HPU2. Nat. Sci. Tech. Vol 03, issue 01 (2024), 30-38.

HPU2 Journal of Sciences:
Natural Sciences and Technology

journal homepage: https://sj.hpu2.edu.vn

Article type: Research article

Smart contract: Revolutionizing transactions in the digital age

Thi-Nhung Nguyen*

Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam

Abstract

Blockchain technology is a revolutionary concept that has transformed various industries, offering decentralized and secure solutions for data management. At its core, a blockchain is a distributed and immutable ledger that records transactions across a network of computers. One of the key features of blockchain is its transparency, as each participant in the network has access to the same information. The application of blockchain technology extends across diverse sectors, with finance being the most promising and well-known application domain. Cryptocurrencies, like Bitcoin and Ethereum, rely on blockchain to facilitate secure and transparent transactions. The decentralized nature of blockchain eliminates the need for intermediaries, reducing transaction costs and increasing efficiency. Beyond finance, blockchain is making significant strides in supply chain management. The emergence of blockchain technology has paved the way for ~~a~~ transformative innovation in the realm of digital transactions: smart contracts. These self-executing contracts encoded in blockchain have garnered significant attention for their potential to revolutionize the way agreements are made, executed, and enforced. This paper explores the concept of smart contracts, delving into the underlying technology, finding applications across various industries, legal implications, and future prospects.

Keywords: mathematics, economic, blockchain, smart contracts, transaction

1. Introduction

In the digital age, innovation has emerged as a driving force that reshapes industries, redefines processes, and revolutionizes the way we conduct transactions. Few innovations have garnered as much attention and promise as blockchain technology. The advent of blockchain has catalyzed a shift from traditional centralized systems to decentralized, trustless networks, offering transformative potential across various domains. At the heart of this blockchain revolution lies the concept of smart

* Corresponding author, E-mail: ntnhung@ictu.edu.vn

https://doi.org/10.56764/hpu2.jos.2024.3.1.30-38

Received date: 16-10-2023 ; Revised date: 08-11-2023 ; Accepted date: 01-12-2023

contracts. This paper explores the profound implications, applications, and legal ramifications of blockchain and smart contracts [1]–[5].

Blockchain, often referred to as a distributed ledger technology, emerged with the inception of Bitcoin in 2008. Its founding principles were to establish a transparent, tamper-resistant, and decentralized ledger of transactions. Blockchain technology, in essence, introduces a new paradigm of trust in an environment where intermediaries are no longer the sole arbiters of truth. Transactions on a blockchain are recorded in a transparent and immutable manner, visible to all participants, and validated by a network of decentralized nodes. This decentralized and transparent ledger has profound implications, enabling a plethora of applications far beyond cryptocurrency [6]–[12].

One of the most significant facets of blockchain technology is its potential to redefine trust and security in the digital realm. Traditional systems often rely on intermediaries such as banks to facilitate and validate transactions. These intermediaries not only introduce inefficiencies but also add to vulnerabilities leading to fraud and breaches. By leveraging cryptographic principles and consensus mechanisms, blockchain can replace the need for intermediaries with a decentralized network that self-validates and secures transactions. This paradigm shift in trust and security lays the foundation for an array of innovations, and at the forefront of this transformation are smart contracts [8], [12]–[16].

Smart contracts represent the transformative power of blockchain. These self-executing contracts, encoded in blockchain, automate and enforce the terms of an agreement without intermediaries. Smart contracts function on the “if-then” Statement, executing actions automatically when predefined conditions are met. For example, in a real estate transaction, a smart contract could facilitate the transfer of ownership to the buyer automatically upon receipt of the agreed-upon payment, eliminating the need for title companies and escrow services [13], [14], [17]–[19].

The significance of smart contracts lies in their potential to streamline processes, reduce costs, and enhance trust in transactions across a multitude of industries. Finance is one of the first industries to have adopted smart contracts for automated lending, insurance claims, and asset tokenization. In supply chain management, blockchain and smart contracts enable end-to-end visibility, tracking the journey of products from source to shelf. Healthcare also benefits from secure and transparent patient records, while the legal industry explores the potential of smart contracts to automate legal agreements [14], [17].

Amidst the burgeoning interest in blockchain and smart contracts, this paper aims to explore their multifaceted world. It first delves into the intricacies of blockchain technology and smart contracts, addressing their underlying mechanisms, benefits, and potential pitfalls. Furthermore, it navigates the legal landscape surrounding smart contracts and examines security considerations vital to their adoption. Finally, this paper peers into a horizon of possibilities, charting the evolving landscape of smart contract technology and envisioning its impact on industries and society.

Since blockchain and smart contracts continue to disrupt traditional paradigms and carve new pathways, understanding their potential, challenges, and implications is paramount. This paper attempts to provide a reference, offering insights and knowledge to researchers, practitioners, policymakers, and all those intrigued by the transformative potential of blockchain and smart contracts. Through an in-depth exploration of these subjects, this paper contributes to the ongoing discourse on blockchain technology, fostering a deeper appreciation of its significance and inspiring further innovation and research in this dynamic field. In the following sections, we explore the world of blockchain and smart contracts, uncovering their boundless potential and profound impact on our digital future.

2. Materials and Methods

In the era of digital technology, smart contracts have emerged as a revolutionary concept with the potential to transform the ways agreements are created, executed, and enforced. These self-executing contracts, enabled by blockchain technology, offer a novel approach to automating and securing a wide array of transactions and contractual relationships. Before delving deeper into the intricacies of smart contracts and their applications, it is crucial to establish a foundational understanding of the major components and principles that underpin this transformative innovation.

At the core of smart contracts lies blockchain technology, a decentralized and distributed ledger system that forms the basis for their functionality. Blockchain, first introduced through the creation of Bitcoin in 2008, serves as a tamper-resistant and transparent digital ledger, recording transactions in a chronological and immutable manner. Unlike traditional centralized systems, blockchain operates on a network of nodes, each maintaining a copy of the ledger. This decentralized structure eliminates the need for a central authority and fosters trust among participants. Blockchains employ consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), to validate and add new transactions to the ledger. These mechanisms ensure the integrity and security of the network.

Once recorded on the blockchain, data cannot be altered or deleted, providing a robust and auditable history of transactions. Blockchain relies on cryptographic techniques to secure transactions and control access to data. Public and private keys are used for authentication and digital signatures in order to verify the authenticity of transactions.

Smart contracts represent the transformative potential of blockchain. These contracts, expressed in code, are deployed and executed on a blockchain network. Smart contracts encode the terms and conditions of an agreement directly into computer code. The code acts as the governing authority, automatically executing actions when predefined conditions are met, adhering to the “if-then” logic. One of the key advantages of smart contracts is their automation capability. They eliminate the need for intermediaries, such as lawyers, notaries, or financial institutions, by automatically enforcing contract terms. Transactions and contract executions conducted through smart contracts are transparent and visible to all participants on the blockchain network. This transparency enhances trust among parties. Trust is established within the code and the blockchain network, reducing the risk of fraud and disputes. Participants do not need to trust each other, but rather the technology itself. To develop and deploy smart contracts, a range of blockchain platforms and ecosystems have emerged, each with its unique features and capabilities. Some of the notable blockchain ecosystems include Ethereum and Binance Smart Chain (BSC). Renowned as the pioneer of smart contracts, Ethereum introduced a Turing-complete scripting language that enables the creation of complex and versatile smart contracts. Binance Smart Chain offers compatibility with Ethereum, providing developers with a familiar environment for creating smart contracts, while offering faster transaction speeds and lower fees [14], [15], [17], [20].

With this foundational understanding of blockchain technology and smart contracts, we embark on a journey to explore their applications, challenges, and transformative potential across various industries. Smart contracts represent a paradigm shift in how we conceptualize and engage in agreements, promising greater efficiency, transparency, and security in an increasingly digitized world.

3. Results and Discussion

In the realm of property rentals, the traditional approach to lease agreements has long brought complexities, inefficiencies, and a lack of transparency. Landlords and tenants alike have navigated a web of paperwork, security deposits, and manual payment processes, often leading to disputes, delays, and concerns over fund security. However, the advent of blockchain technology and the implementation of smart contracts have ushered in a new era of rental agreements, promising efficiency, trust, and transparency. This overview delves into the challenges of traditional rental agreements, the evolution of research in this field, and global insights into the adoption of smart contracts for rental agreements. We give some challenges of traditional rental agreements as follows:

Paperwork and Administrative Burden: Traditional rental agreements involve extensive paperwork, including drafting and signing a physical contract, which can be time-consuming and cumbersome for both landlords and tenants.

Security Deposits: Handling security deposits often raises concerns about fair deposit deductions and tenancy deposit protection.

Payment Delays and Disputes: Manual rent collection can lead to payment delays, disputes over payment dates, and the need for frequent reminders.

Lack of Transparency: Transparency in traditional rental agreements can be compromised, with limited visibility into payment histories, maintenance requests, and lease terms.

The challenges posed by traditional rental agreements have sparked interest in leveraging technology to streamline processes and enhance transparency. Over the years, researchers, entrepreneurs, and technologists have explored innovative solutions. The shift from physical to digital lease agreements marked an initial step toward modernization, reducing paperwork and facilitating remote signing. Online rent payment platforms emerged, allowing tenants to make payments electronically, but these platforms often remained disconnected from the core lease agreement. In addition, the breakthrough came with the integration of blockchain and smart contracts. Blockchain's immutable and transparent ledger, combined with self-executing smart contracts, addressed many of the longstanding challenges in rental agreements.

The adoption of smart contracts for rental agreements is gaining momentum worldwide, with notable developments in many countries and regions in the world. Several startups and real estate companies in the U.S. are pioneering the use of blockchain-based smart contracts for rentals. These platforms offer end-to-end solutions, from lease agreement creation to automated rent collection. Countries like Sweden and Estonia have embraced blockchain technology for real estate transactions and rental agreements. Swedish cities are experimenting with blockchain-based land registries, while Estonia's e-Residency program explores digital lease agreements. Singapore and Hong Kong are exploring blockchain's potential in the property rental sector. In Singapore, government agencies are piloting projects to improve rental processes and enhance transparency. South Africa is witnessing experimentation with blockchain and smart contracts for property rentals, aiming to address challenges related to security deposits and payment delays. Australian real estate firms are exploring blockchain to simplify property transactions, and put the adoption of smart contracts for rentals under consideration.

Therefore, the complexities of traditional rental agreements are gradually giving way to the efficiencies and transparency offered by blockchain-based smart contracts. As a global research network and digital adoption continue to evolve, the integration of technology into the rental sector promises to reshape how landlords and tenants engage in agreements, offering a more seamless, secure, and transparent experience for all parties involved.

In today's fast-paced digital world, smart contracts have gained considerable attention for their potential to automate and streamline various aspects of our lives. One of the practical applications is in the realm of rental agreements. Landlords and tenants often face challenges related to timely rent payments, record-keeping, and trust issues. To address these challenges, we propose a smart contract solution that ensures secure and efficient rental payments.

We give a problem description as follows:

Consider a scenario where a landlord wishes to rent out an apartment to a tenant. Traditional rental agreements involve multiple steps, including paper contracts, security deposits, and manual rent collection, which can be cumbersome and time-consuming. Additionally, both parties may have concerns about the security of the deposits and the transparency of the rental process.

We can create a smart contract on a blockchain platform to facilitate the rental agreement between the landlord and tenant.

Smart Contract Creation: The landlord and tenant agree on the terms of the rental agreement, including the monthly rent amount, security deposit, and duration of the lease. These terms are encoded into a smart contract.

Payment Trigger: The smart contract includes a payment trigger that specifies the due date for rent payment. For example, rent may be due on the first day of each month.

Automatic Payment: On the due date, the smart contract automatically withdraws the specified rent amount from the tenant's cryptocurrency wallet (or designated bank account) and transfers it to the landlord's wallet. This process is entirely automated and does not require manual intervention.

Security Deposit Handling: The smart contract also holds the security deposit. If the tenant fulfills the terms of the lease, such as keeping the property maintenance in good condition, the security deposit is automatically returned to them upon lease termination. If there are any damages or breaches of the agreement, the smart contract can handle deductions and refunds accordingly.

Transparency and Record-Keeping: All transactions and terms of the rental agreement are recorded on the blockchain, providing transparency and an immutable history of payments and interactions between the landlord and tenant.

The smart contract automates the rent payment process, eliminating the need for manual rent collection and record-keeping. This saves time and reduces administrative burdens for both parties. Because the terms of the agreement are encoded in the smart contract and executed automatically, there is a high level of trust and transparency between the landlord and tenant. Deposits are securely held within the smart contract, reducing the risk of disputes over payments and security deposit refunds.

Besides some advantages, we found some challenges. Depending on the jurisdiction, smart contracts may not yet be legally recognized. It's essential to ensure that the smart contract adheres to local laws and regulations. Both parties, moreover, should understand how the smart contract works and how to use cryptocurrency wallets if applicable. The smart contract code also must be thoroughly audited to identify and mitigate security vulnerabilities.

A smart contract can be used to streamline a rental agreement on the Ethereum blockchain. Please note that this is a simplified example for demonstration purposes, and real-world implementations would require additional considerations and security measures. We can demonstrate the solution of problem by the Ethereum blockchain as follows.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract RentalAgreement {
    address public landlord;
    address public tenant;
    uint256 public rentAmount;
    uint256 public securityDeposit;
    uint256 public leaseDuration;
    uint256 public leaseStart;
    uint256 public leaseEnd;
    bool public leaseActive;
    bool public securityDepositRefunded;

    event RentPaid(address indexed payer, uint256 amount);
    event LeaseTerminated(address indexed initiator);
    constructor(
        address _tenant,
        uint256 _rentAmount,
        uint256 _securityDeposit,
        uint256 _leaseDuration)

 landlord = msg.sender;
        tenant = _tenant;
        rentAmount = _rentAmount;
        securityDeposit = _securityDeposit;
        leaseDuration = _leaseDuration;
        leaseStart = block.timestamp;
        leaseEnd = leaseStart + _leaseDuration;
        leaseActive = true;
        securityDepositRefunded = false;

    modifier onlyLandlord() {
require(msg.sender == landlord, "Only the landlord can call this function.");

    modifier onlyTenant() {
        require(msg.sender == tenant, "Only the tenant can call this function.");

    modifier isLeaseActive() {
        require(leaseActive, "Lease is not active. }

    function payRent() public payable onlyTenant isLeaseActive {
        require(msg.value == rentAmount, "Incorrect rent amount sent.");
        emit RentPaid(msg.sender, msg.value); }

    function terminateLease() public onlyLandlord isLeaseActive {
        leaseActive = false;
        emit LeaseTerminated(landlord);}

    function refundSecurityDeposit() public onlyTenant {
```

```
require(!securityDepositRefunded, "Security deposit already refunded.");
require(!leaseActive, "Lease must be terminated to refund security deposit.");

payable(tenant).transfer(securityDeposit);
securityDepositRefunded = true;  }
```

The contract is initialized with the landlord's address, tenant's address, rent amount, security deposit, and lease duration.

The *payRent* function allows the tenant to send the monthly rent to the contract.

The *terminateLease* function allows the landlord to terminate the lease.

The *refundSecurityDeposit* function allows the tenant to receive their security deposit back after the lease is terminated.

We give an example to illustrate as follows. We provide some notation in the example:

Landlord: The address of the landlord can be an Ethereum address, such as 0xAbCdEf0123456789....

Tenant: The address of the tenant can also be an Ethereum address.

RentAmount: This is the monthly rent amount, specified in *wei*. For example, 1 ETH is equivalent to 1e18 wei.

SecurityDeposit: The security deposit, also specified in *wei*. In this example, it's set to 2 ETH.

LeaseDuration: The duration of the lease in seconds. For instance, 30 days are equivalent to 2592000 seconds.

LeaseStart: This is set to the current timestamp when the contract is deployed.

LeaseEnd: The timestamp when the lease ends, calculated based on the lease duration.

LeaseActive and securityDepositRefunded: These are Boolean flags indicating whether the lease is active and if the security deposit has been refunded.

Example

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract RentalAgreement {
    address public landlord;              // Address of the landlord
    address public tenant;                // Address of the tenant
    uint256 public rentAmount;            // Monthly rent amount in wei (ETH's smallest unit)
    uint256 public securityDeposit;       // Security deposit in wei
    uint256 public leaseDuration;         // Lease duration in seconds (e.g., 30 days)
    uint256 public leaseStart;            // Timestamp when the lease starts
    uint256 public leaseEnd;              // Timestamp when the lease ends
    bool public leaseActive;              // Indicates if the lease is active
    bool public securityDepositRefunded; // Indicates if the security deposit has been refunded

    event RentPaid(address indexed payer, uint256 amount);
    event LeaseTerminated(address indexed initiator);

    constructor(
        address _tenant,
        uint256 _rentAmount,
        uint256 _securityDeposit,
```

```
uint256 _leaseDuration )
{landlord = msg.sender;
    tenant = _tenant;
    rentAmount = _rentAmount;            // Example: 1000000000000000000 wei (1 ETH)
    securityDeposit = _securityDeposit; // Example: 2000000000000000000 wei (2 ETH)
    leaseDuration = _leaseDuration;     // Example: 30 days in seconds (2592000 seconds)
    leaseStart = block.timestamp;       // Current block timestamp
    leaseEnd = leaseStart + _leaseDuration;
    leaseActive = true;
    securityDepositRefunded = false; }
  modifier onlyLandlord() {
    require(msg.sender == landlord, "Only the landlord can call this function."); }
  modifier onlyTenant() {
    require(msg.sender == tenant, "Only the tenant can call this function."); }
  modifier isLeaseActive() {
    require(leaseActive, "Lease is not active.");  }
  function payRent() public payable onlyTenant isLeaseActive {
    require(msg.value == rentAmount, "Incorrect rent amount sent.");
    emit RentPaid(msg.sender, msg.value); }
  function terminateLease() public onlyLandlord isLeaseActive {
    leaseActive = false;
    emit LeaseTerminated(landlord); }
  function refundSecurityDeposit() public onlyTenant {
    require(!securityDepositRefunded, "Security deposit already refunded.");
    require(!leaseActive, "Lease must be terminated to refund security deposit.");
    payable(tenant).transfer(securityDeposit);
    securityDepositRefunded = true; }
```

4. Conclusion

In conclusion, smart contracts can revolutionize the rental agreement process by automating rent payments, enhancing trust, and ensuring security. While there are challenges to overcome, such as legal recognition and technical knowledge, efficiency and transparency make smart contracts a promising solution for modernizing rental agreements.

References

[1] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A blockchain based cost effective digital voting system using side chain and smart contracts," in *2020 11th International conference on electrical and computer engineering (ICECE)*, Dhaka, Bangladesh, 2020, pp. 467-470, doi: 10.1109/ICECE51571.2020.9393081.

[2] R. Kesavamoorthy, A. Guptha, A. Gupta, A. Gahlot, and A. Pandey, "A state of art review on blockchain technology," in *International conference on intelligent emerging methods of artificial intelligence & cloud computing. IEMAICLOUD 2021. Smart Innovation, Systems and Technologies*, vol. 273, Springer, Cham, 2022, pp. 451–457 doi: 10.1007/978-3-030-92905-3_55.

[3] D. Marginson, M. King, and L. Mcaulay, "Executives' use of information technology: comparison of electronic mail and an accounting information system," *J. Inf. Technol.*, vol. 15, no. 2, pp. 149–164, Jun. 2000, doi:10.1080/026839600344339.

[4] K. Saini, A. Roy, P. R. Chelliah, and T. Patel, "Blockchain 2.O: A smart contract," in *2021 International conference on computational performance evaluation (ComPE)*, Shillong, India, 2021, pp. 524-528, doi: 10.1109/ComPE53109.2021.9752021.

[5] A. T. Pãnescu, and V. Manta, "Smart contracts for research data rights management over the ethereum blockchain network," *Sci. Technol. Libr.*, vol. 37, no. 3, pp. 235–245, Jul. 2018, doi: 10.1080/0194262x.2018.1474838.

[6] M. di Angelo and G. Salzer, “A survey of tools for analyzing ethereum smart contracts,” in *2019 IEEE international conference on decentralized applications and infrastructures (DAPPCON)*, Newark, CA, USA, 2019, pp. 69-78, doi: 10.1109/DAPPCON.2019.00018.

[7] S. T. Alvi, M. N. Uddin, L. Islam and S. Ahamed, "Classification of blockchain based voting: challenges and solutions," in *2020 IEEE Asia-Pacific conference on computer science and data engineering (CSDE)*, Gold Coast, Australia, 2020, pp. 1-6, doi: 10.1109/CSDE50874.2020.9411598.

[8] Angela Walch, “Blockchain applications to international affairs: reasons for skepticism,” *Georg. J. Int. Aff.*, vol. 19, no.1, pp. 27–35, Jan. 2018, doi: 10.1353/gia.2018.0004.

[9] I. Makarov and A. Schoar, “Cryptocurrencies and decentralized finance (DeFi),” *Brookings Pap. Econ. Act*., vol. 2022, no. 1, pp. 141–215, Mar. 2022, doi: 10.1353/eca.2022.0014.

[10] M. A. Khan, and K. Salah, “IoT security: Review blockchain solutions and open challenges,” *Futur. Gener. Comput. Syst*., vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[11] R. R. Konapure, and S. D. Nawale, “Smart contract system architecture for pharma supply chain,” in *International conference on IoT and blockchain technology (ICIBT)*, Ranchi, India, 2022, pp. 1-5, doi: 10.1109/ICIBT52874.2022.9807744.

[12] Z. Liu *et al.*, “Make web3.0 connected,” *IEEE Trans. Dependable Secur. Comput.(TDSC)*, vol. 19, no. 5, pp. 2965–2981, Sep. 2022, doi: 10.1109/TDSC.2021.3079315.

[13] S. Amani, M. Bégel, M. Bortin, and M. Staples, “Towards verifying ethereum smart contract bytecode in Isabelle/HOL,” in *Proceedings of the 7th ACM SIGPLAN international conference on certified programs and Proofs*, Jan. 2018, doi: 10.1145/3167084.

[14] Y. Yuan, and F. Y. Wang, “Blockchain and cryptocurrencies: Model, techniques, and applications,” in *IEEE transactions on systems, man, and cybernetics: Systems(TSMC)*, vol. 48, no. 9, pp. 1421-1428, Sep. 2018,, doi: 10.1109/TSMC.2018.2854904.

[15] S. A. Rehman Khan, and Z. Yu, *Strategic supply chain management*. Springer International Publishing, 2019. doi: 10.1007/978-3-030-15058-7.

[16] S. Panja, S. Bag, F. Hao, and B. Roy, “A smart contract system for decentralized borda count voting,” in *IEEE transactions on engineering management(TEM)*, vol. 67, no. 4, pp. 1323-1339, Nov. 2020, doi: 10.1109/tem.2020.2986371.

[17] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, “A comprehensive survey on graph neural networks,” in *IEEE transactions on neural networks and learning systems (TNNLS)*, vol. 32, no. 1, pp. 4–24, Jan. 2020, doi: 10.1109/TNNLS.2020.2978386.

[18] D. Macrinici, C. Cartofeanu, and S. Gao, “Smart contract applications within blockchain technology: A systematic mapping study,” *Telemat. Informatics*., vol. 35, no. 8, pp. 2337–2354, Dec. 2018, doi: 10.1016/j.tele.2018.10.004.

[19] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, “Blockchain-enabled smart contracts: architecture applications and future trends,” in *IEEE transactions on systems, man, and cybernetics: Systems(TSMC)*, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[20] R. Ioanna, D. Chaido, and S. Emmanouil, “The bitcoin's network effects paradox-a time series analysis ioanna roussou chaido dritsaki,” *Theor. Econ. Lett.*, vol. 9, no. 6, August 2019, doi:10.4236/tel.2019.96126.