IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13314

Smart Contracts vs. Traditional Contracts: A Comparative Analysis

Selvakumar.M[1], Mrs. A. Sathiya Priya[2]

BSc Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Smart contracts were made famous in the 2017 ethereum blockchain, automating transactions by inserting terms into code which eliminated the requirement of any middlemen. Execution of these contracts is automated, transparent, and secure. Automated contracts provide potent advantages, such as cost-saving, enhanced security, and increased efficiency, which make them integral to decentralized finance (defi), decentralized apps (dapps), and non-fungible tokens (nfts). Smart contracts exceed mere contracts. They enable interoperability of the blockchain with the internet of things (iot) via application logic contracts (alcs) and decentralized autonomous organizations (daos). Despite such promise, some problems persist, from technical difficulties to loopholes in nascent legal frameworks. This article discusses their mechanisms, uses, and limitations and places emphasis on their social implications and future directions.

Keywords: Blockchain Technology; Smart contract, Traditional Contract Decentralized Systems, smart contract security, Internet of Things (IoT), Security, Pay to public key hash (p2pkh), Multi-signature contracts (multisig), Hash time-lock contracts (htlcs), Discrete log contracts (dlcs) Pay to taproot (p2tr).

INTRODUCTION

In the ever-shifting blockchain age, smart contracts have risen to be a pillar technology, remaking transaction and agreement execution. Popularized by the ethereum blockchain in 2017 smart contracts now abound everywhere in things like decentralized finance (defi), decentralized applications (dapps), and non-fungible tokens (nfts). These self-enforcing agreements with terms placed directly within computer code, avoid third-party intermediaries like lawyers or banks, Smart contracts operate as their virtual counterpart to old-style contracts but with the major over traditional aides. They conduct validations automatically on prespecified conditions and terms established and agreed-on automatically without intercession. Time, cost, and errors decline through such automatization while riding on blockchain's immutability to guard with increased guarantee of data guards. In addition to the basic agreement smart contracts implementing applications have involved decentralized autonomous organizations (daos) and application logic Despite all their potential for reform, smart contracts are barriers such as limited flexibility, which depends on the degree of technological sophistication that goes into their programming. In addition legal frameworks underpinning their application are lagging in terms of advancement, and problems linger regarding their imposition across national borders. However, platforms such as etherscan give users interactive information regarding transaction data wallet addresses and contact info making it simplified to make sense of and safer to handle blockchain interfaces.

Among the most important technological developments of the 2020s, smart contracts change the nature of creating and enforcing contracts. This paper discusses their mechanism, types, and applications while discussing the issues and security risks involved in their use. Based on the analysis of the role played by smart contracts in contemporary blockchain-based. systems, we intend to give an integrated view on their contribution to society and future potential impact

LITERATURE REVIEW

1. A review of smart contract technology - Wang et al. 2020

• analyzes the core concepts of smart contracts, dividing them into types and including some well-known platforms supporting them.

• makes a particular emphasis on Ethereum with its extended potential for crafting and keeping smart contracts.

• puts smart contracts into perspective vis-a-vis customary agreements and claims their legality for acceptance.

DOI: 10.17148/IJIREEICE.2025.13314

2. A review of smart contracts in blockchain technology. - Nakamoto & buterin 2018
• explains the function of a smart contract within the context of a blockchain system and its potential for automating contracts in a decentralized platform.
• emphasizes the advantages of smart contracts, including efficiency, cost-effectiveness, and reduced human intervention.
• examine their use across different industries, such as insurance, supply chain, and intellectual property rights.

3. A systematic review of smart contract security. - Atzei, bartoletti & cimoli 2017
• classifies major security weaknesses in smart contracts from their inherent structures and software-related issues.
• reports different tactics and tools utilized to neutralize such security weaknesses.
• assesses the effectiveness and shortcomings of available security analysis tools and techniques in identifying vulnerabilities in smart contracts.

4. Blockchain technology as a catalyst for smart contracts. - hallikas & Dahlberg 2017
• explains how blockchain technology supports smart contracts, reporting challenges and opportunities in different industries.
• describes its application in financial services, healthcare, and supply chain management.
• provides a critical examination of current research issues in this area.

5. Legal issues and obstacles to smart contracts. - Savelyev 2017
• examines the legal environment facilitating smart contracts, concerning their formation and obstacles in legal systems.
• discussed are issues of legitimacy, enforceability, and processes for resolving disputes.
• examines the wider effect of smart contracts on traditional legal systems and processes.

6. Smart contracts in the internet of things (iot): - Christidis & devetsikiotis 2018
• examines smart contract deployment within the internet of things (iot) environment.
• emphasizes their potential to facilitate automated communication between iot devices, making them more efficient and secure.
• examines challenges and opportunities in creating and applying smart contracts for iot deployment.
These literature reviews give a general overview of the research status in the area of smart contracts, ranging from affluent areas like their definition to operation, security, and legal counter-arguments. These can be an excellent source for your journal content.

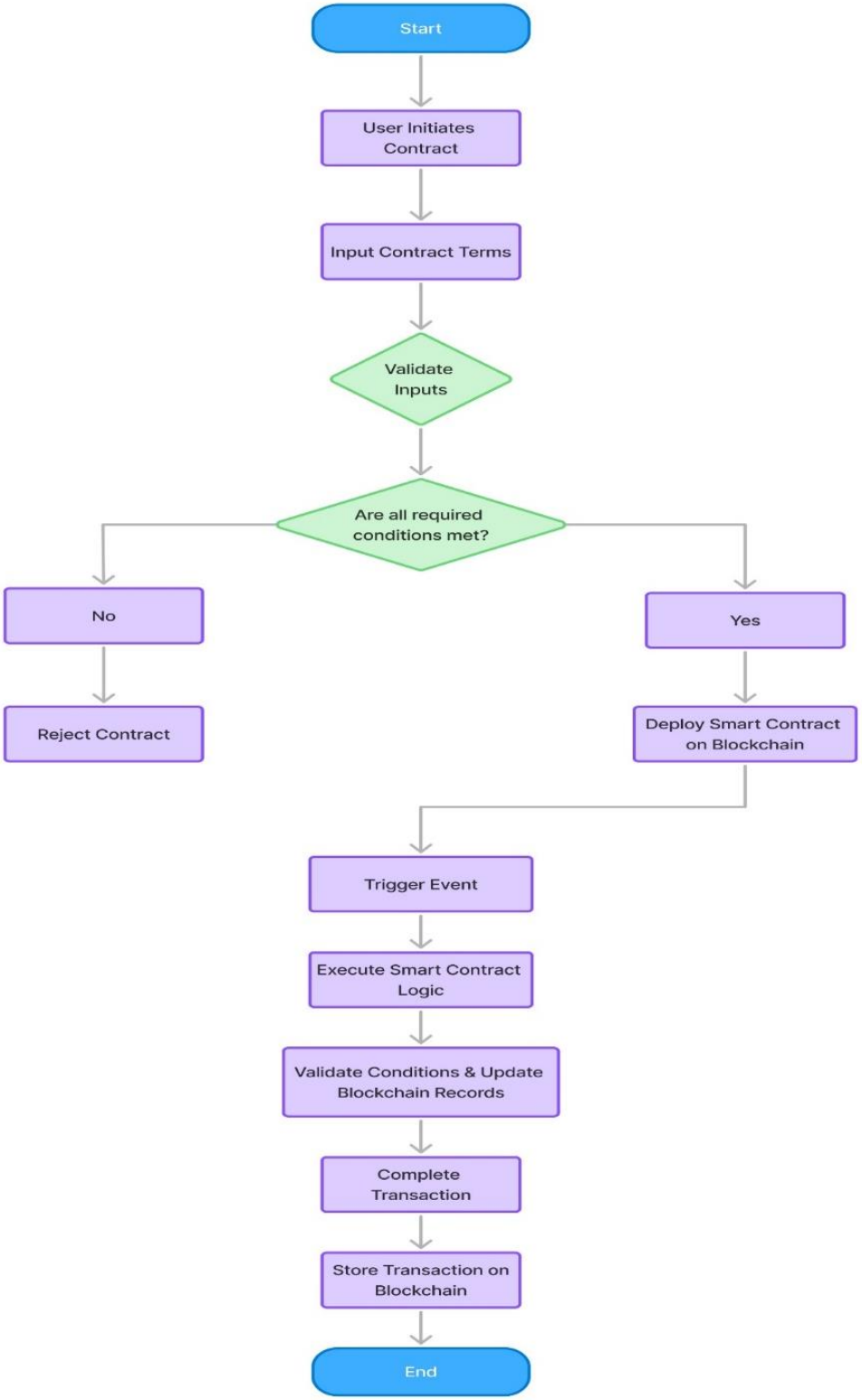
IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13314

DATA FLOW DIAGRAM SMART CONTRACT



© IJIREEICE This work is licensed under a Creative Commons Attribution 4.0 International License

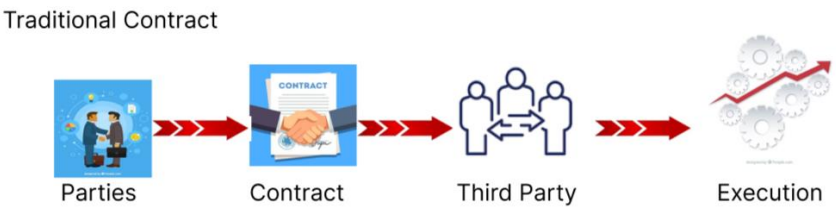
IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13314

Difference between traditional contract and smart contract process.



Difference between the Traditional Contract & Smart Contract

Feature	Traditional Contract	Smart Contract
Definition	A legally binding contract in natural language, enforced by law.	A self-executing contract in code, enforced by blockchain.
Execution	Involves human verification, middlemen (lawyers, notaries, etc.), and legal enforcement.	Automatically executes based on conditions programmed into the code.
Intermediaries	Lawyers, banks, and government agencies are involved.	No middlemen; trust is established using blockchain.
Speed	May take days or weeks to complete and execute.	Executes immediately once conditions are met.
Cost	High because of lawyer fees, paperwork, and third-party involvement.	Lower since it does away with intermediaries and less paperwork.
Transparency	Limited transparency parties can contest terms.	Completely transparent and cannot be changed since it's on a blockchain.
Security	Vulnerable to fraud, tampering, and human error	Very secure thanks to blockchain encryption and decentralization
Enforcement	Enforced through courts and legal actions.	Enforced automatically by the blockchain network.
Modification	Can be changed legal processes.	Immutable once released unless coded with update feature.

 This work is licensed under a Creative Commons Attribution 4.0 International License

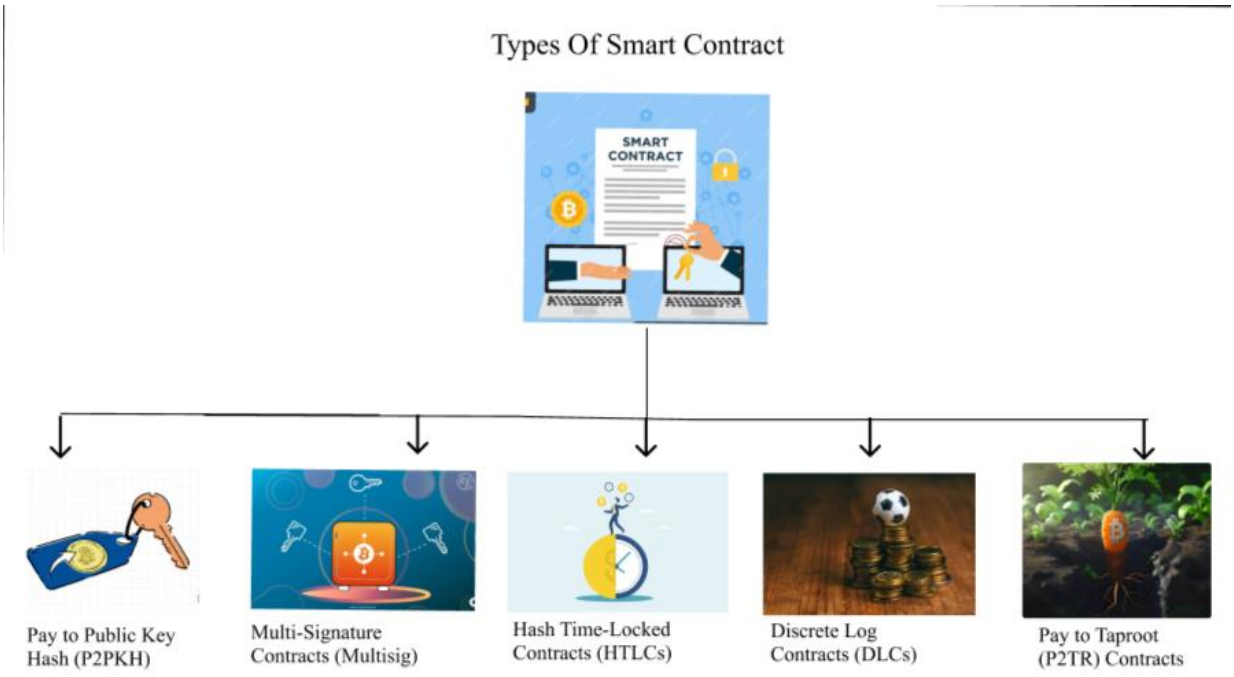
IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13314

TYPES OF SMART CONTRACTS



Contrary to popular belief smart contracts can run on the bitcoin network. However, due to the relative simplicity of the script programming language, which isn't turing complete the functionality of bitcoin smart contracts is limited compared to those on platforms like ethereum. Nevertheless, let's explore various types of smart contracts that thrive on the bitcoin mainnet.

Pay to public key hash (p2pkh)

First up, there's the pay to public key hash (p2pkh) contract, probably the most common smart contract for bitcoin transactions. As its name might suggest you might wonder is this just a simple payment to a hashed public key aka a bitcoin address? Yes, surprisingly even a basic transfer involves a simple smart contract. Think of it as signing a digital agreement with your private key to send funds to another party's address.

Multi-signature contracts (multisig)

Now let's move on to multi-signature contracts also known as multisig. Multisig requires signatures from multiple parties before a transaction can happen. For instance a three-out-of-five scheme means three out of five predetermined signatures are needed to approve the transaction. These types of contracts are used when a wallet with extra security or decentralization of ownership or control is desired.

Hash time-lock contracts (htlcs)

Next, hash time lock contracts (htlcs) introduce conditional time-bound transactions. One example use case for this type of contract is to power atomic swaps, which are cross-chain exchanges of cryptocurrencies without third parties involved. For instance, bob wants to exchange one btc for 15 eth with alice within 1 hour using an htlc. If either of them does not deposit their assets into the contract within the hour, the transaction will be canceled.

Discrete log contracts (dlcs)

Another smart contract enabling conditional p2p transactions is discrete log contracts (dlcs). With dlcs, oracles—which feed blockchains with real-world information—are also involved. Imagine two parties wanting to make a bet or agreement on a future event like the outcome of a sports match. They deposit their wagered funds into a shared dlc and then they agree on terms and pre-sign transactions for potential outcomes. These transactions are like digital agreements that say, if this outcome happens, the bitcoin goes to party a. If that outcome happens, it goes to party b. Finally, they wait for the event to pass and the oracle input before the transaction is settled according to the terms of the contract.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025
DOI: 10.17148/IJIREEICE.2025.13314

Pay to taproot (p2tr)

Lastly, we also have pay to taproot (p2tr) contracts, a product of the taproot upgrade. Taproot is a bitcoin upgrade implemented in late 2021 that improved the privacy, flexibility, and scalability of bitcoin transactions. P2tr transactions, whether simple or complex, appear the same on the blockchain, therefore improving privacy. They also improved flexibility as they enable users to program more sophisticated conditions into the contract and scale better as they are more compact than traditional bitcoin transactions.

These are just a few of the examples of smart contracts available on the bitcoin network. While these smart contracts are simple, they form the foundations of the bitcoin network and enable its use as a financial platform. Many projects are also leveraging the bitcoin mainnet to build scaling and smart contract platforms, which unlocks the functionalities we've come to be familiar with, such as defi, nfts, and more.

CONCLUSION

Smart contracts have revolutionized the way transactions and agreements are carried out within the digital world. By offering automation, transparency, and security, they have set themselves as integral parts of blockchain-based applications, particularly in decentralized finance (defi), decentralized applications (dapps), and non-fungible tokens (nfts). Despite their overpowering advantages, there are disadvantages such as legal complexities, security vulnerabilities, and limited flexibility. As blockchain technology continues to evolve, technological innovation in smart contract platforms and regulatory changes will determine how these concerns are addressed. Future development will likely focus on security enhancements, legal adherence, and support for emerging technologies such as the internet of things (iot). Through ongoing development and research, smart contracts will disrupt industries and redefine the way people interact online, bringing a more efficient and decentralized future

REFERENCES

[1]. Wang et al. (2020). A literature review on smart contract technology.
[2]. Nakamoto & Buterin (2018). A critical review of smart contracts in blockchain technology.
[3]. Atzei, Bartoletti & Cimoli (2017). A systematic review of smart contract security.
[4]. Korpela, Hallikas & Dahlberg (2017). Blockchain technology as a driver for smart contracts.
[5]. Savelyev (2017). Legal perspectives and challenges of smart contracts.
[6]. Christidis & Devetsikiotis (2018). Smart contracts in the Internet of Things (IoT): survey.
[7]. Bhargavan et al. (2016). Formal verification of smart contracts.
[8]. Szabo (1997). The idea of smart contracts.
[9]. Gudgeon et al. (2020). Layer-two blockchain protocols.
[10]. Huang et al. (2019). Smart contract security: Issues, challenges, and solutions.