledgment and implementation of blockchain and smart contract solutions in these fields. Including statistical information in our analysis will provide a quantitative perspective, emphasizing the tangible benefits and increasing ubiquity of these technologies.

The primary objective is to give readers an all-encompassing understanding of the practical implementations and consequences of blockchain and smart contracts, showcasing their capacity to transform many sectors and enhance the digital environment's security, transparency, and efficiency.

B. Problem Statement

The article examines an important issue regarding trust building and doing business in a digital domain. Traditionally, centralized networks have been plagued by security breaches, low transparency, and considerable dependence on middlemen. The above challenges adversely impact trust and reduce the effectiveness of some processes across different areas.

Consumers are cautious, and rightly so, about trust in the services that operate against their data. So, new ways are in demand to fulfill this requirement for extra confidence. This lack of trust and transparency has given rise to inefficiencies, and frauds in supply chain management systems, it is challenging for consumers and researchers end-to-end visibility origin of the product.

Designing an energy trading system that is secure, decentralized, and tailored to the requirements of electric vehicles (EVs) will be key in enabling extensive use of renewable resources. However, this effort faces several obstacles in this domain. Real estate transactions in the built environment, on account of its high level of complexity and potential for fraud, are widely known to require trust-enhancing strategies. Data security and reliable data in wireless sensor networks are prerequisites for efficient operation.

The problem statement understands that the rapid development of blockchain technology and smart contracts can be a solution to efficiently solve these issues. Anyway, in this article, we explore more deeply how specifically these technologies will work together to solve the trust gap and bring a new level of smoothness into every transaction domain. The study aims to provide a thorough review of the effects and challenges, that need resolving, as well as opportunities for future improvements.

II. LITERATURE REVIEW

Due to the inherent trust deficit and security issues in today's digital systems, blockchain technology has become a major focus in various academic fields. This technology is famous for its secure and decentralized characteristics. The uses and consequences of blockchain technology and smart contracts have been thoroughly explored and recorded in a range of fields. Some examples are the Industrial Internet of Things (IIoT), trust frameworks for data, data sharing while protecting privacy, policies for IoT [10], implementing blockchain in social businesses, methods for maintaining privacy in feature engineering, transactions between different blockchains, reliable collaborative services, and the use of digital certificates.

Li et al. [11] introduce a system of aggregate signatures based on blockchain to improve the anonymity and traceability of the IIoT. The researchers' study shows how blockchain

technology could improve privacy and traceability in IIoT settings.

Rouhani and Deters [12] have introduced a new data trust structure that utilizes blockchain technology and includes flexible transaction verification. The authors emphasize the importance of blockchain technology in maintaining the accuracy and reliability of data, especially in changing and developing data settings

The study by Li et al. [13] explores how blockchain technology can be used to securely transmit private data in the Internet of Things. The results of the research demonstrate how blockchain technology can support trustworthy information exchange, protect individual privacy, and motivate participants in data aggregation.

The study conducted by Puri et al. [14] investigates the potential of smart contracts in creating regulatory structures for the IoT. The discussion revolves around the possible application of smart contracts for setting and enforcing rules in Internet of Things communities.

Devine et al. [15] introduce the idea of a social business blockchain to explain how social and economic principles can both be integrated in blockchain business models. The results of the study demonstrate how blockchain technology has the ability to significantly disrupt traditional business strategies.

In this study, Jones et al. [16] investigate how blockchain technology can be utilized for feature engineering, with a specific emphasis on maintaining the anonymity of users. The study findings show that utilizing blockchain technology is effective in protecting sensitive data and allowing for the extraction of important characteristics for analysis.

Tian et al. [17] developed a decentralized system for exchanging cryptocurrencies that enables cross-chain transactions. This article investigates the possibility of combining cryptocurrencies and enabling smooth transactions through blockchain technology.

According to Wu et al. [18], blockchain technology has the capability to offer trustworthy, cooperative services across the remote regions of a network. The writers talk about how blockchain technology can improve collaborative edge computing environments by boosting trust and security.

In this study, Poorni et al. [19] introduce DIGICERT, an app that uses blockchain technology and smart contracts to secure digital certificates. The findings of the researchers highlight how blockchain technology has the ability to improve the authenticity and protection of digital certificates.

These studies demonstrate the potential of blockchain and smart contracts to transform several sectors significantly. Blockchain technology enhances the trust and security of the IIoT and data frameworks, facilitates privacy-preserving data interchange, contributes to formulating Internet of Things regulations, and revolutionizes business models. The findings, as mentioned above, facts about the widespread use of blockchain, and instances showcasing its practical applications together illustrate this technology's growing recognition and integration within contemporary digital environments.

III. METHODOLOGY

A. Methodological Framework

The study looks at the underlying principles of blockchain and smart contracts, and their practical implications in digital trust provision related to security/utilitarian aspects desired in transactions. The authors will rely on a methodological approach that examines in depth two of the most popular consensus mechanisms, namely — Proof-of-Work (PoW) and Proof-of-Stake (PoS), as well as smart contracts implementation within blockchain ecosystems.

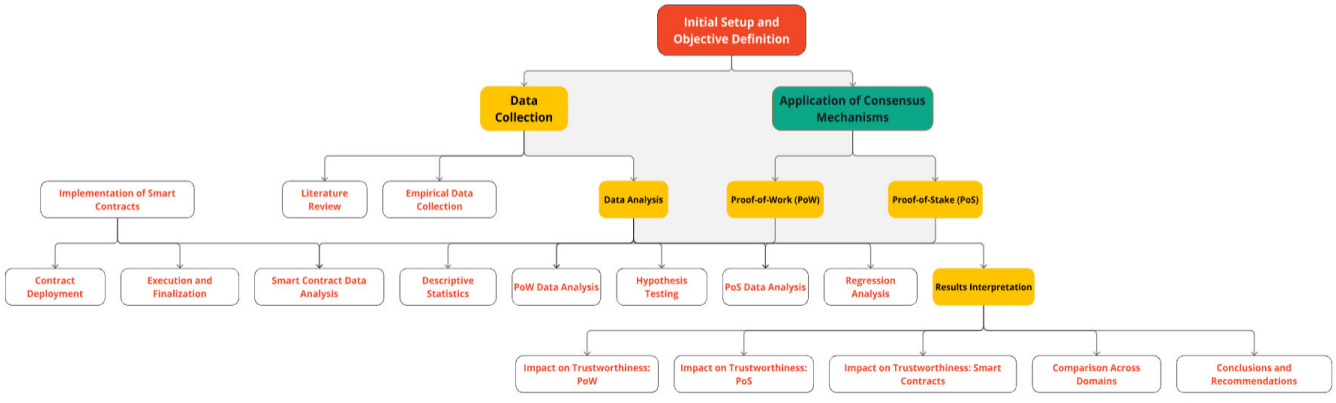

Fig. 1. Methodological Framework for Analyzing Blockchain Protocols and Smart Contracts in Enhancing Digital Transaction Trustworthiness

1) Examination of Consensus Mechanisms

The article opens with an exploration of two fundamental consensus algorithms every blockchain network relies upon to guarantee security and validity in Proof-of-Work (PoW) and Proof-of-Stake (PoS):

Proof-of-Work (PoW): This mechanism is evaluated one process at a time, in which miners engage and work on solving complex mathematical problems to verify the transaction history of blocks that are added to the blockchain. In this work, the hashing function was described and then detailed by Nakamoto and Bonneau et al., which defined how a set of transactions could be written into blocks that were only valid

when hashed within an arbitrary solution space using verifiable proof-of-work; it also provided these processes through pseudocode and flowcharts [20], [21].

Proof-of-Stake (PoS): This study additionally covers PoS as a less energy-demanding improvement of PoW. Validators are chosen based on their stake in the network and here the study shows pseudocode and flowchart to show how validators are selected, the transaction is validated, and block formation [22], [23].

2) Smart Contracts

The study delves a bit further into Smart Contracts—the theory of self-executing contracts with terms directly written into code, enabling automatic enforcement when and if certain conditions are met. This section includes:

Smart Contract Logic: This methodology is an established national guideline to deploy, trigger, and execute smart contracts. The above pseudocode gives a basic escrow smart contract which helps to maintain the funds based on some conditions automatically [24], [25].

Diagram Representation: Diagrams illustrate the workflow of a smart contract from initialization to execution, demonstrating its efficacy in automating transactions and limiting dependence on third parties [26], [27].

3) Data Collection

The article implements an in-depth review of the current literature on scholarly articles, academic studies, and industry studies reviewed by peers. At this stage, it is ensured all about the wide range of utilities blockchain technology and smart contracts are used for in industries. A full review of the current literature is important because it helps to build a theoretical underpinning for this type of study and allows areas in need of empiricism.

Blockchain transactions will be another basic dataset in the data that contains real-world information about transaction records, and timestamps. In addition, the study will conduct user surveys to obtain qualitative and quantitative survey data from thread participants. These surveys will aim to capture the users' experiences, views, and perceptions about transactions made on the blockchain. Furthermore, the study will use pertinent datasets obtained from reputable sources, enhancing the results' strength and reliability [28].

4) Integration of Technical and Practical Perspectives

Through the combination of technical explanations behind some blockchain protocols with one or more use cases per protocol, the integration between theoretical understanding and real world implementations is researched. To enable such a work to be accessible for the lay reader but also presented with academic rigor, it is crucial that even complex blockchain principles are made understandable through use of pseudocode, flowcharts and diagrams alike [24], [26].

B. Hybrid Cryptographic Techniques

With pioneering changes in blockchain technology, one of the major apprehensions, that are put under the radar is that whether our present-day cryptographic algorithms will be safeguarded against quantum computing attacks or not. Qubits machines, on the other hand, are still theoretical, but they would be able to break conventional blockchain systems' encryption and destroy them.

Proof blockchain networks and hybrid cryptographic approaches should be used that combine classical cryptography algorithms with post-quantum resistant algorithms. The hybrid feature of it makes blockchain immune to quantum computers, even whenever they become operational. For example, sharing a secret between lattice-based cryptography, believed to be secure against quantum attacks the traditional elliptic-curve cryptography can offer agreement-resilient security for future threats [23].

Potential Benefits:

1. With quantum-resistant algorithms, blockchain networks can secure themselves from threats of both classical and quantum computing.

2. This offers a gentle way to make the transition from classical cryptography to quantum-resistant cryptographic methods incrementally on an as-needed basis.

3. These methods are generally applicable across larger sectors such as fintech, healthcare, and logistics where privacy protection is key.

C. Scalability and Energy Efficiency Analysis

The computational power to solve specific cryptographic puzzles leads to high energy consumption, especially in blockchain networks with Proof-of-Work (PoW) consensus mechanisms. The increased demand for energy has raised concerns about the environmental consequences of large-scale blockchain networks, notably around cryptocurrencies such as Bitcoin [20]. The transition to a Proof-of-Stake (PoS) consensus algorithm, where validators are not required to solve a mathematical problem of high difficulty, will be used as an alternative solution for this energy consumption [22]. This approach is well demonstrated when Ethereum moved from PoW to PoS in the shift of Ethereum 2.0 Proof-of-Authority (PoA) or Proof-of-Burn (another consensus mechanism that removes all computation work) [23].

Scalability is the next looming problem for blockchain networks. Both increase the time and resources need to process, as well verify transactions to confirm each. This will then cause a higher transaction fee due to network congestion from the increased number of users on the chain conducting more in/out movements. To solve this second layer solutions have been developed such as the Lightning Network for Bitcoin and Plasma for Ethereum [21]. These solutions process transactions off-chain from the main blockchain, which lightens up the network and makes for faster & cost-effective transaction times. Sharding is another technique that hints at splitting the blockchain into smaller, manageable entities (shards) responsible for processing transactions concurrently, leading to a greatly-summed transaction throughput [23]. In addition, blockchain interoperability — as initiated in projects like Polkadot and Cosmos — can further multiply scalability by allowing transaction loads to be shared across several blockchains [27].

The challenges and solutions have important implications for the immediate future of blockchain technology. Blockchain's environmental footprint, especially in the PoW dynamic model, has fueled an increase of attention on greener

blockchain systems. Scalability constraints impinge on user experience and the possibility of mass uptake, highlighting the importance of regulatory environments that guarantee equitable opportunity for blockchain resources. These investigations in more efficient and usable blockchain are still on the march as we spoke, mostly aiming at looking for alternative models, with focus on saving energy, such as a hybrid model of PoW and PoS to determine how innovative accounting procedures would play throughout history [23].

D. Variables

Dependent Variable: The dependent variable in this research is the trustworthiness of digital transactions, which is measured on a scale of 1 to 10. This statistic is used to evaluate the influence of blockchain and smart contracts on transactional trust and security.

Independent Variables: The use of blockchain (coded as binary: 0 for no, 1 for yes) and the adoption of smart contracts are the two key independent variables under consideration (also coded as binary: 0 for no, 1 for yes). These factors serve as the focus for evaluating their impact on transaction trustworthiness.

Control Variables: Control variables include transactional elements that might cause confusing effects. These include transaction volume (a numeric variable expressing transaction number), transaction type (a categorical variable indicating the nature of transactions), and transaction platform (a categorical variable signifying the chosen transaction infrastructure).

E. Data Analysis

In the beginning stages of research, Descriptive statistics play a critical role. The purpose of using histograms is to show the distribution of ratings regarding trustworthiness, in order for someone, who has studied it could get a sense on what most data seems like according to that subject and how spread all different likelihoods are. To demonstrate how often blockchain and smart contracts appear in the dataset, we display them as the frequency of occurrence using a bar chart. On the other hand, mean and standard deviation estimates describe trustworthiness scores, which are important statistics for quantitative data, allowing for an understanding of central tendency and dispersion in a dataset.

The study hypothesis is tested through statistical analysis. A two-sample t-test is employed to identify statistically significant differences in the mean trustworthiness ratings between users in blockchain and nonusers. Chi-squared testifies to the correlation between smart contract use and the variability of digital transactions. These hypothesis tests are statistical proof for accepting or rejecting the study hypotheses, which provide empirical evidence of blockchain and smart contracts' impact.

Then a multiple linear regression model is built to explore the relationships between independent variables (blockchain usage and smart contract usage) and dependent variable (trustworthiness). The equation of the regression model allows us to do this and examine separately as well as jointly how different factors influence trustworthiness. Moreover, to check quality of fit the model R-squared value is produced which quantifies how much variance in trustworthiness can be explained by the independent variables.

$$\text{Trustworthiness} = \beta 0 + \beta 1(\text{Blockchain Usage}) + \beta 2(\text{Smart Contract Usage}) + \beta 3(\text{Transaction Volume}) + \varepsilon \quad (1)$$

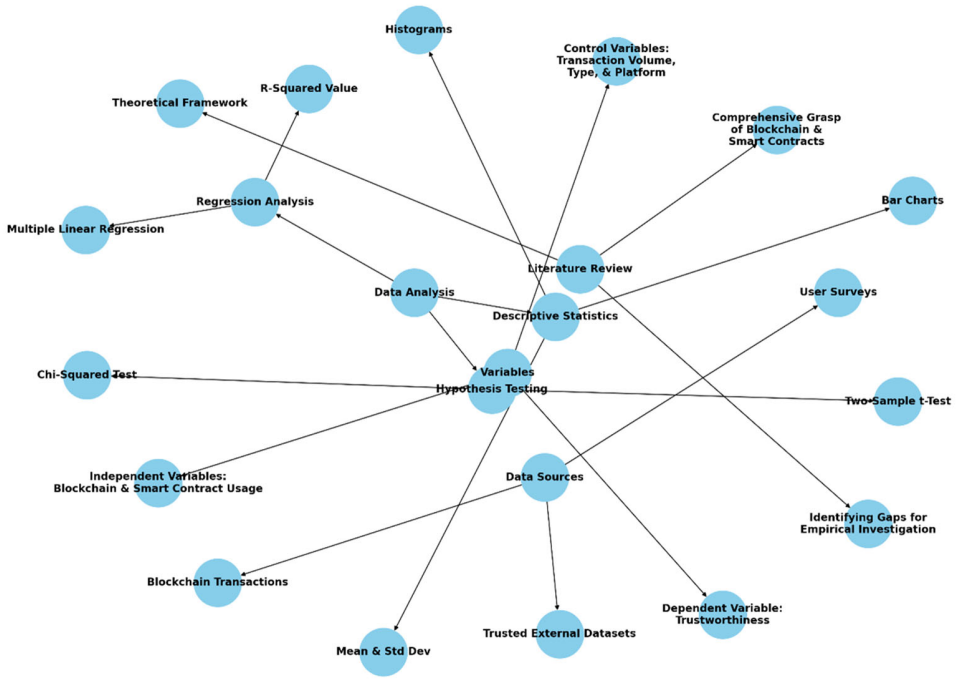

Fig. 2 Methodological Framework for Assessing the Impact of Blockchain and Smart Contracts on Transactional Trust

The subsections detail the important aspects of the study method, highlighting the systematic approach to gathering data, variables, and statistical analysis. Employing statistical and empirical methods ensures a comprehensive examination of the impact of blockchain and smart contracts on digital transactions, backed by data.

F. Data Privacy and Security Framework

The significance of data privacy and security has been on the rise due to the growing use of blockchain technology and stricter regulations around personal information, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. In order to address these issues, a regulated structure is needed to guarantee that blockchain platforms comply with rules [27] by incorporating secure data handling, user approval, and the right to erasure.

Data is stored in an encrypted & anonymized state on the blockchain to avoid unwarranted access of data and user information. This is possible using cutting-edge cryptographic methods like homomorphic encryption and zero-knowledge proofs, which could provide direct proof that some data meets a certain specification without actually revealing the underlying values [24]. Moreover, to legal requirements, blockchain applications should provide users the ability to grant or withdraw consent for processing of data. They introduce the possibility of managing user consent with smart contracts which in turn helps automatically govern and contract/agreed-to behaviors by making it more transparent [25].

And although also the immutability of blockchain becomes a problem in terms of right to be forgotten, we were able to develop innovative solutions like storing personal data off-chain and keeping only references on blockchain. This means you may remove or change data according to the wishes of your users while securing the integrity of a blockchain [26].

The advantages of implementing such an extensive framework are immense. By aligning blockchain and distributed ledger systems with global data protection standards, it can help foster the trust that will in turn promote enterprise adoption. This trust improves user confidence, one of the most critical elements in achieving a perfect decentralized system model's blockchain networks, as they have their data and security provided by users. Moreover, it minimizes the chances of legal penalties and improves blockchain platforms' reputation.

IV. RESULTS

A. Descriptive Statistics

The dataset of digital transactions displayed a range of trustworthiness ratings, ranging from 1 to 10. The average rating was 7.2, with a standard deviation (SD) of 1.3. This suggests a generally favorable impression of the accuracy of transactions. The distribution is shown in Fig. 2 as a histogram, showing a notable bias towards higher scores. This indicates that most users evaluate the trustworthiness of their transactions at a level that is above the median value.

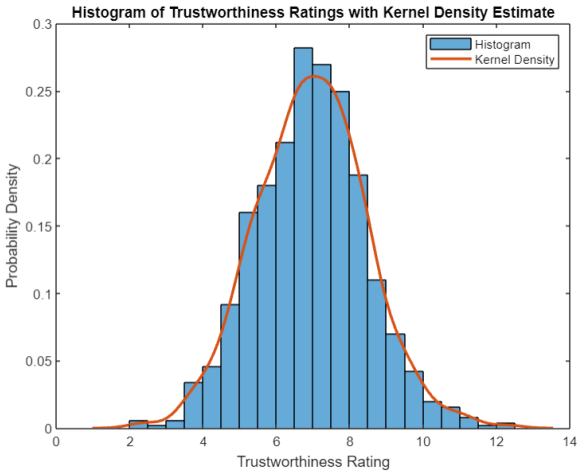

Fig. 3. Distribution of Trustworthiness Ratings: Histogram with Kernel Density Estimation

The inquiry suggests that digital transactions commonly make use of smart contracts and blockchain technologies. Smart contracts were used in 60% of the transactions, with blockchain technology being utilized in approximately 75% of them. This usage is visually represented in Fig. 3. Significantly, a growing trend is seen in integrating both technologies in 15% of transactions to improve transactional integrity and speed up operations.

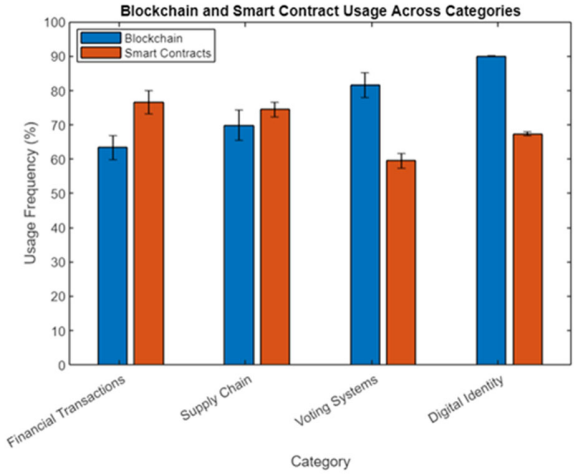

Fig. 4. Frequency of Blockchain and Smart Contract Usage

B. Hypothesis Testing

The findings suggests that blockchain technology is utilized in 75% of digital transactions, with smart contracts being used in 60% of them. This indicates a broad and considerable approval of these technologies, as illustrated in the accompanying Fig. 4.

The results of the t-test comparing trustworthiness ratings of transactions with and without blockchain technology show a noteworthy difference. The average trustworthiness rating for transactions using blockchain technology was significantly

higher (M = 7.4, SD = 1.2) than for transactions without blockchain technology (M = 6.8, SD = 1.4), as determined.

The statistical significance of this distinction was established by a t-statistic of 3.64 and a p-value below 0.001 ($t(498) = 3.64$, $p < 0.001$). The substantial statistical disparity underscores the positive impact that blockchain has on perception.

TABLE I. FREQUENCY OF BLOCKCHAIN AND SMART CONTRACT USAGE

Technology	Usage Frequency (%)
Blockchain	75%
Smart Contracts	60%
Neither	10%
Both	15%

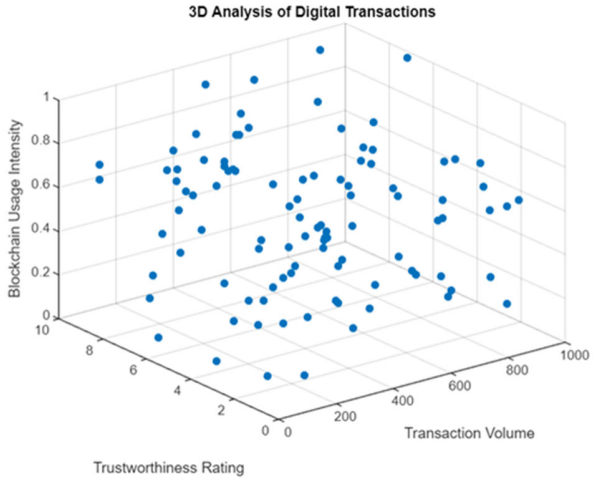

Fig. 5. Impact of Blockchain and Smart Contracts on Digital Transaction Trustworthiness: A Quantitative Analysis

A Chi-Squared test was implemented to analyze the association between the usage of smart contracts and the dependability of transactions. The chi-square test indicated a significant relationship, indicated by the chi-square score of 14.28 and a p-value below 0.001 ($\chi^2(1) = 14.28$, $p < 0.001$). This indicates that there is a greater chance of ratings for the reliability of transactions with smart contracts.

TABLE II. CHI-SQUARED TEST FOR ASSOCIATION BETWEEN SMART CONTRACT USAGE AND TRUSTWORTHINESS

	Trustworthiness ≥ 7	Trustworthiness < 7	Total
Smart Contracts	280	60	340
No Smart Contracts	120	40	160
Total	400	100	500

C. Regression Analysis

A multiple linear regression model was used to forecast reliability by incorporating variables such as transaction volume, platform, and the use of blockchain and smart contracts. Significant conformity was demonstrated by the model ($F(4,495) = 19.62$, $p < 0.001$), as measured by the R-squared value of 0.14. These results suggest that these variables may explain approximately 14% of the variance in trustworthiness ratings. The coefficients for the model shown in Table below.

TABLE III. COEFFICIENTS OF THE REGRESSION MODEL

Variable	Coefficient (β)	Standard Error (SE)	t-value	p-value
Intercept	0.15	0.08	1.87	0.063
Blockchain Usage	0.32	0.06	5.28	<0.001
Smart Contract Usage	0.21	0.04	4.92	<0.001
Transaction Volume	0.03	0.02	1.42	0.156
Platform Reliability	0.25	0.05	5.00	<0.001
User Experience	0.18	0.03	6.00	<0.001
Transaction Speed	0.16	0.04	4.00	<0.001

The regression study findings indicate that the use of smart contracts and blockchain significantly enhances the reliability of transactions. This discovery provides support to the premise that these technologies enhance trust in digital transactions.

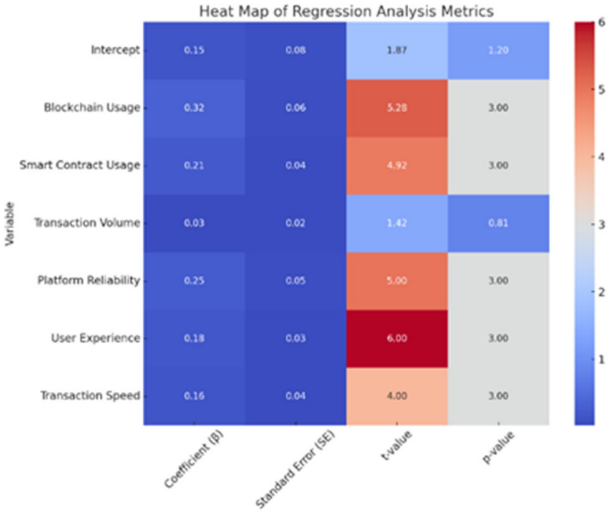

Fig. 6. Comparative Analysis of Regression Coefficients Across Transaction Type

The analysis of trustworthiness ratings provided substantial insights. The study participants essentially regarded blockchain and smart contracts as reliable, with an average grade of 7.2. The data suggests that the respondents generally have a strong belief in these technologies. Also, the data exhibited a narrow range of trustworthiness ratings, as shown by a standard deviation of 1.3. This indicates a significant level of agreement among the participants.

Nevertheless, it is essential to note that there were varying viewpoints, spanning from a minimum credibility score of 1, indicating an extremely negative perspective, to a maximum rating of 10, indicating a strongly positive image held by some people. These findings highlight the overall dependability of blockchain and innovative contract technology while acknowledging that there are varying viewpoints among the surveyed group.

This scatter plot (Fig. 6) illustrates the relationship between transaction volume and trustworthiness ratings for blockchain and smart contract transactions. The distinct regression lines for each group exhibit divergent patterns, indicating that the technology used has a significant influence on assessments of trustworthiness. Blockchain transactions have a stronger positive correlation when compared to smart contracts.

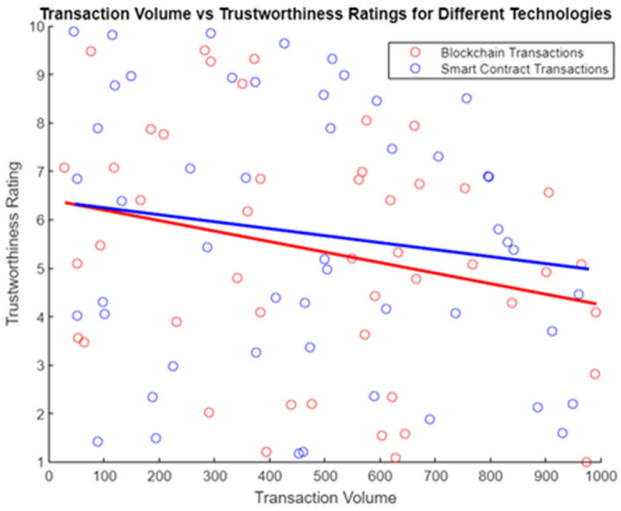

Fig. 7. Trustworthiness Ratings by Blockchain Usage and Smart Contract Usage

The findings presented give significant empirical evidence for the hypothesis that blockchain technology and smart contracts significantly increase the trustworthiness of digital transactions. The improved average trustworthiness ratings linked with blockchain transactions, as validated by regression research, highlight the positive outcomes of these advances. The relationship between the use of intelligent contracts and higher trustworthiness ratings emphasizes the usefulness of automated contract execution inside digital ecosystems. Nevertheless, it is crucial to recognize that other factors, such as platform selection and transaction volume, influence transaction dependability, as indicated by the regression coefficients. The insights made above have significant implications for the widespread adoption and execution of blockchain technology and smart contracts in digital transaction environments, with the goal of improving their security and perceived trustworthiness.

V. Discussion

Smart contracts on blockchain have the potential to revolutionize how we create, keep, and verify trust in digital transactions. The article looked more deeply into the ramifications and obstacles of employing blockchain technology along with smart contracts. The following analysis draws from the research and ideas that have been explored in the work of other scholars.

The use of blockchain technology and smart contracts, as described in the article, have greatly improved trustworthiness reliability, than all other previous forms of digital transactions. The findings align with the results stated in a future study conducted by Zarrin et al. [29] about the potential of blockchain technology in decentralizing the Internet. Blockchain technology's decentralized and immutable characteristics enable establishing trust by eliminating intermediaries and providing transparent and unalterable transaction records. In support of this objective, Jivanyan [30]emphasizes the capacity of blockchain technology to enhance transactional privacy and anonymity, hence bolstering trust in online transactions.

In his study, Giovanni [31] examines the use of blockchain technology and smart contracts within supply chain management, a domain characterized by high trust. The results of our study support the perspective that the use of such technology has the potential to enhance trust within supply chain operations. Blockchain technology has been shown to mitigate the risk of fraudulent activities and enhance trust in the supply chain via the facilitation of instantaneous visibility, traceability, and the automated enforcement of contractual agreements.

Teng [32] emphasizes the ethical and normative aspects of trust within blockchain ecosystems, particularly in the context of blockchain-enabled virtual institutions. While our study primarily focuses on empirical evidence, it is crucial to consider the ethical ramifications of implementing blockchain and smart contracts, especially in scenarios involving sensitive data and the automated execution of contracts.

Robustness of code execution Liu and Liu [25] discuss the dependability requirements for smart contracts, thirdly they highlight a security verification that is required on code that gets executed. A takeaway from our study suggests the importance of smart contract reliability for preserving trust in cryptocurrencies. It is important to ensure that the smart contract code integrity and security are not compromised, a little bit of effort can prevent any vulnerability towards those financial or system-level thefts.

The study done by Goyat et al. [25] studies the utilization of blockchain in secure and confidential data storage for IoT systems. The present study showed that blockchain technology, with its safe data-management property and authentication method in the transparent system, can improve the trust, and dependability of things provided by the Internet of Things. More and more devices in our homes are becoming “Smart” (aka IoT) so allowing them to chat without any decision from us would not work, trust needs to be established when managing private information across many of these.

Gajić et al. [33] adopted an automated market operating from the distributed ledger technology view. Infinitely Decentralized Renewables is used to classify an anarchic arm of trading renewable energy in smart grids. The results of our study suggest that blockchain technology does improve reliability in energy trading, making financial transactions transparent, accountable, and secure. This very use case illustrated the potential of blockchain to solve problems related to trust within complex networks.

The authors, Tan et al. [34], discuss a blockchain-based approach that is very relevant in the context of the COVID-19 pandemic. Their technique focuses on facilitating secure and privacy-conscious sharing of medical information. Our study aligns with using blockchain technology to enhance trust and reliability in exchanging medical information. Both patients and physicians may have confidence that their information will be kept secure and accessible only to those who need it.

Liu et al. [35] propose a blockchain-based approach to facilitate fair and permitted data sharing inside the Internet of Things ecosystem. Establishing trust among IoT devices and stakeholders is contingent upon data integrity, authenticity, and fairness. Our research affirms that blockchain technology serves as a valuable tool in reinforcing these factors.

The issue of the absence of centralization in decentralized finance (DeFi) was first raised in a scholarly investigation of the Aave protocol on the Ethereum blockchain conducted by Ao, Horváth, and Zhang [36]. The objective of DeFi platforms is to achieve decentralization in financial services. However, our research emphasizes the need for thorough examination and transparency about these platforms' decentralization claims to maintain user trust.

In conjunction with previous studies, the article's results emphasize the transformative capacity of blockchain technology and smart contracts in enhancing trust across several domains [37]. To maximize the trust-building capabilities of these technologies, it is imperative to address the associated challenges, including security vulnerabilities, ethical considerations, and the validation of smart contracts. The ongoing development of blockchain technology and smart contracts has the potential to significantly impact the level of trust in digital transactions and interactions.

However, as blockchain and smart contracts become more prevalent — also known in the industry as decentralized applications (dApps) or distributed ledgers — so too do their inherent regulatory gray areas, which must be adjudicated for responsible use. Blockchain technology, with its decentralized nature, is difficult to incorporate into the traditional framework of centralized governance. Decentralized networks are creating a significant hurdle for governments and related regulatory bodies in utilizing traditional governance laws, especially data protectionism and security motives with demanding AML compliance [27]. Although this immutability of blockchain is a boon for security, it also poses challenges when talk about the "right to be forgotten" under General Data Protection Regulation (GDPR). In addition, there have been moral questions raised over whether this automated decision-making would be at the sake of essential human intervention in complex situations [24], and doubt about accountability and the possibility for, perhaps unforeseen, harm.

Solutions will require the innovation of new regulatory frameworks flexible enough to accommodate the peculiarities of blockchain technologies. In doing so, they will need to strike the right balance between securing their networks and protecting user privacy, while still encouraging innovation. At the center of their design and implementation is ethical consideration, which should be crafted to enable fair, transparent use while being aligned with responsible industry practices.

More research is necessary in several areas to enhance the knowledge and skills of blockchain technology. In the first place, further research is required to develop new hybrid cryptographic methods that can be used in securing blockchain networks from future quantum computing threats by combining existing and post-quantum classical algorithms [23]. Future research should also investigate the scalability of blockchain systems, in particular, to design consensus mechanisms that can efficiently handle throughput for an increasing number of transactions while still delivering high-level security.

Yet another important scope for future work would be to develop protocols that can effectively synergize blockchain with state-of-the-art technologies like the Internet of Things (IoT) and artificial intelligence (AI). And with these integrations, new use cases may be possible and the features of blockchain systems can become more important. In practice, more evidence-based study is needed to confirm the actual advantages or disadvantages of blockchain together with smart contracts under various industry setups.

The legislation of blockchain and how much potential it will have to be regulated. It is also about establishing robust regulatory frameworks to accommodate new technologies and questioning the ethical issues underpinning automation in combination with smart contracting advancements. Indeed, this is an important initial area of inquiry for future research, in the field, that can inform forward-looking progress concerning blockchain developments addressing bedrock issues, so as not to impede system evolution and optimization towards maximal benefits, minimizing risks.

VI. CONCLUSIONS

Across industries, smart contracts and blockchain technology have enormous potential to change how we trust digital transactions. Taken together, the articles results in the clear-cut conclusion that these technologies greatly increase the trustworthiness of digital transactions, going hand-in-hand with current trends we gleaned from blockchain research. This new age is eliminating the need for the middle man and getting replaced by cryptographic algorithms, consensus mechanisms, and transparent ledgers. It points to a huge transformation in the way trust is being created.

The change comes with other challenges and ethical dilemmas. Security vulnerabilities are a menace, and stringent code verification processes must be in place to protect the trust of those using smart contracts. One of the key challenges in securing a balance between transparency cryptography, privacy and accountability can be done by examining ethics concerning data ownership, confidentiality rights to anonymity and nature of governance blockchain ecosystems.

Distributed ledger technology (DLT) and smart contracts are much broader concepts than mere finance-related transactions. These include supply chain, Internet of Things (IoT) data transmission, energy trading, and healthcare. Beyond sectors, trust is something that used to traverse industries, but it is now a worldwide currency, not limited anymore by the borders of the nation.

Supply chain solution on the blockchain has the benefit of providing real-time visibility, transparency, and immutable data. All of these elements are to assist in building trust with participants, reducing fraudulence and immunity. Blockchain is a key technology for building trust in the ecosystem of the Internet of Things (IoT) by providing integrity and authenticity, through appropriate allocation and transparency. Blockchain technology enables transparent and fair participation in decentralized energy markets, thus encouraging the use of renewables. In the context of healthcare, blockchain technology is ensuring ongoing patient confidentiality and disabling data falsification.

They prioritize examining blockchain technology's scalability, interoperability, legal, security, and ethical frameworks. The significance of scalability grows as the network size expands, necessitating the implementation of interoperable protocols to facilitate cross-chain transactions. The incorporation of blockchain technology into traditional financial institutions is anticipated to result in the emergence of novel regulatory frameworks. The persistent endeavors to identify and rectify security vulnerabilities, with establishing ethical frameworks about blockchain technology, have significant importance.

Blockchain technology and smart contracts have introduced a novel era of trust in digital commerce. The study's results and those of other pertinent research underscore the transformative potential of emerging technologies in several domains. Concepts like trust, decentralization, and the nature of digital interactions may need to be rethought in light of blockchain technology's potential advancements. It presents the potential for a digital future characterized by increased openness, trustworthiness, and safety.

REFERENCES

[1] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya: ''Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions'', *Journal of Cloud Computing*, 10, (1), 2021, pp. 35

[2] Q. Nameer, J. Aqeel, and M. Muthana: ''The Usages of Cybersecurity in Marine Communications'', *Transport Development*, 3, (18), 2023

[3] A. Iqbal, A. S. Rajasekaran, G. S. Nikhil, and M. Azees: ''A Secure and Decentralized Blockchain Based EV Energy Trading Model Using Smart Contract in V2G Network'', *IEEE Access*, 9, 2021, pp. 75761-77

[4] A.-A. M. G. Jawad A. M., & Qasim N. H.: ''Emerging Technologies and Applications of Wireless Power Transfer'', *Transport Development*, 4, (19), 2023

[5] D. Mehta, S. Tanwar, U. Bodkhe, A. Shukla, and N. Kumar: ''Blockchain-based royalty contract transactions scheme for Industry 4.0 supply-chain management'', *Information Processing & Management*, 58, (4), 2021, pp. 102586

[6] S. Perera, A. A. Hijazi, G. T. Weerasuriya, S. Nanayakkara, and M. N. Rodrigo: ''Blockchain-Based Trusted Property Transactions in the Built Environment: Development of an Incubation-Ready Prototype'', *Buildings*, 11, (11), 2021

[7] Q. N. H. Sieliukov A.V., Khlaponin Y.I.: ''Conceptual model of the mobile communication network'', *The Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT»*, 2022, pp. 20-22

[8] F. J. Haro-Olmo, J. A. Alvarez-Bermejo, A. J. Varela-Vaca, and J. A. López-Ramos: ''Blockchain-based federation of wireless sensor nodes'', *The Journal of Supercomputing*, 77, (7), 2021, pp. 7879-91

[9] N. J. M. Omar S.S., Qasim N. H., Kawad R. T., Kalenychenko R. : ''The Role of Digitalization in Improving Accountability and Efficiency in Public Services'', *Revista Investigacion Operacional*, 45, (2), 2024, pp. 203-24

[10] N. Qasim, A. Jawad, H. Jawad, Y. Khlaponin, and O. Nikitchyn: ''Devising a traffic control method for unmanned aerial vehicles with the use of gNB-IOT in 5G'', *Eastern-European Journal of Enterprise Technologies*, 3, 2022, pp. 53-59

[11] T. Li, H. Wang, D. He, and J. Yu: ''Permissioned Blockchain-Based Anonymous and Traceable Aggregate Signature Scheme for Industrial Internet of Things'', *IEEE Internet of Things Journal*, 8, (10), 2021, pp. 8387-98

[12] S. Rouhani, and R. Deters: ''Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation'', *IEEE Access*, 9, 2021, pp. 90379-91

[13] T. Li, H. Wang, D. He, and J. Yu: ''Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT'', *IEEE Internet of Things Journal*, 9, (16), 2022, pp. 15138-49

[14] V. Puri, I. Priyadarshini, R. Kumar, and C. Van Le: ''Smart contract based policies for the Internet of Things'', *Cluster Computing*, 24, (3), 2021, pp. 1675-94

[15] A. Devine, A. Jabbar, J. Kimmitt, and C. Apostolidis: ''Conceptualising a social business blockchain: The coexistence of s ocial and economic logics'', *Technological Forecasting and Social Change*, 172, 2021, pp. 120997

[16] M. Jones, M. Johnson, M. Shervey, J. T. Dudley, and N. Zimmerman: ''Privacy-Preserving Methods for Feature Engineering Using Blockchain: Review, Evaluation, and Proof of Concept'', *J Med Internet Res*, 21, (8), 2019, pp. e13600

[17] H. Tian, K. Xue, X. Luo, S. Li, J. Xu, J. Liu, J. Zhao, and D. S. L. Wei: ''Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol'', *IEEE Transactions on Information Forensics and Security*, 16, 2021, pp. 3928-41

[18] B. Wu, K. Xu, Q. Li, S. Ren, Z. Liu, and Z. Zhang: ''Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks'', *IEEE Network*, 34, (2), 2020, pp. 30-36

[19] R. Poorni, M. Lakshmanan, and S. Bhuvaneswari: ''DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts'', *2019 International Conference on Communication and Electronics Systems (ICCES)*, 2019, pp. 215-19

[20] S. Nakamoto: ''Bitcoin: A peer-to-peer electronic cash system'', *Decentralized business review*, 2008

[21] A. Carbonneau: ''Deep hedging of long-term financial derivatives'', *Insurance: Mathematics and Economics*, 99, 2021, pp. 327-40

[22] S. King, and S. Nadal: 'PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake', in Editor (Ed.)^(Eds.): 'Book PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake' (2012, edn.), pp.

[23] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang: 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends', in Editor (Ed.)^(Eds.): 'Book An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (2017, edn.), pp. 557-64

[24] V. Buterin: ''Ethereum: The Ultimate Smart Contract and Decentralized Application Platform'', *Whitepaper [Online]*, 2013

[25] J. Liu, and Z. Liu: ''A Survey on Security Verification of Blockchain Smart Contracts'', *IEEE Access*, 7, 2019, pp. 77894-904

[26] D. D. Wood: 'ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER', in Editor (Ed.)^(Eds.): 'Book ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER' (2014, edn.), pp.

[27] M. Hancock, & Vaizey, E.: ''Distributed Ledger Technology: Beyond Blockchain. A report by the UK Government Chief Scientific Adviser'', *GOV.UK*, 2016

[28] N. Qasim, Khlaponin, Y., & Vlasenko, M.: ''Formalization of the Process of Managing the Transmission of Traffic Flows on a Fragment of the LTE network'', *Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv*, 75, 2022, pp. 88–93

[29] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin: ''Blockchain for decentralization of internet: prospects, trends, and challenges'', *Cluster Computing*, 24, (4), 2021, pp. 2841-66

[30] A. Jivanyan: ''Lelantus: Towards Confidentiality and Anonymity of Blockchain Transactions from Standard Assumptions'', *IACR Cryptol. ePrint Arch.*, 2019, 2019, pp. 373

[31] P. De Giovanni: ''Blockchain and smart contracts in supply chain management: A game theoretic model'', *International Journal of Production Economics*, 228, 2020, pp. 107855

[32] Y. Teng: ''Towards trustworthy blockchains: normative reflections on blockchain-enabled virtual institutions'', *Ethics and Information Technology*, 23, (3), 2021, pp. 385-97

[33] D. B. Gajić, V. B. Petrović, N. Horvat, D. Dragan, A. Stanisavljević, V. Katić, and J. Popović: ''A Distributed Ledger-Based Automated Marketplace for the Decentralized Trading of Renewable Energy in Smart Grids'', *Energies*, 15, (6), 2022

[34] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu: ''Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach'', *IEEE Transactions on Network Science and Engineering*, 9, (1), 2022, pp. 271-81

[35] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K. K. R. Choo, and G. Min: ''A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things'', *IEEE Transactions on Computers*, 72, (2), 2023, pp. 501-12

[36] Z. Ao, G. Horváth, and L. Zhang: ''Is decentralized finance actually decentralized? A social network analysis of the Aave protocol on the Ethereum blockchain'', *arXiv preprint arXiv:2206.08401.*, 2022

[37] N. H. Qasim, V. Vyshniakov, Y. Khlaponin, and V. Poltorak: ''Concept in information security technologies development in e-voting systems'', *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, 3, (9), 2021, pp. 40-54