Journal of Informatics and Web Engineering
Vol. 4 No. 1 (February 2025) eISSN: 2821-370X

Comprehensive Insights into Smart Contracts: Architecture, Sectoral Applications, Security Analysis, and Legal Frameworks

Farah Mazlan[1], Nur Faizah Omar[2], Nik Nor Muhammad Saifudin Nik Mohd Kamal[3], Ahmad Anwar Zainuddin[4*]

[1,2,3,4]Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Malaysia

**corresponding author: (anwarzain@iium.edu.my; ORCiD: 0000-0001-6822-0075)*

Abstract - Most conventional contract systems have issues with middlemen, drawn-out implementation procedures, fraud risk, and human error. Considering this, the project uses smart contract technology to provide a decentralized, automated, and safe solution in an effort to address such inefficiencies and the trust issues they raise. Smart contracts enable self-execution of contracts whose conditions are expressed explicitly in lines of code by presenting solutions using blockchain technology. The concept behind a smart contract is that each party may carry out their portion of the duties without depending on a third party and the contract will automatically execute in the meantime. This automation significantly reduces transaction costs while simultaneously improving security and transparency. With the use of this underlying technology, smart contracts may be used to directly code parties' compliance with their duties under the agreement and the blockchain will keep an immutable record of every transaction. For smooth and dependable transactions, smart contracts offer a dependable and effective substitute for conventional contract methods. Furthermore, integrating smart contracts with cutting-edge technologies like machine learning and artificial intelligence could improve decision-making and accelerate operations in a variety of sectors. Their application extends beyond financial transactions to areas such as supply chain management, energy trading, and healthcare, showcasing their versatility. Despite these advantages, issues like energy consumption, scalability, and regulatory compliance still need creative solutions. Ongoing research and development aim to address these issues, fostering the evolution of smarter, more sustainable contract systems. By leveraging these advancements, smart contracts keep opening the door for a revolution in the digital economy that will increase productivity and confidence.

Keywords—Smart Contracts, Blockchain Technology, Decentralization, Automation, Security and Transparency, Immutable Record.

Received: 13 July 2024; Accepted: 13 November 2024; Published: 16 February 2025

Journal of Informatics and Web Engineering
https://doi.org/10.33093/jiwe.2025.4.1.1

Published by MMU Press. URL: https://journals.mmupress.com/jiwe

1. INTRODUCTION

In the era of rapid evolution primarily in the digital field, smart contract technology is a game changer. This evolution has captured significant interest with its potential to leave a huge impact on industries [1]. Smart contracts which are based on blockchain technology have evolved from an abstract idea to a powerful tool capable of transforming a variety of businesses.

Smart contracts are blockchain-based executable algorithms that automate and enforce agreement terms when certain criteria are met. These agreements aim to increase commercial process automation and effectiveness [2]. The global smart contract market was estimated to be USD 190.34 million in 2022 and is expected to grow at a CAGR of 24.2% over the forecast period (2024-2031), rising from USD 236.40 million in 2023 to USD 1338.52 million by 2031 [3], [4]. The expected technological benefits of implementing blockchain-enabled smart contracts to improve project efficiency and effectiveness influence their use in construction projects [5], [6].

Long before blockchain technology was developed, in the mid-1990s, computer scientist and cryptographer Nick Szabo initially put out the idea of smart contracts [7], [8], [9]. Szabo imagined a digital protocol that would allow contracts to be automatically carried out, with the conditions of the contract being incorporated in the code itself [10], [11]. Up to the development of blockchain technology, which offered the decentralized and safe framework required for the implementation of such automated contracts, this concept remained mostly theoretical.

Smart contracts are self-executing agreements where the provisions are expressly written into code. A blockchain network is used to implement these contracts, most notably Ethereum and other platforms that were created expressly to support smart contracts. By eliminating the need for middlemen and drastically minimizing the danger of fraud, the decentralized nature of blockchain guarantees the transparency and immutability records of these contracts [12], [13].

This paper is arranged as follows; Section 1 gives a brief introduction to the implementation of smart contract technology and blockchain. Section 2 summarizes the literature review for this work. Section 3 covers the architecture of smart contract technology and its applications, as well as the strengths and weaknesses of smart contracts and the difficulties in putting them into practice. Section IV presents several suggestions for improving it. Finally, Section V puts the idea of smart contract technology to a close.

2. LITERATURE REVIEW

The research on smart contract technology from a variety of articles has been shown in Table 1. It shows an overview of the existing literature on smart contract technology.

Table 1. Literature Review

Article	Key Findings/ Arguments	Supporting Evidence/ Sample Characteristics/ Methods	Strengths/ Limitations
[14]	The article gives a general introduction of smart contracts by outlining the difficulties they encounter, new developments in their field, and the many blockchain platforms that facilitate them. It highlights platform features and enhancements as well as security and scalability concerns.	The authors' findings are supported by case studies, a comparison of smart contract platforms, and a survey of literature. This method offers a thorough comprehension of the technology and its uses.	The article provides a thorough review of smart contracts, offering detailed insights into various platforms and advancements, but its findings may quickly become outdated due to the fast-paced nature of technological progress and could overlook some emerging aspects.
[15]	The article discusses that Blockchain technology automates and enforces agreements through the smart contract, therefore revolutionizing	The research involves a legal analytical approach to evaluate how smart contracts affect conventional contract law by presenting several	The article discusses that Blockchain technology automates and enforces agreements through the smart contract, therefore

	modern contract law. It states further that even though Smart contracts reduce costs and increase efficiency, they pose new challenges on the interpretation and enforcement of the law.	case studies, theoretical frameworks, and previously published research.	revolutionizing modern contract law. It states further that even though Smart contracts reduce costs and increase efficiency, they pose new challenges on the interpretation and enforcement of the law.
[16]	This research paper presents Vandal, a tool developed to perform large-scale security analyses of smart contracts. The study shows that Vandal is able to handle in-depth analyses and detect possible vulnerabilities in smart contracts.	The authors show, through benchmark tests and case studies pertaining to smart contracts, that Vandal works effectively. They present comparisons with other security analysis tools for discussing accuracy and scalability.	Vandal is also valued for its scalability and its track record of successfully identifying security flaws in smart contracts. However, in order to make sure it performs well, this tool still needs more thorough testing on a variety of real- world scenarios. Additionally, its heuristics might not identify all potential vulnerabilities.
[17]	The article discuss on how smart contract automation and decentralized coordination might be used by blockchain technology to enhance resource sharing and increase efficiency in local energy communities.	From the article, it says that the supporting evidence shows that smart contract technology can demonstrate practical implementation, technical results, and give community configuration.	The strengths of the article lie in its practical implementation, demonstration of efficiency improvements and commitment to open-source principles.
[18]	The article stated that the basic form of smart contract security model can demonstrate the potential for applications utilizing smart contracts across multiple blockchain networks.	This smart contract security system presents a contemporizing mechanism that makes certain valid states are applied and utilizes transition confirmations based on multi- proofs.	Even though smart contract technology security is a good system it still has its own limit. The limitation is the vulnerability of host systems,and the security risks posed by a small number of nodes in charge.
[19]	The article argues that while smart contracts could automate and simplify contracts, there are still some issues that need to be addressed before they can be widely used in business partnerships.	Arizona has incorporated blockchain technology and smart contracts into its legal framework: the subjects explain how these technologies work on platforms like Ethereum and talk about their legal approval.	The article argues that while smart contracts could automate and simplify contracts, there are still some issues that need to be addressed before they can be widely used in business partnerships.
[20]	The article delves into smart contract technology and its many uses, emphasizing how it is safe and efficient transactions have the ability to revolutionize a variety of industries. It follows the development of blockchain technology and shows how smart contracts increase operational efficacy, reduce costs, and promote transparency.	Examines scholarly literature on smart contracts methodically, examining use cases, frameworks, and technical developments. It provides examples from the supply chain, legal, and financial sectors to demonstrate real-world applications.	The article delves into smart contract technology and its many uses, emphasizing how it is safe and efficient transactions have the ability to revolutionize a variety of industries. It follows the development of blockchain technology and shows how smart contracts increase operational efficacy, reduce costs, and promote transparency.
[21]	The article discusses that smart contract technology facilitates and enforces contract performance by offering security, automation, and transparency. However, they also	Demonstrate how well they work to automate processes and save money. It addresses the legal concerns with traditional frameworks and emphasizes the need for good coding	Outlining the benefits and drawbacks while closely analyzing the technical and legal components. However, experts would find technical analysis too imprecise,

	come with disadvantages like hard-to-enforce laws, complex coding, rigidity in handling unforeseen situations, and security holes.	practices to avoid vulnerabilities and other difficulties.	and its study of legal systems lacks specific examples.
[22]	The article discusses how supply chain management and finance could be completely transformed by smart contracts because of their transparent and decentralized character. It emphasizes how enabling safe, open, and unchangeable transactions can result in more reliable and effective systems.	Reviewing studies and analyzing various smart contract uses, exploring consensus methods like Proof of Work (PoW) and Proof of Stake (PoS) and weighing the benefits and downsides of each. They demonstrate the real benefits and challenges of integrating the technologies with case studies from the IoT, healthcare, and finance sectors.	Provides detailed analyses and varied examples to assist audiences understand its consequences and advantages. However, individuals who are not familiar with smart contract technology or computer science may find it difficult to understand due to its technical complexity, and as the subject is developing quickly, information may become out of date as new developments occur
[23]	Automated smart contracts improve efficiency and dependability by decreasing mistakes and boosting operational effectiveness. Alongside blockchain technology ensures secure and immutable transactions, which promotes confidence in decentralized apps.	Decentralized ledgers are used by blockchain technology for ensuring the immutability and transparency of transactions, meanwhile Chain-link provides real-time data to smart contracts so they can react to outside events and carry out predetermined conditions.	Chain link's assistance with several blockchains promotes flexibility where smart contracts offer for the efficient management of high transaction volumes. This technology opens up new possibilities in supply chain management, insurance, banking, and other industries.
[24]	The article argues that by improving the productivity, confidence, and accountability of managing digital rights, blockchain technology and smart contracts have the potential to completely transform copyright licensing.	Using tokenized element registries, smart contracts may automate and standardize a range of copyright-related processes that can facilitate payment processes and grant permission for the use and exploitation of data protected by copyright.	With the use of actual cases, this research explores the possibilities of blockchain technology for copyright licenses. However, because the technology is still in its infancy, there has not been much large- scale adoption, and a lot of important legal and regulatory issues need to be thoroughly investigated.
[25]	The article talked about enhancing security and trust results of supply chains using blockchain technology. Agreements are revolutionized by smart contracts, but they also present special security issues. Taxonomy of security application for smart contracts facilitates the identification and remediation of vulnerabilities.	Using integrated Decision- Making Trial and Evaluation Laboratory (DEMATEL) and Interpretive Structural Modelling (ISM) techniques, obstacles to IoT adoption are identified. Primary Component Analysis (PCA) and fuzzy decision-making are used in this evaluation of how blockchain technology can be used to manage long-term supply chains effectively (DEMATEL).	Development of taxonomy is to tackle the vulnerabilities for smart contract security applications. Exploration of potential futures in which blockchain technology does not require smart contract functionality.
[26]	Due to the limited interactivity, inflexibility with errors and risks of ordinary users controlling data directly, usability issues arise. Security vulnerabilities such as reentrancy attacks, transaction-ordering dependence, and mishandled	Smart contracts are used for clearing and settlement, integration with Know Your Customer and Anti-money Laundering policies, and protection against attacks.	Due to the limited interactivity, inflexibility with errors and risks of ordinary users controlling data directly, usability issues arise. Security vulnerabilities such as reentrancy attacks, transaction-ordering dependence, and

	exceptions, leading to significant financial losses.		mishandled exceptions, leading to significant financial losses.
[27]	This article discusses the security design challenges including the extraction of security patterns from vulnerabilities, the inefficiency of FSM based approaches, and the need for logic-based approaches to mitigate vulnerabilities. The implementation of safety measures focuses on integrating security libraries such as OpenZeppelin, developing high level domain specific languages and guaranteeing formal verification	Weaknesses in smart contracts due to particular language, features of the Blockchain Platform and misunderstandings about common practice. A software lifecycle approach to smart contract security, including vulnerability detection, security modeling, monitoring and bug bounty.	Detailed analysis of security implementation, security design challenges, and testing before deployment in smart contract security. Identification of vulnerabilities in specific languages, misunderstanding of common practices in smart contracts, and features of the blockchain platform in smart contracts.
[28]	The article identifies and proposes a set of 20 Software Design PatternsSDPs as solutions to identified problems in smart contract development, focusing on performance, security, maintainability and functionality. In order to ensure the relevance and applicability of the identified problems and solutions across different distributed ledger technologies, such as Ethereum, EOSIO and Hyperledger Fabric, through expert interviews.	In order to identify existing problems and solutions and to validate the findings of the literature reviews and to gather further information, two rounds of comprehensive literature reviews were carried out and nine semi structured interviews with DLT experts were conducted. Thematic analysis was used to refine and categorize challenges and solutions that lead to the identified of 13 high-level and 3 principal challenges.	The study considers multiple DLTs with a view to improving the generalizability of results. However, the applicability of these findings to other DLTs, such as Ethereum, EOSIO and Hyperledger Fabric, remains unclear.

3. RESEARCH METHODOLOGY

This research methodology based on literature reviews will investigate smart contract technology by looking at its architecture, practical applications in various industries, and security and vulnerability analysis. It will also investigate how smart contracts increase the optimization and efficiency of blockchain systems while addressing compliance and legal issues.

3.1 The Architecture of Smart Contract Technology

Figure 1 shows the smart contract technology architecture. There are four parts in technology that will be discussed in this section. Those four parts of architecture are important to design and build smart contract technology because each part plays its role together. Those parts are Smart Contract Layer, Token Layer, Protocol Layer, and Application Layer [29].

3.1.1 Smart Contract Layer

Smart contract is defined as a program that can self-execute and automate any action by itself which is in the smart contract technology, they have their own blockchain that helps the programmed function automatically [30]. This process is called blockchain transaction which will send and receive each process or step in the smart contract technology and track all the data.

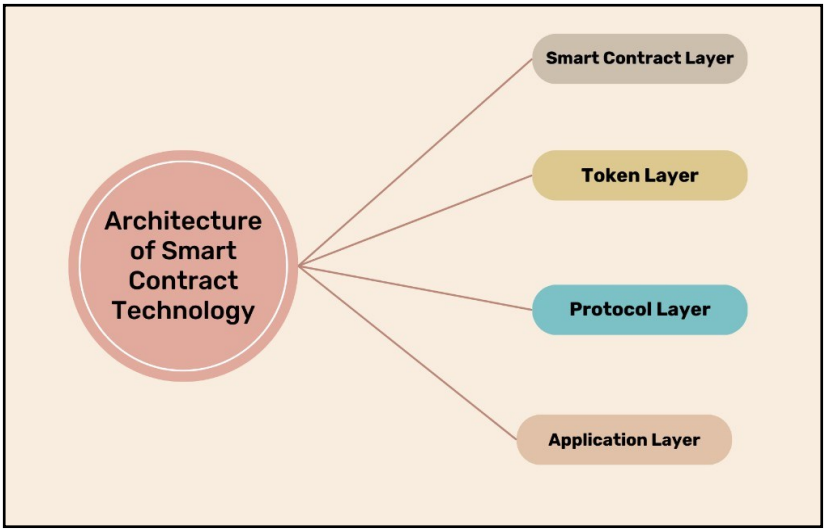

Figure 1. Architecture of Smart Contract Technology Diagram

3.1.2 Token Layer

This layer is the second layer of smart contract architecture, and it is related to a program called Ethereum. This layer has lots of functionalities and it is at the top of smart contract architecture. However, the main function of the token layer is to focus on the scalability issue and transaction issues [31]. Token layer will fix these issues by moving the computational off from the blockchain. This layer will help to enhance the output and reduce the cost.

3.1.3 Protocol Layer

The protocol layer can be defined as a part within the blockchain network which is in the base network and secondary framework. The protocol layer also has a specific function in smart contract technology which is, it enables the modular design of blockchain and maintains each level of the layer in smart contract from getting malfunctioned [32]. Protocol layer is a model of set rules that can help the smart contract technology work in the way it supposed to be.

3.1.4 Application Layer

The application layer applies in every system including smart contract technology because it is a layer that will control the protocol layer such as FTP, HTTP, and SNMP [33]. This layer is also a component that authorizes the communication method between the data sent or received by the user. Even though the application is the last layer, it still relies on and needs support from other layers so it can send the correct data.

3.2 Practical Application in the Energy and Finance Sector

Smart contracts transform the energy and financial sectors in real-world applications. In the energy sector, they manage dispersed resources, streamline trade, and automate and secure transactions. Improving cash flow and risk

management, they support financial procedures such as supply chain finance and reverse factoring. Smart contracts improve productivity and cut expenses in various sectors by offering transparent and automated solutions.

3.2.1. Energy Sector

The energy sector is divided into four categories: Energy Market and Regulations (EMnR), Energy Management and Operations (EMnO), Business Models and Application (BMnA), and Smart Contract Technology (SCT).

Energy Market and Regulations (EMnR)

The Energy Market and Regulations (EMnR) focuses on the laws and regulations of the energy industry. It comprises Energy Policy and Governance, Energy Transactions and Market Mechanisms, and Market Design and Pricing Mechanisms. The Energy Policy and Governance encapsulates policies on energy security, efficiency, and renewable energy; the Energy Transactions and Market Mechanisms go into the trading methods such as spot and futures markets and what roles different players have in the market—for instance, the producers and the suppliers. The Market Design and Pricing Mechanisms go deep into how energy markets are structured, pricing strategies, and price-capping tools.

Energy Management and Operations (EMnO)

Energy Management and Operations (EMnO) is related to the ways in which energy systems can be managed in practice. This category includes Grid Management and Balancing, Demand Response and Energy Flexibility as well as the Asset Administration and Maintenance. Grid Management and Balancing ensure reliability and stability of the energy where supply is the main intervening factor while Demand Response & Energy Flexibility correlate the consumption with respect of supply alterations. The Asset Administration and Maintenance ensures the good status of the energy asset-related structures.

Business Models and Applications (BMnA)

Business Models and Application (BMnA) focuses on utilization of smart contract technology to add value to the customers in the energy sector. The elements like Energy as a Service (EaaS), Peer-to-Peer Energy Trading (P2P), Virtual Power Plants (VPP), and Carbon Credits Exchange are included in it. EaaS allows the use of renewable energy sources as a service while P2P allows the generation to be passed directly to any energy users. VPP helps in the coalescence of diverse energy sources to produce one system, and Carbon Credits Exchange brings about the trading of carbon credits to reach the objectives of sustainability.

Smart Contract Technology (SCT)

Smart Contract Technology (SCT) is the foundation of blockchain platforms like Ethereum and smart contracts. It includes Technological Framework, DApps, and any other blockchain platform that has been deployed in the energy sector. A Technological Framework, on the other hand, focuses on those systems and components needed for developing smart contracts while DApps are themselves applications developed top of blockchains, which rely heavily on smart contracts to achieve a core functionality.

3.2.2. Finance Sector

The finance sector is divided into two categories: Supply Chain Finance (SCF) and Reverse Factoring (RF).

Purpose of Supply Chain Finance (SCF)

Supply Chain Finance (SCF) is a financing system by financial institutions to connect a buyer with its suppliers, aimed at achieving an effective and efficient chain of working capital or cash flow finances within the chain. This is done using highly evolved financial instruments in conjunction with smart contracting technology. SCF, thus, benefits buyers and suppliers since it avails very short-term loans hence reducing the cost of borrowing, boosting the working capital, while enhancing efficiency that is pragmatic to the total operations of doing business.

Reverse Factoring (RF)

Introduction Reverse Factoring (RF) is a supply chain finance technique based on third-party involvement, because through it the suppliers were able to get paid their invoices before they became due. While the manufacturer may not have a solid financial history or sufficient collateral, the buyers themselves are creditworthy and initiate bank guarantees. Good money management enables one to cut costs while using this technique. This also reduces supplier risk by allowing the facilitation of credit risk from suppliers to buyers who have a higher degree of financial stability.

3.3 Comparative Security and Vulnerability Analysis of Conventional Systems and Smart Contracts

The objectives of conventional security and smart contract security are quite different. Conventional security protects the existing systems that are basically comprised of computer networks and software applications from threats due to malware infection, hacking attacks, or data breaches. Smart contract security focuses on the need to ensure the code is free of bugs or free from vulnerabilities, which in turn may lead to financial losses or surprises of any kind.

In conventional methodologies, various security strategies rely on firewalls, encryption, and strong passwords to keep data and systems secure. On the other hand, security in smart contracts relies on a blockchain environment which are programming codes used to secure the contracts themselves by autonomously executing and enforcing an agreement if certain specified conditions are met.

Figure 2 illustrates the concept of conventional security, showcasing the strategies and practices applied in general to protect resources, data, and individuals from threats including theft, damage, espionage, or unauthorized access. Security measures can be procedural or physical and are appropriate for industry.

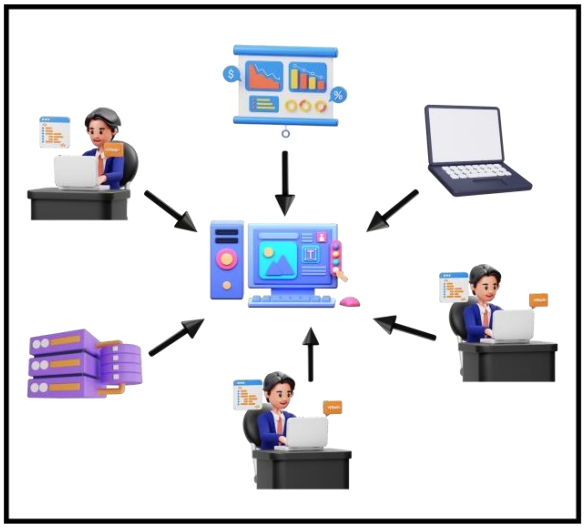

Figure 2. Conventional Security

Figure 3 shows the visual illustration of smart contract security which includes procedures, techniques, and technological advancements used to guarantee that smart contracts function as planned and are not susceptible to malware, assaults, or other security hazards. Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. They are operated on blockchain systems such as Ethereum, where they enforce and carry out the terms automatically upon the fulfillment of predetermined criteria.

Figure 3. Smart Contract Security

In a nutshell, smart contract security is particularly concerned with guaranteeing the security and dependability of blockchain-based code that automates transactions and agreements, whilst conventional security focuses on safeguarding general IT systems and data.

3.4 Optimization and Efficiency in Smart Contract

This section covers the following topics: Reduce Gas Consumption, Accelerating the Speed of Implementation, Efficient Resource Management, and Automatic Optimization Tool.

3.4.1 Reduce Gas Consumption

Gas refers to the computational power used for carrying out a transaction in the context of blockchain networks, such as Ethereum. For this reason, it is crucial to optimize smart contracts to reduce gas consumption by better data structures, coding techniques, and storage operation optimization. Lowering gas prices may make transactions easier and more affordable. This is crucial in situations where excessive gas use would result in surcharges, which would exacerbate the network congestion issue and negatively impact scalability and usability.

3.4.2 Accelerating the Speed of Implementation

To be in a functional condition, smart contracts require optimization. Stated differently, recursive functions should be avoided as they will slow down processes or generate problems. Instead, the code has to be optimized through the

usage of libraries. Applications for supply chain management and financial services that depend on processing can be carried out more effectively by improving the performance and dependability of the contract.

3.4.3 Efficient Resource Management

The way smart contracts are made ensures more effective resource management and efficiency in terms of processing and storage capacity. Scaling solutions, state channels, and computing approaches are all valuable for increasing efficiency. Contract performance can be improved by adding a layer or removing a burden from the chain while maintaining security and openness.

3.4.4 Automatic Optimization Tool

Tools and frameworks like Vandal play a part in spotting bugs and inefficiencies in smart contract programming. These aid the developer in identifying issues with expenses, superfluous code, or potential security threats early on in the process. This solution allows for cost reductions and seamless performance, which simplifies the optimization process in smart contracts.

3.5 Compliance and Legal Challenges

The contract has a significant influence on how enterprises and commerce are conducted globally. They provide ways to foster trust by establishing agreements and maintaining record transparency. The road to adoption has not been easy, though. This covers topic including fostering sustainability concerns, incorporating intelligence and machine learning to facilitate its use in key management, and dealing with operational, regulatory, and governance challenges.

3.5.1 Governance, Operational & Regulatory

Governance

Since each node in the network may be governed by a separate set of laws, the decentralized nature of smart contract technology presents challenges for most regulators. This complicates the business as it might be challenging to guarantee that regulations are followed and enforced. Creating interoperability standards for blockchain systems might help address the issues. As a result, communication will be highly effective, and clients' confidence will grow. Global standards for user privacy, security, authentication, and risk are also desperately needed. The creation of such thorough standards would be difficult and need a lot of labor from professionals worldwide.

Operational

Security is key from an operational standpoint as we have seen with the 2016 DAO hack and WannaCry ransomware. Scalability matters too as more users and transactions means it is hard to maintain performance. A blockchain’s security, efficiency and environmental friendliness is largely determined by the consensus mechanism used (proof-of-work or proof-of-stake). So, these need to be coordinated so the blockchain can be secure and last long. Considering historical incidents like the 2016 DAO hack or WannaCry ransomware, strong security protocols must be in place. Scalability is also important since it is very hard to maintain peak performance when there are many users and transactions. Moreover, the choice between proof of work and proof of stake consensus algorithms has a notable influence on the performance, safety and eco friendliness of a blockchain network. In recognition of the above reason, these variables need to be balanced for blockchains to operate safely and sustainably.

Regulatory

Because of this, several regulatory organizations (like the SEC and ESMA) are developing frameworks to assist them in managing the requirements and dangers presented by smart contract technology, such adhering to financial rules and anti-money laundering statutes. Since blockchains are unable to be truly undone, this presents a challenge for blockchains in terms of "the right to be forgotten" under GDPR. Among the other options under consideration are encrypted data storage and off-chain data management. There should be worldwide collaboration for common regulatory standards because it is challenging to implement legislation in different countries owing to the global and decentralized nature of blockchain technology.

3.5.2 Use of Artificial Intelligence and Machine Learning

The advancement in smart contract technology makes it possible to combine AI and ML for a range of applications and solutions. Through self-governing oracles, artificial intelligence improves smart contract understanding, identification, and judgment. ML improves decision-making much more, enhancing the functionality of smart contracts. This combination has the potential to produce automatic token creation, enhanced security, and sophisticated recommender systems. Big data analytics may also use blockchain data to detect fraud, lower transaction costs, and forecast trade patterns [34].

3.5.3 Usability and Key Management

Smart contract technology is complex. Users need to understand transaction flows because of its unusual architecture, this is difficult. Bitiodine and Bitconeview are two tools that analyze patterns in smart contracts to improve security and privacy. However, because smart APIs—like Bitcoin's—use public key cryptography rather than passwords, utilizing them is challenging. Because of this, key management is difficult for users and requires more research to improve usability for both users and developers.

3.5.4 Sustainability

Despite its innovation and promise, smart contract technology has a lot of sustainability issues to overcome. A significant problem is its high energy usage, especially when it comes to cryptocurrencies like Bitcoin, which have a big carbon footprint because they require a lot of processing power to verify transactions [35]. For example, a single Bitcoin transaction can require more energy than regular financial transactions do—up to several weeks' worth—for the average household (UN News, MDPI) [36], [37]. Furthermore, scalability is still an issue because growing networks typically have lower transaction speeds and throughput overall, which makes them less efficient (MDPI). The absence of infrastructure necessary for blockchain projects in developing nations makes it more difficult to use the technology in international development initiatives (MDPIs). Research is currently being conducted to build consensus procedures that are more energy-efficient in order to solve these concerns.

4. RESULTS AND DISCUSSIONS

Transactions have now started to cross new boundaries with smart contract technology which is providing automated, decentralized and secure transactions in many industries. Nevertheless, there are several issues that need to be improved in order for this technology to live up its full potential. There are continuous improvements for developer tools, privacy, scalability and performance, governance or legal compliance etc. Well, taking a full-stack strategy to overcome these issues can provide them the functionality and security they need at their disposal thereby maximizing smart contracts usage. In this part, we discuss strategies for improving the usability of smart contracts, improving its survivability and easier-to-implement deployment.

4.1 Security Enhancements

Through smart contracts, agreements can be enforced automatically and exchanges facilitated between concerned parties without the need of a third party overseeing but rather as involved from one end to another. This way, will save on costs and at the same time it will give zero error. However, digital contracts are difficult to secure. The hope of smart contracts is to enforce compliance through coding the terms into code, however bugs in the programs can lead them susceptible to severe vulnerabilities. The main things in order to make better smart contracts are extensive code audits, formal verification methods and using multi-signature protocols on decentralized services. These efforts together can reduce risks, maintain the security and trust in smart contracts with blockchain technology recording each transaction permanently and irrevocably.

4.2 Self-Executing Contracts

The core originality of intelligent contracts is observed in the capacity to automatically implement coded conditions that ease execution and increase trustworthiness of contracts [38], [39]. This case reduces the risks resulting from human error, fraud, and all manner of cybercrime. This type of contract is characterized by a high level of security and resilience against tampering which are necessary for facilitating different forms of digital transactions and agreements. In order to enhance their performance further, it is significant to consistently develop coding standards and testing methods so as to guarantee the robustness, flexibility and safeness of smart contracts.

4.3 Emphasize Smart Contract Development and Application

Smart contract technology shows many potential promising applications in the emerging blockchain environment to achieve this goal the technology needs to be developed on an ongoing basis to be able to handle a wider variety of needs and more complex scenarios as time progresses. This tactical move not only helps to incorporate smart contracts into other fields, but also enhances the modularity and resilience of smart contracts as well. Besides that, it also helps their incorporation into other fields which in turn escalates their revolutionary potential in the area of technology.

4.4 Cross-Chain Contracts and Interoperability

The development of smart contracts has placed a major focus on interoperability to guarantee optimal performance across many blockchain networks. This capacity is crucial in leading the blockchain ecosystem towards a better-connected future. But there are important complications involved in attaining cross-chain interoperability that need to be acknowledged. Smart contracts on distinct blockchains may communicate with assets and data on separate networks thanks to cross-chain contracts, which are made possible by protocols like Polkadot [40]. Although this invention encourages a blockchain environment that is more linked and cooperative, it also presents several issues that require attention as stated in Table 2.

Table 2. Key Challenges in Cross-Chain Interoperability

Challenges	Synopsis	Consequence
Security Risks	Cross-chain transactions are susceptible to a variety of attacks, including double-spending and corrupted validators, because they include several blockchains with distinct security standards.	Possibility of asset and data integrity loss necessitates strong security protocols and ongoing chain monitoring.
Scalability and Latency	The time needed to process and validate transactions across various blockchains might cause	longer transaction times and possible bottlenecks, which might affect how

	delays in cross-chain transactions.	well and quickly smart contracts that operate across chains respond.
Disparities in Consensus Mechanisms	The employment of various consensus techniques (such as PoW, PoS, and BFT) by different blockchains makes it more difficult to standardize transaction validation and finality between chains.	Inconsistencies in the validation and processing timeframes of transactions, which might cause delays and disputes in cross-chain transactions.
Standards for Interoperability	The inability to establish common standards for cross- chain interoperability poses a difficulty in developing interoperable smart contracts between networks.	Restricted cross-chain capabilities and dependence on protocols that might not work perfectly with all blockchain networks.

4.5 Scalability and Latency

Cross-chain transaction algorithms can reduce latency by selecting the best channel for data transfer that can also help address scalability and latency problems of on-chain technology. By executing a number of transactions between many chains, they are less likely to become congested and lower the chances of low scalability. Moreover, sharding methods help increase the level of scalability since the blockchain is divided into smaller and more manageable sections. As such, more advanced caching techniques and data compression methods can be employed to minimize latency and enhance scalability as further actions. Still, certain actions that may be performed by a blockchain network, such as data compression before transmission and keeping the most often accessed data closer to where transactions are being executed, can make them faster and more scalable.

4.6 Distinctions in Consensus Mechanism

An instance of the cross-consensus protocol may be best illustrated by the Polka Relay Chain that is primarily intended to facilitate cooperation between multiple blockchains. It enables commercial processes that occur within a single or across various consensus models, to work as one stops at the issue that comes with the disparate consensus mechanisms in cross-chain solutions. Layer 2 solutions such as roll-ups and side chains will add optimisation to how final consensus is reached by presenting the blocks in an intelligently processed manner before going on the main blockchains. Moreover, such protocol-independent solutions might allow blockchains using different consensus mechanisms to exchange information with each other. To improve compatibility with the consensus processes, new hybrid consensus models within which elements from several consensus processes could be combined in order to make a greater variety of blockchain activities more probably should be created. Moreover, there is nothing that can hinder cross-chain implementations from being used to fill specific gaps in consensus validation by providing accurate data feeds and validation services. This helps in ensuring that all the interconnected blockchains retain the data to be accurate as well as consistent helping to reduce inconsistencies in consensus validation.

4.7 Interoperability Standards

As the Internet set global standards for the HTTP protocols, it is time for the blockchain industry to take proactive steps toward developing standards in cross-chain connectivity and interoperability to address issues associated with interoperability standards where cross-chain technology is involved. Thus, a smoother and more homogenous approach to interchain interaction may be facilitated by bringing into practice more commonly used interoperability frameworks such as Polkadot Substance or Cosmos SDK. The fragmentation of blockchains can be reduced by sharing a set of guidelines and standards as numerous blockchain projects, thus, working together to create a more united whole.

5. CONCLUSION

In conclusion, smart contracts transform technological transactions and digital agreements as they are executed. Smart contracts, as applying the concept of blockchain technology, free of intermediaries eliminate the possibility of fraud, human factors and significantly minimize the costs of doing business. The major strength of smart contracts is that there is no one entity that has the power to manipulate the said contract and its execution. Notably, the immutability aspect of relevant blockchain technology offers an audit trail which is irrefutable and a major plus in compliance and authentication points. The application of this technology has led to significant improvements in numerous industries such as banking services, supply chain management among other services since it provides credible, transparent, and efficient solutions. Consequently, this paper aims to first analyze the structure of smart contract technology in its forthcoming sections before proceeding to discuss the numerous application areas including a discussion on its security and privacy aspects. Furthermore, it identifies issues with smart contracts and recommendations to address those issues. Finally, the paper discusses new ideas for the future development of smart contracts and discusses the possible directions of future research.

ACKNOWLEDGEMENT

We thank the anonymous reviewers for the careful review of our manuscript.

FUNDING STATEMENT

This work is funded by the Ministry of Science and Technology the Malaysia, under of FRGS (FRGS/1/2023/TK07/UIAM/02/2). This work is also supported by the Department of Computer Sciences, KICT, IIUM and IoTeams KICT and Silverseeds Lab Network.

AUTHOR CONTRIBUTIONS

Farah Mazlan: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation;
Nur Faizah Omar: Methodology, Graphics and Tables, Writing – Original Draft Preparation;
Nik Nor Muhammad Saifudin Nik Mohd Kamal: Proofreading and Structuring.
Ahmad Anwar Zainuddin: Evaluation, Concluding, Supervision – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests was disclosed.

ETHICS STATEMENTS

No statements to be disclosed.

REFERENCES

[1] E. Negara, A. Hidayanto, R. Andryani, and R. Syaputra, "Survey of Smart Contract Framework and Its Application," *Information,* vol. 12, no. 7, p. 257, Jun. 2021, doi: 10.3390/info12070257.

[2] V. Dwivedi, A. Norta, A. Wulf, B. Leiding, S. Saxena, and C. Udokwu, "A Formal Specification Smart-Contract Language for Legally Binding Decentralized Autonomous Organizations," *IEEE Access,* vol. 9, pp. 76069–76082, 2021, doi: 10.1109/ACCESS.2021.3081926.

[3] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and Smart Contracts for

Insurance: Is the Technology Mature Enough?" *Future Internet,* vol. 10, no. 2, p. 20, Feb. 2018, doi: 10.3390/fi10020020.

[4] Z. Ji, Z. Guo, H. Li, and Q. Wang, "Automated Scheduling Approach under Smart Contract for Remote Wind Farms with Power- to-Gas Systems in Multiple Energy Markets," *Energies,* vol. 14, no. 20, p. 6781, Oct. 2021, doi: 10.3390/en14206781.

[5] E. E. Ameyaw, D. J. Edwards, B. Kumar, N. Thurairajah, D.-G. Owusu-Manu, and G. D. Oppong, "Critical Factors Influencing Adoption of Blockchain-Enabled Smart Contracts in Construction Projects," *Journal of Construction Engineering and Management,* vol. 149, no. 3, p. 04023003, Mar. 2023*,* doi: 10.1061/JCEMD4.COENG-12081.

[6] J. Li, D. Greenwood, and M. Kassem, "Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases," Automation in Construction, vol. 102, pp. 288–307, Jun. 2019*,* doi: 10.1016/j.autcon.2019.02.005.

[7] U. Damisa, N. I. Nwulu, and P. Siano, "Towards Blockchain-Based Energy Trading: A Smart Contract Implementation of Energy Double Auction and Spinning Reserve Trading," *Energies,* vol. 15, no. 11, p. 4084, Jun. 2022, doi: 10.3390/en15114084.

[8] I. Reshi, M. Khan, S. Shafi, S. Sholla, A. Assad, and H. Shafi, "AI-Powered Smart Contracts: The Dawn of Web 4. O." Mar. 06, 2023. doi: 10.36227/techrxiv.22189438.

[9] N. Ivanov, C. Li, Q. Yan, Z. Sun, Z. Cao, and X. Luo, "Security Defense For Smart Contracts: A Comprehensive Survey," *arXiv (Cornell University), Jan. 2023,* doi: 10.48550/arxiv.2302.07347.

[10] P. Hegedűs, "Towards analyzing the complexity landscape of solidity based Ethereum smart contracts," *International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg Sweden: ACM,* May 2018, pp. 35–39*.* doi: 10.1145/3194113.3194119.

[11] P. Du, Z. Liu, B. Huang, G. Jing, L. Feng, and C. Yang, "Blockchain Based Peer-To-Peer Energy Trading Between Wind Power Producer and Prosumers in Short-Term Market," *Frontiers in Energy Research,* vol. 10, p. 923292, Jul. 2022, doi: 10.3389/fenrg.2022.923292.

[12] S. Kalra, S. Goel, M. Dhawan, and S. Sharma, "ZEUS: Analyzing Safety of Smart Contracts," *Network and Distributed System Security Symposium,* San Diego, CA: Internet Society, 2018. doi: 10.14722/ndss.2018.23082.

[13] Z. Fauziah, H. Latifah, X. Omar, A. Khoirunisa, and S. Millah, "Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review," Aptisi Transactions on Technopreneurship (ATT), vol. 2, no. 2, pp. 160–166, Aug. 2020, doi: 10.34306/att.v2i2.97.

[14] Z. Zheng et al., "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems, vol. 105, pp. 475–491, Apr. 2020,* doi: 10.1016/j.future.2019.12.019.

[15] A. A. Papantoniou, "Smart Contracts in the New Era of Contract Law," *Digital Law Journal,* vol. 1, no. 4, pp. 8–24, Dec. 2020, doi: 10.38044/2686-9136-2020-1-4-8-24.

[16] L. Brent et al., "Vandal: A Scalable Security Analysis Framework for Smart Contracts." *arXiv (Cornell University),* 2018. doi: 10.48550/ARXIV.1809.03981.

[17] P. Vionis and T. Kotsilieris, "The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review," *Applied Sciences,* vol. 14, no. 1, p. 253, Dec. 2023, doi: 10.3390/app14010253.

[18] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020*.

[19] "An Introduction to Smart Contracts and Their Potential and Inherent Limitations." *Accessed: Jun. 09, 2024. [Online]. Available: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/*

[20] P. Vionis and T. Kotsilieris, "The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review," *Applied Sciences*, vol. 14, no. 1, p. 253, Dec. 2023, doi: 10.3390/app14010253.

[21] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," *IEEE Access,* vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[22] A. Rijanto, "Blockchain Technology Adoption in Supply Chain Finance," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 7, pp. 3078–3098, Nov. 2021, doi: 10.3390/jtaer16070168.

[23] Z. Zheng et al., "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems,* vol. 105, pp. 475–491, Apr. 2020, doi: 10.1016/j.future.2019.12.019.

[24] B. Bodó, D. Gervais, and J. P. Quintais, "Blockchain and smart contracts: the missing link in copyright licensing?," *International Journal of Law and Information Technology,* vol. 26, no. 4, pp. 311–336, Dec. 2018, doi:

10.1093/ijlit/eay014.

[25] "View of Smart Contracts Security Application and Challenges: A Review." Accessed: Jun. 09, 2024. [Online]. *Available: https://ojs.wiserpub.com/index.php/CCDS/article/view/3271/1593*

[26] "(PDF) Blockchain-based Smart Contracts - Applications and Challenges." *Accessed: Jun. 19, 2024. [Online]. Available: https://www.researchgate.net/publication/328230865_Blockchain-based_Smart_Contracts_-_Applications_and_Challenges*

[27] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart Contract Security: A Software Lifecycle Perspective," *IEEE Access,* vol. 7, pp. 150184–150202, 2019, doi: 10.1109/ACCESS.2019.2946988.

[28] N. Kannengieser, S. Lins, C. Sander, K. Winter, H. Frey, and A. Sunyaev, "Challenges and Common Solutions in Smart Contract Development," *IEEE Transactions on Software Engineering,* vol. 48, no. 11, pp. 4291–4318, Nov. 2022, doi: 10.1109/TSE.2021.3116808.

[29] D. Han, C. Zhang, J. Ping, and Z. Yan, "Smart contract architecture for decentralized energy trading and management based on blockchains," *Energy,* vol. 199, p. 117417, May 2020, doi: 10.1016/j.energy.2020.117417.

[30] "What Are Smart Contracts on the Blockchain and How Do They Work?" *Accessed: Jun. 19, 2024. [Online]. Available: https://www.investopedia.com/terms/s/smart-contracts.asp*

[31] "Layer 2 Tokens on Ethereum: A comparison | Trust." *Accessed: Jun. 19, 2024. [Online]. Available: https://trustwallet.com/blog/layer2-tokens-on-ethereum-a-comparison*

[32] "What is a Protocol Layer? | Koinly." *Accessed: Jun. 19, 2024. [Online]. Available: https://koinly.io/crypto-glossary/protocol- layer/*

[33] "What is the Application Layer? - Definition from Techopedia." *Accessed: Jun. 19, 2024. [Online]. Available: https://www.techopedia.com/definition/6006/application-layer*

[34] P.O. Shoetan, A.T. Oyewole, C.C. Okoye, and O.C. Ofodile, "Retrieving The Role of Big Data Analytics in Financial Fraud Detection," *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 384–394, Mar. 2024, doi: 10.51594/farj.v6i3.899.

[35] V. Kohli, S. Chakravarty, V. Chamola, K. S. Sangwan, and S. Zeadally, "An Analysis of Energy Consumption and Carbon Footprints of Cryptocurrencies and Possible Solutions." *arXiv (Cornell University),* 2022. doi: 10.48550/ARXIV.2203.03717.

[36] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The Carbon Footprint of Bitcoin," *Joule,* vol. 3, no. 7, pp. 1647–1661, Jul. 2019, doi: 10.1016/j.joule.2019.05.012.

[37] "Spotlight on sustainability initiatives in key sectors in Latin America and the Caribbean," *OECD Business and Finance Policy Papers 45,* May 2024. doi: 10.1787/5178fb0d-en.

[38] Q. Wang, R. Y. K. Lau, Y.-W. Si, H. Xie, and X. Tao, "Blockchain-Enhanced Smart Contract for Cost-Effective Insurance Claims Processing:," *Journal of Global Information Management,* vol. 31, no. 7, pp. 1–21, Sep. 2023, doi: 10.4018/JGIM.329927.

[39] F. Santos, R. Pereira, and J. B. Vasconcelos, "Toward robotic process automation implementation: an end-to-end perspective," *Business Process Management Journal,* vol. 26, no. 2, pp. 405–420, Sep. 2019, doi: 10.1108/BPMJ-12-2018-0380.

[40] S. Imoto, Y. Sudo, H. Kakugawa, and T. Masuzawa, "Atomic Cross-Chain Swaps with Improved Space and Local Time Complexity," *in Stabilization, Safety, and Security of Distributed Systems, vol. 11914, M. Ghaffari, M. Nesterenko, S. Tixeuil, S. Tucci, and Y. Yamauchi, Eds., in Lecture Notes in Computer Science,* vol. 11914. 2019, pp. 194–208. doi: 10.1007/978-3-030-34992-9_16.

BIOGRAPHIES OF AUTHORS

	**Nur Faizah Omar** is a student of Kulliyyah of Information and Communication Technology, IIUM. Her interest lies within the intricacies of technology, particularly the inner workings of code, software, and security principles. She is fascinated by the complexities involved and is driven by a desire to learn and discover to expand her knowledge and deepen her interest in innovative advancements that can improve modern civilization. Additionally, she has a keen interest in digital design, understanding that superior design enhances navigation and user functionality. She firmly believes that seamless coding and intuitive design together create outstanding technological experiences. She can be contacted via email: nurfaizah.or@gmail.com
	**Farah Mazlan** is a student in Kulliyyah of Information and Communication Technology, International Islamic University Malaysia. Her interest lies in technological innovation as well as comprehensive data research and analysis. Through data collecting and analysis, she seeks to better understand patterns, forecast behavior, and optimize system performance. She is thus sure that precise data may significantly aid in the solution of challenging issues and in creating a set of decision-making plans that will increase the productivity and effectiveness of various industry operations. Other than that, she has a keen interest in technology innovation as it offers valuable and efficient solutions for everyday problems faced by humans, especially in the AI discipline. She can be contacted via email: arahlan18@gmail.com
	**Nik Nor Muhammad Saifudin Nik Mohd Kamal** is a computer science graduate from Kulliyyah of Information and Communication Technology, International Islamic University Malaysia (KICT, IIUM), majoring in network security. He has a solid background in the concept of computer science and practical experience in the field of Internet of Things (IoT). He, being a person who can labor adeptly with the Arduino IDE, would like to apply the skills learned and knowledge in creative projects within the sectors of computer science and network security. He has a burning desire to contribute toward advanced technological development in these fields. He can be reached at saifudinkamal11@gmail.com.
	**Ahmad Anwar Zainuddin** is an Assistant Professor at the International Islamic University Malaysia (IIUM). He holds a Ph.D. and is recognized for his expertise in Computer Engineering. His research interests include Internet-of-Things (IoT), Artificial Intelligence (AI), Blockchain, and acoustic wave electrochemistry biosensors, indicating a focus on interdisciplinary applications of technology. He emphasizes the importance of AI concepts, problem-solving skills, and adaptability in a fast-paced tech landscape. His contributions to research and academia align with the ICT body of knowledge, particularly in areas such as biosensors and AI integration. He can be contacted via email: anwarzain@iium.edu.my