Proceedings of the 3rd International Conference on Financial Technology and Business Analysis
DOI: 10.54254/2754-1169/134/2024.18813

The Security Payment Based on Blockchain Techniques: Evidence from ETH

Xiran Tao[1,a,*]

[1]*School of Information Science and Technology, North West University, Xi'an, China*
a. taoxiran666@stumail.nwu.edu.cn
**corresponding author*

Abstract: As a matter of fact, with the continuous development of blockchain technology, its potential in various applications is gradually emerging especially in recent years. With this in mind, this article explores the practical experience of applying blockchain technology in e-commerce shopping platforms, especially the challenges and solutions encountered in product management, purchase process, and logistics status tracking. Through the analysis of these experiences, this research summarizes the key points that should be paid attention to in the process of designing and implementing blockchain e-commerce platforms. At the same time, this study puts forward relevant suggestions to provide references for the development of similar projects according to the analysis. These results delve into the application of blockchain technology in e-commerce platforms, focusing on challenges as well as solutions in product management, purchasing, and logistics tracking. Overall, it highlights essential considerations for designing blockchain-based e-commerce systems and offers recommendations for future projects.

Keywords: Blockchain, security payment, ETH.

1. Introduction

The inception of blockchain technology dates back to 2008 when anonymous creator Satoshi Nakamoto released a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". In this white paper, the decentralized digital money known as Bitcoin and the blockchain technology that powers it were introduced. The Bitcoin network was formally launched in 2009 when Satoshi Nakamoto released the first software and mined the Genesis Block. Blockchain technology has been evolving and growing since January 2009. At first, blockchain technology created the following characteristics and backed Bitcoin [1]:

- Financial transactions and the Bitcoin cryptocurrency are decentralized.
- Use a distributed database to decentralize data storage.
- Gets rid of the central body in a centralized system that checks transactions.
- Assistance with data integrity and transparency within a peer-to-peer network.
- Presents the idea of PoW.

Bitcoin gradually gained acceptance, and exchanges and wallet services began to emerge. 2010 the first Bitcoin transaction took place, marking its practical use as a currency. People began to realize

DOI: 10.54254/2754-1169/134/2024.18813

the potential of blockchain technology beyond Bitcoin. Ethereum was launched in 2015, offering smart contract functionality, which allowed blockchain to be used in more complex application scenarios. Ethereum's smart contract functionality sparked an ICO (Initial Coin Offering) boom, with many new projects raising funds by issuing tokens. Meanwhile, the application of blockchain technology in finance, supply chain, and other fields began to increase. Blockchain technology has gradually matured, with its application fields continuously expanding, including decentralized finance (DeFi), non-fungible tokens (NFTs), and enterprise blockchain solutions. Governments and large enterprises have also started exploring the potential of blockchain technology. The development of blockchain technology demonstrates its evolution from a technology-supporting digital currency to an innovative technology with broad application potential.

There may be economic turmoil and even societal upheaval as a result of the antiquated flaws in current currencies and the assortment of hazards, including as inflation, that are partially brought on by poor management. Thus, steps need to be done to avoid these problems. In the years since the 2008 global financial crisis, cryptocurrencies have continued to grow and evolve. The biggest obstacles facing today's online retailers are the outrageous credit card companies' fees, the high expense of escrow services, the limitations on merchant services in numerous nations and areas, the complicated implementation of payment software, and refunds. Online retailers can benefit greatly from employing cryptocurrencies. The bitcoin economy has a total market value of more than $1 billion and is still expanding. Cryptocurrency protocols enable safe digital transactions over the internet by avoiding the need to trust a third party. This lowers indirect costs and offers instantaneous delivery of digital goods in exchange for digital currencies. Cryptocurrency is a type of digital money that is generated and maintained in conjunction with proof-of-work techniques. It is based on cryptography. A decentralized network of synchronized peer-to-peer computer nodes generates and authenticates cash transfers among nodes in the network. Cryptocurrencies have shown to be a developing form of payment in recent years. These innovative solutions allow people and businesses to deal swiftly and efficiently over the Internet without requiring credit card or bank information. By leveraging the characteristics of these currencies, merchants can set up an account and accept payments within minutes, allowing customers worldwide to purchase goods and services [2].

Recently, the rapid advancement of technology has significantly transformed the way commerce is conducted. As online shopping becomes increasingly prevalent, driven by the convenience it offers consumers, there is a growing demand for more sophisticated and secure digital shopping platforms. To meet these needs, integrating blockchain technology into e-commerce platforms has emerged as a promising solution, offering enhanced security, transparency, and transaction efficiency. The program designed in this initiative is a cutting-edge shopping platform that encompasses a multitude of functionalities, aiming to revolutionize the digital shopping experience. This platform is unique in incorporating blockchain technology, specifically interacting with the Ethereum blockchain, to ensure secure and transparent transactions for vendors and consumers. The platform’s primary features include adding and modifying goods, managing shipping logistics, facilitating the purchase of goods, and providing users with the means to check their purchased orders. Each of these functions is carefully integrated to provide a seamless shopping experience, making it easy for users to navigate and manage their transactions. In a groundbreaking implementation, the platform interacts directly with the blockchain. By doing so, it develops a platform-specific currency that operates on the Ethereum blockchain, enabling users to conduct transactions with high security and minimal risk of fraud. This integration not only enhances the trustworthiness of the platform but also leverages the decentralized nature of blockchain to provide users with more control and transparency over their transactions. The inclusion of an Ethereum wallet allows users to transact using cryptocurrency, further modernizing the purchasing process and attracting a tech-savvy audience who are increasingly looking to engage in blockchain-based financial activities. This feature is particularly appealing in an

DOI: 10.54254/2754-1169/134/2024.18813

era where digital currencies are gaining mainstream acceptance and provide a hedge against traditional financial system instabilities. By embracing these cutting-edge technologies, the platform is not only poised to meet current consumer demands but is also well-prepared to adapt to future trends in digital commerce. The ability of the platform to support such a diverse range of functionalities while maintaining a secure and trustworthy environment marks a significant step forward in the evolution of online shopping solutions. Through this comprehensive platform, the fusion of traditional e-commerce practices with modern blockchain technology highlights the innovative trajectory of the industry. This integration serves as a prototype for future developments in the sector, where security, efficiency, and user empowerment are paramount. By continuously evolving and adapting to technological advancements, the platform sets a new standard for digital marketplaces that prioritize consumer confidence and transaction integrity. This paper aims to introduce the famous topic of security payment based on ETH, including basic descriptions of ETH, security payment of ETH, limitations and prospects, and the conclusion part.

2. Basic Descriptions of ETH

Decentralized and open-source, Ethereum (ETH) is a blockchain platform that was first proposed by Vitalik Buterin in 2013 and went live in 2015. Ethereum was created to offer a decentralized virtual computer with smart contract execution capabilities. Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. Ethereum's smart contract capabilities and consensus mechanism are its fundamental components. Ethereum was first based on the Proof of Work (PoW) consensus method like Bitcoin. But Ethereum is switching to a Proof of Stake (PoS) mechanism, dubbed "Ethereum 2.0" or "Serenity," to increase efficiency and scalability. PoS lowers energy consumption by choosing validators at random to build new blocks. Turing-complete Ethereum Virtual Machine (EVM) powers Ethereum smart contracts, enabling programmers to create intricate contracts with languages like Solidity. The deterministic execution of smart contracts ensures security and dependability since the same input will always result in the same output [3].

After Bitcoin, Ethereum is currently the second-largest cryptocurrency globally as of 2023. The dynamic Ethereum ecosystem facilitates a diverse array of decentralized applications (DApps), such as non-fungible token (NFT) exchanges and decentralized finance (DeFi) platforms. Ethereum's current scalability and high transaction price problems are intended to be addressed by its upgrade plans, such as Ethereum 2.0 [4]. Cryptographic Features Ethereum's security is primarily reflected in its cryptographic algorithms and decentralized nature. Ethereum uses the Keccak-256 hash function (a variant of SHA-3) to ensure data integrity and security. Transactions and contract executions require cryptographic signatures for verification, ensuring that only authorized users can initiate transactions. Moreover, Ethereum's decentralized nature means there is no single controlling entity, and the network's security relies on globally distributed nodes. This decentralized structure enhances Ethereum's resilience against censorship and attacks. In summary, through its innovative smart contract functionality and evolving consensus mechanisms, Ethereum has become a crucial component of blockchain technology, driving the development of decentralized applications worldwide.

3. Security Payment of ETH

To comprehensively explore the security payment applications of Ethereum (ETH) in transactions, this research will delve into the mechanisms that ensure secure transactions on the Ethereum network, recent advancements in the field, and scholarly research conducted in recent years. Additionally, this study will include a flowchart to illustrate the transaction process on Ethereum. Ethereum has become

DOI: 10.54254/2754-1169/134/2024.18813

widely recognized not only for its smart contract functionality but also for its robust security mechanisms in financial transactions. Here are some key aspects of Ethereum's security features, along with references to recent scholarly work. Core security features of Ethereum transactions are as follows:

- Smart Contracts: Ethereum's smart contracts are not just about automated execution but also about security. Written mainly in Solidity, these contracts are deployed on the Ethereum blockchain and virtually immutable. They manage and verify transactions automatically to enforce terms without intermediary involvement, eliminating many traditional security risks like contractual fraud or third-party manipulation [5].
- Cryptographic Security: The Keccak-256 hash function, a variant of SHA-3, is used by Ethereum for hashing transactions, ensuring data integrity. Each transaction is signed with the sender's private key and then broadcast to the network; only after recipient nodes verify the sender's signature is the transaction validated. Ethereum uses powerful cryptographic techniques to secure transactions [6].
- Proof of Stake (PoS): Ethereum 2.0 has changed its Proof of Work (PoW) to Proof of Stake (PoS), to strengthen security to fend off frequent cryptocurrency transactional hazards like double-spending and 51% assaults. Validators must "stake" a significant portion of ETH to match their motivations while maintaining the integrity of the network.
- Decentralization: The decentralized nature of Ethereum is a crucial aspect of its security. Ethereum significantly lowers the risks associated with central points of failure by having thousands of nodes verify transactions worldwide. This makes it more difficult to carry out censorship, fraud, and service outages.

Ethereum's scalability issues have pushed for innovations like Layer 2 solutions (e.g., Rollups, State Channels) which enhance both efficiency and security. Privacy techniques such as zero-knowledge proofs (ZKPs) have also been employed to allow private, verifiable transactions without exposing user data on the public ledger [7]. To enable multiple parties to collaboratively compute a function over their inputs while preserving the privacy of their inputs, research has been conducted on the integration of MPC with Ethereum. This has important ramifications for safe Ethereum applications and financial transactions. Formal verification methods have been adopted to combat vulnerabilities in smart contracts. These methodologies mathematically prove the correctness of contract code, thereby preventing common vulnerabilities like reentrancy attacks or integer overflows (seen from Fig. 1) [8].

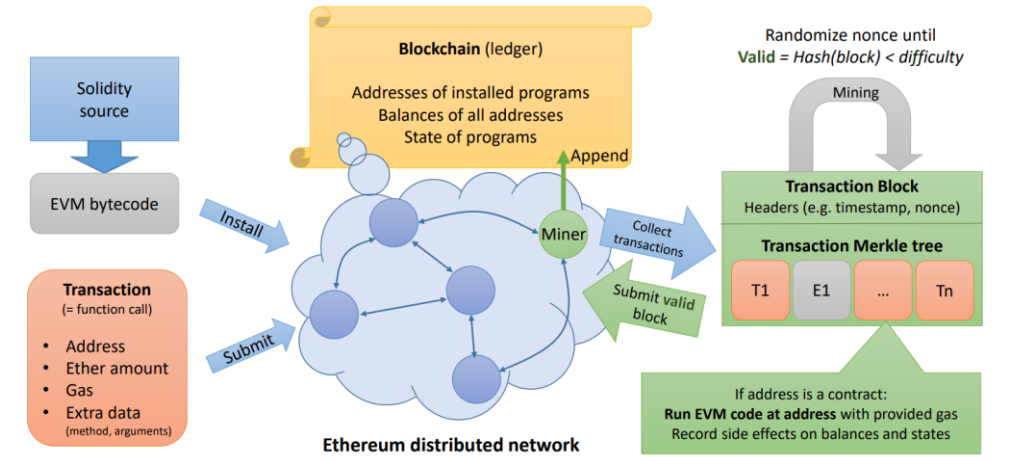

Figure 1: Workflow of ETH [8].

DOI: 10.54254/2754-1169/134/2024.18813

4. Limitations and Future Prospects

Ethereum, as a groundbreaking blockchain platform, has significantly impacted digital transactions while also encountering various challenges. This overview covers its current limitations and prospects. The scalability of Ethereum is one of its main drawbacks. In comparison to more established financial systems like Visa, which can handle hundreds of transactions per second, the network can currently manage just 15–30 transactions per second. Due to this restriction, there is network congestion during times of heavy demand, which raises transaction costs and creates delays. It is challenging for Ethereum to completely support a global financial infrastructure because of the scalability issue. Known as "gas fees," these costs can become prohibitively high when network demand increases, making small transactions economically unfeasible [9]. The variability in transaction costs poses a hurdle for mainstream adoption, particularly for microtransactions or use cases involving numerous small payments. This unpredictability affects the user experience and can deter potential users from using Ethereum-based applications. Although Ethereum is transitioning to Ethereum 2.0 with a Proof of Stake model, the previous Proof of Work mechanism was energy-intensive, contributing significantly to the overall carbon footprint of blockchain operations [10]. The environmental impact of mining operations has raised concerns among environmentally conscious users and regulatory bodies. Writing secure smart contracts demands a comprehensive understanding of blockchain programming. Errors in smart contracts can lead to vulnerabilities, potentially resulting in the loss of funds, as shown in earlier occurrences like The DAO hack [11]. To guarantee security, these risks require stringent development procedures and sometimes expensive audits.

The shift to Ethereum 2.0 offers increased scalability, security, and sustainability. Ethereum wants to drastically improve transaction throughput while lowering energy consumption by switching to Proof of Stake. To increase transaction efficiency off the main chain, Layer 2 solutions like Rollups and State Channels are also being developed [12]. This could significantly reduce congestion on the main Ethereum network. Future developments focus on interoperability with other blockchains, enhancing Ethereum's utility in a multi-chain ecosystem. Projects like Polkadot and Cosmos may offer bridges that enable Ethereum to communicate with other networks, broadening its use cases and facilitating smoother exchanges of value and information across different blockchain platforms [13]. Ethereum is the backbone of DeFi, which continues to grow. The rise of DeFi showcases Ethereum's potential to revolutionize traditional financial services by offering decentralized alternatives for lending, insurance, and trading without intermediaries [14]. This sector represents a significant shift toward decentralized financial models, offering increased accessibility and innovation. Advances in formal verification and programming languages are expected to make smart contracts more secure and easier to develop [15]. These developments could significantly mitigate the risks associated with smart contract vulnerabilities. Improved developer tools and languages will help streamline the smart contract creation process, making Ethereum a more accessible platform for developers. As blockchain technology becomes more integrated into mainstream financial systems, regulatory frameworks are evolving to accommodate cryptocurrencies and digital contracts. Ethereum stands to benefit from clearer regulations, as they could provide the legal certainty necessary for broader institutional adoption and innovation [16].

5. Conclusion

To sum up, Ethereum is a trailblazing blockchain platform that, despite major obstacles, is revolutionizing the world of decentralized apps. In the analysis, this study has emphasized Ethereum's strong security features for financial transactions, which are supported by its cryptographic protocols and the shift to Ethereum 2.0, which seeks to improve energy efficiency and scalability. One reviewed recent studies on smart contract applications and technology advancements, highlighting both the

DOI: 10.54254/2754-1169/134/2024.18813

promise offered by continuing advancements and innovations as well as its drawbacks, such as high transaction prices and scalability problems. Looking to the future, Ethereum's transition to a proof-of-stake consensus mechanism and the implementation of Layer 2 solutions herald a promising era of increased efficiency, reduced energy consumption, and broader adoption across multi-chain ecosystems. These improvements are crucial for enhancing Ethereum's usability and security, ensuring its continued prominence in the blockchain and DeFi sectors. The present study highlights Ethereum's crucial contribution to the advancement of blockchain technology. It also illustrates the technical obstacles and enormous potential that will persist in stimulating innovation and investment in the field of decentralized applications. Ultimately, the integration of blockchain technology into e-commerce platforms poses a number of opportunities as well as challenges. Through tackling problems with product management, procurement procedures, and logistics tracking, blockchain can improve transparency, security, and efficiency. The knowledge gained from real-world applications highlights the significance of strategic planning and innovation in resolving these obstacles. As blockchain technology develops, its impact on e-commerce is expected to increase, opening up new opportunities for growth and customer interaction. Going forward, future initiatives should concentrate on scalability, user experience, and interoperability in order to fully realize the potential of blockchain in the virtual marketplace.

References

[1] *Aggarwal, S. and Kumar, N. (2021) History of blockchain-blockchain 1.0: Currency. Advances in Computers, 121, 147-169.*

[2] *Ahamad, S., Nair, M. and Varghese, B. (2013) A survey on crypto currencies. 4th International Conference on Advances in Computer Science, AETACS. Citeseer, 2013, 42-48.*

[3] *Wood, G. (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.*

[4] *Buterin, V. (2014) A next-generation smart contract and decentralized application platform. White Paper, 3(37), 2-1.*

[5] *Atzei, N., Bartoletti, M. and Cimoli, T. (2017) A survey of attacks on Ethereum smart contracts (SoK). Proceedings of the 6th International Conference on Principles of Security and Trust, 164-186.*

[6] *Bonneau, J., Miller, A., Clark, J., et al. (2015) Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. IEEE symposium on security and privacy, 104-121.*

[7] *Poon, J. and Buterin, V. (2017) Plasma: Scalable autonomous smart contracts. White paper, 1-47.*

[8] *Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Pironti, A., Strub, P. Y. and Swamy, N. (2016) Formal verification of smart contracts: Short paper. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp 91-96.*

[9] *Antal, C., Cioara, T., Anghel, I., Antal, M. and Salomie, I. (2021) Distributed ledger technology review and decentralized applications development guidelines. Future Internet, 13(3), 62.*

[10] *Narayanan, A. (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press*

[11] *Atzei, N., Bartoletti, M. and Cimoli, T. (2017) A survey of attacks on Ethereum smart contracts (SoK). In Proceedings of the 6th International Conference on Principles of Security and Trust, 164-186.*

[12] *Brent, L., Jurisevic, A., Kong, M., et al. (2018) Vandal: A scalable security analysis framework for smart contracts. arxiv preprint arxiv:1809.03981.*

[13] *Zamyatin, A., Harz, D., Lind, J., et al. (2019) Xclaim: Trustless, interoperable, cryptocurrency-backed assets. IEEE symposium on security and privacy (SP), 193-210.*

[14] *Schär, F. (2021) Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review, 17.*

[15] *Bhargavan, K., Delignat-Lavaud, A., Fournet, C., et al. (2016) Formal verification of smart contracts: Short paper. Proceedings of the 2016 ACM workshop on programming languages and analysis for security, 91-96.*

[16] *Zohar, A. (2015) Bitcoin: under the hood. Communications of the ACM, 58(9), 104-113.*