IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

Evolution and Future of Smart Contracts

Roshani Vishnu Thawari, Mrs. Chetna Achar

Student, Institute of Computer Science, Mumbai Educational Trust- MET ICS, Mumbai, India

Professor, Institute of Computer Science, Mumbai Educational Trust- MET ICS, Mumbai, India

ABSTRACT: Since Nick Szabo introduced the concept of smart contracts in the 1990s, there were significant developments in this field. From the first rudimentary versions of simple, code-based contracts to complex autonomous agreements executed atop blockchain platforms like Ethereum, smart contracts evolved drastically. Indeed, smart contracts started reaching sectors far beyond their original purposes in finance and coding. The confluence of more advanced programming languages and protocols resulted in the creation of more sophisticated, versatile, and secure smart contracts. At the same time, the legislation context related to oracles and other systems necessary for smart contracts operation is gaining momentum. This paper learned technological advances and legislative implications for smart contracts.

KEYWORDS: Smart contracts, Evolution, Blockchain, Ethereum, Programmability, Interoperability, Oracles, Decentralized finance (DeFi), Legal contracts, Internet of Things (IoT), Artificial Intelligence (AI).

OBJECTIVES

- Trace the historical evolution of smart contracts and key technological milestones.
- Analyze the role of blockchain platforms like Ethereum in facilitating smart contract advancement.
- Explore the expansion of smart contracts across diverse sectors beyond finance and coding.
- Examine the legal/regulatory landscape and integration with traditional contracts.
- Investigate future developments and applications with emerging technologies like AI and DeFi.

I. INTRODUCTION

A. What is a Smart Contract ?

Smart contract is an automated contract program in which the conditions and statements of the contract are coded into a script. The writings and the provisions of the code are embedded and copied on the ethical blockchain system.

The key characteristics of a smart contract are:The key characteristics of a smart contract are:

1. Automatic execution: This means that once the determined conditions have been met, then the contract is self-executed without the assistance of third parties or human interventions.

2. Decentralized: Smart contracts live in a blockchain platform, which is open, tamper-proof, and can hardly be censored or stopped.

3. Trustless: Smart contracts carry out effectively and do not presuppose trust between the members and the counterpart since the conditions are enforced by the code.

4. Programmable: Smart contracts entail computer code that runs on blockchain, whose nature allows protocol coded conditions to be accomplished.

5. Transparent: This makes it easy to approve the code as well as scrutinize, making smart contracts transparent and accountable.

Smart contracts were proposed even in the 1990s by computer scientist Nick Szabo, and he described smart contracts as effectively creating an open source code that helps to define the terms of a contract, as well as execute it. Despite this, the concept of smart contract has been in existence since 1993; nevertheless, it was not until 2015 that Ethereum brought it to light and made it possible to write smart contracts on a blockchain.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

B. Traditional Contract vs Smart Contract

PARAMETERS	Traditional Contract	Smart Contract
Form and Structure	This is a legal document written in plain language, it states what has been agreed upon by the parties concerned or the conditions to be followed.	A computer program that runs on a blockchain with a self-executing code having the terms of the contract directly coded therein.
Execution and Enforcement	It is enforced manually through legal channels, and its execution relies on actions of involved parties as well as judicial intervention whenever disputes arise.	Blockchain network automatically enforces it once certain predefined conditions are satisfied. Execution is autonomous and deterministic.tion.
Trust and Intermediaries	It usually relies on legal frameworks, institutions, or intermediaries such as lawyers and notaries for purposes of validation and enforcement.	The trust resides in consensus mechanism together with cryptographic security of blockchain technology therefore intermediaries are not needed.
Transparency and Immutability	Privacy can be maintained through confidential documents but changes can only be opaque and enforcement actions are subjected to manipulation.	Often after deployment on blockchain, code becomes transparent while transactions become immutably resulting into publicly verifiable history.
Efficiency and Costs	Can be time-consuming and costly due to legal expenses, administrative procedures, and participation of multiple third parties..	Typically, it is executed faster and at a lower cost; this will result in low transaction costs as well as reduced intermediaries.

II. HISTORY AND EVOLUTION FROM TRADITIONAL CONTRACTS TO SMART CONTRACTS

Traditional Contracts: Origin and Development

For centuries, traditional contracts have been the basis of legal agreements. Initially they were simply written agreements that formalized obligations with natural language. Traditional enforcement methods included courts, lawyers and notaries who acted as intermediaries in validating and executing these contacts. Making a contract has historically been an expensive, time-consuming process involving manual operations and voluminous paperwork.

The Emergence of Smart Contracts

Nick Szabo introduced the concept of smart contracts in the 1990s where he conceptualized blockchain-based self-executing digital contracts. However, the resolution to this issue came with the introduction of the Ethereum blockchain platform in 2015 which made it practically possible to implement smart contracts. This was done through Ethereum's deployment of decentralized applications (dApps) and smart contracts that enforce pertinence without any middleman participation. For instance, this innovation led to real-time automatic execution of contracts thereby reducing costs and streamlining processes at all levels in the supply chain from sourcing inputs through production to final distribution channels.

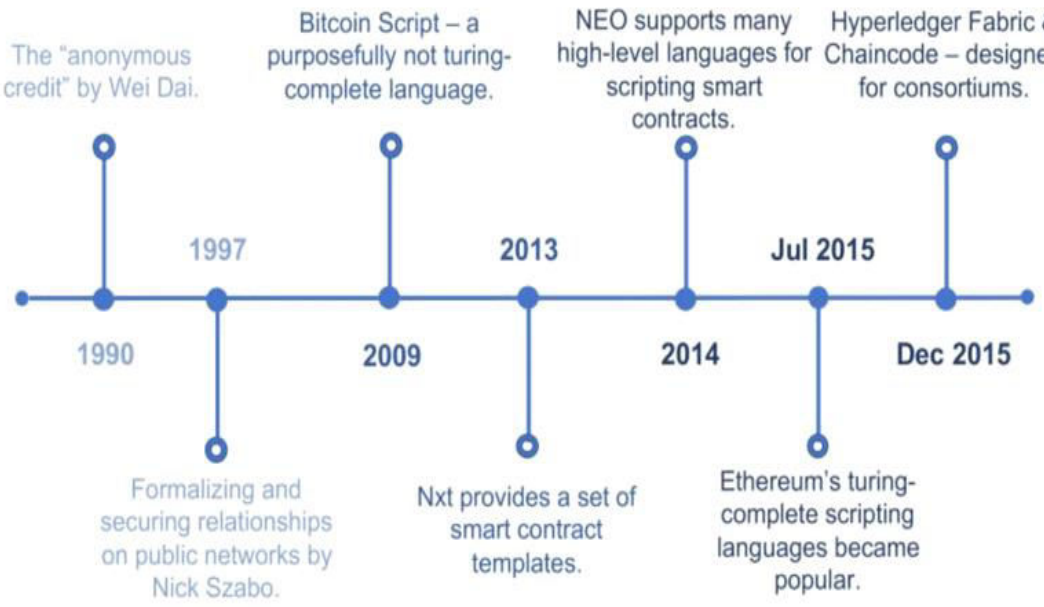
Smart Contracts and the Development of Evolution

Since their first introduction, smart contracts have changed into a more advanced form. They used to be limited to simple transactions and token transfers; today they can handle complex business logic as well as decentralized applications. There are now methods that can allow smart contracts to work across different blockchain networks while improvements on safety through formal verification have made them dependable. Incorporation of regulatory compliance functionality ensures that smart contracts follow strict legal standards, making it possible for them to fit standard applications in finance, healthcare, supply chain management among many others. These advances represent a significant shift from conventional methods of contracting towards digital agreements that are flexible, effective and safe.

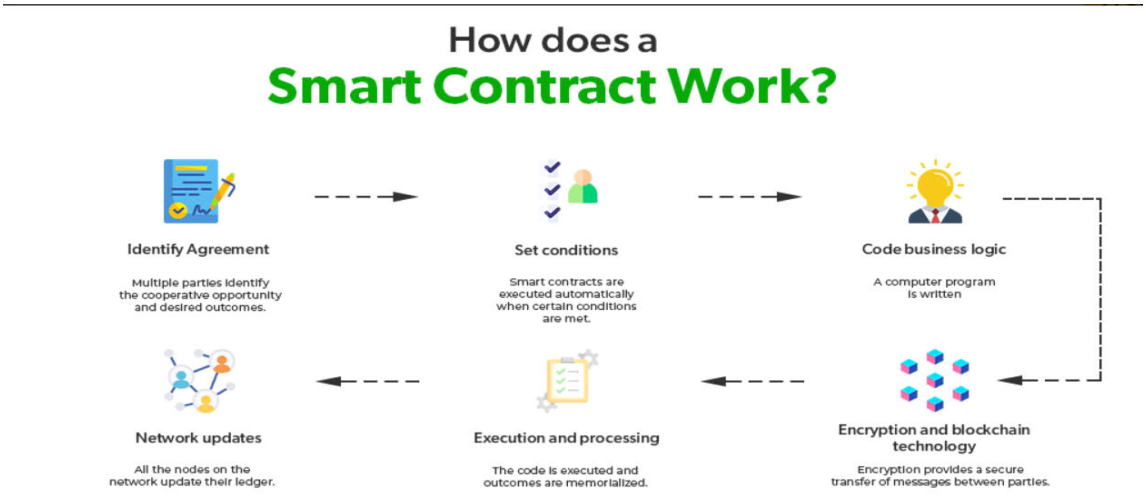
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |



How doesSmart Contract work?



Agreement Identification: Several parties identify a joint opportunity and the desired outcomes while agreements may involve business processes, swapping of assets amongst other things.

Creating conditions: Parties themselves can initiate smart contracts or if certain factors are met such as financial market indices, events like GPS locations etc.Writing computer programs for business logic: Once the conditional parameters are met, an automatic execution program is written to be executed.

Encryption and blockchain technology: Encryption plus secure authentication and messages transfer between contracting parties that relates to smart contracts.

Execution and processing: In blockchain iteration, whenever consensus is reached by the parties for purposes of authentication and verification, then the code gets executed whereupon results get memorialized for compliance and verification needs.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

Updating networks: After running smart contracts all nodes on the network update their ledger to show a new state. Once it has been posted as well as verified on the blockchain network there cannot be any further amendments made; it only works under add mode.

Latest trend in Smart contract:-

The global smart contracts market is experiencing rapid growth and transformation. This innovative technology is redefining how contractual agreements are executed, eliminating the need for intermediaries and enhancing efficiency across various industries.

The global smart contracts market was valued at USD 1.71 billion in 2023.

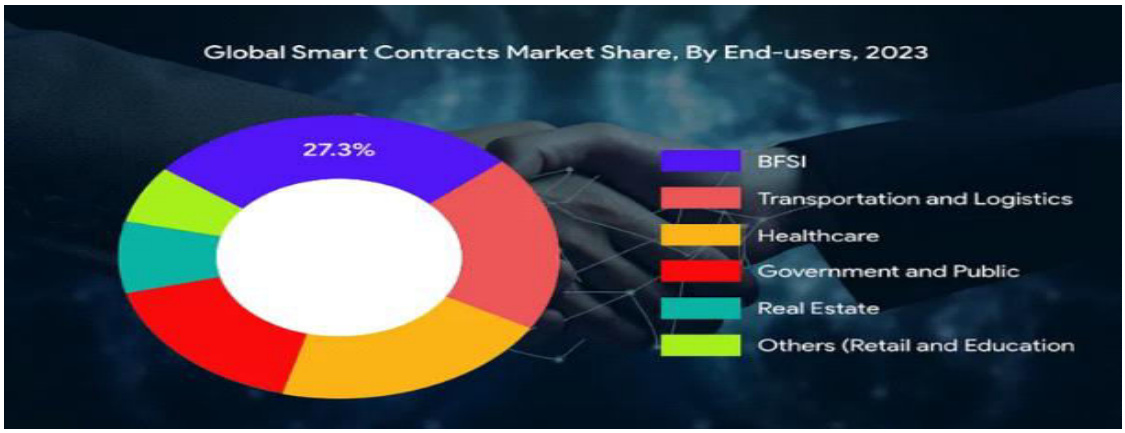
The market is projected to reach USD 2.14 billion in 2024.

It is expected to grow to USD 12.55 billion by 2032.

The market is anticipated to exhibit a CAGR of 24.7% during the forecast period (2024–2032).

The market growth is driven by several factors, including:

The increasing adoption of blockchain technology across various industries and supply chains.



III. ADVANTAGES OF SMART CONTRACT

Transparency and Trust

When it comes to smart contract, one of the outstanding features is when any updated information is provided to all the involved parties at once, thus reducing manipulation. In addition, the non alterability of data on the blocks assures that one cannot tamper with the data on the block chain hence minimizing the risks of fraud or mistakes in contract review and fulfillment.

Autonomy and Independence

The legal contract also does not involve middlemen in form of lawyers or banks as adopted in most business deals. They are self-directed and work on instructions that are embedded within their program, thereby enabling the parties to have a higher level of control and self-sufficiency on the contracts entered. This independence facilitates fast processing since all related parties can independently make their decisions.

Cost Savings

Another interesting aspect of smart contract development is the complete elimination of the cost if intermediaries. As outlined with regard to the numerous intermediaries presented above, the utilization of smart contracts negates the necessity for different operations, thereby eradicating fees and transaction charges, which in turn will significantly lower costs for your businesses.

Speed and Efficiency

This is because smart contracts reduce the time of transactions as it does not require multiple approvals or even manual processing. The contracts are structured in a way that enables those who enter them to introduce automation, making contracts more efficient since they do not require much human intervention to implement. This speed proves very helpful in enhancing different business activities such as financial and health care business so as to eliminate long business transactions.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

Automatic Updates

It is pertinent to note that smart contracts self-optimise and re-calibrate contract provisions: with this, there is no necessity to constantly update contracts. This feature helps to mitigate the risk of old contracts becoming outdated and containing potential inaccuracies all without extra steps. The use of smart contracts offers an automation of contracts, which increases the flexibility as well as the dynamism of contracts.

IV. LATEST TECHNOLOGIES WHICH USES SMART CONTACT

Smart Contracts for Claims—A Revolution in Insurance(gcf)

It is also proving to be quite revolutionary in the insurance industry and as a tool for managing claims especially in procedures concerning payments to customers. Such contracts minimize the whole process of claims and it is a procedure of submitting the claim, analyzing the claim, following up the results and settling the claim, as it has no intermediaries. With the help of IPFS, claims can be assessed on the basis of parameters defined in the contract and coded within smart contracts, allowing the rapid and automatic approvement of the valid claims and rejection of suspicious or fraudulent ones. This not only saves time when making payouts, instead of waiting for payroll cycles, but also helps to avoid many administrative expenses and the risk of fraud.Moreover, applications of smart contracts in the insurance industry make it possible to design separate micro-insurance offers relevant to clients that are underserved by insurance offers commonly offered on the market. Such solutions provide basic insurance for certain perils, i. e. health costs or losses from crops, at low prices per unit and they are also similarly prepaid and postpaid. Smart contracts, developed through the use of blockchain technology, increase insurance availability and make services for various populations, including those excluded from insurance services before, more secure and financially protected.

Innovative Use Case: Flight Delay Insurance It is an insurance that covers all delays that a passenger might encounter from the time they checked in until they are boarded and accommodates any delay that the flight might experience.One of the more prominent use cases of smart contracts in the insurance industry is in using them to build new flight delay insurance products. There are new companies like Etherisc that aim to develop decentralized insurance solutions that are based on blockchain and smart-contracts, such as parametric flight delay insurance. In this model, the conditions of the payments are pre-specified and embedded into the smart contract; the payouts will then be delivered by the system once the predefined conditions are met, for example, the duration of flight delays. This makes it quite easier not to process claims manually and also to ensure that those affected are compensated as soon as possible.

Through the use of smart contracts, flight delay insurance policy solutions make customers more satisfied with their insurance products since they also get compensated for any delayed flights. Furthermore, it helps insurers to control risks as they develop methods of charging for coverage by examining past flight records and fresh data. Consequently, those innovative insurance solutions gain the potential to improve the efficiency and customer-oriented approach in the insurance market environment.

Information Technology and Digital Knowledge: Smart Contracts in Digital Identity Management

Smart contracts have the potential of being the next wave of advancement in the establishment of secure means of identity and other personal information management. Thus, smart contracts based on blockchain technology allow for decentralization and complete data integrity in handling digital identity, letting people retain exclusive rights to their data while collectively engaging in transactions with businesses, service providers, and other organizations.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

1. Decentralized Identity Verification
Smart contracts enable users to authenticate identities based on decentralized networks, and people will not need to go through a centralized authority to get their identity authenticated. In self-sovereign identity solutions, use can store their identity on a blockchain by putting other information like passports or driving licenses. Smart contracts play a key role in verifying such credentials since they are authentic, whole, and, simultaneously, the users' information remains personal.

2. Secure Authentication Processes
Smart contracts expand the means of authentication as they are capable of forming cryptographically secure methods of identifying users. Smart contracts, for instance, through multiple signatures, can adhere to multiple-factor authentication mechanisms to mitigate risks inherent in phishing scams and identity thefts. Besides, smart contracts raise the question of the recognition of biometric data, such as fingerprints or facial recognition for greater security and user satisfaction.

3. It focuses on areas such as Data Privacy and Consent Management.
Personal data privacy and consent management can be fulfilled by implementing a granular control hierarchy in smart contracts. With regard to data privacy smart contracts, citizens are able to define the rights to use their information in a certain way due to the enactment of legislation. Such privacy preferences are regulated by smart contracts making it possible for data to be shared to authorized third parties or as authorized for particular uses to improve on issues of transparency and compliance with some privacy laws such as GDPR.

4. Immutable Audit Trails
Smart contract can hold a record of the identity-associated transactions and interactions forming an unalterable audit trail, this facilitates accountability and transparency in digital identity operations. Each of the new or changed identity credentials is stored on the block; therefore, all changes made to the identity credentials are sorosable and provide a history of the identity-related activities.

V. SMART CONTRACTS FOR INTELLECTUAL PROPERTY (IP) PROTECTION

Contracting tools that are automatically activated upon infringement of certain rules: the specifics of smart contracts to protect intellectual property.
Smart contracts are also appearing as a useful platform for IP, especially in terms of creating protections, exercising ownership, and licensing of various forms of intellectual property.
1. Digital Rights Management The use of smart contracts allows for digital rights management since ownership rights and licensing regimes can be included in the contract's code, which can be immediately executed. Its usage can be observed when authors establish terms and conditions which regulate their work usage and distribution; incorporating elements of copy right protections in case of violation by the contract smart, the protected content cannot be accessed or used by a third party without his/her permission.

2. A key protection for the original work is inherent in the very nature of digital production and authoring tools because each 'object' created carries an implicit temporal marker, or 'timestamp', a name to identify the time and circumstances of creation and which embodies the concept of 'Proof of creation'.

Smart contracts have timestamping provisions and proof of creation that can be used in proving the originality and right to priority of ownership of an idea. In this way, smart contracts generate the original record of creation or registration of an intellectual asset at a specific timestamp registered in the blockchain. This stamping feature acts as proof of ownership and can be vital especially in Intellectual Property, patents and Legal cases/Disputes.

3. A royalty payment is another way of distributing benefits; here the percentage or fraction of revenues is divided among the partners.

Smart contracts enable the sharing of revenues derived from the use of intellectual assets in that they effectively manage royalties. Using self-executing contracts, it is possible to design certain actions for royalty payments and shares of revenue for the collaborators, licensors, or investors. Smart contracts monitor the use of the licensed IP and the related revenues; the implemented terms and conditions enable proper settlement of payments.

4. It means the mechanisms for fighting against the piracy, such as Anti-Counterfeiting and Digital Rights Enforcement.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

Anti-counterfeiting and digital rights protection are made possible through smart contrcts due to the possibility to set up the necessary conditions for checking the origin and credibility of the values that belong to the specific domain of intellectual property. Using IDs or signatures implanted into smart contracts allows creators to monitor the extent of ownership and use of their IP assets in the blockchain. This creates increased accountability and to quickly act against abusive use or violation through application of algorithms.

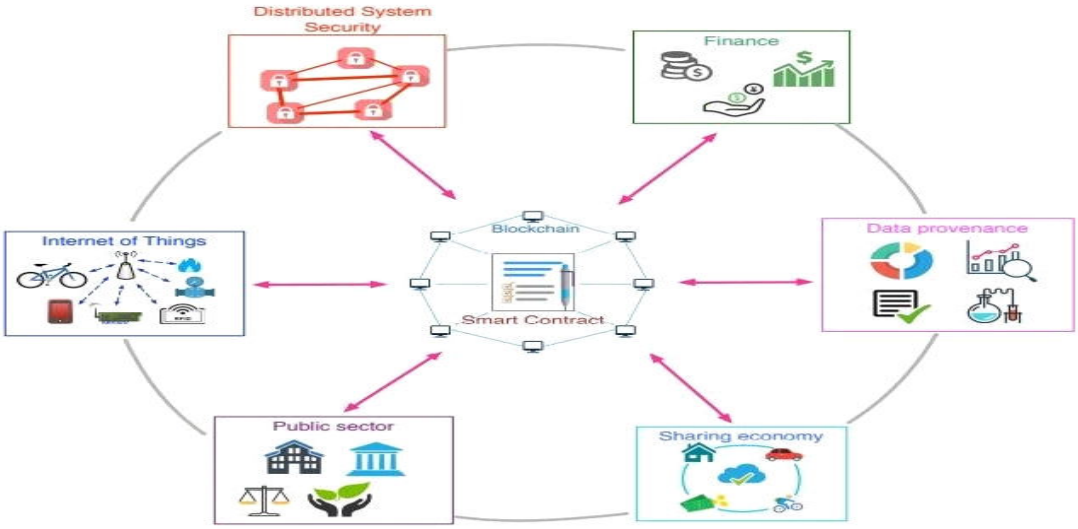
VI. RETAIL AND E-COMMERCE INDUSTRIES TRANSFORMED BY SMART CONTRACTS

Smart contracts are prevalent in the retail industry where fresh changes have been brought to the sector by embedding the principle of reducing transaction complexity and incorporating automation into purchases, payments, and conflict settlements. Here's how smart contracts are revolutionizing retail and eCommerce:Here's how smart contracts are revolutionizing retail and eCommerce:

1. Automated Purchase Processes
Smart contracts eliminate or gain significant manipulation in the most common steps in purchasing which include ordering, verification, and delivery. On the basis of this information, these contracts can perform transactions automatically as soon as the set conditions are triggered, thus cutting down on the occurrence of transaction-related activities.

2. Efficient Payment Management
The security facet of the smart contracts helps in providing efficient payment management solutions. They facilitate and also accomplish the direct transfer of funds from one individual to another and do away with third party intermediation which are expensive and time consuming. Further, smart contracts can contribute to the proper payment terms and time as it follows the payment schedule from the buyer and seller's sides.

3. Seamless Loyalty Programs
Popular use of smart contracts includes automating loyalty programs where a customer's spendings are tracked and later incentivized with loyalty points or tokens. These contracts they may be designed to pay bonuses of loyalty in line with well defined rules such as number and common value of purchases. Another advantage of smart contracts is ability in speeding up the different loyalty programs that helps in keeping the customer engaged.



VII. FINDINGS

Smart Contracts: Overview of their Background and Use:-Smart contract history dates back to the 1990s when Nick Szabo first proposed a novel idea. He believed that such contracts could be used by people to make digital deals without intermediaries. However, this only remained theoretical until 2015 came along with Blockchain technology such as Ethereum which made it possible for his vision to become a reality. The major difference between traditional contracts and smart ones is that the former must be enforced manually while the latter do so automatically through code execution; thus increasing effectiveness while reducing legal intervention.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

Enhanced Security & Trust: The evolution of smart contracts has seen integration of formal verification techniques as one of its most significant milestones. These methods involve proving mathematically that there are no bugs in the design or code of a system so that it works as expected under all circumstances. For instance, this approach has instilled confidence in using them across various industries particularly within DeFi (Decentralized Finance) where they have also been applied to supply chain management systems. Human errors which are known to cause the majority if not all security breaches have been eliminated hence making these agreements more solid and reliable thus attracting different sectors.

Real-world applications for smart contracts have been found. DeFi platforms use them for automated trading, lending or borrowing among others to do away with middlemen thus cutting on costs incurred during financial transactions. Furthermore, supply chain management benefits a lot from smart contracts as they automate tracking and transferring of goods which saves time and money by streamlining operations across different stages involved in production up to delivery.

From my own experience I can say that these examples show how powerful this technology really is when it comes down to optimizing processes within any given industry while at the same time minimizing expenses related to such optimizations.

VIII. SUGGESTIONS

A. Promoting Formal Verification: There are 100% of agreement that we should encourage more developers to use the formal verification. This will make smart contracts more secure and reliable, so that the terms of a contract are fulfilled as intended. It is necessary to work on the development of applications and frameworks that help to apply FV with less effort and straightforward technical background for a broader group of developers. This will help keep smart contracts strong and eliminate potential risks that have not been covered by current safety measures.

B. Expanding Cross-Chain Solutions: Yet, if we are to reap the benefits of interoperability, we could and should contribute into creating the cross-chain solutions. It could be achieved through the development of pre-defined pattern and rules for Cross-chain communication and the optimization of the Cross-chain bridges. These implementations will make it far easier to share smart contracts with other blockchains platforms.

C. Enhancing Regulatory Compliance: These one-off contract scenarios illustrate that to make smart contracts more widespread and integrated into organizational practices, regulatory compliance needs to be part of the broader frameworks that are being designed. In this respect, the use of ID systems along with smart contracts, KYC, and AML must be embedded into the PLONKs. That way, legal compliance could be achieved to check and balance smart contracts without centrally controlling them.

IX. CONCLUSION

Smart contracts represent a significant evolution from traditional contract methods, offering automated, efficient, and secure ways to execute agreements. Their development has been driven by advancements in blockchain technology, formal verification for enhanced security, and interoperability for cross-chain functionality. As they integrate regulatory compliance features, smart contracts are poised to transform various industries by providing reliable, decentralized solutions that reduce costs and streamline operations. The continuous improvement in smart contract technology, coupled with educational initiatives and industry collaboration, will be key to realizing their full potential and addressing the challenges of mainstream adoption.

REFERENCES

1. Szabo, N. (1997). The Idea of Smart Contracts is a form of electronic contract that is self-executable through software applications and other computational machinery. [Nick Szabo's Papers and Articles](http://(Access September 30, 2008) Available from http://www. fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best. vwh. net/smart. contracts. html). Introduce and discuss smart contracts and explain how they can be used to automate contracts between peoples without brokers.
2. Buterin, V. (2014). Ethereum White Paper: An Emergent Next Generation Smart Contracting and Distributed Application Execution Network. [Ethereum](https://ethereum. org/en/whitepaper/). Explains the story of Ethereum

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206073 |

which is one of the most popular and promising blockchain platforms for the creation and performance of smart contracts and DApps.

3. Wood, G. (2014). Ethereum: A traffic light SNOW directory of a secure decentralized generalized transaction ledger. [Ethereum Yellow Paper](https:It also establishes the blockchain's consensus algorithm, known as proof of work (Watanabe, 2018, para. 3; etherum. github. IO/yellow paper/paper. PDF). Explains a technical approach for Ethereum, and describes the architecture of Ethereum and the ways of implementing smart contracts.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details