Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

Review

Smart Contracts Security Application and Challenges: A Review

Fadele Ayotunde Alaba[1*], **Hakeem Adewale Sulaimon**[1], **Madu Ifeyinwa Marisa**[2], **Owamoyo Najeem**[1]

[1]Department of Computer Science, Federal College of Education, Zaria, Kaduna State, Nigeria
[2]Industrial and computational Mathematics, Morgan State University, Baltimore Maryland, the United States
Email: ayotundefadele@yahoo.com

Received: 25 June 2023; **Revised:** 11 August 2023; **Accepted:** 23 August 2023

Abstract: There has been a rise in the demand for blockchain-based smart contract development platforms and language implementations. On the other hand, smart contracts and blockchain applications are generated using non-standard software life cycles, which means that, for example, distributed applications are rarely updated, or bugs are fully addressed by releasing a newer version, leading to security flaws and challenges for users to adopt the technology. Smart contracts have gained significant attention due to their potential to automate and secure various transactions in diverse domains. However, the increasing adoption of smart contracts has also raised concerns about security vulnerabilities and potential risks. In this paper, an overview of smart contracts is discussed in detail. It further distinguished and compared smart contracts security with conventional security regarding security, privacy, communication channel, etc. Different platforms for smart contracts, such as Bitcoin, Ethereum, Counterparty, Stellar, Monax, and Lisk, are also discussed in this paper. Some proposed techniques are used in different areas for handling security threats in smart contracts. In addition, a taxonomy of the smart contracts security application was proposed, which attempts to solve some of the flaws and inadequacies in smart contracts. The study also provides a comprehensive smart contracts security scenario with different techniques. Lastly, the possible attacks posed by threats and vulnerabilities of the smart contracts are provided. The security threats and vulnerabilities addressed in this study are unique to smart contracts.

***Keywords*:** blockchain, smart contract, security, bitcoin, ethereum, counterparty, stellar, monax, lisk

1. Introduction

The blockchain has been recognized as a decentralized system for over ten years, wherein a distributed database documents all transactions within a peer-to-peer network. The approach referred to is a form of distributed computing that effectively resolves the trust issue in a centralized party, as noted by [1]. The collaborative efforts of numerous nodes within a blockchain network enable the safeguarding and upkeep of communal transaction records in a decentralized manner without reliance on any authoritative entity [2]. According to [3], blockchain is a novel technology that can potentially be a highly transformative innovation, following the footsteps of the Internet and the TCP/IP protocol. Distributed Ledger Technology (DLT) is a commonly used term that can execute secure transactions due to its foundation on the distributed digital application of transaction ledgers, as noted by [4]. Blockchain technology is distinguished from contemporary information and transaction systems by four primary attributes: decentralization,

DOI: https://doi.org/10.37256/ccds.5120243271

stability, audibility, and smart execution [5]. These characteristics enable the Blockchain to function as a properly distributed system, resist any changes, allow for adequate scrutiny of financial transactions, and facilitate intelligent execution. According to [5], a blockchain is a decentralized database that assembles encrypted data blocks and subsequently links them to establish a unified and authoritative source of information.

Digital assets are distributed instead of duplicated or transmitted, providing an accurate asset count. The decentralized nature of the support allows for real-time public access and transparency. According to [6], utilizing a transparent change ledger ensures preserving the document's integrity, instilling confidence in the asset. Blockchain technology's incorporation of security measures and government ledger renders it a highly effective solution for businesses of varying scales. The Blockchain has exhibited a notable surge in interest since late 2015, primarily due to its robustness and security features. According to [7], implementing blockchain technology offers a decentralized and reliable platform that eliminates the need for a single centralized authority to regulate business applications. As per [8], it is possible to utilize blockchain technologies as an application framework to establish the fundamental trust infrastructure of a decentralized system. According to [5], the global accessibility of public blockchain systems renders them attractive to businesses and communities, thereby prompting a rapid recognition of the potential of blockchain technology. Furthermore, [9] has identified several instances of blockchains, including but not limited to Bitcoin, Ethereum, Counterparty, Stellar, Monax, and Lisk.

Implementing blockchain technology has proven advantageous for the financial sector as it offers transparent digital payment mechanisms and has introduced a transformative approach by eliminating intermediaries such as banks or government institutions [10]. Although initially perceived as a significant advancement in the financial sector, blockchain technology can generate vast economic, social, and environmental implications [11]. [12] argue that a notable outcome of this phenomenon is the mitigation of financial deficiencies. According to [13], implementing blockchain technologies can simplify and enhance the safety of processes by removing obstacles in hierarchical systems, such as intermediary or third-party entities. Furthermore, this technology is poised to avoid complexity by promoting effective communication and interaction among pertinent stakeholders.

Moreover, blockchain technology is expected to enhance the supply chain network's transparency, as [14] noted. The innovation mentioned above presents novel prospects for improved traceability and regulation of commodities, as it enables comprehensive tracking of a product's complete history with greater precision [15]. The notion of sustainability is also introduced in this context. As a result, incorporating sustainability into the supply chain concept can be more pragmatic, given the importance of transparency in environmental sustainability, as highlighted by [16]. According to [10], this technology offers various opportunities for quality control of individuals, commodities, and transportation, facilitating a more feasible and lucid implementation of a sustainable supply chain. According to [15], implementing traceability measures can increase awareness among individuals and communities regarding supply chain processes, thereby exposing any participant to questionable practices within the supply chain.

The rapid proliferation of blockchain solutions presents a challenge for software-producing corporations in selecting an appropriate blockchain application due to the lack of a comprehensive evaluation methodology for existing options. Consequently, the acquisition, arrangement, preservation, and convenient retrieval of data about blockchain systems is imperative.

Many blockchain applications have been developed in contemporary times, encompassing public, consortium, and proprietary blockchains, which can be effectively employed in diverse contexts [17]. Implementing a secure supply chain system can enhance security and minimize the risk of data breaches by limiting the participation of intermediaries, whose operations are frequently susceptible to malfunctions, exploitation, and cyber attacks [18]. The technology has garnered significant attention and research in the domains of currency and finance. However, its potential applications extend beyond economics and markets, encompassing areas such as government, health, and literature, as posited by [19]. Recently, many blockchain technology systems have surfaced and have found applications in diverse business platforms [20]. Blockchain technology networks are present in various media, such as Hyperledger and Ethereum, as noted by [8]. The fundamental differentiation between Hyperledger and Ethereum pertains to their respective objectives. Hyperledger is a project that offers diverse blockchain solutions for facilitating collaboration among distributors in the production of blockchains. In contrast, Ethereum is a blockchain network that is open to the public and enables the execution and deployment of decentralized programs through smart contracts [21].

Scholars have devised various methodologies to address security concerns in blockchain technology on smart contracts, employing diverse multi-criteria analyses. One of the works in this area is the proposal by [8] for a multi-criterion analysis framework that centers on reluctant fuzzy blockchain technology sets. The framework under consideration has been implemented in the medicine/drug and jewelry domains. Using a framework can benefit researchers and managers who aspire to operate within this domain. [22] conducted a multidimensional analysis of adversaries concerning Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). The study aims to facilitate the advancement of blockchain research and expansion. This may also enable individuals in enhancing their comprehension of privacy entitlements within this realm. In their recent study, [17] proposed a novel approach involving introducing a credit value system. This system utilizes the Multiple-Attribute Decision Making (MADM) to convert user credit data into credit values, which are then stored alongside transaction information using blockchain technology. Additionally, the authors propose a credit value reward mechanism that addresses the issue of anonymous zone [22] construction through a double-part game between two parties.

The remainder of this paper is organized as follows. Section 2 presents an overview of smart contracts and the difference between smart contracts' security and conventional security. Section 3 provides smart contract platforms. Section 4 discusses the smart contract techniques for handling security threats. Section 5 describes the taxonomy of the smart contracts security application. Section 6 provides smart contracts security scenario. Section 7 discusses possible attacks posed by threats and vulnerabilities of smart contracts. Section 8 provides suggestions for future directions. Finally, Section 9 concludes the paper.

2. Overview of smart contracts

The application of smart contracts for transactional purposes in Bitcoin has established it as the most prevalent illustration of blockchain technology. In contrast, smart contracts facilitate reliable transactions and agreements among disparate, decentralized entities without requiring a central governing body, legal framework, or external regulatory mechanism [11]. According to [23], a smart contract is a type of contract capable of self-execution, wherein the conditions of the agreement between the buyer and seller are explicitly encoded into computer code. The blockchain network is responsible for distributing and decentralizing the code and arrangements. According to [24], the code assumes responsibility for the execution process, and transfers are traceable and irreversible.

According to [23], a smart contract is a computer protocol that employs blockchain technology as a virtual machine (VM) for execution. Although the smart contract has the potential to be utilized across diverse industries, including finance and engineering, its implementation poses a significant challenge [25]. The selection of the virtual machine utilized, such as Ethereum and Corda, is contingent upon the specific implementation domain for the smart contract, as noted by [26]. The execution of the smart contract is executed to insert an access policy into the Blockchain, as posited by [27]. According to [28], individual virtual machines require distinct programming languages and blockchain networks to function, offering unique benefits for each virtual machine. The utilization of an appropriate virtual machine can significantly enhance the efficiency of smart contract execution, resulting in a reduction in transaction time. Hence, it is imperative to establish the smart contract's fundamental standards to ensure its security. However, the salient criteria that are emphasized may differ across various application domains.

A smart contract is a contractual agreement that involves multiple parties. [29] states that the system employs predetermined protocols for data storage, input processing, and outcome dissemination. An instance of a smart contract may incorporate a datatype method that enables the formation of smart contracts. The act of initiating the generation and implementation of a smart contract can be achieved by employing a transaction whereby the sender assumes the role of the smart contract proprietor. This process facilitates the deployment of a fresh, smart contract on the blockchain. Implementing a self-destruct mechanism is an example of a function that can be specified within a smart contract. Typically, the ability to execute the function that destroys the contract is limited to the operator of the smart contract.

Furthermore, it should be noted that the fundamental standards for various applications, including but not limited to recordkeeping, client screening, data management, security, privacy, transaction, and trade processing, exhibit distinct variations. Furthermore, technological advancements According to [30], blockchain technology can supersede conventional contracts by incorporating commitments made among various parties. Additionally, it surpasses traditional contracts by automating the implementation of agreements in a decentralized setting, where conditions are met through smart contracts. According to [31], hosting a smart contract on the blockchain involves initiating a transaction to the blockchain network to call the constructor function. Subsequently, the constructor function is executed, and the final code of the smart contract is deployed on the network. The developer is provided with the returned parameters, such as the contract address, after successful implementation of the smart contract. Subsequently, users can execute any accessible function of the smart contract by submitting a message. Figure 1 illustrates the smart contracts landscape.

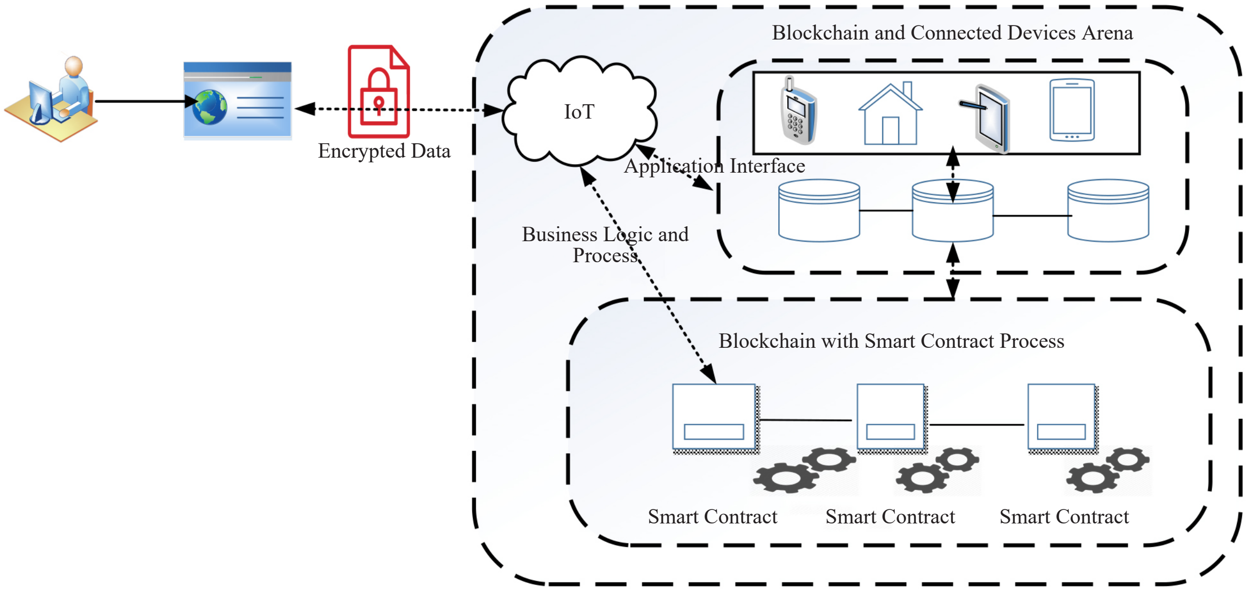
Blockchain and Connected Devices Arena
IoT
Encrypted Data
Application Interface
Business Logic and Process
Blockchain with Smart Contract Process
Smart Contract
Smart Contract
Smart Contract

Figure 1. Landscape of Smart Contracts

Each smart contract can incorporate declarations of the following types of data.

- Variables of status: entries that are held in a contract consistently.
- Functions: executable code units within a contract.
- Function modifiers: These are used to expand functionality and functions straightforwardly and clearly.
- Events: functionality for communication with Ethereum Virtual Machine (EVM) logging tools for smart contract code debugging or alarms.
- Structures: These are customizable data types that may combine several variables.
- Enumerations: Enumerations can be used to build custom data types that reflect a limited number of status options.

In summary, an Illustration of the smart contract is shown in Algorithm 1.

Algorithm 1: Smart Contracts Illustration Sample

```
program contract;
contract SimpleStorage {
unit storedData;
function set(unit x) public {
storedData = x;
      }
function get() public view returns (uint) {
return storedData;
      }
}
```

2.1 *Smart contracts security versus conventional security*

In terms of security and privacy, the Internet of Things (IoT) and traditional wireless networks differ in several important ways. The smart contracts are built on Low Power and Lossy Networks (LLNs), while others feature highly dynamic topologies dependent on the application [32]. Resilience, storage, and computational power are all constraints for LLNs [33]. These characteristics are not taken into account when using the conventional Internet. Due to node impersonation, LLNs suffer significant data losses. As a result, the security characteristics and needs of smart contracts and traditional network security are distinct [34-35]. Smart security contract deployments are unusual compared to conventional security deployments; for example, a "smart contract" is a part of computer code connected to a database and executes on every node in a blockchain network. Similarly, a blockchain and a centralized database may be used to compare a smart contract with a code on the server [36]. There is no difference between a blockchain and a centralized database in terms of the sorts of data that may be maintained. The primary differentiating feature of blockchain technology is what is known as "decentralization". They do not require a central administrator. Decentralization is an appealing concept in and of itself. That is, smart contracts are spread across several nodes on a blockchain and cannot be altered indiscriminately. Every data is run individually by each node, and the results are automatically cross-checked. As a result, no one can defraud [37]. The fact that every node has a complete view of the data means that secrecy is compromised. Smart contracts execute on all nodes, therefore they operate slower than code operating on a server.

Smart contracts may also be used to automate the online execution of certain clauses in a legal contract, such as "if A happens, do B." A smart contract can only communicate with the information on a blockchain, therefore there's a catch. It is thus impossible for a smart contract to withdraw money in digital currencies unless central banks issue their monetary policies on a distributed ledger (blockchain). A legal contract can also include a smart contract via reference [38]. Parties to a legal contract in human language may include a provision that links to a smart contract that says "we agree to abide by the outcomes of the code" [39]. In addition, sensor nodes at the Smart Contracts perception layer have limited processing capability, making wavelength-hopped communication and public-key encryption to protect Smart Contracts devices unfeasibly. Smart Contracts employ lightweight encryption technology, which comprises a lightweight cryptographic method. The network layer of the Smart Contracts network contains security problems such as man-in-the-middle and counterfeit attacks. Both attacks can steal information from and deliver it to network nodes that are interacting with one another [38]. To eliminate illegal nodes, identity authentication and data secrecy methods are employed. Data sharing is the key functionality at the application layer. Data encryption and exposure of data are among the security issues that arise as a result of data sharing [8]. Authorization, strong authentication, and preservation of user privacy over diverse networks are among the security needs for the application layer.

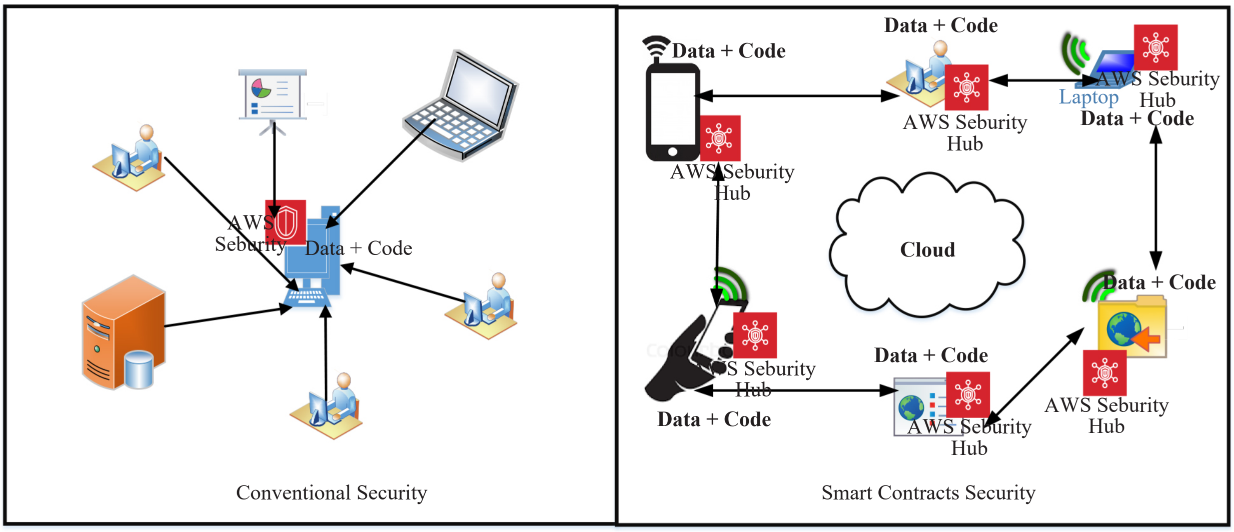

Figure 2. Conventional Network Security vs. Smart Contracts Security

Moreover, the communication channels in the two networks are different from one another. Every layer in the network has its protocol for communicating with the other layers. IPv6 is utilized via low-power wireless personal area networks in the Smart Contracts perception/physical layer, whilst wireless fidelity is employed in the physical layer of traditional networks. This is because the Smart Contracts network layer employs Datagram Transport Layer Security (DTLS) instead of Transmission Control Protocol (TCP). For communication, Smart Contracts employ Constrained Application protocols (CoAP), while traditional networks use Hypertext Transport protocols (HTTP) [19]. In addition, a smart contract can reduce controversies in certain aspects by evading ambiguity in human languages. It can also prevent performance defaults because a computer always operates as intended. A centralized server's code also operates as designed and clearly defines its programming language. However, the administrator cannot control it since no one can modify a smart contract or its execution outcomes [40].

To summarize, the conventional security architecture is developed with users in mind and is inappropriate for machine-to-machine communication. Although the security challenges in both networks are similar, various approaches and techniques are utilized to deal with every network security issue [41]. Figure 2 illustrates the difference between smart contracts and conventional security.

3. Smart contracts platforms

This section examines several platforms for smart contracts. The previous few years have seen an explosion of alternative platforms to Bitcoin and Ethereum, many of which integrate cryptocurrencies or smart contracts. As illustrated in Figure 3, Bitcoin, Ethereum, Counterparty, Stellar, Monax, and Lisk [42], are six examples of smart contracts platforms that will be discussed in this section.

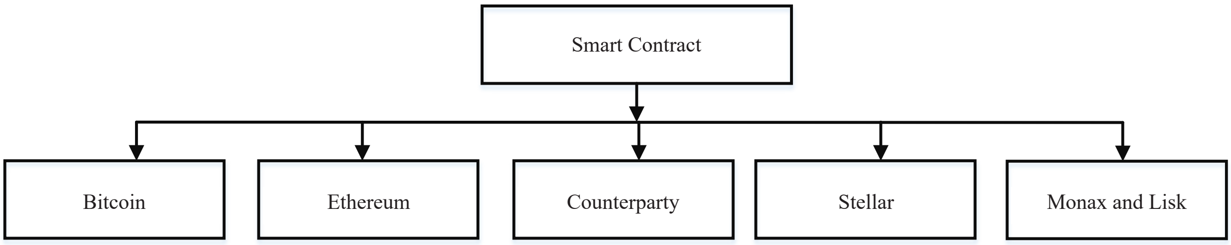

Figure 3. Smart Contracts Platforms

Bitcoin (BTC): The inception of Bitcoin, the initial decentralized digital currency, was attributed to an enigmatic entity or collective known as Satoshi Nakamoto [43]. According to [42], the BTC serves as a means of transmitting digital currency. The initial creation of blockchain technology was attributed to this particular system, which presently boasts the greatest cumulative worth. The technological system relies on a blockchain-based platform to document the complete series of financial transactions. Bitcoin nodes utilize a smart contract that relies on a moderately challenging "proof-of-work" puzzle to ascertain how to incorporate a fresh block of transactions into the blockchain. The nodes engage in a competitive process to generate the subsequent block within the blockchain. According to [44], a reward in BTC is granted to the initial node that successfully resolves the issue. Maintaining data integrity is a crucial characteristic of Bitcoin, enabling its utilization beyond the scope of mere monetary transactions [45].

The advent of smart contracts can be attributed to the transparency of its underlying blockchain technology and the formulation of corresponding protocols for their execution. The BTC network provides access to a non-Turing complete scripting language that enables users to define the conditions under which transactions can be withdrawn. The scripting language is notably limited, featuring fundamental arithmetic, logical, and cryptographic operations, such as hashing and digital signature verification. However, BTC's expressiveness has been constrained because only a small fraction of its nodes are equipped to process transactions that require more than just signature verification [46].

Ethereum (ETH): Ethereum is an open-source platform based on blockchain technology that enables the creation of applications by utilizing smart contracts. The decentralized architecture of the Blockchain network guarantees the safety and integrity of data storage, impervious to external interference. Ethereum ranks second to Bitcoin in market capitalization. Similar to Bitcoin, this particular cryptocurrency depends on a publicly accessible blockchain and employs an identical consensus mechanism. According to [42], the currency utilized by Ethereum is referred to as ETH. Smart contracts are scripted in a bytecode language that operates on a stack-based architecture instead of the Turing-complete language employed by Bitcoin.

Furthermore, several high-level programming languages exist, with Solidity being the most notable, that compile into bytecode. By transmitting transactions to the blockchain, individuals can generate contracts and execute their corresponding functions, with the network serving to authenticate their outcomes. According to [34], both clients and contracts can store funds and facilitate the transfer of Ethereum to other contracts or users. The Blockchain network provides security due to its consensus method and all nodes maintaining the data, as [47] noted. According to the transcription, to modify or eliminate information stored within a network, it is necessary to alter a majority of the nodes in the network, specifically 51%.

Moreover, the Ethereum network was specifically created to thwart potential attackers from overwhelming the system with excessive traffic. Under this system, every transaction is liable to incur a transaction fee. Fuel prices should be at a low level during the time of the transaction for consumers. The Solidity programming language, created by Ethereum specifically for implementation on the Ethereum network, is utilized for composing smart contracts related to cryptocurrency [14]. These instructions are interpreted by the Ethereum virtual machine and translated into byte code for use on the Ethereum network. The smart contracts ecosystem of Ethereum has been constructed accordingly [48].

Counterparty: Unlike alternative platforms, Counterparty incorporates its data into Bitcoin transactions. While the nodes of the Bitcoin network do not scrutinize the information contained in these transactions, the nodes of the Counterparty can translate and understand it [49]. Ethereum's programming language may be used to write smart contracts. Counterparty is an open-source protocol that has been tested extensively and is available for download. As well as enabling the creation of digital tokens and the trading of those tokens, Counterparty enables anybody to design and execute smart contracts on the BTC network [34]. As a new technology, smart contracts offer limitless potential. Real-world events may be turned into code and performed automatically, without an intermediary, utilizing Bitcoin's decentralized ledger network and Counterparty's built-in script language [50].

Moreover, ETH's smart contract capability is supported by Counterparty as well. Any Ethereum Solidity or Serpent smart contract should operate on Counterparty with little or no modification (e.g., hardcoded addresses needing to be changed) [34, 51]. Unlike Ethereum, however, no resolution process is utilized to verify computing results [51]. Counterparty features its cryptocurrency that can be exchanged across users and expended on contractual terms. In Ethereum, miners do not get payments for executing contracts; instead, the payments made by users are eliminated, and miners benefit indirectly from the currency's inflation [34].

Stellar: Instead of a smart contract language or virtual machine, Stellar is designed for transferring, storing, and trading value [52]. In contrast, Stellar smart contracts (also known as SSCs) combine transactions with different limitations to accomplish the desired result. The following are some examples of restrictions that may be coupled to construct SSCs, according to the Stellar.org SSCs guide: Multisignature (Multiple persons are required to sign transactions on an account. You may additionally set signatory strengths and limitations), Batching/Atomicity (Batching is the concept of including multiple operations in a single transaction), Sequence (On Stellar, sequence numbers are used to represent sequences.) A transaction's sequence number can be manipulated to ensure that it does not succeed if an alternative is submitted (Time bounds are limitations on the period that a transaction is valid and can be used to represent time in a Stellar smart contract).

Using a consensus mechanism inspired by the federated Byzantine agreement, Stellar has a public blockchain and coin. The basic idea is that a node will agree to a transaction if the nodes in its immediate vicinity (which are regarded to be more trustworthy than the rest) agree with it as well, Unable to roll back a transaction once it has been accepted by a sufficient number of nodes in the network means that the transaction has been confirmed [53]. This technique uses far less processing resources than proof-of-work since it does not need to solve cryptographic problems**.** Assume, for example, that Participant A wishes to pay B only if B commits to reimburse C after receiving the money from A. This may be implemented by keeping both transactions in almost the same sequence. While this particular scenario may also be accomplished on Bitcoin, Stellar also enables batch activities other than payments, such as creating new accounts [54-55].

Monax and Lisk: Despite not having their cryptocurrency, Monax allows the implementation of Ethereum contracts. As a result of Monax, clients can establish smart contracts and specify access permission restrictions for such blockchains [56]. There are rounds in its consensus protocol when one member proposes and the others vote on a new transaction block. When a block refuses to be authorized, the protocol goes through to the next round, because another member will be in control of proposing new blocks. half of the entire voting power must support a block for it to become official [56].

On the contrary, Lisk has its cryptocurrency as well as a public blockchain that uses a decentralized proof-of-stake consensus method [57]. In particular, 101 active delegations, individually selected by stakeholders, can produce blocks. Stakeholders can participate in the election process by voting for delegates or running for office personally. Lisk can execute Turing-complete smart contracts implemented in either JavaScript or Node.js. Unlike Ethereum, the language does not guarantee determinism of executions; rather, developers must take care of it, for example, by avoiding utilizing procedures like Math.random [47].

In summary, Table 1 provides each platform’s blockchain type and contract languages [42].

Table 1. Blockchain Type and Contract Languages for Each Platform

Platform	Blockchain Type	Contract Language
Bitcoin	Public	Bitcoin Scripts and Signatures
Ethereum	Public	EVM Bytecode
Counterparty	Public	EVM Bytecode
Stellar	Public	Transaction Chains + Signatures
Monax	Private	EVM Bytecode + Agreement
Lisk	Private	JavaScript

4. Smart contracts techniques for handling security threats

However, despite recent advances, smart contracts still face some difficulties. Decentralized Autonomous Organization (DAO) smart contract re-entrance vulnerability was exploited in 2016 to steal about 2 million Ether (50 million USD). The privacy, legal, and performance concerns that smart contracts confront are in addition to security issue [58]. Moreover, some techniques have been proposed and used in different areas. Detail of these techniques is provided in subsequent sections.

4.1 *System services*

The employment of automobiles has experienced an upsurge due to the latest developments in automotive technologies. Safeguarding knowledge and financial transactions between production and consumption is of utmost importance in light of the growing prevalence of electric vehicles. Using petroleum-based oils results in the emission of greenhouse gases, which give rise to global concerns. Europe is undergoing a comprehensive energy transition, which involves the substitution of low-carbon and renewable energy sources, such as wind and solar, for fossil fuels and nuclear power. [20] have developed an energy ecosystem on the Ethereum Blockchain that records all processes from electricity generation to end-users. The prevalence of autonomous vehicles is on the rise, with a growing number of consumer vehicles already equipped with related functionalities. The increasing prevalence of artificial intelligence (AI) in real-world missions is accompanied by its inevitable integration as a simulation component. According to [59], AI has the potential to not only facilitate simulations but also contribute to the development of AI itself. [13] have presented a framework that suggests evaluating novel technologies through a multi-criteria hierarchy. This study's primary focus pertains to comprehending emerging technologies' dynamic mechanisms.

4.2 *Prevent inaccuracies*

The regulation of data entry, collection, and sharing can be achieved by establishing mutually agreed-upon computer-processable data-sharing agreements. Both regulatory bodies responsible for overseeing this data must draft an electronic data submission agreement (e-DSA). The study conducted by [60] encompasses a range of considerations, from legal limitations to consumer preferences, to establish a set of guidelines. The implementation of Blockchain technology has resulted in a significant reduction of errors in smart objects and devices during their operational processes. Numerous methodologies aimed at minimizing errors in intelligent machines have been suggested. [61] proposed a knowledge-based framework (KBS) that utilizes smart devices and a data fusion paradigm to facilitate decision-making in industrial management within a clothing manufacturing enterprise. The Knowledge-Based System (KBS) proposed can address a diverse range of decision-making challenges, such as factory tracking, manufacturing preparation and monitoring, efficiency management, real-time monitoring, and data acquisition and processing. Chen and colleagues (2018) present a novel autonomous integrity model that utilizes graphs to facilitate service provisioning in fog computing. The proposed framework comprises a fog node authentication model and a consensus mechanism for composite transactions within the Function-as-a-Service (FaaS) paradigm.

Moreover, the healthcare system proposed by [62] endeavors to attain enhanced diagnostic precision despite indeterminate particulars. Empirical evidence in the form of numerical case studies supports the proposed theoretical framework. The empirical results indicate that the proposed methodology presents a feasible strategy that can function across diverse domains. [63] developed an initial iteration of an intelligent assessment system that allows individuals residing in rural communities to self-evaluate their current status according to the smartness criteria established by a global community of experts. The system utilizes the Electre Tri multi-criteria analysis to enable a comprehensive evaluation of six distinct dimensions, namely mobility, governance, economics, environment, livelihoods, and people, through the application of criteria assessment.

Furthermore, the integration process poses various challenges for each sector, including technological, socioeconomic, operational, and environmental issues, as [64] discussed. The present study employed the fuzzy Analytic Hierarchy Process (AHP) and fuzzy Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) methodologies, which are suitable for handling uncertain scenarios and can assess multiple criteria simultaneously. The decision model for the blockchain platform selection problem was introduced by [5]. The efficacy of the decision model has been assessed in three software companies through the analysis of three real-world case studies. According to the case study participants, this approach yields a more comprehensive understanding of the selection process for blockchain platforms, generates a more hierarchical catalog of alternatives as opposed to self-conducted research, and diminishes the duration and expenses associated with decision-making.

Furthermore, the utilization of digitalization in business processes was deliberated by [65]. The authors have proposed a methodology that facilitates organizations in identifying the most appropriate digital technology for a specific business process. This is achieved by integrating Adversary's Resources (ADR) as an analytical model with small and medium-sized enterprises (SMEs) as research methods. The authors [116] employed the best-worst method to ascertain the determinants of model supremacy in business-to-government data exchange. The authors have identified the principal determinants that underlie the prevalence of these commercial reporting standards within the Netherlands. To attain this objective, the researchers examine conventional dominance factors documented in the literature and ascertain those pertinent to this particular conflict. [62] introduced a new decision-making network model specifically designed to diagnose neutrosophic sets. The results indicate that the proposed methodology offers a feasible strategy to implement across diverse domains. The paper by [66] outlines the utilization of various ranking methodologies to augment risk assessments in the field of cybersecurity. Assigning weight to a parameter is a complex task requiring considering the other parameters involved. The implementation of ranking-weight techniques significantly streamlines the process. [67] proposed a mechanism to address the energy efficiency issue in shipping. Within this framework, shipowners and energy managers are confronted with obstacles. This enables us to concentrate and overcome significant barriers to achieve a continuous enhancement of energy standards. Furthermore, the system remains applicable to researchers and decision-makers as it effectively highlights energy conservation concerns.

4.3 *Unpredictability*

The advent of blockchain technology has enhanced users' trust and assuaged skepticism owing to its resilient security features. Furthermore, several scholars have recognized that blockchain technology has generally enhanced user confidence in this field. [68] proposed a model for government Blockchain resource sharing and exchange, consisting of three main components: the network, infrastructure, and business implementation. There are currently five service networks that receive funding to facilitate the exchange of knowledge services among governmental entities effectively. The proposed approach provides novel resolutions to address issues about confidence intervals and consistency in anticipated outcomes. [69] proposed a methodical examination of Fuzzy Logic decisions in the context of maritime operations. The authors expound upon the analytical significance of Fuzzy Logic in the context of maritime activities, with a focus on its political, logistical, and organizational implications. Moreover, a comprehensive categorization of decision-making issues in marine logistics. Furthermore, a novel Pythagorean fuzzy linguistic multi-attribute decision-making model was formulated by [70] to attain a uniform ranking of alternatives. In addition, [71] presents an alternative approach known as the Fuzzy ANN traceability chain algorithm, which utilizes the Takagi-Sugeno (T-S) method. The proposed algorithm is subjected to computational analysis, and optimal decision-making is examined in the context of blockchain mining. The proposed methodology effectively achieves mitigation efforts for processing the traceability chain.

The authors, [72], put forth an initial proposition to illustrate the notion and progression of LSDM occurrences to define the developing set of policy frameworks-the recently introduced LSDM Decision Making (LSDM) framework. Secondly, the literature on LSDM is categorized. Effectively resolving a Large-Scale Distributed Management (LSDM) problem is a complex and dynamic process that requires achieving a high level of agreement and considering the interdependencies among the involved parties. In the context of assessing warehouse resource requirements, [4] introduces the Learn To Rate (LTR) model, which incorporates both machine learning and multi-criteria decision analysis (MCDA) techniques for application prioritization. The mechanism in question pertains to the renegotiation of the distribution rating of capital for smart contracts associated with various blockchain assets. [73] have employed a hybrid methodology that integrates simulation and mechanical education to investigate its effectiveness in facilitating data-driven decision-making for identifying resilient suppliers. The distribution of goods within a suitable timeframe is employed as a metric to assess the supplier's reliability. Additionally, strategies to establish robust supply output profiles are investigated to meet the necessary standards. Theoretical considerations have been made regarding the notion of risk profile and the efficacy of a resilient supply chain. The authors exhibit the efficacy of their methodology in discerning the correlations between deviations from the resilient supply chain value profile and vulnerability performance profiles. [74] introduce a novel context-aware selection mechanism for Context-aware Radio Access Technology (CRAT) that considers both device context and network considerations. The NS3 modeling tool was utilized to implement and validate the proposed CRAT. The process entails a mechanism for selecting the optimal Radio Access Technology (RAT) to operate within an Ultra-Dense Network (UDN) setting.

4.4 *Supply chain management*

Recent advancements in the field have yielded valuable insights; however, Ivanov et al. have identified forthcoming research avenues and ripple effect taxonomies (2019). The contemporary supply chain network comprises multiple phases or stages, wherein various stakeholders vie for a portion of the market. Regarding the form of business, each echelon can be classified as a monopoly, duopoly, or oligopoly. The domain of blockchain technology encompasses multiple entities competing for market share and can be classified as an oligopolistic industry [75]. The study conducted by [76] investigates the feasibility of integrating financial and vendor ratings to formulate a credit rating model for the supply chain. The authors conduct a further analysis of the advantages and difficulties that a paradigm presents to all stakeholders involved. According to [43], the study demonstrated a thorough assessment of the ability of the supply chain and logistics industry to adapt to increasingly competitive economic conditions while also identifying novel growth strategies to tackle potential macroeconomic challenges. The achievement of this objective is facilitated through a comprehensive assessment of the supply and demand mechanisms, which incorporates the fundamental concerns of all stakeholders involved. The introduction of novel perspectives for risk management, such as the cascade impact and resilience of supply chains in Business 4.0, has been proposed by [77]. These perspectives emphasize risk analysis for the supply chain.

Table 2. Comparative Analysis

Criteria	System Services	Preventing Inaccuracies	Unpredictability	Supply Chain Management
Technique 1	Intrusion Detection	Data Validation	Randomization	Blockchain Technology
Technique 2	Intrusion Prevention	Error Correction	Encryption	RFID Tracking
Technique 3	Access Control	Audit Trails	Redundancy	Vendor Assessment
Technique 4	Authentication	Regular Backups	Diversity	Supplier Collaboration
Technique 5	Vulnerability Scanning	Consistency Checks	Chaos Engineering	Risk Assessment

Table 3. Existing Work Summary

Publication Year	Studies/References	Types of Study
2016	[23, 45, 81-83]	Survey
2017	[46, 48, 84-85]	Survey
2018	[48, 86-88]	Review
2019	[6, 34, 47, 55, 89]	Survey
2020	[14, 27, 54, 90-92]	Review
2021	[93-96]	Survey
2022	[97-101]	Survey

The study by [78] aims to identify the barriers hindering the adoption of IoT technology in the retail supply chain of India. Additionally, the research investigates the interconnectedness of these barriers by applying integrated Interpretive Structural Modeling (ISM) and Decision-Making Trial and Evaluation Laboratory (DEMATEL) methodologies. [79] conducted an analysis on the utilization of blockchain (BC) technologies as a means to enhance sustainable supply chain management (SSCM) efficacy, as opposed to ineffective supply chain management (SCM). Following discussions with academic and business professionals, significant variables associated with BC have been identified from the existing literature. The variables mentioned above undergo additional assessment and construction by utilizing the Primary Component Analysis (PCA) laboratory for Fuzzy Decision (DEMATEL). [80] developed a model of outcomes for the integrated industrial strategy of 14.0 solutions for SMEs. Within this particular context, the authors consolidate the sixteen primary areas of operation and establish suitable output metrics for evaluation. This approach aims to facilitate the creation of a comprehensive and structured inventory of relevant characteristics for assessing the 14.0 solutions. [8] introduced a multi-criteria optimization framework that utilizes reluctant fuzzy sets to address blockchain technologies in supply chain management. The framework was developed by applying the Delphi tool, hesitant fuzzy Analytic Hierarchy Process (HF-AHP), and Hesitant Fuzzy Technique for Order Performance by Similarity to Ideal Solution (HF-TOPSIS).

Thus, a comparative analysis table for security threat handling techniques related to System Services, Preventing Inaccuracies, Unpredictability, and Supply Chain Management is provided in Table 2.

The research is motivated by the observation that a significant void exists in the scholarly discourse regarding a thorough review of security challenges associated with smart contracts during application planning, development, maintenance, and testing within blockchain technology. As a result, our research aims to bridge the existing knowledge deficiency. All of the reviews and surveys, together with their types, are shown in Table 3.

5. Taxonomy of the smart contracts security application

A taxonomy of smart contracts has been presented, classified into six [6] distinct categories based on their respective application domains. The present study introduces the Smart Contract Security Taxonomy to address certain deficiencies and limitations observed in prior endeavors. The current taxonomy establishes a correlation between contemporary security threats and security services. In this regard, we have incorporated the roster of security services proposed by [56] as a fundamental axis of our taxonomy. The taxonomy presented herein facilitates the development of a comprehensive security framework for smart contracts across diverse contexts. The utilization of the Smart Contract Security Taxonomy is expected to facilitate the assessment of security measures on Smart Contracts, a matter of considerable importance and complexity. The taxonomy that has been developed will function as a framework for conducting a thorough investigation of specific vulnerabilities and threats previously identified in smart contracts. The proposed taxonomy is expected to facilitate the development of security models for constrained devices by security developers while also serving as a valuable knowledge repository for cybersecurity professionals.

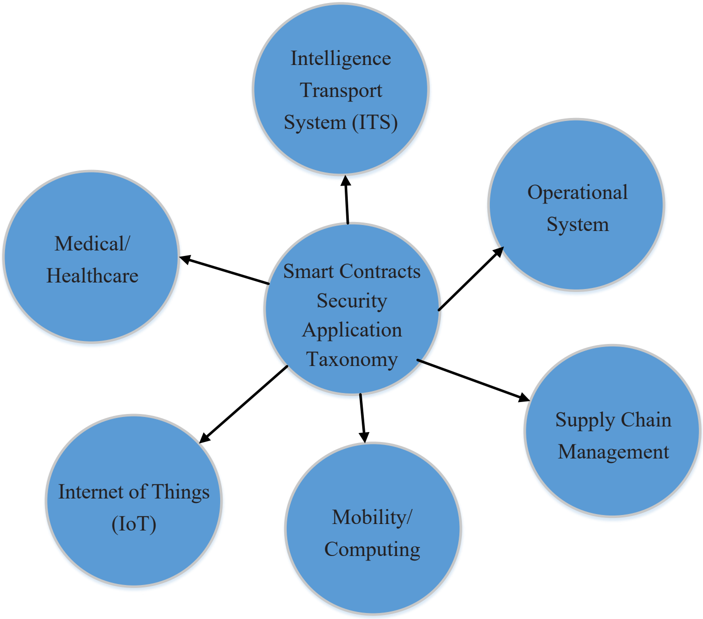

Figure 4. Smart Contracts Security Application Taxonomy

The initial phase of our taxonomy development involves the establishment of a novel categorization scheme for the application domain, architectural domain, communication channel, and data domain of Smart contracts. A novel matrix taxonomy is proposed for Smart Contract security, which establishes a linkage between each classification and its corresponding components. Finally, as indicated in Figure 4, we examine and analyze each security component, evaluate its impact, and relate it to one or more potential security countermeasures.

5.1 *Medical/healthcare*

Medical administration and provision are undergoing radical changes due to the advent of new technologies. Access to data in real-time and using ever-evolving digital tools are facilitating the quest for service flexibility, shortening hospital stays, and aiding multi-professional activities. Many hospitals have adopted digital technology to improve the quality of treatment they provide patients while enhancing their efficiency and productivity [12]. Health concerns are higher for those living in developed nations. As a result, progress in the medical industry has been one of the most active areas of study. Heart disease is by far the most common among all diseases and deaths. There are numerous factors to consider while diagnosing heart disease, making the practitioner's job difficult. In addition, the clinician's facts and information for diagnosis are often insufficient and buried. The IoT has recently allowed several new features and online services in the healthcare industry [32]. Because of these applications, millions of individuals can access timely health information that may help them make informed decisions about their health and well-being. With the recent emergence of Blockchain technology for eHealth, a secure, decentralized, and patient-driven record management system is possible [102]. Since the use case for storing IoT data collected in remote patient management (RPM) situations necessitates a rapid consensus process, careful keys management, and improved privacy safeguards, Blockchain technology cannot handle such storage. However, mobile and wireless networks may introduce additional risks to the m-health systems. These dangers may harm the patient, such as when an insulin pump injects the incorrect amount or when heart implant procedures are halted. Therefore, if the severity of the risks is to be anticipated well before the occurrence, safety risk management is required and should be implemented. Therefore, risk assessment is fundamental to any m-health security management system [103].

5.2 *Mobility/computing*

These days, individuals are more connected than ever because of mobile devices and internet tools like social networking, mobile phones, and texting. Expanding beyond human connections, the IoT may now interconnect devices and machinery via IoT applications [74]. Fifth Generation mobile networks, also known as 5G, are an upcoming revolutionary digital wave that aims to facilitate efficient connectivity between smart devices and applications across a variety of cutting-edge service categories and deployment contexts. It's vital to remember that computing is the foundational function that enables the use of MCDM inside BC. In this context, [104] offered a reputation model for FaaS service providers. To guarantee the availability of third-party fog nodes, it expands FogSEA by providing a decentralized graphic trust mechanism. A portion of the Service Level Agreements (SLAs) may be negotiated without the presence or knowledge of all the service providers, and this also offers a tool for creating reference pricing for that purpose. FaaS users might benefit from this solution since it helps them get high-quality service at affordable rates. Using computational methods, a novel decision-making model based on Pythagorean Fuzzy linguistic information measures and its application to the issue of a sustainable Blockchain product assessment was developed by [70]. [50] employed computational methods to construct RSA and ECC in Blockchain for multi-dimensional adversary analysis. The general evaluation of transaction sizes and efficiency has been used to compare the proposed approach to the RSA and ECC algorithms most often used in blockchain. [105] look at possibly employing a BC big data platform to create a new smart city with low carbon emissions and a green environment via computing services. To that end, a novel trust model that accommodates multiple certification authorities (CAs) and public key infrastructures (PKIs) is developed using blockchain technology.

5.3 *Internet of things*

The IoT is an innovative technology that will likely have far-reaching consequences for the future of IT optimization and integration. The effects of this technology are far-reaching, touching on almost every major business sector. Thankfully, it seems that both the creation and the widespread use of IoT are only getting started [78]. The emergence of mobile communication technology as a service z has had a major impact on creating the fundamental framework of smart cities. A "smart city" aims to optimize and connect urban operations and services with people via Big Data and the Internet of Things. Blockchain technology has emerged as a promising new approach to improving smart city infrastructure. Data sent and recorded using blockchain technology is legitimate and trustworthy because it is immutable, centrally controlled, and protected from assault. The rising popularity of IoT in recent years has opened up fascinating possibilities for developing multiple home automation systems and a wide range of enterprises. These benefits are used to automate the kind of businesses that give birth to the IIoT. Since IoT is vulnerable to several cyber attacks, stringent measures are necessary to provide adequate security. Blockchain offers a secure and decentralized Internet of Things that may help solve the abovementioned problems. According to the research of [106], a blockchain is "essentially a chain of blocks connected by cryptographs" that acts as a distributed leader whose data is shared over a peer network.

Because of blockchain's superior value transfer properties, data from mobile devices may be economically valuable at a low cost. Since cloud computing is deployed on demand, it saves resources and provides significant flexibility. Using an acyclic graph to depict the workflow for each edge node and measuring the success rate of tasks influenced by uncertainties, [31] presented Blockchain-enabled Resourcing Processing (BPRP) for workflow planning under uncertainty. Their work uses approved private blockchain technology to document the current operational state of all system edge nodes and the planned execution of all system procedures. Blockchain is a decentralized public ledger managed by the network's periphery nodes.

5.4 *System for Intelligent Transportation (ITS)*

The MCDM is applied to many different services inside the ITS via the usage of BC. For instance, [34] have constructed an energy ecosystem that utilizes the Ethereum Blockchain network to keep track of all the steps involved in bringing power from its generation to the final customer. Participants in this study range from electric vehicle owners and drivers to energy suppliers, distributors, and dealers. Users can do business with one another with the use of smart contracts. All transactions related to the developed decentralized application are recorded on the Blockchain ledger, and smart contracts do away with the necessity for intermediaries. Blockchain and smart contracts ensure that all logged transactions adhere to the privacy, security, and transparency triad. In addition, [107] provided a method for implementing this system based on network entities exchanging and sharing data. Provided is a Blockchain-based scenario that facilitates virtual payments for Vehicular Cloud Computing (VCC) participants and consumption of network resources and gateway functionality in V2V routing mode.

5.5 *Methods of operation*

[108] provide a framework to direct Blockchain-based Life cycle assessment (LCA) implementation; this is only one example of many firms using MCDM as part of BC to carry out specific services. It provides a framework for systems that integrates Blockchain with IoT visualization and application-research with massive amounts of data. Blockchain application developers have validated the proposed framework and system architecture. The study also looks at the potential managerial and policy repercussions and the cost of deploying the system. [4] suggests using MCDA with the machine learning framework Learn to Rank (LTR) for a ranking application using warehouse resources. In addition, they investigate a framework for asset rankings on blockchains to be renegotiated using smart contracts. The strategic, tactical, and operational significance of Fuzzy Logic in maritime activities is discussed by [32]. In addition, we present a comprehensive classification of maritime logistics decision problems. The framework permits a thorough evaluation of six distinct elements, including Mobility, Governance, Economy, Environment, Living, and People, with weightings of the criterion using the Electre Tri multi-criteria analysis. This allows village representatives to self-assess their current state concerning smartness criteria defined by an international panel of experts.

5.6 *Logistics planning and control*

The MCDM is utilized as a part of the application of BC for different services in the supply chain management (SCM) industry, which is concerned with economics. For instance, [39] used blockchain technology to try to build a future monitoring and planning framework for many industries in India. A decision-making framework for handling fake goods and fighting the counterfeiting issue is developed using the SWARA-WASPAS method. [109] discussed how the Internet of Things has helped the food business. The IoT can revolutionize the food business by assisting shoppers and retailers to find things more quickly, providing more accurate information about the food's nutritional worth and cost, and highlighting current discounts or deals. The Internet of Things helps monitor the logistics chain and shorten delivery times when dealing with perishable goods. In addition, it is expected that the Internet of Things will help retailers control the quality of food products, the waste management of items that have outlived their shelf life, the shop's temperature, and other equipment that helps decrease energy usage. In their study of a hybrid strategy that blends simulation and machine teaching in digital manufacturing, data-driven assistance for selecting resilient suppliers is explored by [73]. We analyze the need for constructing dependable supply performance profiles since they consider on-time delivery a hallmark of a trustworthy provider. They propose the idea of a supplier's performance risk profile and the value of a resilient supply chain.

Additionally, [45] used value-focused thinking (VFT), a multi-objective decision analytics approach, to the issue of cybersecurity to demonstrate how corporations may evaluate the worth of blockchain technology to maximize value-add inside financial institutions. Because investigating blockchain use for monetary transactions in the context of cyber security is crucial for understanding how firms in the financial industry might respond to these worries. In addition, [43] proposed a strategic evaluation process that has critically assessed numerous obstacles to the DLT implementation in both industry and service sectors based on the DEMATEL framework and management inputs of senior managers working in rail, e-commerce, banking, media technology, IT, insurance, and financial services. The proposed model can provide a comprehensive set of problems afflicting sectors and services, then elaborate on the probable links between these problems.

6. Smart contract security scenario

With security in mind, [67] suggested constructing an automated engine charging platform on the Ethereum blockchain using a network of multi-criteria decision support systems utilizing the PROMETHEE method. This study aims to safeguard the transfer of information and capital across the energy sector, from generation to consumption. This research covers the whole energy industry, from producers to consumers, traders to retailers, and charging stations to drivers of electric vehicles. In addition, smart contracts are utilized to simplify the business process with other customers. In addition to preventing the need for intermediaries, Bitcoin ensures that all transactions involving the distributed software created are recorded and publicly available. [21] presented a method for evaluating the efficacy of a blockchain for managing power that uses fuzzy DEMATEL technology. The authors of this study took into account a distributed generation setting in which individual households produce electricity on their own or buy it from utilities or other users. The blockchain also facilitates the management of smart contracts and peer-to-peer transactions. A novel modeling strategy for smart data-finding applications in Blockchain was also presented [90]. "A guidance approach" is another name for the suggested paradigm. This paper draws from three scientific frameworks-the basic idea of complex information systems, systems theory, and the ISO 25,001 software quality standard-to propose a methodology for assessing novel technologies.

Today's businesses have a better idea of how to make items that sell because of the availability of analytics, data analysis, and statistical modeling tools. However, [110] show how big data plays a crucial role in the tourism and hospitality industry by differentiating and explaining the analytical mechanisms to support an integrated B2C interface based on numerous internal datasets and external data sources, thereby striking a balance between operational goals and tourist needs. The full potential of big data in tourism and hospitality is shown, along with the responsibilities of stakeholders and the necessary resources. In addition, [12] spoke about how the digital revolution is changing the health industry. The purpose of this study is twofold: first, to determine whether or not existing digital technologies can improve healthcare quality and safety, and second, to analyze the development of digital medicine. Likewise, [103] presents a fresh approach to risk analysis in M-Health systems. Estimation, appraisal, archiving, and trading of risk parameters are the four pillars of the authors' methodology. We could confirm and verify their correctness by comparing their findings to the Weighted Average method results. The authors modified their approach to testing its efficiency against a targeted Onion Attack. [34] propose an eHealth system that uses multiple instances of a three-tier software patient agent (sensing, NEAR processing, and FAR processing). It improves the reliability and robustness of the eHealth system.

In addition, [111] provides a statistical model of mutual trust and risk. Joint Trust and Risk Model (JRTM) is a paradigm that deals with threats in several domains, including security, privacy, and service efficiency. It lends itself to automated care by enabling the visualization of the delivery chain and the intricate risk tracking according to profiles established in the CC. Regarding CC expectations, JRTM risk management can distinguish between good and bad results. A multidimensional adversary analysis of RSA and ECC for Blockchain encryption was suggested [22]. The authors looked at the RSA and ECC algorithms and compared their performance. They aim to provide a more comprehensive rationale for their widespread use in blockchain applications. [100] have suggested using Blockchain to power a crowdsourcing technique that safeguards user data in a mobile setting. We create a mobile crowdsourcing framework based on the blockchain to maintain communications privacy and prevent the loss of work in progress.

Even more intriguing is the possibility that Blockchain technology may address the problem of cyber security in monetary exchanges. Using the VFT-based goal framework, [25] examines blockchain's potential to increase the safety of financial transactions. Using the VFT-based goal framework proposed in this study, a business may first scale this idea up to the tactical level. [32] offered a comprehensive overview of the threats to and security issues with IoT and IIoT, as well as potential blockchain-based solutions. The authors discuss the most significant Blockchain-based solutions that have emerged recently to solve traditional cloud-based apps' issues. [112] present a new Emission Trading Scheme (ETS) architecture for adopting Industry 4.0. The suggested framework incorporates blockchain technology and smart devices to improve ETS regulatory laws.

The immutability and ease of use offered by blockchain technology ensures the scheme's data consistency. This will improve the scheme's overall efficiency, reliability, and robustness. Another method for reducing cyber threats is Enhanced Prioritized Gap Analysis (EPGA), developed by [66]. The effectiveness of the suggested system is shown by comparing it to existing relevant frameworks and testing it against cyber injections in a real-world cyber-attack. In addition, [113] investigates the central problem of product counterfeiting in the modern world. Distributed ledger systems' capabilities and requirements are analyzed here. The research uses the Step-wise Weight Assessment Ratio Analysis (SWARA) and Weighted Aggregated Sum Product (WASPS) method. The parameter weights are calculated using SWARA, and the alternatives are ranked and weighted using WASPS. Finally, [105] presented a three-tier Blockchain government information resource sharing and exchange architecture consisting of the network, infrastructure, and business application layers. Five infrastructure networks confirm the validity of the suggested approach to solve the issue of sharing government-related information services. It presents new ways of thinking about data ownership, peer management, standards compatibility, non-real-time exchange, and trust islands in information sharing. This research also evaluates the progress made by Smart Hefei between 2012 and 2017 by developing a rigorous evaluation methodology based on the TOPSIS framework.

Blockchain technology provides a safe way for employees from different departments to communicate with one another during policy development. For instance, [114] addressed how blockchain may increase the security of financial transactions. From a managerial perspective, understanding how blockchain technology impacts cyber security for financial transactions is paramount. Create a method for investigating obstacles to blockchain adoption and efficient implementation in different sectors [3]. The writers outline these challenges by drawing on prior research and the opinions of specialists. The study's findings will help management eliminate the most pressing problems. Similarly, [10] used the hierarchical decision-making model (HDM) to create a sound procedure for evaluating electronic authentication policies. The suggested model improves the multiparty process by demonstrating, using numerical results from HDM models, that the decision-making components are of relative worth. Knowledge-based economies need new approaches to fiscal, monetary, and social policy. [115] advocated using blockchain algorithms for secure control and fog computing. It's a method for calculating how much people pay for various government assistance. It is an election system that consistently uses either proportional representation or direct voting.

Blockchain technology also opens new doors for privacy and anonymity in a different sphere. Examples include implementing a virtual payment service for users of VCC via the scenario for resource usage and the gateway service in V2V mode presented by [107]. [116] employed the best-worst technique to determine the underlying causes of the preeminence of these firm reporting criteria in B2G data sharing. The results show that eXtensible Business Reporting Language (XBRL) is likely to replace Ego-Dissolution Inventory (EDI) as the dominant standard for market reporting because it best considers the contributions of key players, the timing of entrance, and the installed base. Finally, a framework was developed [43] using the fuzzy DEMATEL method. The DEMATEL is a method for evaluating the interdependence of framework impacts using a multi-criteria decision-making approach. It concludes things based on the combined knowledge of experts.

6.1 *Lessons learned from smart contracts and security threats*

Smart contracts, powered by blockchain technology, have revolutionized how agreements are executed in various domains, including finance and supply chain. However, they also introduce unique security challenges that must be addressed to ensure their robustness and reliability. This essay explores the lessons learned from various aspects of smart contracts and the techniques employed to handle security threats. Smart contracts are self-executing agreements with the terms of the contract directly written into code, eliminating the need for intermediaries, automating processes, and enhancing transparency. The decentralized and immutable nature of blockchain ensures trustworthiness in smart contract execution. Platforms like Ethereum provide the infrastructure for deploying and executing smart contracts, offering a rich ecosystem for developers to create various applications. However, these platforms also make them targets for attackers. Smart contracts security techniques include code audits, static and dynamic analysis, and formal verification. Code audits involve reviewing code to identify vulnerabilities, while static study examines code without executing it. Dynamic analysis tests the code during execution to identify runtime vulnerabilities. Formal verification employs mathematical proofs to validate the correctness of the code. A taxonomy of smart contracts security application categorizes security issues into different classes, aiding in understanding and addressing vulnerabilities. A secure smart contract requires careful consideration of inputs, logic, and outputs, as flaws in any of these aspects can lead to security breaches. Possible attacks on smart contracts include reentrancy attacks, integer overflow attacks, and denial-of-service attacks. To mitigate vulnerabilities, smart contracts must undergo thorough auditing, formal verification, secure design patterns, continuous monitoring, education and training, community collaboration, and regulatory compliance.

In summary, smart contracts offer transformative potential but are not immune to security threats. Developers can mitigate vulnerabilities and build robust smart contracts that drive innovation while safeguarding assets and data by implementing thorough audits, embracing formal verification, and adhering to secure design patterns.

7. Discussion on possible attacks posed by threats and vulnerabilities of the smart contracts

7.1 *Threats of the smart contracts*

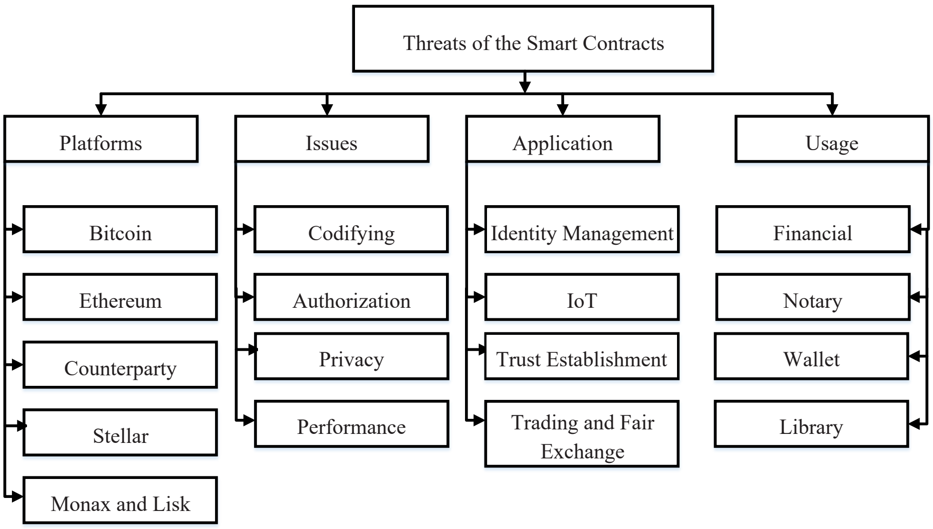

Figure 5. Threats of the Smart Contracts

The possible attacks posed by threats of the Smart Contracts [30], are illustrated in Figure 5.

The possible threats of smart contracts are categorized into four [4]: platforms, issues, application, and usage, as shown in Figure 5. Each threat is exposed to different types of attacks, as indicated in the figure.

7.2 *Vulnerabilities of the smart contracts*

The risks associated with smart contracts are discussed here [91]. Examples of such vulnerabilities include;

For example, if a Solidity primitive used to call a function or send ether cannot find the position it is looking for, it will instead call a default function declared in all contracts (whose code may be unknown to the caller). Without using any gas: Using basic SEND to send ether might run into a gas depletion issue if the recipient is a contract with an intricate fallback mechanism. Disruption due to exceptions may occur in many different ways in Solidity, such as when the contract's execution hits a gas limit, the call stack is exhausted, or when the throw command is executed. In contrast, whether an exception occurs through a direct function call or via the primitive CALL, Solidity handles them differently. In the first case, the processing is paused, and unintended consequences, such as ether transfers, are undone.

The Solidity compiler will not detect a type conversion error if a programmer makes a mistake and calls another contract with an integer-waiting function or functions with a certain structure or if a contract makes a mistake and calls another contract with a function with the same name. Secrets: Secrets in Solidity contracts are either public or private fields. This might be useful if sensitive information has to be concealed between contract conversations. However, this method is inefficient since it requires private changes to be broadcast to mining nodes before they can be included in the public Blockchain. Ether is a decentralized, open-source technique that supplies the technologies used by the Bitcoin network. Hence its condition is unpredictable. Its absence of a keyboard, among other things, makes it quite difficult to use. The status of a contract may change after a transaction is mined and added to the chain. A chain fork may occur if two miners continuously mine the same valid block. The outcome would be skewed because some miners would attach their block to one string, while others would append to the other.

Thus, Table 4 breaks down the publications based on empirical validations.

Table 4. Publications Based On Empirical Validations

Ref.	Technology	Description	Dataset components	Findings
[117]	Ethereum	Applying static OO metrics to Solidity contracts. Solidity is a contract-oriented software program.	Out of 10,206 Solidity smart contract source code files, over 45,000 contracts were found.	Smart contracts are concise, straightforward, and minimally annotated.
[100]	Ethereum	Using a benchmarking method, we can determine if the CPU use fees miners get for developing and executing smart contracts are reasonable.	There are 80 smart contracts.	As a result of inconsistencies, incentives are not properly matched, and the blockchain's reliability suffers.
[90]	Ethereum	Test suites may be generated at low cost utilizing one of two multi-objective test creation strategies.	8 Dapps.	The proposed method has the potential to save money on gas and time while still allowing for the protection of strands.
[118]	Ethereum	Examine whether there are statistically significant variations between smart contract and conventional metrics.	12,000 digital contracts.	In contrast to their counterparts in conventional software systems, the ranges of smart contract measurements are limited.
[119]	Ethereum	An effective infrastructure for running smart contracts in parallel.	An algorithmic benchmark suite for Ballot, Simple Auction, and Coin contracts.	The newly proposed protocols are more efficient than the prior method, which relied on a sequence of operations.
[120]	Ethereum	Examining the present state of blockchain and the proposed enhancements to it.	Over a thousand Ethereum nodes.	Ethereum is secure and independent. However, it is not very adaptable.
[94]	Ethereum	In Solidity, there are several security patterns.	Information was gathered from a variety of places.	There are 6 coding security design patterns to avoid.

Table 4. (cont.)

Ref.	Technology	Description	Dataset components	Findings
[121]	Ethereum	"A framework for grouping similar contracts".	"998 smart contracts"	Identification of the purpose of a contract with clustering.
[122]	Ethereum	"Analysis of the different tools to detect bugs in smart contracts"	"1,010 smart contracts in 200 files".	"Most smart contracts lack security".
[123]	Ethereum	Using graph analysis, pinpoint the most significant use cases of Ethereum.	The total number of external transactions was 28,502,131, whereas the total number of internal transactions was 19,751,821.	The results shed light on Ethereum's internal dynamics.
[124]	Ethereum	"Smart Contract Classification With a Bi-LSTM Based Approach".	15,213 smart contracts.	The proposed method is active.
[125]	Ethereum	Identifying Ponzi Schemes in Digital Transactions.	The number of smart contracts is three thousand.	In comparison to more conventional approaches,
[126]	Ethereum	"Pattern to optimize gas consumption."	"24 design patterns divided into five categories".	"Applying these patterns, the gas consumption can be mitigated."
[127]	Bitcoin	A comprehensive evaluation of a theoretical blockchain protocol deployment.	Extraction at random.	The test suite validates the blockchain attributes to ensure they are satisfied.
[128]	"Bitcoin-core, Ethereum, Monero, Dogecoin, Ripple".	Identifying dissimilarities in the statistical distribution of 10 software components between the two types of projects.	Top 5 Free C++ Projects	The test suite validates the blockchain attributes to ensure they are maintained.
[129]	"Blockchain-oriented and 5 traditional java software systems".	"Metrics analysis could identify differences in programming and reveal meaningful differences between the two projects' domain".	Extraction at random	Metrics analysis could identify differences in programming and reveal meaningful differences between the two projects' domains.
[130]	"Hybrid software architectures".	"Impact of design patterns in smart contracts on transaction costs".	"Processing fee comparison modeling three use cases.	Finding the sweet spot for a hybrid app's features is still challenging.
[131]	Ethereum	"Benchmark approach to assessing the CPU usage required per EVM opcode; comparison with the set gas cost".	"EVM opcodes are classified into eleven categories".	This study offers some intriguing insights into the payoff for CPU resources invested in terms of opcodes and computer environment.

Each table's columns are arranged in a way that makes sense in light of the technologies at hand. It's important to note that in the blockchain ecosystem, many smart contracts are either almost identical to one another or represent several iterations of the same contract [98]. Therefore, one must use care when interpreting the results in Table 3.

7. Open challenges in smart contract

This section provides some challenges confronting smart contracts, as stated by [6, 47, 93, 132, 133].

1. Testing Phase: Examination of the irreversibility of blockchain and the requirement to test smart contracts on testnets, prior to real deployment; includes unit and integration and system testing, modification testing, test case creation, and testing and debugging.

2. Contract Analysis: Smart contract analysis and optimization techniques identification; construct measures for evaluating the quality of code that are applicable just to smart contracts; provide language-agnostic approaches to code analysis that may be used to languages other than Solidity and Go.

3. Codes and Metrics: Recommendations for application developers; using agile techniques of software development; a one-of-a-kind tool for determining a variety of metrics; locating novel language-specific measures for the creation of smart contracts.

4. Contract Security: Effective techniques of security testing; patterns to identify particular attacks; a centralized taxonomy of vulnerabilities in smart contracts; the exploration for security flaws.

5. Performance Measurement: Performance metrics to assess scalability, precision, and effect of various consensus algorithms; extensive frameworks to discover benefits and potential bottlenecks in various blockchain technologies and architectures methods for calculating the possible influence of using blockchain technology on both functional and non-functional specifications.

6. Blockchain Application: Blockchain integration with preexisting infrastructure; methods for weighing the pros and cons of it implementation.

9. Future directions

Smart contracts cover much more than simply the advantages of blockchain technology. However, the article relates to a contract's complete digital life cycle, from negotiation through control and certification of contractual terms. Smart contracts may now be used without the usage of blockchain technology. Contract management systems might thus solve both the trustless problem and the irrevocable aspect of blockchain by controlling the contract's life-cycle without removing the digital technology restrictions. To secure the basis of confidence, modern contract management solutions require all contract parties to show evidence of identification and validate their access to data. Furthermore, all contract-related data are saved in a revision-secure and encrypted format on a cloud-based platform created and maintained in Europe. This enables transparency and accountability for all occurrences, control mechanisms, and the identification of those affected. One of the latest contract management solutions, Fabasoft Contracts [134], is a cloud-based software solution that supports users all through the full contract life cycle, from contract preparation across companies to cost-effective review and approval procedures to revision-secure contract digitized and storing of modifications. Contract rights and obligations can be modeled and then validated and enforced. In addition to enabling traceability when monitoring the cold chain of food delivery or confirming the validity of replacement automotive components as opposed to counterfeit products, revision-secure contract management offers numerous other benefits.

10. Conclusion

The attributes inherent in smart contracts facilitate the execution of their encrypted security prerequisites within a decentralized network, wherein each node holds an equivalent status and lacks any substantial power unless a trusted authority or central server intervenes. Smart contracts can potentially provide significant advantages to various established industries, including but not limited to the financial and healthcare sectors. Furthermore, the scope of investigation regarding the security of smart contracts is constrained. Despite the abundance of tools available to developers, it is perceived that the extensive array of options can be overwhelming and pose a challenge in determining a starting point. This article could potentially serve as a valuable resource for initiating further scholarly inquiry. This paper provides a comprehensive analysis of smart contracts. The study compared the security of smart contracts and conventional security measures, considering factors such as security, privacy, and communication channels. This paper also examines various platforms that facilitate the implementation of smart contracts, including but not limited to Bitcoin, Ethereum, Counterparty, Stellar, Monax, and Lisk. Multiple techniques have been suggested and implemented across diverse domains to address security threats in smart contracts.

Furthermore, a taxonomy has been proposed to enhance the security of smart contracts. This taxonomy aims to address the limitations and deficiencies within smart contracts. The research additionally presents a particular security scenario for smart contracts, encompassing various techniques. Finally, the potential security breaches arising from the vulnerabilities and threats associated with smart contracts are presented. This study focuses on the security threats and vulnerabilities specific to smart contracts.

Conflict of interest

This manuscript is original and has not been published elsewhere, nor is it under consideration for publication in any other journal, and there is no Conflicts of Interest.

References

[1] Oleribe OO, Momoh J, Uzochukwu BSC, Mbofana F, Adebiyi A, Barbera T, et al. Identifying key challenges facing healthcare systems in Africa and potential solutions. *International Journal of General Medicine*. 2019; 12: 395-403.

[2] Khan R, Ali I, Jan MA, Zakarya M, Khan MA, Alshamrani SS, et al. A hybrid approach for seamless and interoperable communication in the internet of things. *IEEE Networks*. 2021; 35(6): 202-208.

[3] Biswas B, Gupta R. Analysis of barriers to implement blockchain in industry and service sectors. *Computing Industrial Engineering*. 2019; 136: 225-241. Available from: https://doi.org/10.1016/j.cie.2019.07.005.

[4] Pongpech WA. On application of learning to rank for assets management: Warehouses ranking. In: Yin H, Camacho D, Novais P, Tallón-Ballesteros A. (eds.) *Intelligent Data Engineering and Automated Learning-IDEAL 2018. IDEAL 2018. Lecture Notes in Computer Science, vol 11314.* Springer, Cham. 2018. p.336-343. Available from: https://doi.org/10.1007/978-3-030-03493-1_36

[5] Farshidi S, Jansen S, Espana S, Verkleij J. Decision support for blockchain platform selection: Three industry case studies. *IEEE Transaction Engineering Management*. 2020; 67(4): 1109-1128.

[6] Moudoud H, Cherkaoui S, Khoukhi L. An IoT blockchain architecture using oracles and smart contracts: The use-case of a food supply chain. *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. Istanbul, Turkey: IEEE; 2019. p.1-6. Available from: https://doi.org/10.1109/PIMRC.2019.8904404.

[7] Kwon S, Park S, Cho HJ, Park Y, Kim D, Yim K. Towards 5G-based IoT security analysis against Vo5G eavesdropping. *Computing*. 2021; 103(3): 425-447. Available from: https://doi.org/10.1007/s00607-020-00855-0.

[8] Çolak M, Kaya I, Özkan B, Budak A, Karaşan A. A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management. *Journal of Intellegence Fuzzy System*. 2020; 38(1): 935-946.

[9] Yadav J, Misra M, Singh K. Sensitizing netizen's behavior through influencer intervention enabled by crowdsourcing-a case of reddit. *Behaviour of Information Technology*. 2022; 41(6): 1286-1297.

[10] Melkonyan A, Krumme K, Gruchmann T, Spinler S, Schumacher T, Bleischwitz R. Scenario and strategy planning for transformative supply chains within a sustainable economy. *Journal of Clean Production*. 2019; 231: 144-160. Available from: https://doi.org/10.1016/j.jclepro.2019.05.222.

[11] Son W, Sheikh NJ. Assessment of electronic authentication policies using multi-stakeholder multi-criteria hierarchical decision modeling. *2018 Portland International Conference on Management of Engineering and Technology (PICMET)*. Honolulu, HI, USA: IEEE; 2018. p.1-11. Available from: https://doi.org/10.23919/PICMET.2018.8481798.

[12] Marques ICP, Ferreira JJM. Digital transformation in the area of health: Systematic review of 45 years of evolution. *Health Technol*. 2020; 10(3): 575-586.

[13] Akoka J, Comyn-Wattiau I. A method for emerging technology evaluation. application to blockchain and smart data discovery. In: Cabot J, Gómez C, Pastor O, Sancho M, Teniente E. (eds.) *Conceptual Modeling Perspectives*. Springer, Cham; 2017. p.247-258. https://doi.org/10.1007/978-3-319-67271-7_17.

[14] Sengupta J, Ruj S, Das Bit S. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Networks Computer Applications*. 2020; 149(12): 102-115. Available from: https://doi.org/10.1016/j.jnca.2019.102481.

[15] Chandel S, Cao W, Sun Z, Yang J, Zhang B, Ni TY. A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption. In: Arai K, Bhatia R. (eds.) *Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70*. Springer, Cham; 2020. p.988-1003. Available from: https://doi.org/10.1007/978-3-030-12385-7_67.

[16] Kumar A, Kumar KS, Sharma M, Menaka C, Naaz R, Vekriya V. Machine learning in molecular communication and applications for health monitoring networks. *Software Computing*. 2023. Available from: https://doi.org/10.1007/s00500-023-08400-9.

[17] Wang H, Liu Z, Ge C, Sakurai K, Su C. A privacy-preserving data feed scheme for smart contracts. *IEICE*

Transaction of Information System. 2022; E105D(2): 195-204.

[18] Alabool H, Kamil A, Arshad N, Alarabiat D. Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review. *Journal of System Software*. 2018; 139: 161-188. Available from: https://doi.org/10.1016/j.jss.2018.01.038.

[19] Ivanov D, Dolgui A, Sokolov B. Ripple effect in the supply chain: definitions, frameworks and future research perspectives. In: Ivanov D, Dolgui A, Sokolov B. (eds.) *Handbook of Ripple Effects in the Supply Chain. International Series in Operations Research & Management Science, vol 276*. Springer, Cham; 2019. p.1-33. Available from: https://doi.org/10.1007/978-3-030-14302-2_1.

[20] Zhang Q, Jin T, Cai J, Xu L, He T, Wang, T, et al. Wearable triboelectric sensors enabled gait analysis and waist motion capture for IoT-based smart healthcare applications. *Advanced Science*. 2022; 9(4): 2103694.

[21] Farshidi S, Jansen S, España S, Verkleij J. Decision support for blockchain platform selection: Three industry case studies. *IEEE Transaction Engineering Management*. 2020; 67(14): 1109-1128. Available from: https://doi.org/10.1109/TEM.2019.2956897.

[22] Dubey A, Gupta R, Chandel GS. An efficient partition technique to reduce the attack detection time with web based text and pdf files. *International Journal of Advance Computing Research*. 2013; 3(1): 9.

[23] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *IEEE Access*. 2016; 4: 2292-2303.

[24] Liang Z, Zhou R, Zhang L, Li L, Huang G, Zhang Z, et al. EEGFuseNet: Hybrid unsupervised deep feature characterization and fusion for high-dimensional EEG with an application to emotion recognition. *IEEE Transactions Neural System Rehabilitation Engineering*. 2021; 29(3): 1913-1925.

[25] Smith KJ, Dhillon G. Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managing Financial*. 2019; 46(6): 833-848.

[26] Cai T, Zhou Y, Zheng H. Cost-quality adaptive active learning for chinese clinical named entity recognition. *Proc-2020 IEEE Int Conf Bioinforma Biomed BIBM 2020*. 2020; 4(2): 528-533.

[27] Zheng Z, Xie S, Dai HN, Chen W, Chen X, Weng J, et al. An overview on smart contracts: Challenges, advances and platforms. *Future General Computing System*. 2020; 105: 475-491.

[28] Meijin L, Zhiyang F, Junfeng W, Luyu C, Qi Z, Tao Y, et al. A systematic overview of android malware detection. *Appl Artificial Intelligence*. 2022; 36(1): 2007327. Available from: https://doi.org/10.1080/08839514.2021.2007327.

[29] Goscinski A, Delicato FC, Fortino G, Kobusińska A, Srivastava G. Special issue on distributed intelligence at the edge for the future internet of things. *J Parallel Distrib Comput*. 2023; 171: 157-162.

[30] Leka E, Selimi B, Lamani L. Systematic literature review of blockchain applications: smart contracts systematic literature review of blockchain applications: Smart contracts. *Proceeding 2019 IEEE International Conference of Information Technology*. 2020; 19: 1-4.

[31] Huang S, Lin C, Xu W, Gao Y, Feng Z, Zhu F. Identification of active attacks in internet of things: Joint model- and data-driven automatic modulation classification approach. *IEEE Internet Things Journal*. 2021; 8(3): 2051-2065.

[32] Alaba FA, Jegede A, Eke CI. Robust data security framework for IoT. *IJAMML*. 2020; 1: 5-23.

[33] Alaba FA. Ransomware attacks on remote learning systems in 21st century: A survey. *Biomedical Journal of Scientific & Technical Research*. 2021; 35(1): 27322-27330. Available from: https://doi.org/10.26717/BJSTR.2021.35.005649.

[34] Akin Y, Dikkollu C, Kaplan BB, Yayan U, Yolacan EN. Ethereum blockchain network-based electrical vehicle charging platform with multi-criteria decision support system. *2019 1st International Informatics and Software Engineering Conference (UBMYK)*. Ankara, Turkey: IEEE; 2019. p.1-5. Available from: https://doi.org/10.1109/UBMYK48245.2019.8965557.

[35] Khader R, Eleyan D. Survey of DoS/DDoS attacks in IoT. *Sustainable Engineering Innovation*. 2021; 3(1): 23-28.

[36] Takahashi K. Blockchain and smart contract for contract management (dispute prevention and generation). *IEEE Access*. 2019; 2: 2-12.

[37] Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE Access*. 2020; 8: 118433-118471.

[38] Beillahi SM, Ciocarlie G, Emmi M, Enea C. Behavioral simulation for smart contracts. *Proc ACM SIGPLAN Conference Program Langauge Implemention*. 2020; 20(4): 470-486.

[39] Lu Y. Blockchain and the related issues: A review of current research topics. *Journal of Managemnet Analysis*. 2018; 5(4): 231-255.

[40] Ng G, Cheuk H, Singh S, Sharma B. Amalgamation of smart AIoT based construction site monitoring with robotics: viAct's extended horizon. *International Journal of Research in Engineering and Science*. 2021; 9(10): 24-

27.

[41] Fadele AA, Othman M, Hashem IAT, Alotaibi F. Internet of things security: A survey. *Journal Networks Computer Application*. 2017; 88: 10-28.

[42] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: Platforms, applications, and design patterns. *IEEE Communication Survey Tutorials*. 2021; 2(6): 1-16.

[43] Biswas A, Roy A. *Blockchain and Ipfs Based Secure Cloud Banking System Using Smart Card*. Research Square preprint; 2022. p.1-34. Available from: https://doi.org/10.21203/rs.3.rs-1684189/v1.

[44] Panoff M, Dutta RG, Hu Y, Yang K, Jin Y. On sensor security in the era of IoT and CPS. *SN Computer Science*. 2021; 2(1): 1-14. Available from: https://doi.org/10.1007/s42979-020-00423-5.

[45] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on Blockchain technology?-A systematic review. *PLoS One*. 2016; 11(10): 1-27.

[46] Eze P, Eziokwu T, Okpara C. A triplicate smart contract model using blockchain technology. *Circuit Computer Science*. 2017; 201(1): 1-10. Available from: https://doi.org/10.22632/ccs-2017-cps-01.

[47] Bayhan S, Zubow A, Gawlowicz P, Wolisz A. Smart contracts for spectrum sensing as a service. *IEEE Transactions on Cognitive Communications and Networking*. 2019; 5(3): 1-13. Available from: https://doi.org/10.1109/TCCN.2019.2936190.

[48] Lutz O, Chen H, Sendner C, Mar CR. *ESCORT: Ethereum Smart COntRacTs Vulnerability Detection using Deep Neural Network and Transfer Learning, Vol. 1*. Woodstock '18: ACM Symposium on Neural Gaze Detection, Woodstock, NY. Association for Computing Machinery; 2017.

[49] Anjum A, Ahmed T, Khan A, Ahmad N, Ahmad M, Asif M, et al. Privacy preserving data by conceptualizing smart cities using MIDR-Angelization. *Sustain Cities Soc*. 2018; 40: 326-334.

[50] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future General Computing System*. 2018; 82: 395-411.

[51] Tao Y, Li B, Jiang J, Ng HC, Wang C, Li B. On sharding open blockchains with smart contracts. *2020 IEEE 36th International Conference on Data Engineering (ICDE)*. Dallas, TX, USA: IEEE; 2020. p.1357-1368. Available from: https://doi.org/10.1109/ICDE48307.2020.00121.

[52] Ahmadjee S, Bahsoon R. Assessing smart contracts security technical debts. *IEEE Communication Survey Tutorials*. 2021; 3(3): 1-10.

[53] Zhang Z, Guo B, Shen Y, Li C, Suo X, Su H. Nakamoto consensus to accelerate supervised classification algorithms for multiparty computing. *Secure Communication Networks*. 2021; 8(3): 1-11. Available from: https://doi.org/10.1155/2021/6629433.

[54] Norta A. Self-aware smart contracts with legal relevance. *IEEE Des Test Computing*. 2020; 3: 1-9.

[55] Leka E, Selimi B, Lamani L. Systematic literature review of blockchain applications: Smart contracts. *2019 International Conference on Information Technologies (InfoTech)*. Varna, Bulgaria: IEEE; 2019. p.19-20. Available from: https://doi.org/10.1109/InfoTech.2019.8860872.

[56] Agarwal R, Thapliyal T, Shukla SK. Vulnerability and transaction behavior based detection of malicious smart contracts. *IEEE Communication Management*. 2021; 4(2): 1-13.

[57] Parveen T, Arora HD, Alam M. Intuitionistic fuzzy shannon entropy weight based multi-criteria decision model with TOPSIS to analyze security risks and select online transaction method. In: Sharma H, Govindan K, Poonia R, Kumar S, El-Medany W. (eds.) *Advances in Computing and Intelligent Systems*. *Algorithms for Intelligent Systems*. Springer, Singapore; 2020. p.1-17. Available from: https://doi.org/10.1007/978-981-15-0222-4_1.

[58] Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Network Application*. 2021; 14: 2901-2925. Available from: https://doi.org/10.1007/s12083-021-01127-0.

[59] Su D, Liu J, Wang X, Wang W. Detecting android locker-ransomware on chinese social networks. *IEEE Access*. 2019; 7: 20381-20393.

[60] Egea M, Matteucci I, Mori P, Petrocchi M. Definition of data sharing agreements the case of Spanish Data Protection Law. *Lect Notes Comput Science*. 2015; 8937: 248-272. Available from: https://doi.org/10.1007/978-3-319-17199-9-11.

[61] Agrawal S, Vieira D. A survey on internet of things architectures. *Abakós, Belo Horiz*. 2013; 1(2): 78-95.

[62] Abdel-Basset M, Gamal A, Manogaran G, Son LH, Long HV. A novel group decision making model based on neutrosophic sets for heart disease diagnosis. *Multimedia Tools Application*. 2020; 79(15-16): 9977-10002.

[63] Martinez-Gil J, Pichler M, Beranič T, Brezočnik L, Turkanović M, Lentini G, et al. Framework for assessing the smartness maturity level of villages. *Communication Computer Information Science*. 2019; 1064: 501-512.

[64] Öztürk C, Yildizbaşi A. Barriers to implementation of blockchain into supply chain management using an

integrated multi-criteria decision-making method: A numerical example. *Soft Computing*. 2020; 24(19): 14771-14789.

[65] Denner MS, Püschel LC, Röglinger M. How to exploit the digitalization potential of business processes. *Business Information System Engineering*. 2018; 60(4): 331-349.

[66] Gourisetti SNG, Mylrea M, Patangia H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Futur Gener Computer System*. 2020; 105: 410-431. Available from: https://doi.org/10.1016/j.future.2019.12.018.

[67] Jafarzadeh S, Utne IB. A framework to bridge the energy efficiency gap in shipping. *Energy*. 2014; 69: 603-612.

[68] Meng Q, Zhang Y, Li Z, Shi W, Wang J, Sun Y, et al. A review of integrated applications of BIM and related technologies in whole building life cycle. *Engineering Construction Architectural Management*. 2020; 27(8): 1647-1677.

[69] Ries J, González-Ramírez RG, Voß S. Review of fuzzy techniques in maritime shipping operations. In: Bektaş T, Coniglio S, Martinez-Sykora A, Voß S. (eds.) *Computational Logistics. ICCL 2017. Lecture Notes in Computer Science, vol 10572*. Springer, Cham; 2017; p.253-269. Available from: https://doi.org/10.1007/978-3-319-68496-3_17.

[70] Lin Y-J, Chuang C-W, Yen C-Y, Huang S-H, Chen J-Y, Lee S-Y. An AIoT wearable ECG patch with decision tree for arrhythmia analysis. *2019 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. Nara, Japan: IEEE; 2019. p.1-4. Available from: https://doi.org/10.1109/BIOCAS.2019.8919141.

[71] Chen S, Su T, Fan L, Meng G, Xue M, Liu Y, et al. Are mobile banking apps secure? what can be improved? *ESEC/FSE 2018: Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. ACM Digital Library; 2018. p.797-802. Available from: https://doi.org/10.1145/3236024.3275523.

[72] Ding RX, Palomares I, Wang X, Yang GR, Liu B, Dong Y, et al. Large-scale decision-making: Characterization, taxonomy, challenges and future directions from an Artificial Intelligence and applications perspective. *Informative Fusion*. 2020; 59: 84-102.

[73] Cavalcante IM, Frazzon EM, Forcellini FA, Ivanov D. A supervised machine learning approach to data-driven simulation of resilient supplier selection in digital manufacturing. *International Journal of Information Management*. 2019; 49: 86-97. Available from: https://doi.org/10.1016/j.ijinfomgt.2019.03.004.

[74] Habbal A, Goudar SI, Hassan S. A context-aware radio access technology selection mechanism in 5G mobile network for smart city applications. *Journal of Networks Computer Application*. 2019; 135: 97-107. Available from: https://doi.org/10.1016/j.jnca.2019.02.019.

[75] Jain V, Al Ayub Ahmed A, Chaudhary V, Saxena D, Subramanian M, Mohiddin MK. Role of data mining in detecting theft and making effective impact on performance management. *Smart Innovation System Technology*. 2023; 290: 425-433.

[76] Moretto A, Grassi L, Caniato F, Giorgino M, Ronchi S. Supply chain finance: From traditional to supply chain credit rating. *Journal of Purch Supply Management*. 2019; 25(2): 197-217. Available from: https://doi.org/10.1016/j.pursup.2018.06.004.

[77] Ivanov D, Dolgui A. New disruption risk management perspectives in supply chains: Digital twins, the ripple effect, and resileanness. *IFAC-PapersOnLine*. 2019; 52(13): 337-342. Available from: https://doi.org/10.1016/j.ifacol.2019.11.138.

[78] Kamble SS, Gunasekaran A, Parekh H, Joshi S. Modeling the internet of things adoption barriers in food retail supply chains. *Journal Retail Consumer Service*. 2019; 48: 154-168. Available from: https://doi.org/10.1016/j.jretconser.2019.02.020.

[79] Sanjay Y, Singh DB, Arora PK, Kumar H. *Proceedings of International Conference in Mechanical and Energy Technology*. Springer Singapore; 2020. p.799. Available from: https://doi.org/10.1007/978-981-15-2647-3.

[80] Essakly A, Wichmann M, Spengler TS. A reference framework for the holistic evaluation of Industry 4.0 solutions for small-And medium-sized enterprises. *IFAC-PapersOnLine*. 2019; 52(13): 427-432. Available from: https://doi.org/10.1016/j.ifacol.2019.11.093.

[81] Vieira GG, Varela LR, Ribeiro RA. A knowledge based system for supporting sustainable industrial management in a clothes manufacturing company based on a data fusion model. *Lect Notes Business Information Process*. 2016; 250: 113-126.

[82] Hillbom E, Tillström T. *Applications of Smart-Contracts and Smart-Property Utilizing Blockchains*. Gothenburg, Sweden; 2016. p.51.

[83] Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. *Proceeeding ACM Conference Computer Communication Secure*. ACM Digital Library; 2016. p.254-269. Available from: https://doi.

org/10.1145/2976749.2978309.

[84] Raskin M. The law and legality of smart contracts. *1 Georgetown Law Technology Review*. 2017; 305: 205-207. Available from: http://dx.doi.org/10.2139/ssrn.2842258.

[85] Liao CF, Cheng CJ, Chen K, Lai CH, Chiu T, Wu-Lee C. Toward a service platform for developing smart contracts on blockchain in BDD and TDD styles. *2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA)*. Kanazawa, Japan: IEEE; 2017. p.133-140. Available from: https://doi.org/10.1109/SOCA.2017.26.

[86] Ramezan G, Leung C. A blockchain-based contractual routing protocol for the internet of things using smart contracts. *Wirel Commun Mob Comput*. 2018; 2018: 1-14.

[87] Jo BW, Khan RMA, Lee YS. Hybrid blockchain and internet-of-things network for underground structure health monitoring. *Sensors*. 2018; 18(12): 4268. Available from: https://doi.org/10.3390/s18124268.

[88] Voelter M. The design, evolution, and use of kernelf: An extensible and embeddable functional language. In: Rensink A, Sánchez Cuadrado J. (eds.) *Theory and Practice of Model Transformation. ICMT 2018. Lecture Notes in Computer Science, vol 10888*. Springer, Cham; 2018. p.3-55 Available from: https://doi.org/10.1007/978-3-319-93317-7_1

[89] Leka E, Selimi B, Lamani L. Systematic literature review of blockchain applications: Smart contracts. *2019 International Conference Information Technology 2019-Proceeding*. Varna, Bulgaria: IEEE; 2019. Available from: https://doi.org/10.1109/InfoTech.2019.8860872.

[90] Sharma A, Sarishma, Tomar R, Chilamkurti N, Kim BG. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electron*. 2020; 9(10): 1-14.

[91] Vivar AL, Castedo AT, Lucila A, Orozco S, Javier L, Villalba G. Smart contracts: A review of security threats alongside an analysis of existing solutions. *MDPI-Entropy*. 2020; 5(7): 1-29.

[92] Gong S, Lee C. BLOCIS: Blockchain-based cyber threat intelligence sharing framework for sybil-resistance. *Electronics*. 2020; 9(3): 521. Available from: https://doi.org/10.3390/electronics9030521.

[93] Vacca A, Di Sorbo A, Visaggio CA, Canfora G. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *J Syst Softw*. 2021; 174: 110891. Available from: https://doi.org/10.1016/j.jss.2020.110891.

[94] Chen X, Luo J, Xia X, Chen J, Luo X, Yang X, et al. Smart contract security: A practitioners' perspective. *IEEE Access*. 2021; 5(12): 12-23. Available from: https://ink.library.smu.edu.sg/sis_research.

[95] Hilal AA, Badra M, Tubaishat A. Building smart contracts for COVID19 pandemic over the blockchain emerging technologies. *Procedia Computer Science*. 2021; 198: 323-328. Available from: https://doi.org/10.1016/j.procs.2021.12.248.

[96] Gonzalez-Amarillo C, Cardenas-Garcia C, Mendoza-Moreno M, Ramirez-Gonzalez G, Corrales JC. Blockchain-iot sensor (Biots): A solution to iot-ecosystems security issues. *Sensors*. 2021; 21(13): 1-22.

[97] Qian P, Liu ZG, He QM, Huang BT, Tian DZ, Wang X. Smart contract vulnerability detection technique: A survey. *Ruan Jian Xue Bao/Journal Softw*. 2022; 33(8): 3059-3085.

[98] Zhang W. Beak: A directed hybrid fuzzer for smart contracts. *International Core Journal of Engineering*. 2022; 8(4): 480-498.

[99] Ye X, Zeng N, König M. Systematic literature review on smart contracts in the construction industry: Potentials, benefits, and challenges. *Front Engineeering Management*. 2022; 9(2): 196-213.

[100]Kushwaha SS, Joshi S, Singh D, Kaur M, Lee HN. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access*. 2022; 10: 6605-6621.

[101]Alhabardi FF, Beckmann A, Lazar B, Setzer A. *Verification of Bitcoin Script in Agda Using Weakest Preconditions for Access Control*. Leibniz International Proceeding Informatics, LIPIcs; 2022. p.239. Available from: https://doi.org/10.4230/LIPIcs.TYPES.2021.1.

[102]Uddin MA, Stranieri A, Gondal I, Balasubramanian V. Blockchain leveraged decentralized IoT eHealth framework. *Internet of Things*. 2020; 9: 100159.

[103]Karoui K, Ftima FB. New engineering method for the risk assessment: Case study signal jamming of the m-health networks. *Mobile Networks Application*. 2018; 26(4): 2525-2544. Available from: https://doi.org/10.1007/s11036-018-1098-8.

[104]Chen RY. A traceability chain algorithm for artificial neural networks using T-S fuzzy cognitive maps in blockchain. *Futur Gener Computer System*. 2018; 80: 198-210. Available from: https://doi.org/10.1016/j.future.2017.09.077.

[105]Sun M, Zhang J. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Computer Communication*. 2020; 149: 332-342. Available from:

https://doi.org/10.1016/j.comcom.2019.10.031.

[106]Shit PK, Adhikary PP, Sengupta D, Habib A. Spatial modeling and assessment of environmental contaminants. *Risk Assessment and Remediation*. Springer Cham; 2021. Available from: https://doi.org/10.1007/978-3-030-63422-3.

[107]Alouache L, Nguyen N, Aliouat M, Chelouah R. Credit based incentive approach for V2V cooperation in vehicular cloud computing. In: Skulimowski A, Sheng Z, Khemiri-Kallel S, Cérin C, Hsu CH. (eds.) *Internet of Vehicles. Technologies and Services Towards Smart City. IOV 2018. Lecture Notes in Computer Science, vol 11253*. Springer, Cham; 2018. p.92-105 Available from: https://doi.org/10.1007/978-3-030-05081-8_7.

[108]Zhang A, Zhong RY, Farooque M, Kang K, Venkatesh VG. Blockchain-based life cycle assessment: An implementation framework and system architecture. *Resources Conservation Recycle*. 2020; 152: 104512. Available from: https://doi.org/10.1016/j.resconrec.2019.104512.

[109]Luthra S, Garg D, Mangla SK, Singh Berwal YP. Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context. *Procedia Computer Science*. 2018; 125: 733-739.

[110]Goh E, Sigala M. Integrating Information & Communication Technologies (ICT) into classroom instruction: teaching tips for hospitality educators from a diffusion of innovation approach. *Journal Teaching Travel Tour*. 2020; 20(2): 156-165. Available from: https://doi.org/10.1080/15313220.2020.1740636.

[111]Cayirci E, de Oliveira AS. Modelling trust and risk for cloud services. *Journal of Cloud Computing*. 2018; 7(1): 14. Available from: https://doi.org/10.1186/s13677-018-0114-7.

[112]Khaqqi KN, Sikorski JJ, Hadinoto K, Kraft M. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Appl Energy*. 2018; 209: 8-19. Available from: http://dx.doi.org/10.1016/j.apenergy.2017.10.070.

[113]Modgil S, Sonwaney V. Planning the application of blockchain technology in identification of counterfeit products: Sectorial prioritization. *IFAC-PapersOnLine*. 2019; 52(13): 1-5. Available from: https://doi.org/10.1016/j.ifacol.2019.11.080.

[114]Alexander J, Smith DAE, Ehlers Smith YC, Downs CT. Drivers of fine-scale avian functional diversity with changing land use: an assessment of the effects of eco-estate housing development and management. *Landsc Ecology*. 2019; 34(3): 537-549. Available from: https://doi.org/10.1007/s10980-019-00786-.

[115]Pokrovskaia NN. Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation. *Proceeding 2017 20th IEEE International Conferferenc Soft Computing Meas SCM 2017*. St. Petersburg, Russia: IEEE; 2017. p.709-712. Available from: https://doi.org/10.1109/SCM.2017.7970698.

[116]van de Kaa G, Janssen M, Rezaei J. Standards battles for business-to-government data exchange: Identifying success factors for standard dominance using the Best Worst Method. *Technology Forecast Social Change*. 2018; 137: 182-189. Available from: https://doi.org/10.1016/j.techfore.2018.07.041.

[117]Kumar A, Kumar S. Secured ethereum transactions using smart contracts & solidity. *Ymer*. 2022; 21(5): 432-442.

[118]Patil PD, Mhatre DJ, Gharat NH, Tinsu J. Transparent charity system using smart contracts on ethereum using blockchain. *International Jurnal of Reseach Application Science Engineering Technology*. 2022; 10(4): 743-748.

[119]Azzopardi S, Ellul J, Falzon R, Pace GJ. Tainting in smart contracts: Combining static and runtime verification. *IEEE Access*. 2022; 23: 143-161.

[120]Liu Y, Zhou Z, Yang Y, Ma Y. Verifying the smart contracts of the port supply chain system based on probabilistic model checking. *Systems*. 2022; 10(1): 19. Available from: https://doi.org/10.3390/systems10010019.

[121]Zhang L, Li Y, Jin T, Wang W, Jin Z, Zhao C, et al. SPCBIG-EC: A robust serial hybrid model for smart contract vulnerability detection. *Sensors*. 2022; 22(12): 4621. Available from: https://doi.org/10.3390/s22124621.

[122]Castell E, Berman I, Kapitonov A, Manaenko V, Chernyaev M, Tarasov P, et al. Self-employment for autonomous robots using smart contracts. *ACM Computer Survey*. 2022; 4(12): 12-23.

[123]Zhang L, Chen W, Wang W, Jin Z, Zhao C, Cai Z, et al. CBGRU: A detection method of smart contract vulnerability based on a hybrid model. *Sensors*. 2022; 22(9): 3577. Available from: https://doi.org/10.3390/s22093577.

[124]Gilani K, Ghaffari F, Bertin E, Crespi N. Self-sovereign identity management framework using smart contracts. *Proceeding IEEE/IFIP Networks Operation Management Symposium 2022 Networks Service Management Era Cloudification, Softwarization Artificial Intelligent NOMS 2022*. Budapest, Hungary; 2022. p.1-7.

[125]Ndiaye M, Konate K. Security strengths and weaknesses of blockchain smart contract system: A survey. *Intional Journal Information Communication Engineering*. 2022; 16: 1-11. Available from: https://www.researchgate.net/publication/360624196.

[126]Yadav JS, Yadav NS, Sharma AK. Security analysis of smart contract based rating and review systems: The

perilous state of blockchain-based recommendation practices. *Connectivity Science*. 2022; 34(1): 1273-1298. Available from: https://doi.org/10.1080/09540091.2022.2066065.

[127]Sivakumar E, Chawla P. Correction to: Role-based smart contract: An intelligent system for scholarly communication. *SN Computer Science*. 2022; 3(4): 1-3. Available from: https://doi.org/10.1007/s42979-022-01201-1.

[128]Khan KM, Zahid A. Empirical analysis of vulnerabilities in blockchain-based smart contracts. *Journal of Engineering Technol*. 2022; 12(1): 78-85.

[129]Samreen NF, Alalfi MH. *VOLCANO: Detecting Vulnerabilities of Ethereum Smart Contracts Using Code Clone Analysis*. arXiv:2203.00769 [cs.CR]. 2022. Available from: http://arxiv.org/abs/2203.00769.

[130]Rameder H, di Angelo M, Salzer G. Review of automated vulnerability analysis of smart contracts on ethereum. *Front Blockchain*. 2022; 5: 1-20.

[131]Khan AA, Laghari AA, Gadekallu TR, Shaikh ZA, Javed AR, Rashid M, et al. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. *Computing Electronics Engineering*. 2022; 102: 108234. Available from: https://doi.org/10.1016/j.compeleceng.2022.108234.

[132]Steffen S, Bichsel B, Baumgartner R, Vechev M. ZeeStar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. *Proceeing-IEEE Symposium Security Privacy*. IEEE; 2022. p.179-197.

[133]Gibaja-Romero DE, Cantón-Croda RM. Auction and classification of smart contracts. *Mathematics*. 2022; 10(7): 1-18.

[134]Olsthoorn M, Stallenberg D, Van Deursen A, Panichella A. SynTest-solidity: Automated test case generation and fuzzing for smart contracts. *2022 IEEE/ACM 44th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*. Pittsburgh, PA, USA: IEEE; 2022. p.202-206. Available from: https://doi.org/10.1145/3510454.3516869.