UNIVERSITY OF TRENTO

Blockchain

Project Report

JANUS

GitHub

Matteo Beltrami, Luca Pedercini, Christian Sassi

August 22, 2025

Contents

Chapter 1
Introduction

1.1 Problem Statement

The increasing global adoption of cryptocurrencies as a method of payment is undeniable. However, this emerging ecosystem faces significant challenges that hinder broader acceptance and trust. For many, cryptocurrencies remain an enigmatic and often perceived as unreliable payment mechanism, frequently associated with illicit activities and lacking traditional oversight mechanisms. Despite this, a growing number of legitimate businesses are exploring and adopting cryptocurrencies to expand their customer segments [12] [19] [20].

In most decentralized payment scenarios, a fundamental issue is the irreversibility of transactions. Once funds are dispatched, they are irrevocably transferred, necessitating complete reliance on the seller's integrity. As history has repeatedly demonstrated across various digital payment methods, this inherent trust is not always warranted. Furthermore, while some existing services (e.g., [13], [14], [15], and [25]) offer escrow-like functionalities [23], they frequently compromise a core tenet of cryptocurrency: user anonymity. These services typically mandate account creation and stringent identity verification procedures (e.g., using official identification documents). Although such measures may enhance security, they invariably link a user's real-world identity to their transactional history, thereby undermining the privacy cryptocurrencies inherently offer.

This prevailing lack of inherent safeguards, coupled with the compromise of anonymity in existing third-party solutions, creates a significant barrier to mainstream cryptocurrency adoption for both buyers and sellers. Buyers face considerable risk, while sellers struggle to establish trust with their customers in an environment lacking of robust, privacy-preserving transactional security.

1.2 Project Goals and Objectives

The primary goal of this project is to address the aforementioned limitations by developing Janus, a smart contract-based escrow system. Janus is designed to introduce a layer of security and guarantees for buyers, simultaneously enabling sellers to cultivate trust with their customers and facilitate increased sales within the cryptocurrency payment domain.

Our specific objectives are to:

- **Enhance Buyer Protection**: Implement a robust escrow mechanism that holds funds in trust for a defined period, allowing buyers to request refunds in the event of transactional disputes or non-compliance by the seller.

- **Foster Seller Trust**: Provide a reliable service that mitigates buyer risk, thereby encouraging greater adoption of cryptocurrency payments by legitimate businesses and enhancing their credibility.

- **Preserve User Anonymity**: Design a solution that identifies users solely by their wallet addresses, eliminating the need for personal identity verification and thereby upholding the principle of anonymity inherent to cryptocurrencies. This approach ensures that personal information provided during a refund request cannot be linked back to the user. While total anonymity in blockchain is a complex challenge, and advanced blockchain analysis and forensic techniques exist to investigate and interpret on-chain activity [18], Janus strives to provide a significant level of privacy for its users, identifying them only by their on-chain addresses.

1.3 Scope of the Project

The scope of this project encompasses the application of knowledge acquired during the Blockchain course, particularly concerning the technical and implementation aspects of blockchain network setup and smart contract development. This includes:

- **Smart Contract Development**: The core deliverable is the Janus smart contract, meticulously developed using Solidity.

- **Comprehensive Testing**: The developed smart contract underwent exhaustive testing, with more than 100 distinct test cases designed to verify its logic, ensure correct execution of all functionalities, and confirm the robustness of the contract to prevent erroneous or malicious operations. This rigorous testing aims to assure the absence of critical bugs in its core logic.

- **Business Analysis and Strategy**: A significant aspect of this project involves analyzing the business viability and strategic positioning of a service like Janus within the cryptocurrency payment ecosystem. This includes conducting a market overview, validating the problem statement with market needs, formulating a clear value proposition, and outlining a foundational business model.

- **Basic Web Demonstration**: A supplementary web application has been developed using Python Flask to provide a user-friendly interface for testing and demonstrating the smart contract's functionalities.
- **Operational Assumptions**: For demonstration purposes, the project assumes the existence of an off-chain, anonymous communication channel between the contract owner, buyer, and seller for resolving refund disputes. The development of such a channel is considered beyond the scope of this project's objectives.

1.4 Report Structure

This report is structured to provide a comprehensive overview of the Janus project, from its foundational problem statement to its technical implementation and future implications.

- **Section 1: Introduction** will set the context by outlining the problem Janus aims to solve in the cryptocurrency payment space, defining the project's goals and objectives, and clarifying its scope and limitations.
- **Section 2: Market Analysis and Business Opportunity** will delve into the market overview for cryptocurrency payments, validate the existing problems for both buyers and sellers, articulate Janus's unique value proposition, and detail its business model elements.
- **Section 3: Janus: System Design and Architecture** will provide a high-level overview of Janus as a smart contract, explain its core functionalities and escrow mechanism, describe the smart contract's design principles, and list the underlying technology stack.
- **Section 4: Practical Considerations and Future Work** will discuss the implications of decentralization, the importance of event-driven monitoring for practical applications, and outline potential future enhancements for the Janus project.

Chapter 2

Market Analysis and Business Opportunity

2.1 Market Overview

The cryptocurrency payment market, which includes escrow services like Janus, is experiencing robust growth driven by the increasing adoption of digital currencies and the need for secure transaction mechanisms.

2.1.1 Current Market Size and Key Market Segments

Research suggests the global cryptocurrency payment apps market was valued at approximately USD 557 million in 2024 and is projected to grow at a compound annual growth rate (CAGR) of 17.8% through 2033 [11]. This growth is fueled by the rising acceptance of cryptocurrencies as a payment method, particularly in e-commerce and peer-to-peer transactions, alongside advancements in blockchain technology that enhance transaction security and efficiency.

The market is segmented by application [10], with key areas including:

- **E-commerce**: Online retailers increasingly accept cryptocurrencies, driven by lower transaction fees and faster processing times.
- **Online Services**: Platforms offering digital services, such as freelancing or subscription-based models, are integrating crypto payments.
- **Decentralized Marketplaces**: Blockchain-based platforms, including those for NFTs and other digital assets, rely on secure payment solutions like escrow services.

The target demographic primarily includes tech-savvy males aged 18-45 with higher education and income levels, concentrated in developed countries with significant cryptocurrency adoption, such as the United States, China, Japan, South Korea, and various European and other non-European countries [3] [4]. This demographic values the anonymity and security offered by cryptocurrencies, aligning with Janus's focus on privacy and trust.

2.1.2 Market Trends and Driving Factors

Several trends are shaping the cryptocurrency escrow market:

- **Rise of Decentralized Escrow Services**: Smart contract-based platforms are gaining popularity due to their automation and reduced need for central authorities [17].
- **Integration with Multiple Blockchains**: Escrow services are expanding to support various cryptocurrencies, enhancing flexibility for users.
- **Focus on Security and Volatility Mitigation**: Services are adopting stablecoin conversions and multi-signature wallets [2] to protect against price fluctuations and fraud.
- **Emphasis on Regulatory Compliance**: As regulatory oversight increases, platforms are integrating Know Your Customer (KYC) [24] and Anti-Money Laundering (AML) [22] measures to align with legal requirements.

These trends are driven by:

- **Growing Cryptocurrency Adoption**: Approximately 15,174 businesses worldwide accepted cryptocurrencies as payment in 2024, with Bitcoin being the most popular [16].
- **Need for Trust and Security**: The irreversible nature of cryptocurrency transactions heightens the demand for escrow services to mitigate fraud risks.
- **Blockchain Advancements**: Improvements in smart contract technology enable more efficient and secure escrow solutions.
- **Expansion of DeFi Applications**: The growth of decentralized finance, including NFT marketplaces and lending protocols, increases the need for escrow services.

2.1.3 Competitive Landscape Analysis

The competitive landscape for cryptocurrency escrow services comprises both centralized and decentralized platforms. Janus distinguishes itself from centralized services, such as the Crypto.com exchange [7], which provide escrow-like solutions, as well as from decentralized platforms like Uniscrow [21], Counos [6], and Escrow.com [8]. Unlike these alternatives, Janus employs a smart contract-based escrow system that preserves user anonymity by relying solely on wallet addresses rather than identity verification, thereby upholding the core privacy principles of cryptocurrencies.

2.2 Problem Validation (Market Need)

The cryptocurrency payment market is experiencing significant growth, driven by the rising adoption of digital currencies and the increasing demand for secure transaction mechanisms. However, despite this expansion, key challenges remain, particularly the lack of trust and security, which continue to hinder the widespread acceptance of cryptocurrencies as a reliable means of payment.

In contrast, traditional payment services like PayPal are widely and globally adopted. As of December 2024, PayPal has 434 million active users and is integrated into 10.3 million live websites, holding a 45% share of the global payments market, making it the leading payment option worldwide [1]. One of PayPal's key strengths lies in the security it provides for both buyers and sellers, managing disputes and handling refunds when necessary.

These data reflect the high level of trust users place in the platform and highlight the growing need for services that protect online purchases and enhance the shopping experience. Users feel safe using PayPal and recognize its essential role in e-commerce.

Janus seeks to bring these same benefits to the cryptocurrency ecosystem. By addressing two critical market needs, the lack of security and trust in crypto transactions, and the demand for anonymity within secure frameworks, Janus aims to offer a trusted, user-friendly environment akin to PayPal, but tailored for the world of digital currencies.

2.2.1 Lack of Security and Trust in Cryptocurrency Transactions

Cryptocurrency transactions are irreversible, exposing buyers to risks such as fraud and non-delivery, especially when dealing with unknown parties. The absence of recourse mechanisms undermines trust and limits broader adoption. Mutambik et Al. in [19] state that ”if cryptocurrencies are to attract mass adoption for settlement, they will need to have merchant and consumer trust” and analyze the factors that contribute to the development of trust in cryptocurrencies. The market is rapidly expanding highlighting the urgent need for secure, trust-enhancing solutions. The rise of decentralized escrow services using smart contracts reflects this demand for safer, intermediary-free transactions.

2.2.2 Need for Anonymity in Secure Transaction Mechanisms

While cryptocurrencies offer pseudonymity, many escrow services compromise user privacy by enforcing KYC procedures. This discourages users who value anonymity, a core appeal of crypto. The convergence of these needs within a growing market segment underscores the demand for a solution like Janus, that addresses this by providing a smart contract-based escrow that requires no identity verification, identifying users only by wallet address.

2.3 Value Proposition (Why Janus?)

In a cryptocurrency payment market where trust and privacy remain elusive for many users, Janus emerges as a pioneering solution that bridges these gaps through a decentralized escrow service. By leveraging smart contract technology, Janus offers a compelling blend of security, anonymity, and user autonomy that distinguishes it from both centralized and decentralized competitors. This section explores how Janus delivers unique value to its target audience providing tangible benefits to both buyers and sellers.

- **Addressing Security Concerns**: Janus tackles the inherent risks of cryptocurrency transactions by implementing a robust escrow mechanism. When a buyer initiates a purchase, their payment is securely held by the Janus smart contract for a 30-day warranty period. During this time, if issues such as non-delivery or product defects arise, buyers can request a refund through an anonymous communication process with the seller. If approved, funds are returned to the buyer, minus minimal network fees; otherwise, sellers can withdraw the payment post-warranty with a 1% fee deduction. This system not only safeguards buyers against fraudulent sellers but also establishes a structured resolution process that enhances confidence in cryptocurrency-based commerce.

- **Preserving Anonymity**: Unlike many escrow services that mandate identity verification to comply with regulatory standards or facilitate dispute resolution, Janus prioritizes the privacy inherent to cryptocurrencies. It identifies users exclusively by their wallet addresses, ensuring that transaction details and dispute communications remain unlinked to real-world identities.

- **Decentralization and User Control**: Users retain full control over their funds via custodial or non-custodial wallets, such as MetaMask [5], rather than entrusting them to third-party custodians. This decentralized framework reduces the risk of mismanagement or data breaches while empowering users with autonomy over their financial interactions. The absence of a central authority further enhances transparency, as all transaction logic is encoded and verifiable on the blockchain.

- **Benefits for Sellers**: Janus offers more than just buyer protection, it also creates a supportive environment for sellers to succeed. By using this escrow service, sellers show they are trustworthy, helping to ease buyers' concerns about potential transaction risks. This trust-building feature can boost sales, especially from cautious buyers who might normally avoid using cryptocurrency. The low 1% fee on completed transactions is a cost-effective trade-off to pay for the added marketability and customer trust that Janus provides.

2.4 Business Model Canvas

The Business Model Canvas for *Janus* delineates the operational and strategic framework of its decentralized escrow service, designed to facilitate secure and anonymous cryptocurrency transactions. This section outlines the nine core components that underpin Janus's business model, emphasizing its unique positioning in the cryptocurrency payment ecosystem.

- **Key Partners**: Blockchain platforms, such as Ethereum, provide the infrastructure for smart contract deployment [9]. Wallet providers, notably MetaMask, enable user access and interaction with the service [5]. Additionally, legal advisors are critical for navigating the regulatory landscape of cryptocurrency transactions.

- **Key Activities**: The primary activities revolve around the development and maintenance of the Janus smart contract, ensuring its reliability and security. Ongoing efforts focus on enhancing anonymity features and establishing a decentralized dispute resolution process to handle refund requests efficiently.

- **Key Resources**: Janus leverages technical expertise in blockchain and smart contract programming as its cornerstone resource. The smart contract itself serves as the central operational asset, supported by decentralized infrastructure that ensures scalability and resilience.

- **Value Propositions**: Janus delivers a distinctive blend of security, anonymity, and trust, enabling safe cryptocurrency transactions without compromising user privacy or control, as detailed in earlier sections.

- **Customer Relationships**: The service operates on a self-service model, with users interacting directly via the smart contract. Optional community-driven support or automated systems may supplement dispute resolution.

- **Channels**: Distribution occurs primarily through the Janus online platform, with potential integrations into e-commerce sites and decentralized marketplaces to broaden reach and usability for its tech-savvy audience.

- **Customer Segments**: Janus targets a niche yet growing demographic: tech-savvy males aged 18–45 with higher education and income, located in cryptocurrency hubs such as the United States, China, Japan, South Korea, Europe, and other non-European countries, as identified in the market overview.

- **Cost Structure**: Major costs encompass smart contract development and maintenance, operational expenses for decentralized infrastructure, and targeted marketing initiatives to build awareness among cryptocurrency users.

- **Revenue Streams**: Janus sustains itself through a streamlined revenue model, charging a 1% fee on completed transactions.

This model capitalizes on decentralization to eliminate intermediaries, reduce operational overhead, and reinforce user autonomy, distinguishing Janus in a competitive landscape increasingly focused on privacy and security. By integrating these elements, Janus positions itself as a forward-thinking solution in the evolving cryptocurrency payment market.

Chapter 3

Janus: System Design and Acrhitecture

3.1 Overview of Janus

As discussed in the introduction, Janus is designed to provide an additional layer of security for buyers while enabling sellers to build trust with their customers and promote broader adoption of cryptocurrency payments. A key characteristic of Janus is the absence of such a mechanism to identify users beyond their wallet addresses. No personal information is collected, and no identity verification is required. Although it is theoretically possible to de-anonymize users through advanced blockchain analysis and forensic techniques, such analysis falls outside the scope of this project.

Additional information is available at the following GitHub repository.

3.2 Core Functionality

As previously introduced, Janus is built around three core functionalities:

- **Buyer Protection**: one of the primary objectives of Janus is to enhance customer protection. Cryptocurrency users are regularly exposed to significant risks of fraud, particularly when purchasing goods or services from unknown or unverified sources. These risks are intensified in cryptocurrency transactions due to the anonymity and irreversibility of payments, which can incentivize malicious actors. Janus mitigates this risk by holding customer funds in escrow through its smart contract, rather than transferring them directly to the seller. Assuming Janus is considered a trusted and impartial intermediary, this design makes it considerably more difficult for a malicious seller to commit fraud. To succeed, a scammer would need to withhold the promised product or service and also convince the Janus dispute resolution process (assumed to occur off-chain) that the buyer's refund request is invalid. This introduces a level of accountability that is typically absent in traditional peer-to-peer cryptocurrency payments. While Janus does not eliminate the possibility of fraud entirely, since no system is perfectly secure, it significantly reduces the likelihood of successful scams. Similar risk-reduction models are employed by widely adopted services such as PayPal.

- **Seller Trust**: Janus also provides advantages for sellers. When a potential customer visits an unfamiliar e-commerce website for the first time, they may be hesitant to complete a purchase due to a lack of trust. This hesitation can arise from various factors such as the novelty of the site, limited user reviews, or other suspicious indicators. However, if the site offers a reliable and secure payment method such as PayPal, which protects users against fraud, the customer may feel more confident proceeding with the transaction. Similarly, by integrating Janus, sellers can offer a trustworthy payment method that uses an escrow mechanism to protect the buyer. This increases the likelihood of initial purchases and can help build long-term trust between buyers and sellers. For the seller, offering a secure and privacy-preserving payment method can lead to improved customer confidence and increased sales over time.

- **User Anonymity**: anonymity is a fundamental principle of cryptocurrencies and is central to the Janus design. While many blockchain-based services do not prioritize anonymity, often due to regulatory or operational constraints, Janus considers anonymity essential to its purpose. The goal is to provide a service where users' identities remain private, as many individuals in the cryptocurrency space value this characteristic. To support this, users are identified only by their wallet addresses, with no collection of personal data. Furthermore, for enhanced privacy, the use of non-custodial wallets is recommended. This ensures that no third-party service has knowledge of a user's real-world identity. With this structure, Janus provides a strong level of anonymity. It should be noted, however, that complete anonymity cannot be guaranteed in practice, as stated in the system overview. The aim is to offer a meaningful degree of anonymity without claiming absolute guarantees.

3.3 Smart Contract Design & Development

The Janus smart contract was developed in Solidity and encapsulates the core escrow logic that underpins the service. Its primary purpose is to hold funds temporarily during a transaction, allowing the buyer to request a refund within a predefined warranty period. This ensures buyer protection while also establishing a trustworthy and verifiable transaction environment for the seller.

The contract is structured around a `Transaction` data structure, which maintains the relevant details for each escrow event, including buyer and seller addresses, transaction value, status flags, and timestamps. A mapping from transaction IDs to `Transaction` instances is used to efficiently manage and retrieve transaction data.

Key functionalities implemented in the smart contract include:

- **Transaction Initialization**: buyers can initiate a transaction by sending funds along with the address of the intended seller. The contract records the deposit, stores the timestamp, and marks the transaction as active.
- **Refund Requests**: during the warranty period, buyers can request a refund. This action flags the transaction as disputed. For the sake of simplicity and privacy, refund justifications and discussions are assumed to occur off-chain.
- **Refund Approval**: the designated dispute resolver can approve a refund. Once approved, the funds are released back to the buyer's wallet address.
- **Seller Withdrawal**: if the warranty period of 30 days elapses without a refund request or once a refund is denied, the seller is allowed to withdraw the funds. A 1% service fee is deducted from the payout to fund the platform.

The contract also leverages selected `OpenZeppelin` libraries to strengthen its security. In particular, `Ownable` is used to define clear ownership and restrict access to administrative functions, `Pausable` provides the ability to temporarily halt operations in emergency situations, and `ReentrancyGuard` protects against reentrancy attacks. These widely adopted and community-audited modules reduce the risk of vulnerabilities that might arise from implementing such mechanisms manually.

In addition, the contract includes standard `require` statements to enforce access control and prevent invalid or malicious operations. Each function ensures that only authorized users (buyer, seller, or contract owner) can execute sensitive actions.

Furthermore, the contract was designed with simplicity and auditability in mind. All relevant data and events are recorded on-chain to ensure transparency, while sensitive actions are minimized to maintain gas efficiency and reduce potential vulnerabilities. The contract does not store any personally identifiable information and relies solely on wallet addresses, thereby preserving user anonymity.

The overall design reflects a balance between functionality, user protection, and adherence to the decentralization and privacy principles central to the cryptocurrency ecosystem.

3.4 Testing

The Janus smart contract was subjected to an extensive suite of automated tests using the Hardhat development framework in conjunction with Chai for assertions. The test suite includes a total of 108 individual cases designed to validate the correctness, security, and resilience of all implemented functionalities. These tests cover contract deployment, ownership transfers, access control, pause and unpause mechanisms, transaction lifecycle events (such as order creation, acceptance, and withdrawal), as well as refund logic, including request, revocation, resolution, and fund withdrawal.

Testing was performed under both valid and invalid conditions to ensure appropriate error handling and event emission. Role-based behavior was verified by simulating interactions from buyers, sellers, owners, and unauthorized users. Temporal conditions, such as warranty periods and maximum seller response delays, were simulated using EVM time manipulation to assess compliance with contractual constraints. This comprehensive testing strategy contributes to ensuring the robustness and functional correctness of the smart contract in a variety of operational scenarios.

3.5 Demo Application (Web Interface)

To demonstrate the functionality of the Janus smart contract in a user-accessible format, a lightweight web application was developed using the Python Flask framework, with pure HTML, CSS, and JavaScript for the frontend.

The demo is organized into three core sections:

- **Service Presentation**: This is the landing page of the application and serves as a public-facing introduction to Janus. The goal was to create a visually appealing and impactful presentation that clearly communicates the purpose of Janus, how it works, and how it benefits users in cryptocurrency transactions. As the theoretical homepage of a commercial product, emphasis was placed on aesthetic quality and clarity of message, making this section the virtual calling card of the Janus platform.

- **Buyer Demo**: This section allows users to interact with Janus as a buyer via MetaMask. It presents a mock online marketplace where buyers can make purchases using Ethereum. For realism, product prices are randomly generated and scaled to reflect the real-time price of ETH, retrieved periodically through the official Binance API. Once a purchase is made, the buyer can manage the order from a private dashboard, including actions such as requesting a refund (provided the order has been accepted) and withdrawing funds if a refund is granted.

- **Seller Demo**: This section provides a seller-facing interface, also integrated with MetaMask. The seller can view and manage incoming orders, accept them, and withdraw funds once the warranty period has passed or a refund request has been denied. The seller is presented as the owner of the marketplace, reflecting a realistic operational model.

For simplicity and consistency with course practices, MetaMask was chosen as the exclusive wallet provider. As one of the most widely adopted non-custodial wallets, it aligns well with the privacy-preserving philosophy of Janus.

To simplify implementation, the demo retrieves and displays orders using a basic approach: once a user accesses their dashboard, the total number of active orders is first queried, and then each order is fetched in sequence using a for-loop. While this method is functional, future iterations could replace it with a more efficient, event-driven model.

More information about the demo is available here.

Chapter 4

Practical Considerations and Future Work

Janus operates as a fully decentralized smart contract on the Ethereum blockchain, ensuring that all transaction data resides exclusively on-chain, without reliance on centralized servers or databases. This architecture aligns with the foundational principles of blockchain technology, offering a range of benefits while also introducing specific challenges that must be addressed to facilitate real-world adoption.

4.1 Benefits of Decentralization

- **Transparency and Trustlessness**: All transaction logic, including escrow management, refund handling, and fund releases, is encoded within the smart contract and verifiable on the blockchain. This removes the need for trusted intermediaries, thereby fostering confidence among users who prioritize trustless interactions.

- **Data Integrity and Immutability**: Storing all transaction data on-chain ensures tamper-proof records that are publicly auditable, enhancing both security and accountability.

- **User Autonomy**: Due to Janus's versatility and flexibility, the system supports the use of non-custodial wallets such as MetaMask. This enables users to retain complete control over their funds, reducing risks associated with third-party custodians, such as mismanagement or data breaches, and enhancing anonymity by limiting the possibility of linking wallet addresses to real-world identities.

- **Global Accessibility**: As a decentralized platform, Janus can be accessed by users worldwide, provided they have an internet connection and a compatible wallet. This aligns with the inherently borderless nature of blockchain technologies.

- **Open Source**: Upon deployment, the source code of the Janus smart contract will be made publicly available, allowing users, particularly those with technical expertise, to review and analyze it. This approach enhances transparency and builds trust in the system, while also encouraging community involvement in the development and continuous improvement of the platform.

4.2 Challenges of Decentralization

Some challenges associated with decentralization are specific to Janus, while others are general in nature and may similarly affect other decentralized platforms.

- **Lack of Centralized Monitoring**: Unlike centralized platforms, Janus does not include built-in services for actively monitoring contract activity. Participants are required to implement or integrate external mechanisms to listen for smart contract events in order to remain informed about transaction updates. This introduces an additional layer of responsibility, particularly for sellers. A potential solution to address this limitation is described in the Future Work 4.3 section.

- **Dispute Resolution Dependency**: The resolution process itself is assumed to occur off-chain. The absence of a centralized authority to manage or enforce dispute outcomes may complicate resolution procedures, especially in complex cases. For the purposes of this project, it is assumed that a fully anonymous, chat-based service exists to facilitate such communication. A more in-depth discussion is provided in the Future Work Section 4.3.

- **Scalability and Gas Costs**: Transactions on the Ethereum network incur gas fees, which can become prohibitively high during periods of network congestion. This may discourage participation in low-value transactions or limit accessibility in regions with constrained financial resources. To address this, future integration with Layer-2 solutions could help reduce transaction costs and improve scalability.

4.3 Future Work

Several enhancements have been identified to address the current limitations of Janus. These have not been implemented either due to time constraints or because they extend beyond the defined scope of this project. Nevertheless, the following proposals offer theoretically viable paths for future development:

- **Reputation System**: Given the immutable nature of blockchain data, incorporating a reputation system for both sellers and buyers could enhance overall trust in the platform. For sellers, metrics such as the number of completed orders and accepted refunds could provide an overview of reliability, while for buyers, indicators such as a history of fair dispute outcomes could serve as measures of trustworthiness. Such systems would require safeguards against manipulation, for instance, preventing the artificial inflation of ratings through fake transactions. It is also essential to provide visibility into the number of contributors to each rating to ensure transparency and enable users to assess the credibility of the score. Overall, a dual reputation system would also assist dispute resolvers in better understanding the reliability of both parties involved, thereby supporting fairer and more informed resolution processes.

- **Secure Messaging System**: The current design assumes off-chain communication for dispute resolution, introducing potential vulnerabilities related to security and centralization. A possible solution could involve integrating a secure, encrypted, and anonymous off-chain messaging system. This system would enable communication between buyers, sellers, and dispute resolvers using wallet addresses as identifiers, while ensuring message privacy and integrity. Although the implementation of an on-chain messaging system was also considered, such a solution is currently impractical due to high transaction costs. Therefore, an off-chain alternative is presented as a conceptual solution.

- **Rate Limiting for Refund Requests**: To prevent misuse, such as spamming refund requests, a rate-limiting mechanism could be introduced. This feature would restrict excessive refund attempts by tracking the number of requests per wallet address over a specified time window and temporarily suspending refund capabilities for accounts that exceed a defined threshold.

- **Upgradeable Contracts via Proxy Pattern**: Since smart contracts are immutable once deployed, future upgrades typically require redeployment, which can disrupt users and state continuity. Introducing an upgradeable architecture using the proxy pattern would allow Janus to evolve without changing its deployed address. The proxy holds the state, while delegating calls to an implementation contract that can be replaced with newer versions. This approach would enable the introduction of new features, security patches, or optimizations without interrupting ongoing operations or requiring migration of user funds.

- **JavaScript SDK**: The development of a JavaScript Software Development Kit (SDK) could simplify the integration of Janus into e-commerce platforms and marketplaces. Similar to how traditional payment services such as PayPal provide libraries for easy adoption, the SDK would abstract complex blockchain operations, such as event listening and transaction initiation, into user-friendly APIs. This would lower the technical barrier for integration and promote adoption among online retailers and decentralized marketplaces.

- **Support for ETH and Stablecoins Only**: To reduce exposure to volatile or low-liquidity cryptocurrencies, Janus could be limited to accepting Ethereum (ETH) and widely-used stablecoins such as USDC. This would help maintain transactional stability and enhance user confidence by relying on established, stable digital assets.

Bibliography

[1] Chargeflow. *PayPal Statistics and Facts 2025*. https://www.chargeflow.io/blog/paypal-statistics-facts. 2025.

[2] Coinbase. *What is a multi signature multi-sig wallet*. https://www.coinbase.com/it/learn/wallet/what-is-a-multi-signature-multi-sig-wallet. 2025.

[3] CoinLaw. *Crypto User Demographics Statistics 2025: Who's Investing, Trading, and Holding*. https://coinlaw.io/crypto-user-demographics-statistics/. 2025.

[4] CoinPedia. *Global Crypto Adoption Report 2025*. https://coinpedia.org/research-report/global-crypto-adoption-report. 2025.

[5] Consensys Software Inc. *MetaMask: A crypto wallet & gateway to blockchain apps*. https://metamask.io. 2024.

[6] Counos Platform. *Counos Escrow System: Secure cryptocurrency payment gateway*. https://www.counos.io/. 2024.

[7] Crypto.com. *Crypto.com: The leading cryptocurrency platform*. https://crypto.com. 2024.

[8] Escrow.com. *Escrow.com: Secure online escrow service for buyers and sellers*. https://www.escrow.com. 2024.

[9] Ethereum Foundation. *Ethereum: Open-source blockchain platform*. https://ethereum.org. 2024.

[10] Fortune Business Insights. *Cryptocurrency Market Size, Share Growth Analysis*. https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149. 2025.

[11] Grand View Research. *Cryptocurrency Payment Apps Market Size, Share & Trends Analysis Report*. https://www.grandviewresearch.com/industry-analysis/cryptocurrency-payment-apps-market-report. Accessed 2024. 2024.

[12] K. Kajol et al. “Drivers Influencing the Adoption of Cryptocurrency: A Social Network Analysis Approach”. In: *Financial Innovation* 11.1 (2025), p. 74. ISSN: 2199-4730. DOI: 10.1186/s40854-025-00757-0. URL: %5Curl%7Bhttps://doi.org/10.1186/s40854-025-00757-0%7D.

[13] Kleros. *Escrow - Trade, hire and pay secured by trustless dispute resolution.* https://kleros.io/escrow/. Accessed: 26 June 2025.

[14] LEXR. *Escrow Services for Fiat Crypto Transactions.* https://www.lexr.com/en-ch/services/escrow/. Accessed: 26 June 2025.

[15] Lindemann Law. *Blockchain Crypto Assets Escrow Services.* https://lindemannlaw.ch/expertise/mergers-acquisitions-transactions/escrow-services/blockchain-crypto-escrow/. Accessed: 26 June 2025.

[16] Market Data Forecast. *Cryptocurrency Market Size, Share & Growth Report.* https://www.marketdataforecast.com/market-reports/cryptocurrency-market. Accessed 2025. 2025.

[17] Medium - NEST. *Trust Redefined: The Rise Of Escrow Smart Contracts.* https://nes-tech.medium.com/trust-redefined-the-rise-of-escrow-smart-contracts-25a48c001bd2. 2024.

[18] Merkle Science. *What is Blockchain Forensics? An In-Depth Guide.* https://www.merklescience.com/blog/what-is-blockchain-forensics-an-in-depth-guide. Accessed: 21 August 2025.

[19] Ibrahim Mutambik et al. “Trust in Cryptocurrency Payments:” in: *Journal of Organizational and End User Computing* 36 (Aug. 2024), pp. 1–36. DOI: 10.4018/JOEUC.353910.

[20] Wei Quan et al. “Mobile, traditional, and cryptocurrency payments influence consumer trust, attitude, and destination choice: Chinese versus Koreans”. In: *International Journal of Hospitality Management* 108 (2023), p. 103363. ISSN: 0278-4319. DOI: https://doi.org/10.1016/j.ijhm.2022.103363. URL: %5Curl%7Bhttps://www.sciencedirect.com/science/article/pii/S0278431922002298%7D.

[21] Uniscrow. *Uniscrow: Decentralized escrow infrastructure for Web3.* https://www.uniscrow.com/. 2024.

[22] Wikipedia. *Anti-money Laundering.* https://en.wikipedia.org/wiki/Anti-money_laundering. 2025.

[23] Wikipedia. *Escrow.* https://en.wikipedia.org/wiki/Escrow. 2025.

[24] Wikipedia. *Know your customer.* https://it.wikipedia.org/wiki/Know_your_customer. 2025.

[25] XREX Inc. *BitCheck - The most secure online payment guarantee to escrow funds for global transactions*. `https://xrex.io/bitcheck/`. Accessed: 26 June 2025.