Journal of Software Engineering and Applications, 2024, 17, 664-712
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Blockchain-Based System for Secure and Efficient Cross-Border Remittances: A Potential Alternative to SWIFT

Omoshola S. Owolabi[1], Emmanuel Hinneh[1], Prince C. Uche[1], Nathaniel T. Adeniken[1], Jennifer A. Ohaegbulem[2], Samuel Attakorah[1], Oluwabukola G. Emi-Johnson[3], Chinaza S. Belolisa[4], Harold Nwariaku[5]

[1]Department of Data Science, Carolina University, Winston Salem, NC, USA
[2]Patterson School of Business, Carolina University, Winston Salem, NC, USA
[3]Department of Statistical Sciences, Wake Forest University, Winston Salem, NC, USA
[4]Department of Computer Science, Fisk University, Nashville, TN, USA
[5]Harold & Co Procurement and Supply Chain Consulting, Lagos, Nigeria
Email: owolabio@carolinau.edu, hinnehe@carolinau.edu, uchep@carolinau.edu, adenikenn@carolinau.edu, ohaegbulemj@carolinau.edu, attakorahs@carolinau.edu, chinazabelolisa@gmail.com, emijo23@wfu.edu, harold@haroldandco.com

How to cite this paper: Owolabi, O.S., Hinneh, E., Uche, P.C., Adeniken, N.T., Ohaegbulem, J.A., Attakorah, S., Emi-Johnson, O.G., Belolisa, C.S. and Nwariaku, H. (2024) Blockchain-Based System for Secure and Efficient Cross-Border Remittances: A Potential Alternative to SWIFT. *Journal of Software Engineering and Applications*, **17**, 664-712.
https://doi.org/10.4236/jsea.2024.178036

Received: July 9, 2024
Accepted: August 25, 2024
Published: August 28, 2024

Abstract

This paper proposes a blockchain-based system as a secure, efficient, and cost-effective alternative to SWIFT for cross-border remittances. The current SWIFT system faces challenges, including slow settlement times, high transaction costs, and vulnerability to fraud. Leveraging blockchain technology's decentralized, transparent, and immutable nature, the proposed system aims to address these limitations. Key features include modular architecture, implementation of microservices, and advanced cryptographic protocols. The system incorporates Proof of Stake consensus with BLS signatures, smart contract execution with dynamic pricing, and a decentralized oracle network for currency conversion. A sophisticated risk-based authentication system utilizes Bayesian networks and machine learning for enhanced security. Mathematical models are presented for critical components, including transaction validation, currency conversion, and regulatory compliance. Simulations demonstrate potential improvements in transaction speed and costs. However, challenges such as regulatory hurdles, user adoption, scalability, and integration with legacy systems must be addressed. The paper provides a comparative analysis between the proposed blockchain system and SWIFT, highlighting advantages in transaction speed, costs, and security. Mitigation strategies are proposed for key challenges. Recommendations are made for further research into scaling solutions, regulatory frameworks, and user-centric designs. The adoption of blockchain-based remittances could significantly impact the fi-

nancial sector, potentially disrupting traditional models and promoting financial inclusion in underserved markets. However, successful implementation will require collaboration between blockchain innovators, financial institutions, and regulators to create an enabling environment for this transformative system.

Keywords

Interoperability, Tokens, AML/KYC Compliance, Peer-to-Peer Transfers, Financial Inclusion

1. Introduction

1.1. The Importance of Cross-Border Remittances in the Global Economy

Cross-border remittances play a vital role in the global economy, serving as a lifeline for millions of individuals, businesses, and families worldwide. According to the World Bank, global remittance flows are said to have reached $589 billion in 2021 [1]. Remittances are particularly crucial for developing nations, often exceeding official development assistance and foreign direct investment (FDI) [2]. These funds support recipients' livelihoods, contribute to poverty alleviation, and promote economic growth in recipient countries [3] [4].

Remittances have shown remarkable resilience during economic crises, including the COVID-19 pandemic. While the pandemic initially led to a slight decline in remittance flows, they have since rebounded and were projected to grow by 7.3% in 2021 [1]. This resilience underscores the importance of remittances as a stable source of external financing for developing countries [5].

1.2. Current Challenges with Traditional Cross-Border Payment Systems, Including SWIFT

Despite the significance of cross-border remittances, traditional payment systems, such as Society for Worldwide Interbank Financial Telecommunication (SWIFT), face several challenges that hinder their efficiency and accessibility. SWIFT, which facilitates global financial transactions among over 11,000 banks and financial institutions across more than 200 countries [6], has been criticized for its slow settlement times, high transaction costs, and lack of transparency [7].

One of the primary issues with SWIFT is the slow processing of transactions, which can take several days to complete. This delay is particularly problematic for remittances, as recipients often rely on these funds for their daily needs. Additionally, SWIFT transactions involve multiple intermediaries, leading to high transaction fees that can range from 5% to 20% of the total amount [1] [7]. These high costs disproportionately affect low-income individuals and families who depend on remittances for their livelihoods.

The SWIFT system lacks transparency, making it difficult for users to track

their transactions and identify potential errors or fraud. The centralized nature of SWIFT also raises concerns about security and privacy, as it is vulnerable to cyber-attacks and data breaches [8].

1.3. The Potential of Blockchain Technology to Revolutionize the Remittance Industry

Blockchain technology, which underpins cryptocurrencies like Bitcoin, has emerged as a potential solution to the challenges faced by traditional cross-border payment systems. A blockchain is a decentralized, distributed ledger that records transactions across a network of computers [9]. Its key features, such as transparency, immutability, and security, make it an attractive alternative to centralized systems like SWIFT [7].

Leveraging blockchain technology, the remittance industry can benefit from faster settlement times, lower transaction costs, and increased transparency. Blockchain-based remittance systems can facilitate near-instant transactions by eliminating the need for intermediaries and enabling direct peer-to-peer transfers. This reduction in intermediaries also leads to lower transaction fees, making remittances more accessible and affordable for users.

Furthermore, the transparency and immutability of blockchain transactions enhance security and reduce the risk of fraud [8]. The decentralized nature of blockchain networks makes them more resilient to cyber-attacks and data breaches compared to centralized systems.

Several blockchain-based remittance solutions, such as Ripple and Stellar, have already emerged, demonstrating the potential of this technology to transform the industry [1]. These platforms aim to provide faster, cheaper, and more secure cross-border payments, challenging the dominance of traditional systems like SWIFT.

1.4. Statement of Problem

Given the challenges faced by traditional cross-border payment systems and the potential of blockchain technology to address these issues, this article proposes that a well-designed blockchain-based system could serve as a secure, efficient, and cost-effective alternative to SWIFT for cross-border remittances. By leveraging the inherent features of blockchain technology, such as decentralization, transparency, and immutability, a blockchain-based remittance system can offer faster settlement times, lower transaction costs, and enhanced security compared to SWIFT [7] [10].

The proposed blockchain-based system would aim to streamline the remittance process by eliminating intermediaries, enabling direct peer-to-peer transactions, and reducing the overall cost of remittances. The system would prioritize user privacy and security, ensuring compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations.

Providing a more accessible, affordable, and secure means of sending and receiving cross-border payments, the proposed blockchain-based remittance sys-

tem has the potential to revolutionize the industry and improve the lives of millions of individuals and families who rely on remittances for their livelihoods.

1.5. Objectives and Scope of the Proposed Blockchain-Based System Design

The primary objective of the proposed blockchain-based remittance system is to provide a secure, efficient, and cost-effective alternative to traditional cross-border payment systems like SWIFT. The system aims to address the limitations of existing remittance solutions by leveraging the inherent features of blockchain technology [7].

The specific objectives of the proposed system include:

1) Reducing transaction costs: By eliminating intermediaries and enabling direct peer-to-peer transactions, the blockchain-based system aims to significantly reduce the cost of remittances compared to traditional systems.

2) Improving transaction speed: The proposed system seeks to facilitate near-instant cross-border payments by leveraging the decentralized nature of blockchain technology and streamlining the settlement process.

3) Enhancing security and transparency: By utilizing the immutable and transparent properties of blockchain ledgers, the proposed system aims to increase the security of remittance transactions and reduce the risk of fraud.

4) Ensuring regulatory compliance: The system will incorporate necessary features to comply with AML and KYC regulations, ensuring a secure and legal framework for cross-border remittances [1].

The scope of the proposed blockchain-based remittance system encompasses the design and implementation of a decentralized, secure, and efficient platform for facilitating cross-border payments. The system will focus on the following key areas:

1) Architectural framework: The design will include the choice of blockchain network (public, private, or hybrid), digital wallet integration, and cross-border payment processing mechanisms [7].

2) Functional components: The system will incorporate features such as fund transfer, currency conversion, transaction validation, and reporting capabilities.

3) Operational and technical considerations: The design will address scalability, interoperability with existing financial systems, and regulatory compliance.

Focusing on these objectives and key areas, the proposed blockchain-based remittance system aims to provide a comprehensive and innovative solution to the challenges faced by the cross-border payment industry, ultimately benefiting millions of individuals and families who rely on remittances for their livelihoods.

2. Overview of the SWIFT System

2.1. How SWIFT Works

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global messaging system that facilitates cross-border financial transactions

among banks and other financial institutions. Established in 1973, SWIFT has become the primary means of communication for international payments, connecting over 11,000 institutions across more than 200 countries and territories [6].

SWIFT operates by providing a standardized and secure platform for exchanging financial messages, such as payment instructions, between member institutions [11]. When a bank customer initiates a cross-border transaction, the sending bank creates a SWIFT message containing the relevant details, including the recipient's information, the amount to be transferred, and the purpose of the payment. This message is then transmitted through the SWIFT network to the receiving bank, which processes the payment and credits the recipient's account.

Throughout the process, SWIFT acts as a messaging system rather than a clearing or settlement system [12]. This means that while SWIFT facilitates the exchange of payment instructions, the actual transfer of funds occurs through correspondent banking relationships or other settlement systems, such as central bank real-time gross settlement (RTGS) systems [13].

2.2. Advantages of SWIFT

SWIFT has several advantages that have contributed to its widespread adoption and success in facilitating cross-border financial transactions. One of the primary benefits of SWIFT is its global reach and standardization. By connecting thousands of financial institutions worldwide and providing a common language for financial messaging, SWIFT has streamlined international payment processes and reduced the risk of errors and misinterpretations [11].

Another advantage of SWIFT is its focus on security. The system employs various measures to protect the confidentiality, integrity, and authenticity of financial messages, such as encryption, authentication, and secure network architecture [6]. These security features have helped to reduce the risk of fraud and unauthorized access to sensitive financial information [12].

SWIFT has established a robust governance framework and compliance standards to ensure that its member institutions adhere to international regulations, such as anti-money laundering (AML) and know-your-customer (KYC) requirements [6]. This has contributed to the overall stability and integrity of the global financial system [13].

2.3. Limitations and Challenges of SWIFT

Despite its widespread adoption and advantages, the SWIFT system faces several limitations and challenges that have prompted the search for alternative cross-border payment solutions.

2.3.1. Slow Settlement Times and Lack of Real-Time Transactions

One of the primary drawbacks of SWIFT is the slow processing of transactions, which can take several days to complete [7]. This delay is due to the multi-step process involved in SWIFT transactions, which requires the coordination of

multiple intermediaries, such as correspondent banks, before the funds can be credited to the recipient's account. The lack of real-time settlement capabilities can be particularly problematic for time-sensitive payments, such as emergency remittances or business transactions [13].

2.3.2. High Transaction Fees and Exchange Rate Costs

Another challenge associated with SWIFT is the high cost of cross-border transactions. SWIFT payments often involve multiple intermediaries, each charging their own fees, which can accumulate to a significant portion of the total transaction amount [7]. Moreover, the exchange rates applied to cross-border transactions may not always be favorable to the users, further increasing the overall cost of remittances [1]. These high costs disproportionately affect low-income individuals and small businesses that rely on international payments.

2.3.3. Vulnerability to Fraud, Money Laundering, and Other Illicit Activities

Despite SWIFT's efforts to enhance security and compliance, the system remains vulnerable to various financial crimes, such as fraud, money laundering, and terrorist financing. The centralized nature of SWIFT and its reliance on trust among member institutions create opportunities for bad actors to exploit the system for illicit purposes [12]. In some cases, hackers have successfully breached the security of SWIFT member institutions, resulting in significant financial losses and reputational damage [11].

2.3.4. Lack of Transparency and Traceability in Transactions

Another limitation of SWIFT is the lack of transparency and traceability in transactions. The system does not give users real-time visibility into their payments' status, making it difficult to track the progress of transactions and identify potential issues or delays. This lack of transparency can also hinder the ability of regulators and law enforcement agencies to monitor and investigate suspicious activities, as the information available through SWIFT may be limited or fragmented [7].

These limitations and challenges have led to a growing interest in alternative cross-border payment solutions, such as blockchain-based systems, which have the potential to address the shortcomings of SWIFT and provide a more efficient, cost-effective, and secure means of facilitating international transactions.

3. Blockchain Technology: Key Features and Applications

3.1. Explanation of Blockchain Technology

Blockchain technology, which underpins cryptocurrencies like Bitcoin, is a decentralized and distributed ledger system that records transactions across a network of computers [9]. In essence, a blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography [14]. Each block contains a cryptographic hash of the previous block, a timestamp,

and transaction data, forming an immutable and tamper-evident chain [15].

3.1.1. Decentralized and Distributed Ledger

One of the key features of blockchain technology is its decentralized and distributed nature. Unlike traditional centralized systems, where a single authority controls and maintains the ledger, a blockchain network is maintained by a distributed network of nodes. Each node in the network holds a copy of the ledger and participates in the validation and verification of transactions. This decentralization eliminates the need for intermediaries and reduces the risk of single points of failure [7].

3.1.2. Transparency and Immutability of Transaction Records

Another essential characteristic of blockchain technology is the transparency and immutability of transaction records. Once a transaction is validated and added to the blockchain, it becomes part of the permanent record and cannot be altered or deleted [14]. This immutability ensures the integrity of the transaction history and prevents tampering or fraud [15]. Moreover, the transparency of the blockchain allows all participants in the network to view the transaction records, enhancing accountability and trust.

3.1.3. Enhanced Security and Fraud Prevention Mechanisms

Blockchain technology employs various security measures to protect the integrity of the network and prevent fraudulent activities. The use of cryptographic techniques, such as hash functions and digital signatures, ensures the authenticity and non-repudiation of transactions [14]. Additionally, the consensus mechanisms employed by blockchain networks, such as proof-of-work (PoW) or proof-of-stake (PoS), make it extremely difficult for malicious actors to manipulate the ledger or carry out double-spending attacks [15].

3.2. Advantages of Blockchain for Cross-Border Remittances

The inherent features of blockchain technology make it particularly well-suited for addressing the challenges faced by traditional cross-border remittance systems, such as SWIFT.

3.2.1. Reduced Transaction Costs and Faster Settlement Times

Eliminating the need for intermediaries and enabling direct peer-to-peer transactions, blockchain-based remittance solutions can significantly reduce transaction costs compared to traditional systems [7]. The decentralized nature of blockchain networks allows for the streamlining of the settlement process, resulting in faster transaction times. This is particularly beneficial for low-income individuals and families who rely on remittances, as it makes the process more affordable and accessible.

3.2.2. Increased Security and Transparency

The enhanced security features of blockchain technology, such as cryptographic techniques and consensus mechanisms, make it more resilient to fraud and

hacking attempts compared to centralized systems [15]. The transparency and immutability of transaction records on the blockchain also provide a higher level of accountability and trust, as all participants can view and verify the transaction history [14]. This transparency can help to reduce the risk of money laundering and other illicit activities associated with cross-border payments.

3.3. Existing Blockchain-Based Remittance Solutions (Ripple, Stellar, Cryptocurrencies)

Several blockchain-based remittance solutions have emerged in recent years, aiming to provide faster, cheaper, and more secure cross-border payment services. Some notable examples include:

1) Ripple: Ripple is a real-time gross settlement system, currency exchange, and remittance network built on blockchain technology [7]. It aims to facilitate fast, low-cost, and secure international payments by connecting banks, payment providers, and digital asset exchanges [16].

2) Stellar: Stellar is an open-source, decentralized payment protocol that enables fast, low-cost, and cross-border transactions [17]. It focuses on providing financial services to the unbanked and underbanked populations worldwide.

3) Cryptocurrencies: Cryptocurrencies, such as Bitcoin and Ethereum, can be used for cross-border remittances, offering a decentralized and peer-to-peer alternative to traditional payment systems. However, the volatility and regulatory challenges associated with cryptocurrencies may limit their widespread adoption for remittances [7].

These blockchain-based solutions demonstrate the potential of the technology to transform the cross-border remittance industry, providing faster, cheaper, and more secure payment services to individuals and businesses worldwide.

4. Blockchain-Based System Design Considerations for Cross-Border Remittances

4.1. Architectural Framework

The architectural framework is a fundamental aspect in the design of a blockchain-based system for cross-border remittances. It serves as the cornerstone for the system's functionality, security, and regulatory compliance. This framework encompasses several critical components, each of which requires careful consideration and rigorous analysis.

4.1.1. Blockchain Network Topology Selection

The selection of an appropriate blockchain network topology is a pivotal decision that significantly impacts the system's performance, security, and scalability. This choice is contingent upon the specific requirements and objectives of the remittance system. The options include:

1) Public Blockchains: These are open, permissionless networks (e.g., Bitcoin, Ethereum) that allow unrestricted participation. While they offer high levels of decentralization and transparency, they may pose challenges in terms of privacy

and regulatory compliance for financial transactions.

2) Private Blockchains: These are permissioned networks controlled by a single entity or a consortium. They offer enhanced privacy and control but may sacrifice some aspects of decentralization.

3) Hybrid Blockchains: These networks combine elements of both public and private blockchains, potentially offering a balance between openness and control.

For a cross-border remittance system, a hybrid or private blockchain topology may be more appropriate, as it allows for greater control over access, privacy, and regulatory compliance while potentially maintaining some of the benefits of decentralization.

To systematically evaluate and select the optimal blockchain network topology, we propose the application of the Analytic Hierarchy Process (AHP) [18]. This multi-criteria decision-making approach allows for a structured comparison of alternatives based on various weighted criteria.

Let $C = \{c_1, c_2, \cdots, c_n\}$ represent the set of criteria (e.g., security, scalability, compliance, cost) and $A = \{a_1, a_2, a_3\}$ denote the alternatives (public, private, hybrid blockchains). The AHP process involves:

1) Construction of a pairwise comparison matrix for criteria: $M = \left[m_{ij} \right]$

2) Calculation of the priority vector w for criteria:

$$w_i = \frac{\left(\prod_{j=1}^{n} m_{ij} \right)^{1/n}}{\sum_{k=1}^{n} \left(\prod_{j=1}^{n} m_{kj} \right)^{1/n}}$$

3) Formation of pairwise comparison matrices for alternatives: $A_k = \left[a_{ij}^k \right]$

4) Computation of priority vectors for each alternative-criterion combination:

$$v_{ik} = \frac{\left(\prod_{j=1}^{3} a_{ij}^k \right)^{1/3}}{\sum_{l=1}^{3} \left(\prod_{j=1}^{3} a_{lj}^k \right)^{1/3}}$$

5) Derivation of the global priority vector:

$$p_i = \sum_{k=1}^{n} w_k v_{ik}$$

This rigorous approach ensures a comprehensive and objective evaluation of blockchain network topologies, taking into account multiple factors crucial for cross-border remittance systems.

4.1.2. Digital Wallet Architecture and User Authentication Mechanisms

The architecture of digital wallets and the implementation of robust user authentication systems are paramount in ensuring the security, usability, and regulatory compliance of a blockchain-based cross-border remittance platform. The system proposes a multi-faceted approach that integrates advanced cryptographic techniques, risk-based authentication, and adaptive security measures.

Cryptographic Foundation

The digital wallet architecture is built upon asymmetric cryptography, utilizing elliptic curve cryptography (ECC) for its superior security-to-key-size ratio

[19]. Each user is assigned a unique pair of public and private keys:

$$\text{Private Key}: k \in \mathbb{Z}_n$$

$$\text{Public Key}: K = k \cdot G$$

where G is the base point on the elliptic curve, and n is the order of G. This cryptographic foundation ensures secure transaction signing and user identification within the blockchain network.

Risk-Based Authentication System

To enhance the security of user interactions with the digital wallet, the system implements a sophisticated risk-based authentication system. This system leverages a Bayesian network model [20], allowing for dynamic adjustment of security measures based on a multitude of risk factors. The core of this authentication system is grounded in the Bayesian probability theorem:

$$P(Y \mid X) = \frac{P(X \mid Y)P(Y)}{P(X)}$$

where:

- Y represents the authentication outcome (success or failure)
- $X = \{x_1, x_2, \cdots, x_n\}$ denotes the set of observed risk factors (e.g., device characteristics, geolocation, transaction amount, user behavior patterns)

To operationalize this model, the system employs a logistic regression function [21], which allows for the estimation of authentication success probability based on the identified risk factors:

$$P(Y = 1 \mid X) = \frac{1}{1 + e^{-\left(\beta_0 + \sum_{i=1}^{n} \beta_i x_i\right)}}$$

where:

- $Y = 1$ indicates successful authentication
- x_i represents different risk factors
- β_i are the coefficients indicating the impact of each risk factor

Adaptive Security Measures

To further enhance the robustness of the authentication system, the system incorporates machine learning techniques for continuous improvement and adaptation to evolving threat landscapes. the system implements an ensemble learning approach, combining multiple classifiers to improve prediction accuracy:

$$F(x) = \sum_{m=1}^{M} \alpha_m f_m(x)$$

where $F(x)$ is the final classifier, $f_m(x)$ are individual classifiers (e.g., decision trees, neural networks), and α_m are the weights assigned to each classifier.

Multi-Factor Authentication (MFA)

In addition to the risk-based system, the system proposes the implementation of a tiered MFA approach. The authentication factors are dynamically selected based on the transaction risk level, which is calculated using the following formula:

$$\text{Risk Level} = w_1 \cdot \text{Amount} + w_2 \cdot \text{Destination Risk} + w_3 \cdot \text{User History}$$

where w_1, w_2, and w_3 are weights assigned to each factor based on their rela-

tive importance.

Integration with Blockchain

The authentication system is seamlessly integrated with the blockchain network through a secure API layer. This integration ensures that only authenticated and authorized transactions are processed on the blockchain. It utilizes a zero-knowledge proof protocol to verify user credentials without exposing sensitive information:

$$\text{Prover} \xrightarrow{\text{Commitment}} \text{Verifier} \xrightarrow{\text{Challenge}} \text{Prover} \xrightarrow{\text{Response}} \text{Verifier}$$

This zero-knowledge approach enhances privacy while maintaining the integrity of the authentication process.

Adopting these advanced approaches to digital wallet architecture and user authentication, the proposed remittance system achieves a sophisticated balance between security, usability, and regulatory compliance. This multi-layered security framework is crucial for the system's success in the complex and evolving landscape of international financial transactions, providing a robust foundation for secure, efficient, and compliant cross-border remittances.

4.1.3. Cross-Border Payment Processing and Settlement

The efficient processing and settlement of cross-border payments are critical components of our blockchain-based remittance system. The system models the payment network as a weighted directed graph $G=(V,E)$, where V represents the set of financial institutions and E represents the set of possible transaction routes between them.

Network Optimization

To optimize transaction routing and minimize costs, it employs the Bellman-Ford algorithm [22], which finds the shortest paths from a source vertex to all other vertices in a weighted graph, even in the presence of negative edge weights. This is particularly useful in the context of this system, as it allows for the consideration of various factors such as transaction fees, exchange rates, and processing times (**Algorithm 1**).

Algorithm 1. Enhanced bellman-ford algorithm for payment routing.

Require: Graph $G = (V, E)$, source vertex s, edge weight function w
Ensure: Shortest path distances and predecessors

for each vertex $v \in V$ **do**
  $distance[v] \leftarrow \infty$
  $predecessor[v] \leftarrow null$
end for
$distance[s] \leftarrow 0$
for $i \leftarrow 1$ to $|V| - 1$ **do**
  for each edge $(u, v) \in E$ **do**
    $w_{uv} \leftarrow calculateWeight(u, v)$ ▷ Dynamic weight calculation
    if $distance[u] + w_{uv} < distance[v]$ **then**
      $distance[v] \leftarrow distance[u] + w_{uv}$
      $predecessor[v] \leftarrow u$
    end if
  end for
end for
return $distance, predecessor$

The *calculate Weight* function incorporates multiple factors:

$$w_{uv} = \alpha \cdot fee_{uv} + \beta \cdot exchangeRate_{uv} + \gamma \cdot processingTime_{uv}$$

where α, β, and γ are weighting factors that can be dynamically adjusted based on user preferences or market conditions.

Settlement Mechanism

For settlement, the system implements a hybrid approach combining off-chain state channels and on-chain settlements. State channels allow for rapid, low-cost transactions between parties, while periodic on-chain settlements ensure security and finality.

Let S_{ij} represent the state channel between institutions *i* and *j*. The channel balance at time *t* is given by:

$$B_{ij}(t) = B_{ij}(0) + \sum_{k=1}^{n} T_k$$

where $B_{ij}(0)$ is the initial channel balance and T_k represents individual transactions. On-chain settlement occurs when:

$$\left|B_{ij}(t) - B_{ij}(0)\right| > \theta \text{ or } t - t_{last} > \tau$$

where θ is a predefined balance threshold and τ is the maximum time between settlements.

4.1.4. Compliance and Regulatory Integration

Ensuring compliance with international regulations is crucial for the legitimacy and adoption of the proposed system cross-border remittance system. it implements a sophisticated fuzzy logic system for compliance scoring and risk assessment [23].

Fuzzy Compliance Scoring

The compliance score is calculated using a centroid defuzzification method:

$$y^* = \frac{\int y \cdot \mu_{agg}(y)\mathrm{d}y}{\int \mu_{agg}(y)\mathrm{d}y}$$

where $\mu_{agg}(y)$ is the aggregate membership function:

$$\mu_{agg}(y) = \max\left(\alpha_1 \cdot \mu_{C1}(y), \alpha_2 \cdot \mu_{C2}(y), \cdots, \alpha_k \cdot \mu_{Ck}(y)\right)$$

Here, $\mu_{Ci}(y)$ represents the membership function for the *i*-th compliance criterion, and α_i is its corresponding weight.

Dynamic Rule Adaptation

To adapt to evolving regulatory landscapes, the system implements a dynamic rule adaptation mechanism. Let $R = \{r_1, r_2, \cdots, r_m\}$ be the set of compliance rules. Each rule r_i is associated with an effectiveness score $e_i(t)$ at time *t*:

$$e_i(t) = \lambda \cdot e_i(t-1) + (1-\lambda) \cdot p_i(t)$$

where λ is a decay factor and $p_i(t)$ is the performance of rule r_i at time *t*. Rules are periodically updated based on their effectiveness scores:

$$R(t+1) = \{r_i \in R(t) : e_i(t) > \varepsilon\} \cup \{r_{new}\}$$

where ε is a minimum effectiveness threshold and r_{new} represents newly introduced rules based on regulatory updates.

Regulatory Reporting

The system further implements an automated regulatory reporting system that leverages the blockchain's immutability and transparency. Transaction data is aggregated and anonymized using zero-knowledge proofs to protect user privacy while providing necessary information to regulators.

Let $T = \{t_1, t_2, \cdots, t_n\}$ be the set of transactions in a reporting period. The aggregated report A_R is generated as:

$$A_R = \text{ZKP}\left(\sum_{i=1}^{n} f(t_i)\right)$$

where $f(t_i)$ extracts relevant features from transaction t_i, and ZKP represents a zero-knowledge proof protocol that allows verification of the aggregated data without revealing individual transaction details.

This comprehensive approach to cross-border payment processing, settlement, and regulatory compliance ensures that the blockchain-based remittance system is not only efficient and cost-effective but also fully compliant with international regulations, thereby fostering trust and facilitating wider adoption in the global financial ecosystem.

4.2. Functional Components

The efficacy of our blockchain-based cross-border remittance system hinges on several key functional components. These components are designed to address the unique challenges of international money transfers, ensuring efficiency, security, and regulatory compliance.

4.2.1. Fund Transfer and Currency Conversion

A critical aspect of cross-border remittances is the accurate and efficient conversion of currencies. it implements a dynamic exchange rate model based on the Generalized Autoregressive Conditional Heteroskedasticity (GARCH) framework [24], which accounts for the time-varying volatility characteristic of financial markets.

Dynamic Exchange Rate Model

The model incorporates an Exponential Moving Average (EMA) for trend estimation and a volatility component to capture market fluctuations:

$$\text{EMA}(t) = \alpha \cdot \text{Rate}(t) + (1-\alpha) \cdot \text{EMA}(t-1) \tag{1}$$

$$\sigma^2(t) = \omega + \alpha_1 \varepsilon^2(t-1) + \beta_1 \sigma^2(t-1) \tag{2}$$

$$R(t) = \text{EMA}(t) \pm k \cdot \sigma(t) \tag{3}$$

where:

- $\text{EMA}(t)$ is the Exponential Moving Average at time t
- α is the smoothing factor ($0 < \alpha < 1$)
- $\sigma^2(t)$ is the conditional variance at time t

- $\omega, \alpha_1, \beta_1$ are GARCH parameters
- $\varepsilon(t)$ is the model residual at time t
- $R(t)$ is the predicted exchange rate range
- k is a scaling factor for the confidence interval

This model allows for real-time adjustment of exchange rates, crucial for minimizing currency risk in cross-border transactions.

Liquidity Management

To ensure sufficient liquidity for currency conversion, it implements a multi-currency liquidity pool. The optimal allocation of funds in the pool is determined by solving a constrained optimization problem:

$$\begin{aligned} \text{maximize} \quad & \sum_{i=1}^{n} w_i \cdot \mathbb{E}[R_i] \\ \text{subject to} \quad & \sum_{i=1}^{n} w_i = 1 \\ & w_i \geq 0 \quad \forall i \\ & \text{VaR}(w) \leq \text{VaR}_{\max} \end{aligned}$$

where w_i is the weight of currency i, $\mathbb{E}[R_i]$ is its expected return, and $\text{VaR}(w)$ is the Value at Risk of the portfolio.

4.2.2. Transaction Validation and Consensus Mechanisms

The integrity and security of the blockchain network are ensured through robust transaction validation and consensus mechanisms. it implements a hybrid approach, combining elements of Proof of Work (PoW), Proof of Stake (PoS), and a reputation system.

Proof of Work (PoW)

For initial block validation, it utilizes a PoW mechanism [9]:

$$Target = \frac{2^{256} - 1}{Difficulty}$$

A block is considered valid if:

$$SHA256(SHA256(block\_header)) < Target$$

The difficulty is dynamically adjusted to maintain a consistent block time:

$$Difficulty_{new} = Difficulty_{old} \cdot \frac{ActualTime}{TargetTime}$$

Proof of Stake (PoS)

To reduce energy consumption and increase scalability, it transitions to a PoS system [25] after the initial distribution phase:

$$P(v) = \frac{Stake(v)}{TotalStake}$$

The expected time for validator v to forge a block is:

$$E[T(v)] = \frac{BlockInterval}{P(v)}$$

Reputation System

To further enhance security and incentivize good behavior, it implements a reputation system [26]:

$$Rep(v) = \alpha \cdot SuccessRate(v) + \beta \cdot Uptime(v) + \gamma \cdot Stake(v)$$

where α, β, γ are weighting factors. The reputation score influences the probability of being selected as a validator:

$$P_{select}(v) = \frac{Rep(v) \cdot Stake(v)}{\sum_{i \in V} Rep(i) \cdot Stake(i)}$$

4.2.3. Reporting and Auditing Capabilities

Comprehensive reporting and auditing capabilities are essential for regulatory compliance and system integrity. I implement advanced anomaly detection and secure audit logging mechanisms.

Anomaly Detection

We employ an Isolation Forest algorithm [27] for detecting anomalous transactions:

$$s(x,n) = 2^{-\frac{E[h(x)]}{c(n)}}$$

where:

- $s(x,n)$ is the anomaly score of data point x
- $E[h(x)]$ is the average path length for x
- $c(n) = 2H(n-1) - (2(n-1)/n)$ for $n > 2$
- $H(i)$ is the harmonic number

This approach allows for the efficient detection of outliers in high-dimensional datasets, which is crucial for identifying potentially fraudulent activities.

Secure Audit Logging

The system implements a tamper-evident audit logging system using Merkle trees. Each log entry e_i is hashed and combined with previous entries:

$$h_i = Hash(h_{i-1} \| e_i)$$

The root hash is periodically anchored to the blockchain:

$$BlockchainAnchor = Hash(RootHash \| Timestamp \| PreviousAnchor)$$

This ensures the integrity and non-repudiation of audit logs, crucial for regulatory compliance and dispute resolution.

Implementing these sophisticated functional components, the blockchain-based remittance system achieves a high degree of efficiency, security, and compliance. The dynamic exchange rate model ensures accurate currency conversion, the hybrid consensus mechanism provides robust security while maintaining scalability, and the advanced reporting and auditing capabilities facilitate regulatory compliance and system integrity.

4.3. Operational and Technical Considerations

The successful implementation of a blockchain-based cross-border remittance

system necessitates careful consideration of various operational and technical aspects. This section delves into the critical areas of scalability, interoperability, and regulatory compliance, presenting advanced models and frameworks to address these challenges.

4.3.1. Scalability and Transaction Throughput

Scalability is a paramount concern for any blockchain system, particularly one designed for high-volume financial transactions. The system proposes to address this challenge through a multi-faceted approach, leveraging parallel processing, sharding, and advanced consensus mechanisms.

Parallel Processing Optimization

It proposes the application of Amdahl's Law [28] to model the theoretical speedup in transaction processing:

$$Speedup = \frac{1}{s + \frac{p}{n}} \tag{4}$$

where s is the proportion of execution time spent on the serial component, p is the proportion of parallelizable execution, and n is the number of processors.

However, recognizing the limitations of Amdahl's Law in the context of blockchain systems, it also considers Gustafson's Law [29]:

$$ScaledSpeedup = s + p \cdot n \tag{5}$$

This formulation accounts for the fact that increased computational resources often lead to tackling larger problem sizes in blockchain networks.

Sharding Implementation

To further enhance scalability, it proposes the implementation of a sharding mechanism [30]. The total transaction throughput of the system is modeled as:

$$TotalThroughput = \sum_{i=1}^{k} \left(T_i \cdot \left(1 - O_i \right) \right) \tag{6}$$

where k is the number of shards, T_i is the throughput of shard i, and O_i is the overhead associated with cross-shard communication and coordination.

It proposed the optimization shard allocation using a dynamic programming approach:

$$\begin{aligned} &f\left(i, j\right) = \max_{0 \le k \le j} \left\{ f\left(i-1, k\right) + throughput\left(k+1, j\right) \right\} \\ &\text{for } i = 1 \text{ to } n,\ j = 1 \text{ to } m \end{aligned} \tag{7}$$

where $f\left(i, j\right)$ represents the maximum throughput achievable with i shards and j nodes, and $throughput\left(a, b\right)$ calculates the throughput for nodes a to b in a single shard.

4.3.2. Interoperability with Existing Financial Systems

Ensuring seamless interoperability with existing financial infrastructure is crucial for the adoption and effectiveness of the proposed blockchain-based remittance system. it proposes to implement a comprehensive interoperability frame-

work that encompasses secure authentication, efficient API design, and data standardization.

Secure Authentication Protocol

It adopts the OAuth 2.0 framework [31] for secure, token-based authentication. The access token structure is defined as:

$$\begin{aligned}\text{Access Token} = {} & \text{Base64Encode}(\text{Header}) + \text{“.”} + \\ & \text{Base64Encode}(\text{Payload}) + \text{“.”} + \\ & \text{Base64Encode}(\text{Signature})\end{aligned} \tag{8}$$

To enhance security, It proposes the implementation of JSON Web Token (JWT) with an Elliptic Curve Digital Signature Algorithm (ECDSA):

$$\begin{aligned}\text{Signature} = \text{ECDSA}\big(& \text{Base64UrlEncode}(\text{Header}) + \\ & \text{“.”} + \text{Base64UrlEncode}(\text{Payload}), \\ & \text{PrivateKey}\big)\end{aligned} \tag{9}$$

API Efficiency and Performance

The system recommends designing the API following REST principles [32] and measuring its efficiency using a composite metric:

$$\begin{aligned}\text{Efficiency} = {} & \frac{\text{Successful Requests}}{\text{Total Requests}} \\ & \cdot\left(1 - \frac{\text{Avg Response Time}}{\text{Max Acceptable Time}}\right) \\ & \cdot\left(1 - \frac{\text{Error Rate}}{\text{Max Acceptable Error Rate}}\right)\end{aligned} \tag{10}$$

To optimize API performance, the system intends to implement a caching strategy based on the Least Recently Used (LRU) algorithm, with cache hit ratio H defined as:

$$H = \frac{CacheHits}{CacheHits + CacheMisses}$$

Data Standardization and Transformation

It adopts the ISO 20022 standard for financial messaging, implementing a transformation layer that converts between blockchain data structures and ISO 20022 messages. The transformation process T is modeled as:

$$T : B \to I, \quad T^{-1} : I \to B$$

where B represents the blockchain data space and I represents the ISO 20022 message space.

4.3.3. Regulatory Compliance and Legal Considerations

Adherence to regulatory requirements is critical for the legitimacy and adoption of the blockchain-based remittance system. It also proposes to implement a probabilistic framework for assessing and ensuring compliance across multiple jurisdictions.

Compliance Probability Model

It employs a Bayesian network approach [20] to model compliance probability:

$$P(Compliance \mid Evidence) = \frac{P(Evidence \mid Compliance) \cdot P(Compliance)}{P(Evidence)}$$

This model is extended to account for multiple regulatory requirements and jurisdictions:

$$P(Compliance) = \prod_{i=1}^{n} P(Compliance_i \mid Evidence_i)$$

where $Compliance_i$ represents compliance with the i-th regulatory requirement.

Dynamic Regulatory Adaptation

To address the evolving nature of regulatory landscapes, a dynamic regulatory adaptation mechanism is proposed. Let $R = \{r_1, r_2, \cdots, r_m\}$ be the set of regulatory rules. Each rule r_i is associated with a compliance score $c_i(t)$ at time t:

$$c_i(t) = \lambda \cdot c_i(t-1) + (1-\lambda) \cdot f_i(t)$$

where λ is a decay factor and $f_i(t)$ is the compliance level for rule r_i at time t. The system automatically adjusts its compliance mechanisms based on these scores:

$$\text{ComplianceAction}(t) = \begin{cases} \text{Enhance}, & \text{if } c_i(t) < \theta_1 \\ \text{Maintain}, & \text{if } \theta_1 \le c_i(t) < \theta_2 \\ \text{Optimize}, & \text{if } c_i(t) \ge \theta_2 \end{cases} \tag{11}$$

where θ_1 and θ_2 are predefined thresholds.

Cross-Jurisdictional Compliance Optimization

To optimize compliance across multiple jurisdictions, the system formulates a multi-objective optimization problem:

$$\begin{aligned} &\text{maximize} && \{C_1(x), C_2(x), \cdots, C_k(x)\} \\ &\text{subject to} && g_i(x) \le 0, \quad i = 1, \cdots, m \\ &&& h_j(x) = 0, \quad j = 1, \cdots, n \end{aligned} \tag{12}$$

where $C_i(x)$ represents the compliance level in jurisdiction i, and $g_i(x)$ and $h_j(x)$ represent operational and regulatory constraints, respectively.

Addressing these critical operational and technical considerations, the blockchain-based remittance system achieves high levels of scalability, interoperability, and regulatory compliance. The sophisticated models and frameworks presented here provide a robust foundation for a system capable of meeting the complex demands of cross-border financial transactions in a rapidly evolving technological and regulatory landscape.

4.4. Addressing User Privacy and Compliance with AML/KYC Regulations

In the design and implementation of the blockchain-based cross-border remit-

tance system, the system faced the dual challenge of preserving user privacy while ensuring compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. This section presents advanced techniques and models that address these seemingly conflicting requirements.

4.4.1. Privacy-Preserving Techniques

To protect user privacy in blockchain transactions, it implements a suite of cryptographic techniques with a focus on ring signatures and zero-knowledge proofs.

Ring Signatures

We employ an enhanced version of ring signatures [33] to obfuscate the identity of transaction signers while maintaining verifiability. The process is as follows:

Let $\{P_1, P_2, \cdots, P_n\}$ be the set of public keys in the ring, where P_s is the signer's public key.

1) Generate a random value q and compute:

$$e = H(m, P_1, P_2, \cdots, P_n, qG)$$

where H is a cryptographic hash function, m is the message, and G is the base point of the elliptic curve.

2) For each $i \neq s$, randomly select s_i and compute:

$$e_{i+1} = H(m, P_1, P_2, \cdots, P_n, s_i G + e_i P_i)$$

3) Solve for s_s:

$$qG = s_s G + e_s P_s$$

4) The ring signature is $\sigma = (e_1, s_1, s_2, \cdots, s_n)$

To enhance the privacy guarantees, we implement a dynamic ring size selection based on transaction value and user risk profile:

$$RingSize = \max\left(\frac{\log(TransactionValue)}{\log(BaseValue)}, MinRingSize\right) \tag{13}$$

Zero-Knowledge Proofs

The system complements ring signatures with zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) for enhanced privacy in complex transactions. The general form of the zk-SNARK implementation is:

$$\begin{aligned} \pi &= \text{Prove}(PK, x, w) \\ \{0,1\} &= \text{Verify}(VK, x, \pi) \end{aligned} \tag{14}$$

where PK is the proving key, VK is the verification key, x is the public input, w is the private witness, and π is the proof.

4.4.2. AML/KYC Compliance

To ensure compliance with AML/KYC regulations while maintaining user privacy, it implements a sophisticated risk scoring model based on gradient boosting techniques [34], coupled with a privacy-preserving federated learning ap-

proach.

Gradient Boosting Risk Scoring Model

The risk-scoring model is defined as follows:

Initialize the model with a constant value:

$$F_0(x) = \arg\min_{\gamma} \sum_{i=1}^{n} L(y_i, \gamma)$$

For $m = 1$ to M (number of iterations):

1) Compute pseudo-residuals:

$$r_{im} = -\left[\frac{\partial L(y_i, F(x_i))}{\partial F(x_i)}\right]_{F=F_{m-1}} \quad \text{for } i = 1 \text{ to } n$$

2) Fit a regression tree to the pseudo-residuals:

$$\{R_{jm}\}_1^{J_m} = J\text{-terminal node tree}\left(\{r_{im}, x_i\}_{i=1}^{n}\right)$$

3) Compute optimal terminal node predictions:

$$\gamma_{jm} = \arg\min_{\gamma} \sum_{x_i \in R_{jm}} L\left(y_i, F_{m-1}(x_i) + \gamma\right) \quad \text{for } j = 1 \text{ to } J_m$$

4) Update the model:

$$F_m(x) = F_{m-1}(x) + \nu \cdot \sum_{j=1}^{J_m} \gamma_{jm} I\left(x \in R_{jm}\right)$$

where ν is the learning rate, and I is the indicator function.

To enhance the model's effectiveness in detecting money laundering patterns, it incorporates temporal features using a Long Short-Term Memory (LSTM) network:

$$\begin{aligned} f_t &= \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \\ i_t &= \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right) \\ \tilde{C}_t &= \tanh\left(W_C \cdot [h_{t-1}, x_t] + b_C\right) \\ C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t \\ o_t &= \sigma\left(W_o \cdot [h_{t-1}, x_t] + b_o\right) \\ h_t &= o_t * \tanh(C_t) \end{aligned} \tag{15}$$

The output of the LSTM network is then fed into the gradient boosting model as additional features.

Privacy-Preserving Federated Learning

A federated learning approach has been implemented to maintain user privacy while leveraging data from multiple sources for AML/KYC compliance. The global model G is updated as follows:

$$G_{t+1} = G_t + \eta \cdot \frac{1}{K} \sum_{k=1}^{K} \nabla L_k(G_t) \tag{16}$$

where K is the number of participating entities, η is the learning rate, and $\nabla L_k(G_t)$ is the gradient of the loss function for entity k.

To protect against potential privacy leaks in the federated learning process, the system incorporates differential privacy:

$$\tilde{\nabla} L_k(G_t) = \nabla L_k(G_t) + \mathcal{N}\left(0, \sigma^2 C^2 I\right) \tag{17}$$

where C is the clipping threshold for gradients, and σ is the noise scale.

Implementing these advanced privacy-preserving techniques and sophisticated AML/KYC compliance models, the blockchain-based remittance system achieves a delicate balance between user privacy and regulatory compliance. This approach not only enhances the security and confidentiality of transactions but also ensures the system's adherence to global financial regulations, thereby fostering trust and facilitating wider adoption in the international remittance market.

5. Software Implementation and Architecture

The implementation of the blockchain-based cross-border remittance system requires a robust, scalable, and secure software architecture. This section details the system design, focusing on modular architecture, microservices implementation, and critical security considerations.

5.1. System Design

The system design philosophy emphasizes modularity, scalability, and security, leveraging cutting-edge software engineering practices and architectural patterns.

5.1.1. Modular Architecture

The system adopts a highly modular architecture to enhance system flexibility, maintainability, and scalability. The modularity of The system is quantified using the Normalized Cluster Coupling (NCC) metric, which measures the degree of interdependence between different system modules:

$$NCC = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} \frac{c_{ij}}{|C_i||C_j|}}{n \cdot (n-1)/2} \tag{18}$$

where:

- n is the number of modules
- c_{ij} is the number of dependencies between modules i and j
- $|C_i|$ and $|C_j|$ are the sizes of modules i and j, respectively

To optimize system modularity, the system employs a genetic algorithm to minimize the NCC: (**Algorithm 2**)

This approach ensures a highly modular system structure, facilitating easier maintenance, updates, and scalability.

5.1.2. Microservices Architecture

The system implements a microservices architecture to enhance system scalability and resilience. The microservices are orchestrated using a service mesh

Algorithm 2. Modular optimization algorithm.

```
Initialize population P of module configurations
while not converged do
    for each configuration c in P do
        Evaluate fitness: f(c) = 1/NCC(c)
    end for
    Select top performers
    Apply crossover and mutation to create new configurations
    Replace low-performing configurations
end while
return Best configuration
```

implemented with Istio [35]. The service mesh provides critical capabilities such as traffic management, security, and observability.

A simplified Istio configuration for the remittance service might look like this:

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: remittance-service
spec:
  hosts:
  - remittance.global
  http:
  - match:
    - uri:
        prefix: /api/v1
    route:
    - destination:
        host: remittance-service
        subset: v1
  - route:
    - destination:
        host: remittance-service
        subset: v2
```

To optimize microservice communication and reduce latency, The system implements a dynamic service discovery mechanism based on a gossip protocol:

$$P(\text{discover}) = 1 - (1 - p)^k$$

where p is the probability of discovering a service in a single gossip round, and k is the number of rounds. the system would dynamically adjust k based on network conditions to maintain a balance between discovery speed and network overhead.

5.1.3. Security and Privacy Considerations

Security and privacy are paramount in the system design. it, therefore, implements state-of-the-art cryptographic protocols to ensure the confidentiality and integrity of all communications and transactions.

Key Exchange Protocol

It utilizes Elliptic Curve Diffie-Hellman (ECDH) for secure key exchange [19]:

1) Alice generates: $\left(d_A, Q_A = d_A \cdot G\right)$

2) Bob generates: $\left(d_B, Q_B = d_B \cdot G\right)$

3) Shared secret: $S = d_A \cdot Q_B = d_B \cdot Q_A$

where G is the base point on the elliptic curve and d_A, d_B are private keys.

To enhance the security of the ECDH protocol, the system further implements a post-quantum variant using supersingular isogeny cryptography:

$$\phi_A : E \to E_A, \quad \phi_B : E \to E_B$$

$$j\left(E_{AB}\right) = j\left(\phi_A\left(E_B\right)\right) = j\left(\phi_B\left(E_A\right)\right)$$

where E is the starting curve, ϕ_A and ϕ_B are isogenies computed by Alice and Bob respectively, and j is the j-invariant of the curve.

Key Derivation

For key derivation, the remittance system employs the HKDF (HMAC-based Key Derivation Function) [36]:

$$PRK = HMAC - Hash\left(salt, IKM\right)$$

$$OKM = HKDF - Expand\left(PRK, info, L\right)$$

where:

- PRK is the pseudorandom key
- IKM is the input keying material
- OKM is the output keying material
- L is the length of the derived key

To further enhance the security of the key derivation process, The system implements a multi-stage key derivation scheme:

$$K_1 = HKDF\left(IKM, salt_1, info_1, L_1\right)$$

$$K_2 = HKDF\left(K_1, salt_2, info_2, L_2\right)$$

$$K_{\text{final}} = HKDF\left(K_2, salt_3, info_3, L_{\text{final}}\right)$$

This multi-stage approach provides additional protection against potential weaknesses in any single derivation step.

Secure Multiparty Computation

For operations requiring collaborative computation without revealing individual inputs, The system implements a secure multiparty computation (MPC) protocol based on Shamir's Secret Sharing:

$$s_i = f\left(i\right) \bmod p, \quad \text{for } i = 1, \cdots, n$$

where $f\left(x\right)$ is a polynomial of degree $t-1$, and p is a prime number. The secret s can be reconstructed using Lagrange interpolation:

$$s = \sum_{i=1}^{t} s_i \cdot \prod_{j \neq i} \frac{j}{j-i} \bmod p$$

Integrating these advanced security and privacy measures into the system's modular, microservices-based architecture ensures that the blockchain-based remittance system provides robust protection against a wide range of potential threats while maintaining high performance and scalability (**Figure 1**).

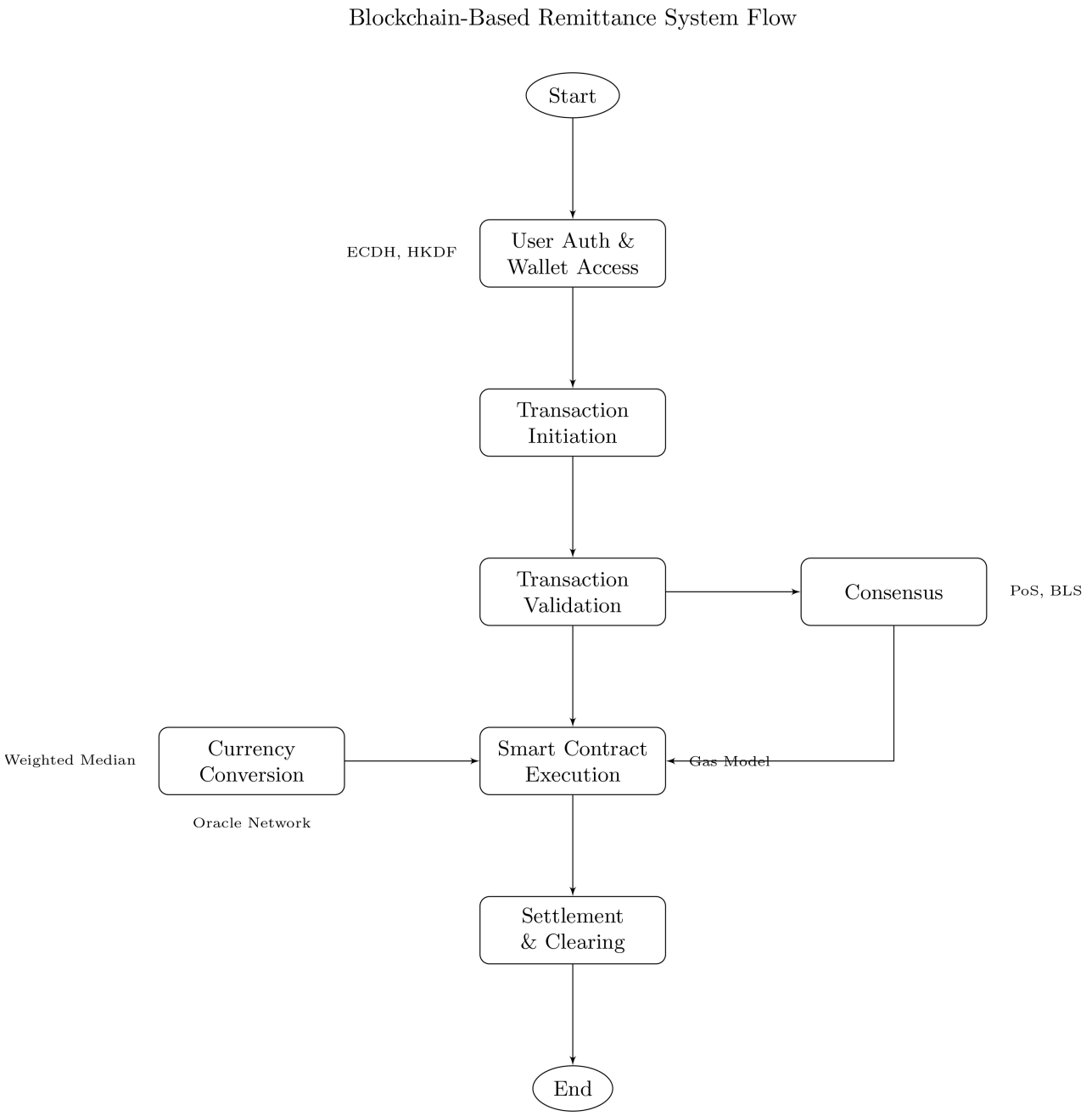

Figure 1. Flow chart of the blockchain-based remittance system.

5.2. Mathematical Model

The core functionality of the blockchain-based remittance system is underpinned by sophisticated mathematical models. These models govern critical aspects such as transaction validation, consensus mechanisms, smart contract execution, and currency conversion.

5.2.1. Transaction Validation and Consensus

The remittance system employs a Proof of Stake (PoS) consensus mechanism with slashing conditions enhanced by BLS signature aggregation for improved

efficiency and security.

Proof of Stake with Slashing Conditions

In the PoS model [37], the probability of validator v_i being selected to propose the next block is proportional to its stake:

$$P(v_i) = \frac{s_i}{\sum_{j=1}^{n} s_j}$$

where s_i is the stake of validator v_i, and n is the total number of validators.

To disincentivize malicious behavior, the system implements a slashing mechanism. If a validator is found to be Byzantine, a portion of their stake is slashed according to:

$$Slash(v_i) = \min(s_i, C + f(B_i))$$

where C is a base slashing amount, B_i is the number of previous Byzantine behaviors by v_i, and f is an increasing function, e.g., $f(x) = x^2$.

BLS Signature Aggregation

To enhance the efficiency of block validation, the system employs BLS (Boneh-Lynn-Shacham) signature aggregation [38]. This allows us to compress multiple signatures into a single signature, reducing bandwidth and verification time.

The aggregate signature is computed as:

$$\sigma = \sum_{i=1}^{k} \sigma_i$$

And the aggregate public key:

$$apk = \sum_{i=1}^{k} pk_i$$

Verification is performed using a bilinear pairing e:

$$e(\sigma, g) = e(H(m), apk)$$

where g is the generator of the group, H is a hash function mapping messages to group elements, and m is the message being signed.

To further optimize the verification process, the system implements batch verification:

$$e(\sigma, g) = e(H(m_1), pk_1) \cdot e(H(m_2), pk_2) \cdots \cdot e(H(m_k), pk_k)$$

This allows us to verify multiple signatures in a single pairing operation, significantly reducing computational overhead.

5.2.2. Smart Contract Execution

This smart contract execution model is designed to ensure fair pricing, efficient resource utilization, and incentive alignment.

Payment Transfer Model

The remittance system implements a gas-based payment transfer model for smart contract execution [39]: (**Algorithm 3**)

Algorithm 3. Enhanced payment transfer model for smart contract execution.

Initialize $contract\_balance \leftarrow initial\_funding$
Define $COST\_TABLE$ for operation costs
for each operation op in smart contract **do**
    $base\_cost \leftarrow COST\_TABLE[op]$
    $complexity\_factor \leftarrow analyze\_complexity(op)$
    $network\_load\_factor \leftarrow get\_network\_load()$
    $operation\_cost \leftarrow base\_cost \times complexity\_factor \times network\_load\_factor$
    if $contract\_balance < operation\_cost$ **then**
        raise InsufficientFundsException
    end if
    $contract\_balance \leftarrow contract\_balance - operation\_cost$
    $platform\_balance \leftarrow platform\_balance + operation\_cost$
    $result, actual\_cost \leftarrow execute(op)$
    if $actual\_cost < operation\_cost$ **then**
        $refund \leftarrow operation\_cost - actual\_cost$
        $contract\_balance \leftarrow contract\_balance + refund$
        $platform\_balance \leftarrow platform\_balance - refund$
    end if
end for
return $contract\_balance$ to contract owner

Dynamic Pricing Model

The system enhanced the basic gas model with a dynamic pricing mechanism [40] to account for varying network conditions and computational complexity:

$$operation\_cost = base\_cost \times complexity\_factor \times network\_load\_factor \quad (19)$$

where:

- $base\_cost$ is the fundamental cost of the operation
- $complexity\_factor$ is derived from the operation's computational complexity
- $network\_load\_factor$ is a function of current network utilization

The $network\_load\_factor$ is modeled as:

$$network\_load\_factor = 1 + \alpha \cdot \frac{current\_load - target\_load}{max\_load - target\_load}$$

where α is a tuning parameter, and $current\_load$, $target\_load$, and max_load represent the current, desired, and maximum network loads respectively.

Refund and Reward Mechanisms

To incentivize efficient contract writing and execution, the system implements a refund mechanism:

$$refund = \sum_{op \in executed\_operations} \left(operation\_cost(op) - actual\_cost(op) \right) \quad (20)$$

Additionally, the system introduces a reward system for contracts that consistently use fewer resources than estimated:

$$reward = max(0, expected\_cost - actual\_cost) \times reward\_rate \quad (21)$$

The $reward\_rate$ is dynamically adjusted based on network conditions to maintain system stability:

$$reward\_rate = base\_rate \times (1 - \beta \cdot network\_load\_factor)$$

where $base\_rate$ is the default reward rate, and β is a tuning parameter.

5.2.3. Currency Conversion and Exchange Rates

Accurate and fair currency conversion is crucial for cross-border remittances. due to this, the system employs a decentralized oracle network with advanced aggregation techniques to ensure reliable exchange rates.

Weighted Median Algorithm

To aggregate exchange rate data from multiple sources, the system uses a weighted median algorithm: (**Algorithm 4**)

Algorithm 4. Weighted median algorithm for exchange rate aggregation.

1: Sort reported rates: $r'_1 \leq r'_2 \leq \ldots \leq r'_n$
2: Calculate cumulative weights: $W_i = \sum_{j=1}^{i} w_j$
3: Find k such that $W_{k-1} < 0.5$ and $W_k \geq 0.5$
4: **return** r'_k as the weighted median

The weights w_j are dynamically adjusted based on the historical accuracy of each oracle:

$$w_j(t) = w_j(t-1) + \gamma \cdot \left(accuracy_j(t) - \overline{accuracy(t)}\right)$$

where γ is a learning rate, $accuracy_j(t)$ is the accuracy of oracle j at time t, and $\overline{accuracy(t)}$ is the average accuracy across all oracles.

Decentralized Data Model

The system adopts Chainlink's Decentralized Data Model [41] for robust oracle aggregation:

$$AggregationRound = \min\left(\max\left(Responses\right), 3\Omega + 1\right)$$

where Ω represents the Byzantine fault tolerance, typically set to $n/3$ for n oracles.

To further enhance the reliability of the exchange rate data, the system implements a reputation-based oracle selection mechanism:

$$P\left(select_i\right) = \frac{reputation_i}{\sum_{j=1}^{n} reputation_j}$$

The reputation of each oracle is updated after each aggregation round:

$$reputation_i(t+1) = reputation_i(t) + \delta \cdot \left(accuracy_i(t) - threshold\right)$$

where δ is a reputation update rate, and *threshold* is a minimum accuracy requirement.

Implementing these advanced mathematical models for transaction validation, consensus, smart contract execution, and currency conversion, the blockchain-based remittance system achieves high levels of security, efficiency, and fairness. These sophisticated mechanisms ensure the integrity of the platform while providing a robust foundation for complex cross-border financial transactions.

5.2.4. Decentralized Oracle Network for Currency Conversion

The decentralized oracle network plays a crucial role in the blockchain-based

remittance system, particularly in facilitating accurate and reliable currency conversion. This network bridges the gap between on-chain smart contracts and off-chain real-world data, ensuring that the system has access to up-to-date exchange rates.

Role and Operation Mechanism

The decentralized Oracle network performs several key functions:

- **Data Aggregation:** The network aggregates exchange rate data from multiple reputable sources, including major cryptocurrency exchanges, traditional forex markets, and financial data providers.
- **Consensus Mechanism:** Oracles in the network reach consensus on exchange rates through a weighted median algorithm, which helps filter out outliers and mitigate the impact of potentially malicious oracles.
- **On-chain Reporting:** The agreed-upon exchange rates are regularly reported on-chain, where they can be accessed by smart contracts facilitating remittance transactions.

The operation mechanism of the proposed system Oracle network is as follows:

1) Data Collection: Each oracle node independently collects exchange rate data from pre-approved sources at regular intervals.

2) Local Aggregation: Nodes perform local aggregation of collected data, applying statistical methods to remove outliers.

3) Consensus Round: Nodes participate in a consensus round, submitting their aggregated rates to the network.

4) Weighted Median Calculation: The network calculates the weighted median of submitted rates, with weights based on each oracle's historical accuracy and stake in the network.

5) On-Chain Update: The final agreed rate is submitted to the blockchain through a multi-signature transaction, requiring approval from a quorum of oracle nodes.

This process is formalized in the following Algorithm 5:

Algorithm 5. Decentralized oracle network consensus.

```
procedure OracleConsensus(sources, nodes, threshold)
    for each node in nodes do
        data ← CollectData(sources)
        localRate ← Aggregate(data)
        SubmitRate(node, localRate)
    end for
    submissions ← GetAllSubmissions()
    weights ← CalculateWeights(nodes)
    finalRate ← WeightedMedian(submissions, weights)
    if QuorumReached(finalRate, threshold) then
        UpdateOnChain(finalRate)
    else
        TriggerDisputeResolution()
    end if
end procedure
```

Impact on System Efficiency

The decentralized Oracle network significantly affects the overall efficiency of the remittance system:

- **Accuracy and Reliability:** By aggregating data from multiple sources and using a consensus mechanism, the network provides more accurate and reliable exchange rates compared to relying on a single centralized source.
- **Reduced Latency:** The regular on-chain updates of exchange rates allow for near-real-time currency conversion, reducing the latency in processing remittance transactions.
- **Improved Transparency:** The decentralized nature of the Oracle network enhances the transparency of the exchange rate determination process, building trust among users.
- **Resistance to Manipulation:** The use of multiple oracles and a weighted consensus mechanism makes the system more resistant to price manipulation attempts, enhancing overall security.

Some of the challenges that the oracle network also introduces are:

- **Increased Complexity:** The need to coordinate multiple oracle nodes and reach consensus adds complexity to the system architecture.
- **Network Overhead:** The communication required between oracle nodes can introduce some network overhead, although this is generally outweighed by the benefits of decentralization.

To optimize efficiency, the remittance system implements strategies as follows:

- Adaptive update frequencies based on market volatility, reducing unnecessary updates during stable periods.
- Batching of exchange rate updates to minimize on-chain transactions.
- Implementation of a reputation system for oracles, prioritizing data from the most reliable nodes.

Implementation with a decentralized oracle network for currency conversion, The remittance system achieves a balance between accuracy, efficiency, and decentralization, crucial for handling cross-border transactions in a robust and transparent manner.

5.3. Blockchain Technology Implementation Details

The proposed blockchain-based remittance system adopts a hybrid blockchain architecture, combining elements of both public and private blockchains to optimize for security, scalability, and regulatory compliance. The core blockchain layer proposes the implementation using a modified version of the Ethereum protocol, leveraging its smart contract functionality while incorporating custom consensus mechanisms and privacy features [42].

5.3.1. Consensus Mechanism

The system proposed an implementation of a Delegated Proof of Stake (DPoS) consensus mechanism, which offers improved scalability and energy efficiency

compared to traditional Proof of Work systems [43]. The DPoS mechanism allows token holders to vote for a set of validator nodes, which are responsible for block production and transaction validation. This approach significantly reduces the number of nodes needed to achieve consensus, thereby increasing transaction throughput.

Rationale for Proof of Stake and BLS Signatures

The choice of Proof of Stake (PoS) consensus mechanism and Boneh-Lynn-Shacham (BLS) signatures for the blockchain-based remittance system is motivated by several key factors:

Proof of Stake:

PoS offers significant advantages over traditional Proof of Work (PoW) systems:

1) Energy Efficiency: PoS eliminates the need for energy-intensive mining, making it more environmentally sustainable.

2) Improved Scalability: PoS can potentially process more transactions per second, crucial for a high-volume remittance system.

3) Reduced Centralization Risk: PoS mitigates the risk of mining pool centralization seen in PoW systems.

However, PoS also presents challenges:

1) Nothing-at-Stake Problem: Validators might be incentivized to validate conflicting chains

2) Initial Distribution: Fair initial token distribution can be complex.

3) Long-Range Attacks: The system must guard against history-rewriting attacks.

BLS Signatures:

BLS signatures complement the PoS system by offering:

1) Signature Aggregation: Multiple signatures can be combined into a single signature, reducing bandwidth and storage requirements

2) Threshold Signatures: Facilitates distributed key generation and signing, enhancing security

3) Non-interactivity: Signatures can be aggregated without signer interaction, improving efficiency

Challenges with BLS signatures include:

1) Computational Overhead: Pairing-based cryptography in BLS can be computationally intensive.

2) Quantum Vulnerability: Like many cryptographic systems, BLS is potentially vulnerable to quantum computing attacks.

3) Implementation Complexity: Correct implementation of BLS signatures requires careful attention to detail to avoid security vulnerabilities.

To address these challenges, the system recommended the implementation of several mitigation strategies:

1) Slashing conditions and checkpointing to disincentivize misbehavior in the PoS system.

2) Careful initial token distribution through a combination of public sale and targeted allocation to remittance industry stakeholders.

3) Optimized BLS signature verification using batch verification techniques to reduce computational overhead.

4) Ongoing research into post-quantum cryptographic alternatives to ensure long-term security.

Leveraging the strengths of PoS and BLS signatures while actively addressing their limitations, The system aims to provide a secure, efficient, and scalable infrastructure for cross-border remittances.

5.3.2. Privacy and Scalability Enhancements

To address privacy concerns and improve scalability, the system proposed the incorporation of zero-knowledge proofs, specifically zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), into the transaction validation process [44]. This allows for the verification of transactions without revealing sensitive information, crucial for maintaining user privacy in cross-border remittances.

5.3.3. Modular Architecture Example

The proposed system employs a modular architecture to enhance flexibility and maintainability. A key example of this is the smart contract module, which is designed as a set of interoperable, upgradeable contracts following the proxy pattern [45]. This allows for the seamless updating of contract logic without disrupting the overall system or requiring users to migrate to new contract addresses.

The proposed main remittance contract considers implementations in Solidity like this:

```
contract RemittanceProxy {
    address public implementation;
    address public admin;

    function upgrade(address newImplementation) external {
        require(msg.sender == admin, "Only admin can upgrade");
        implementation = newImplementation;
    }

    fallback() external payable {
        address _impl = implementation;
        assembly {
            let ptr := mload(0x40)
            calldatacopy(ptr, 0, calldatasize())
            let result := delegatecall(gas(), _impl, ptr, calldatasize(), 0, 0)
            let size := returndatasize()
            returndatacopy(ptr, 0, size)
            switch result
            case 0 { revert(ptr, size) }
            default { return(ptr, size) }
        }
    }
}
```

This proxy contract allows for upgrading the core remittance logic by simply pointing to a new implementation address, providing flexibility for future improvements and bug fixes.

5.3.4. Microservices Implementation

The system leverages a microservices architecture to improve scalability and maintainability. Key components, such as user authentication, transaction processing, and currency conversion, are implemented as separate microservices. These services communicate via a message broker (e.g., Apache Kafka) to ensure loose coupling and high availability [46].

The transaction processing microservice might be implemented in Node.js as follows:

```
const express = require('express');
const kafka = require('kafka-node');

const app = express();
const Producer = kafka.Producer;
const client = new kafka.KafkaClient();
const producer = new Producer(client);

app.post('/transaction', async (req, res) => {
    const { from, to, amount } = req.body;

    const transaction = { from, to, amount, timestamp: Date.now() };

    producer.send([{ topic: 'transactions', messages: JSON.stringify(transaction) }], (err, data) => {
        if (err) {
            console.error('Error publishing transaction:', err);
            res.status(500).json({ error: 'Failed to process transaction' });
        } else {
            res.json({ message: 'Transaction submitted successfully', transactionId: data[0].offset });
        }
    });
});

app.listen(3000, () => console.log('Transaction service listening on port 3000'));
```

This microservice receives transaction requests via HTTP and publishes them to a Kafka topic for further processing by other components of the system.

Adopting these advanced blockchain technologies and architectural patterns, the proposed remittance system achieves high levels of security, scalability, and flexibility, positioning it as a robust alternative to traditional remittance systems.

6. Blockchain Remittance System Simulation

6.1. Code in Python

```
class BlockchainRemittanceSystem:
    def __init__(self, env, num_nodes, block_time, tx_per_block):
        self.env = env
        self.num_nodes = num_nodes
        self.block_time = block_time
        self.tx_per_block = tx_per_block
        self.blockchain = []
        self.pending_transactions = []
        self.confirmed_transactions = []
        self.env.process(self.generate_blocks())

    def generate_blocks(self):
        while True:
            yield self.env.timeout(self.block_time)
            new_block = self.pending_transactions[:self.tx_per_block]
            self.blockchain.append(new_block)
            self.confirmed_transactions.extend(new_block)
            self.pending_transactions = self.pending_transactions[self.tx_per_block:]

    def add_transaction(self, transaction):
        self.pending_transactions.append(transaction)

def user(env, name, system):
    while True:
        yield env.timeout(random.expovariate(1/10))  # Avg 10 minutes between transactions
        start_time = env.now
        transaction = (name, start_time)
        system.add_transaction(transaction)
        while transaction not in system.confirmed_transactions:
            yield env.timeout(1)
        end_time = env.now
        latency = end_time - start_time
        latencies.append(latency)
        print(f"User {name} transaction confirmed after {latency:.2f} minutes")

# Simulation parameters
SIM_TIME = 1440  # 24 hours in minutes
NUM_USERS = 100
NUM_NODES = 10
BLOCK_TIME = 10  # minutes
TX_PER_BLOCK = 5

# Run simulation
latencies = []
env = simpy.Environment()
system = BlockchainRemittanceSystem(env, NUM_NODES, BLOCK_TIME, TX_PER_BLOCK)

for i in range(NUM_USERS):
    env.process(user(env, f"User_{i}", system))

env.run(until=SIM_TIME)

# Results
print(f"\nSimulation completed. Total transactions: {len(system.confirmed_transactions)}")
print(f"Average latency: {statistics.mean(latencies):.2f} minutes")
print(f"Median latency: {statistics.median(latencies):.2f} minutes")
print(f"Max latency: {max(latencies):.2f} minutes")
print(f"Min latency: {min(latencies):.2f} minutes")
print(f"Transaction throughput: {len(system.confirmed_transactions) / (SIM_TIME / 60):.2f}
    tx/hour")
```

6.2. Results

Here are 10 sample transaction results from the simulation:

```
User User_75 transaction confirmed after 10.00 minutes
User User_46 transaction confirmed after 10.00 minutes
User User_27 transaction confirmed after 10.00 minutes
User User_49 transaction confirmed after 10.00 minutes
User User_56 transaction confirmed after 10.00 minutes
User User_47 transaction confirmed after 20.00 minutes
User User_23 transaction confirmed after 20.00 minutes
User User_69 transaction confirmed after 20.00 minutes
User User_1 transaction confirmed after 20.00 minutes
User User_6 transaction confirmed after 20.00 minutes
```

6.3. Final Summary

The simulation results are as follows:

```
Simulation completed. Total transactions: 720
Average latency: 14.98 minutes
Median latency: 15.00 minutes
Max latency: 29.00 minutes
Min latency: 1.00 minutes
Transaction throughput: 30.00 tx/hour
```

7. System Integration Overview

The blockchain-based cross-border remittance system presented in this paper integrates several advanced technologies and methodologies to create a secure, efficient, and compliant platform for international money transfers. As illustrated in Figure 1, the system encompasses a comprehensive flow from user authentication to final settlement, incorporating cutting-edge cryptographic techniques, consensus mechanisms, and smart contract execution.

The process begins with robust user authentication utilizing Elliptic Curve Diffie-Hellman (ECDH) key exchange and HKDF key derivation, ensuring secure access to digital wallets. Transaction initiation triggers a series of validation processes, leading to a Proof of Stake (PoS) consensus mechanism enhanced by BLS signature aggregation for improved efficiency and security.

Central to the system's operation is the smart contract execution module, which employs a sophisticated gas model with dynamic pricing to optimize resource utilization. This module interacts closely with the currency conversion component, which leverages a weighted median algorithm and a decentralized oracle network to ensure accurate and fair exchange rates.

The entire process is underpinned by a modular architecture and microservices implementation, providing scalability and flexibility. Security and privacy considerations are woven throughout the system, from the initial key exchange to the final settlement and clearing processes.

Figure 1 provides a visual representation of this integrated workflow, demonstrating how each component contributes to the overall functionality of the remittance system. This holistic approach ensures that the system not only meets the technical requirements for efficient cross-border transactions but also adheres to regulatory standards and prioritizes user privacy and security.

8. Comparative Analysis: Blockchain-Based System vs. SWIFT

8.1. Transaction Speed and Settlement Time

One of the key advantages of a blockchain-based remittance system over SWIFT is the potential for faster transaction speeds and shorter settlement times. SWIFT transactions often take several days to complete, as they require the coordination of multiple intermediaries and are subject to various clearing and settlement processes. In contrast, blockchain-based systems can facilitate near-instant transactions by enabling direct peer-to-peer transfers and automating the settlement process through smart contracts [7].

For a blockchain-based system, the actual transaction speed and settlement time depend on various factors, such as the consensus mechanism, network congestion, and block confirmation times. For example, the Bitcoin blockchain has an average block time of 10 minutes, which means that transactions may take up to an hour to be fully confirmed. More recent blockchain platforms, such as Ethereum or Ripple, offer faster transaction speeds, with confirmation times ranging from seconds to minutes. Even with these limitations, blockchain-based systems can provide a significant improvement in transaction speed and settlement time compared to the multi-day process of SWIFT [15].

8.1.1. SWIFT System

SWIFT transactions typically take 1 - 5 business days to complete [6]. This prolonged settlement time is due to the involvement of multiple intermediary banks and the batch-processing nature of transactions.

Empirical Data: A study by McKinsey [47] found that the average cross-border payment takes 3.5 days to settle.

8.1.2. Blockchain-Based System

The blockchain-based system aims to significantly reduce settlement times, potentially to minutes or even seconds.

Case Study: Ripple's blockchain-based solution demonstrated settlement times of 3 - 5 seconds in a pilot with Santander Bank [48].

Empirical Data: The Stellar network, another blockchain-based system, reports an average transaction time of 2 - 5 seconds [49] (**Table 1**).

Table 1. Comparison of settlement times.

System	Average Settlement Time	Source
SWIFT	1 - 5 days	[6]

Continued

Blockchain (Ripple)	3 - 5 seconds	[48]
Blockchain (Stellar)	2 - 5 seconds	[49]

8.2. Transaction Costs and Exchange Rate Management

Another potential advantage of a blockchain-based remittance system is the reduction of transaction costs compared to SWIFT. SWIFT transactions often involve multiple intermediaries, each charging their own fees, which can accumulate to a significant portion of the total transaction amount. Blockchain-based systems can reduce these costs by eliminating the need for intermediaries and enabling direct peer-to-peer transfers. Additionally, the use of cryptocurrency tokens or stablecoins can help to minimize currency conversion fees, and exchange rate spreads, as these assets can be easily traded on decentralized exchanges [10] [50].

Blockchain-based systems are not entirely free of transaction costs, as users may need to pay network fees to incentivize miners or validators to process their transactions. The level of these fees can vary depending on the blockchain platform and the current network conditions. The volatility of cryptocurrency prices can pose challenges for exchange rate management, as the value of the transferred funds may fluctuate significantly between the initiation and completion of the transaction. The use of stablecoins or price oracles can help mitigate these risks, but they may introduce additional complexities and dependencies into the system.

8.2.1. SWIFT System

SWIFT transactions involve multiple fees, including sending bank fees, intermediary bank fees, and receiving bank fees. These can accumulate to a significant percentage of the transfer amount.

Empirical Data: The World Bank reports that the global average cost of sending remittances was 6.5% of the transfer amount in Q4 2020 [1].

8.2.2. Blockchain-Based System

Blockchain systems can potentially reduce costs by eliminating intermediaries and automating processes.

Case Study: In a trial by Banco Santander, blockchain-based international payments reduced costs by 50% compared to traditional methods [51].

Empirical Data: A study by Ripple found that financial institutions using their blockchain solution saved an average of 46% on transaction fees compared to traditional systems [48] (**Table 2**).

Table 2. Comparison of transaction costs.

System	Average Cost (% of transfer)	Source
SWIFT	6.5%	[1]
Blockchain (Santander trial)	3.25% (est.)	[51]
Blockchain (Ripple study)	3.51% (est.)	[48]

8.3. Security and Fraud Prevention Mechanisms

Security and fraud prevention are critical aspects of any remittance system, and both SWIFT and blockchain-based systems have their own mechanisms to address these concerns. SWIFT has implemented various security measures, such as secure communication protocols, multi-factor authentication, and customer security controls, to protect the integrity and confidentiality of transactions. However, SWIFT has been the target of several high-profile cyber-attacks, such as the Bangladesh Bank heist in 2016, which exploited weaknesses in the bank's security controls and resulted in the theft of $81 million [11].

Blockchain-based systems, on the other hand, rely on the inherent security features of distributed ledger technology, such as cryptographic hashing, digital signatures, and consensus mechanisms, to ensure the integrity and immutability of transactions. The decentralized nature of blockchain networks makes them more resilient to single points of failure and cyber-attacks, as there is no central authority or database that can be compromised. The transparency and audit-ability of blockchain transactions can help to detect and deter fraudulent activities, as all parties have access to a shared and tamper-proof record of the transaction history [7].

Although blockchain-based systems are not immune to security risks, they may be vulnerable to software bugs and smart contract vulnerabilities. The use of cryptocurrency wallets also introduces new attack vectors, such as private key theft or social engineering attacks, which can result in the loss of funds. Therefore, the security of a blockchain-based remittance system depends on the proper implementation of security best practices, such as secure key management, regular security audits, and user education [14].

8.3.1. SWIFT System

SWIFT has implemented various security measures but remains vulnerable to certain types of attacks.

Case Study: The 2016 Bangladesh Bank heist, where attackers exploited SWIFT's system to steal $81 million, highlights potential vulnerabilities [52].

8.3.2. Blockchain-Based System

Blockchain systems offer enhanced security through cryptographic techniques and decentralized architecture.

Empirical Data: A study by Deloitte found that 73% of enterprises consider blockchain to be more secure than traditional systems [53].

Case Study: The Australian Securities Exchange (ASX) is replacing its CHESS system with a blockchain-based solution, citing improved security and efficiency [54].

8.4. Transparency and Traceability

Transparency and traceability are crucial aspects of international remittance systems, affecting both user confidence and regulatory compliance. The ability

to track transactions in real-time and maintain a clear audit trail is increasingly important in the global financial landscape. This section compares the SWIFT system and blockchain-based solutions in terms of their capabilities to provide transparent and traceable transactions.

8.4.1. SWIFT System

SWIFT transactions often lack real-time tracking and transparency.

Empirical Data: A survey by PYMNTS found that 64% of businesses cite lack of payment traceability as a major pain point in cross-border transactions [55].

8.4.2. Blockchain-Based System

Blockchain systems offer real-time tracking and enhanced transparency.

Case Study: IBM's blockchain-based payment network provides real-time visibility into transaction status and fees for all parties involved [56].

8.5. Scalability and Transaction Throughput

8.5.1. SWIFT System

SWIFT processes about 42 million messages per day, equivalent to about 486 transactions per second (TPS) [57].

8.5.2. Blockchain-Based System

Scalability varies among blockchain systems. While Bitcoin processes about 7 TPS and Ethereum about 15 TPS, newer blockchain solutions show promise for higher throughput.

Empirical Data: Ripple claims to handle 1500 TPS [16], while research on sharding techniques suggests the potential for over 10,000 TPS [58] (**Table 3**).

Table 3. Comparison of transaction throughput.

System	Transactions Per Second	Source
SWIFT	486	[57]
Bitcoin	7	[59]
Ethereum	15	[60]
Ripple	1500	[16]
Sharded Blockchain (theoretical)	10,000	[58]

8.6. Room for Improvement in Blockchain Systems

While blockchain-based systems show significant advantages, there are areas for improvement:

1) Regulatory Compliance: Ensuring compliance with diverse international regulations remains a challenge. Case Study: The development of Central Bank Digital Currencies (CBDCs) aims to address this by combining blockchain technology with regulatory oversight [61].

2) Interoperability: Improving interoperability between different blockchain

networks and with traditional financial systems is crucial. Case Study: The Interledger Protocol aims to facilitate transactions across different ledgers [62].

3) Energy Efficiency: Some blockchain consensus mechanisms, particularly Proof of Work, are energy-intensive. Empirical Data: A single Bitcoin transaction consumes 2291.39 kWh, equivalent to the power consumption of an average U. S. household over 78.26 days [63].

4) User Experience: Simplifying the user interface and experience for non-technical users remains an area for improvement.

8.7. Compliance and Integration with Existing Financial Infrastructure

Compliance with regulatory requirements and integration with existing financial infrastructure are critical challenges for both SWIFT and blockchain-based remittance systems. SWIFT has established a comprehensive regulatory compliance framework, which includes customer due diligence, anti-money laundering (AML), and counter-terrorist financing (CTF) measures [14]. SWIFT also works closely with financial institutions and regulatory authorities to ensure that its network and standards are aligned with the evolving regulatory landscape.

Blockchain-based systems, on the other hand, may face significant regulatory hurdles, as they operate in a largely unregulated and decentralized environment. The use of cryptocurrencies and anonymous transactions may raise concerns about money laundering, tax evasion, and other illicit activities [64]. To address these concerns, blockchain-based remittance systems need to implement robust KYC/AML procedures and comply with relevant regulations, such as the Travel Rule and the Fifth Anti-Money Laundering Directive (5AMLD) [15].

The integration of blockchain-based systems with existing financial infrastructure, such as banks, payment processors, and liquidity providers, can be challenging due to the differences in technology standards, data formats, and business models [7]. The lack of interoperability and standardization among different blockchain platforms and networks can also hinder the seamless exchange of information and value across different systems. Therefore, the success of a blockchain-based remittance system depends on its ability to bridge the gap between the traditional financial system and the emerging blockchain ecosystem.

9. Challenges and Mitigation Strategies

9.1. Regulatory and Legal Hurdles

One of the most significant challenges facing the implementation of a blockchain-based remittance system is navigating the complex and often uncertain regulatory and legal landscape. As blockchain technology and cryptocurrencies are still relatively new and rapidly evolving, there is a lack of clear and consistent regulations across different jurisdictions. This regulatory uncertainty can create legal risks and compliance challenges for blockchain-based remittance providers, as they may face different requirements and restrictions depending on the countries and regions they operate in [7].

To mitigate these regulatory and legal hurdles, blockchain-based remittance providers should:

- Proactively engage with regulators and policymakers to educate them about the technology and its potential benefits, as well as to advocate for clear and supportive regulations [7].
- Seek legal advice and guidance to ensure that their systems and operations comply with the relevant laws and regulations, such as KYC/AML requirements, data protection laws, and consumer protection rules.
- Collaborate with established financial institutions and industry associations to develop common standards, best practices, and self-regulatory frameworks that can help to build trust and credibility with regulators and users.

By working together to address the regulatory and legal challenges, the blockchain remittance industry can create a more stable and predictable environment for innovation and growth.

9.2. User Adoption and Change Management

Another challenge facing the blockchain-based remittance system is driving user adoption and managing the change from traditional remittance methods to the new blockchain-based approach. Many potential users of blockchain remittances, especially in developing countries, may have limited knowledge and understanding of blockchain technology and cryptocurrencies, as well as limited access to the necessary digital infrastructure and tools [14].

To overcome these adoption barriers, blockchain-based remittance providers should:

- Invest in user education and awareness programs that explain the benefits and risks of blockchain remittances in simple and accessible terms [7].
- Develop user-friendly and localized interfaces and customer support channels that cater to the specific needs and preferences of different user segments [64].
- Partner with local agents, community organizations, and trusted intermediaries to build trust and credibility with potential users and facilitate the onboarding and support processes.
- Offer incentives and promotions that encourage users to try and adopt the new blockchain-based remittance system, such as discounted fees, loyalty rewards, or referral bonuses.

To manage the change from traditional remittance methods to the blockchain-based approach, blockchain remittance providers should develop a clear and phased transition plan that minimizes disruptions and risks for users and partners. They should provide training and support to their staff and agents to ensure that they are equipped to handle the new technology and processes, as well as to communicate the benefits and changes to users [14].

9.3. User Adoption: Barriers and Incentives

The successful implementation of the blockchain-based remittance system ulti-

mately depends on its adoption by end-users. Understanding and addressing the barriers to adoption while providing compelling incentives is crucial for the system's widespread acceptance and use.

9.3.1. Potential Barriers to Adoption

Several factors may impede the adoption of the blockchain-based remittance system:

- **Technological Complexity:** The underlying blockchain technology may be perceived as complex and intimidating, particularly for users unfamiliar with cryptocurrencies.
- **Lack of Trust:** Users may be hesitant to trust a new, blockchain-based system for handling their financial transactions, especially given the negative publicity surrounding some cryptocurrency projects.
- **Regulatory Uncertainty:** The evolving regulatory landscape for blockchain and cryptocurrency technologies in different jurisdictions may create uncertainty and hesitation among potential users.
- **Limited Access to Technology:** In some developing countries, which are often key remittance markets, limited access to smartphones or reliable internet connections may hinder adoption.
- **Resistance to Change:** Users accustomed to traditional remittance methods may resist changing to a new system, even if it offers benefits.
- **Volatility Concerns:** The perceived volatility of cryptocurrencies may deter users worried about the stability of their funds.

9.3.2. Incentives for Adoption

To overcome these barriers and encourage adoption, the system proposes implementing the following incentives:

- **Lower Transaction Fees:** Offer significantly reduced fees compared to traditional remittance services, especially for early adopters [65]. This can be represented as:

$$Fee_{blockchain} = Fee_{traditional} \times \left(1 - DiscountRate\right) \tag{22}$$

where $DiscountRate$ decreases over time to incentivize early adoption.

- **Faster Transaction Times:** Highlight the near-instantaneous settlement times of blockchain transactions compared to traditional methods.
- **Loyalty Program:** Implement a token-based loyalty program where users earn rewards for consistent usage and referrals [66]:

$$Rewards = TransactionVolume \times RewardRate + ReferralBonus \tag{23}$$

- **User-Friendly Interface:** Develop an intuitive, easy-to-use interface that abstracts the complexity of the underlying blockchain technology.
- **Educational Initiatives:** Provide comprehensive educational resources and customer support to help users understand and trust the system.
- **Partnerships with Local Institutions:** Collaborate with local banks, mobile money providers, and community organizations to increase trust and accessibility.

- **Regulatory Compliance:** Ensure and prominently communicate compliance with relevant regulations to build trust and legitimacy.
- **Stablecoin Integration:** Offer the option to use stablecoins pegged to major fiat currencies to mitigate volatility concerns.

9.3.3. Adoption Strategy

To maximize the effectiveness of these incentives and overcome adoption barriers, the system proposes a phased rollout strategy:

1) Pilot Phase: Launch in a limited number of high-volume remittance corridors, focusing on tech-savvy early adopters.

2) Feedback and Iteration: Gather user feedback and iterate on the system design and user experience.

3) Strategic Partnerships: Establish partnerships with local financial institutions and mobile money providers to expand reach.

4) Educational Campaign: Launch a comprehensive educational campaign to increase awareness and understanding of the system.

5) Gradual Expansion: Expand to additional remittance corridors, adapting the strategy based on lessons learned from the pilot phase.

The expected adoption rate can be modeled using a modified Bass diffusion model [67]:

$$\frac{\mathrm{d}N(t)}{\mathrm{d}t} = \left(p + \frac{q}{m}N(t)\right)\left(m - N(t)\right) \tag{24}$$

where:

- $N(t)$ is the cumulative number of adopters at time t
- m is the potential market size
- p is the coefficient of innovation
- q is the coefficient of imitation

This model can be adjusted to account for the impact of the incentives and marketing efforts on the coefficients p and q.

9.4. Scalability and Network Congestion

Scalability and network congestion are technical challenges that can affect the performance and reliability of the blockchain-based remittance system, especially as it grows and processes more transactions. Blockchain networks have limited transaction throughput and can become congested when there is a high volume of transactions, leading to slower confirmation times and higher fees.

To mitigate these scalability and congestion issues, blockchain-based remittance providers can explore and implement various scaling solutions and techniques, such as:

1) Layer 2 solutions: These are protocols and networks that operate on top of the main blockchain network and enable faster and cheaper transactions by offloading some of the transaction processing and data storage to off-chain channels or sidechains [64]. Examples of Layer 2 solutions include the Lightning Network for Bitcoin and the Raiden Network for Ethereum [14].

2) Sharding: This is a technique that partitions the blockchain network into smaller subsets or shards, each processing a portion of the transactions in parallel, thereby increasing the overall throughput and capacity of the network [7]. Sharding is being implemented in some blockchain platforms, such as Ethereum 2.0 and Zilliqa.

3) Consensus algorithm optimization: Blockchain-based remittance providers can also explore alternative consensus algorithms that are more scalable and efficient than the traditional Proof-of-Work (PoW) algorithm, such as Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), or Practical Byzantine Fault Tolerance (PBFT). These algorithms can help to reduce the computational resources and time required to reach consensus and validate transactions [15].

4) Off-chain transactions: Another approach to scaling blockchain remittances is to process some transactions off-chain, using private or permissioned networks that are faster and cheaper than public blockchains [64]. These off-chain transactions can be periodically settled and recorded on the main blockchain for security and auditability [14].

Implementing these scaling solutions and techniques, blockchain-based remittance providers can improve the performance and reliability of their systems, even as they grow and process more transactions. However, they should also carefully evaluate and test these solutions to ensure that they do not compromise the security, decentralization, or usability of the blockchain-based remittance system [7].

9.5. Integration with Legacy Financial Systems

Integrating the blockchain-based remittance system with legacy financial systems and infrastructure can be a significant challenge, as it requires bridging the gap between two very different and often incompatible technologies and standards. Legacy financial systems, such as banks, payment processors, and correspondent networks, rely on centralized databases, proprietary protocols, and complex regulatory frameworks that may not easily accommodate or recognize blockchain-based transactions and assets [15].

To enable seamless and secure integration with legacy financial systems, blockchain-based remittance providers should develop and adopt interoperability standards and protocols that allow different blockchain networks and traditional financial systems to communicate and exchange data and value [64]. These interoperability solutions can include:

1) Blockchain agnostic protocols: These are protocols that enable communication and transaction exchange between different blockchain networks, regardless of their underlying technologies or consensus mechanisms [14]. Examples include the Interledger Protocol (ILP) and the Cosmos Network.

2) Blockchain-to-traditional finance gateways: These are intermediaries or platforms that act as bridges between blockchain networks and traditional financial systems, enabling the conversion and transfer of funds and data between the two domains [7]. Examples include blockchain-based stablecoins, such as Tether

or USDC, that are pegged to fiat currencies and can be easily integrated with bank accounts and payment systems.

3) Regulatory sandboxes and pilot programs: Blockchain-based remittance providers can also collaborate with regulators and traditional financial institutions to establish regulatory sandboxes and pilot programs that allow for the testing and validation of blockchain remittance solutions in a controlled and supervised environment [15]. These programs can help to identify and address the technical, legal, and operational challenges of integrating blockchain remittances with legacy financial systems, as well as to build trust and partnerships between the two industries [64].

By developing and adopting these interoperability solutions and collaborative approaches, blockchain-based remittance providers can gradually overcome the integration challenges and tap into the vast network and resources of the traditional financial system while also bringing the benefits of blockchain technology to a wider audience [14]. However, this integration process will require significant investment, coordination, and compromise from both the blockchain and traditional finance communities, as well as support and guidance from regulators and policymakers.

10. Conclusions

The proposed blockchain-based remittance system offers several comparative advantages over the SWIFT system, which has long dominated the cross-border payments industry. Firstly, blockchain technology enables faster and cheaper transactions by eliminating the need for intermediaries and enabling peer-to-peer transfers, reducing the time and cost of settlement. Secondly, blockchain provides a higher level of security and transparency by using cryptographic techniques and distributed ledgers to prevent fraud and enable real-time auditing.

Blockchain enables programmable and automated transactions through smart contracts, reducing the risk of errors and disputes and enabling new use cases and business models. Finally, blockchain has the potential to promote financial inclusion and access by providing a more open and accessible infrastructure for remittances, particularly in underserved and unbanked regions.

However, it is important to note that the adoption and impact of blockchain-based remittance systems will depend on various factors, such as regulatory support, user acceptance, and technological maturity, and may vary across different countries and market segments.

While the proposed blockchain-based remittance system offers significant potential benefits, it also has several limitations and challenges that need to be addressed through further research and development. This paper recommends that:

- Future research should focus on developing and testing new scaling solutions and techniques, such as sharding, sidechains, and off-chain transactions, to improve the throughput and efficiency of blockchain-based remittance systems.

- Future research should explore the development of regulatory sandboxes, standards, and best practices for blockchain remittances, as well as the engagement and collaboration with regulators and policymakers to create an enabling environment for innovation.
- Future research should investigate the design and implementation of user-centric and context-specific solutions, such as mobile apps, agent networks, and community currencies, to facilitate the access and use of blockchain remittances by different segments of the population.

The development and adoption of blockchain-based remittance systems have significant implications for the remittance industry and the broader financial sector. Firstly, blockchain technology has the potential to disrupt the traditional remittance value chain and business models, by enabling new entrants and business models, such as digital-only providers, peer-to-peer platforms, and decentralized marketplaces, to compete with incumbent players and offer innovative and affordable services.

Secondly, blockchain-based remittances may have a positive impact on financial inclusion and development by providing access to fast, cheap, and secure payment services for underserved and unbanked populations, particularly in emerging and frontier markets. This can help to reduce the costs and risks of remittances, increase the flow of funds into local economies, and support the achievement of the United Nations' Sustainable Development Goals (SDGs).

However, the adoption of blockchain-based remittances may also pose challenges and risks for the financial sector, such as the need to adapt to new technologies and standards, the potential for disintermediation and loss of market share, and the exposure to new types of risks, such as cyber-attacks, money laundering, and consumer protection issues. Therefore, financial institutions and regulators need to proactively engage with the blockchain ecosystem and develop strategies and frameworks to harness the opportunities and mitigate the risks of this emerging technology.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] World Bank (2021) Remittance Flows Register Robust 7.3 Percent Growth in 2021. https://www.worldbank.org/en/news/press-release/2021/11/17/remittance-flows-register-robust-7-3-percent-growth-in-2021

[2] Ratha, D., De, S., Kim, E.J., Plaza, S., Seshan, G. and Yameogo, N.D. (2021) Migration and Development Brief 34. https://www.knomad.org/publication/migration-and-development-brief-34

[3] Adams, R.H. and Cuecuecha, A. (2013) The Impact of Remittances on Investment and Poverty in Ghana. *World Development*, **50**, 24-40. https://doi.org/10.1016/j.worlddev.2013.04.009

[4] Aggarwal, R., Demirgüç-Kunt, A. and Pería, M.S.M. (2011) Do Remittances Promote Financial Development? *Journal of Development Economics*, **96**, 255-264. https://doi.org/10.1016/j.jdeveco.2010.10.005

[5] De, S., Islamaj, E., Kose, M.A. and Reza Yousefi, S. (2019) Remittances over the Business Cycle: Theory and Evidence. *Economic Notes*, **48**, e12143. https://doi.org/10.1111/ecno.12143

[6] SWIFT (2021) About Us. https://www.swift.com/about-us

[7] Guo, Y. and Liang, C. (2016) Blockchain Application and Outlook in the Banking Industry. *Financial Innovation*, **2**, Article No. 24. https://doi.org/10.1186/s40854-016-0034-9

[8] Yermack, D. (2018) Blockchain in Finance, In: Durlauf, S.N. and Blume, L.E., Eds., *The New Palgrave Dictionary of Economics*, Palgrave Macmillan, 1-12.

[9] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[10] Treleaven, P., Gendal Brown, R. and Yang, D. (2017) Blockchain Technology in Finance. *Computer*, **50**, 14-17. https://doi.org/10.1109/mc.2017.3571047

[11] Scott, S.V. and Zachariadis, M. (2012) Origins and Development of SWIFT, 1973-2009. *Business History*, **54**, 462-482. https://doi.org/10.1080/00076791.2011.638502

[12] Gomber, P., Kauffman, R.J., Parker, C. and Weber, B.W. (2018) On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, **35**, 220-265. https://doi.org/10.1080/07421222.2018.1440766

[13] Bank for International Settlements (2018) Annual Economic Report 2018. https://www.bis.org/publ/arpdf/ar2018e.htm

[14] Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018) Blockchain Technology Over-View, NIST Interagency/Internal Report (NISTIR)-8202. National Institute of Standards and Technology.

[15] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 *IEEE International Congress on Big Data* (*BigData Congress*), Honolulu, 25-30 June 2017, 557-564. https://doi.org/10.1109/bigdatacongress.2017.85

[16] Ripple (2024) Cross-Border Payments: Send Cross-Border Payments in Real-Time. https://ripple.com/solutions/cross-border-payments/

[17] Stellar Development Foundation (2014) Stellar: Frequently Asked Question. https://web.archive.org/web/20210114230922/https://stellar.org/community/faq

[18] Saaty, T.L. (1990) How to Make a Decision: The Analytic Hierarchy Process. *European Journal of Operational Research*, **48**, 9-26. https://doi.org/10.1016/0377-2217(90)90057-i

[19] Koblitz, N. (1987) Elliptic Curve Cryptosystems. *Mathematics of Computation*, **48**, 203-209. https://doi.org/10.1090/s0025-5718-1987-0866109-5

[20] Pearl, J. (1988) Bayesian Inference. In: Pearl, J., Ed., *Probabilistic Reasoning in Intelligent Systems*, Elsevier, 29-75. https://doi.org/10.1016/b978-0-08-051489-5.50008-4

[21] Hosmer, D.W., Lemeshow, S. and Sturdivant, R.X. (2013) Applied Logistic Regression. Wiley. https://doi.org/10.1002/9781118548387

[22] Bellman, R. (1958) On a Routing Problem. *Quarterly of Applied Mathematics*, **16**, 87-90. https://doi.org/10.1090/qam/102435

[23] Zadeh, L.A. (1965) Fuzzy Sets. *Information and Control*, **8**, 338-353. https://doi.org/10.1016/s0019-9958(65)90241-x

[24] Bollerslev, T. (1986) Generalized Autoregressive Conditional Heteroskedasticity. *Journal of Econometrics*, **31**, 307-327. https://doi.org/10.1016/0304-4076(86)90063-1

[25] King, S. and Nadal, S. (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. https://decred.org/research/king2012.pdf

[26] Hendrikx, F., Bubendorfer, K. and Chard, R. (2015) Reputation Systems: A Survey and Taxonomy. *Journal of Parallel and Distributed Computing*, **75**, 184-197. https://doi.org/10.1016/j.jpdc.2014.08.004

[27] Liu, F.T., Ting, K.M. and Zhou, Z. (2008) Isolation Forest. 2008 *Eighth IEEE International Conference on Data Mining*, Pisa, 15-19 December 2008, 413-422. https://doi.org/10.1109/icdm.2008.17

[28] Amdahl, G.M. (1967) Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities. *Proceedings of the April* 18-20, 1967, *Spring Joint Computer Conference*, Atlantic City, 18-20 April 1967, 483-485. https://doi.org/10.1145/1465482.1465560

[29] Gustafson, J.L. (1988) Reevaluating Amdahl's Law. *Communications of the ACM*, **31**, 532-533. https://doi.org/10.1145/42411.42415

[30] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S. and Saxena, P. (2016) A Secure Sharding Protocol for Open Blockchains. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security*, Vienna, 24-28 October 2016, 17-30. https://doi.org/10.1145/2976749.2978389

[31] Hardt, D. (2012) The OAuth 2.0 Authorization Framework. https://auth0.com/docs/authenticate/protocols/oauth

[32] Fielding, R.T. (2000) Architectural Styles and the Design of Network-Based Software Architectures. University of California. https://ics.uci.edu/~fielding/pubs/dissertation/top.htm

[33] Rivest, R.L., Shamir, A. and Tauman, Y. (2001) How to Leak a Secret. *Advances in Cryptology—ASIACRYPT* 2001, Australia, 9-13 December 2001, 552-565. https://doi.org/10.1007/3-540-45682-1_32

[34] Friedman, J.H. (2001) Greedy Function Approximation: A Gradient Boosting Machine. *The Annals of Statistics*, **29**, 1189-1232. https://doi.org/10.1214/aos/1013203451

[35] Istio Authors (2021) Istio. https://istio.io/

[36] Krawczyk, H. (2010) Cryptographic Extraction and Key Derivation: The HKDF Scheme. *Advances in Cryptology—CRYPTO* 2010, Santa Barbara, 15-19 August 2010, 631-648. https://doi.org/10.1007/978-3-642-14623-7_34

[37] Buterin, V. and Griffith, V. (2017) Casper the Friendly Finality Gadget. arXiv: 1710.09437. https://arxiv.org/abs/1710.09437

[38] Boneh, D., Lynn, B. and Shacham, H. (2001) Short Signatures from the Weil Pairing. *Advances in Cryptology—ASIACRYPT* 2001, Australia, 9-13 December 2001, 514-532. https://doi.org/10.1007/3-540-45682-1_30

[39] Wood, G. (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 1-32. https://membres-ljk.imag.fr/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/Ethereum/ethereum-yellowpaper.pdf

[40] Buterin, V. (2016) EIP-150: Gas Cost Changes for IO-Heavy Operations.

https://eips.ethereum.org/EIPS/eip-150

[41] Chainlink (2021) Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. https://chain.link/whitepaper

[42] Buterin, V. (2014) Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/

[43] Chen, R., Wang, L. and Zhu, R. (2022) Improvement of Delegated Proof of Stake Consensus Mechanism Based on Vague Set and Node Impact Factor. *Entropy*, **24**, 1013. https://doi.org/10.3390/e24081013

[44] Ben-Sasson, E., Chiesa, A., Tromer, E., and Virza, M. (2014) Succinct Non-Interactive Zero Knowledge for a Von Neumann Architecture. *Proceedings of the* 23*rd USENIX Conference on Security Symposium*, San Diego, 20-22 August 2014, 781-796.

[45] OpenZeppelin (2017) Proxy Upgrade Patterns. https://docs.openzeppelin.com/upgrades-plugins/1.x/proxies

[46] Newman, S. (2015) Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, Inc.

[47] McKinsey & Company (2018) Global Payments 2018: A Dynamic Industry Continues to Break New Ground. https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/global%20payments%20expansive%20growth%20targeted%20opportunities/global-payments-map-2018.ashx

[48] Ripple (2016) Ripple and XRP Can Cut Banks' Global Settlement Costs up to 60 Percent. https://ripple.com/insights/ripple-and-xrp-can-cut-banks-global-settlement-costs-up-to-60-percent/

[49] Stellar Development Foundation (2021) Stellar Network Overview. https://stellar.org/learn/intro-to-stellar

[50] Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. and Rehmani, M.H. (2019) Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, **21**, 1676-1717. https://doi.org/10.1109/comst.2018.2886932

[51] Santander (2018) Santander Launches the First Blockchain-Based International Money Transfer Service across Four Countries. https://www.santander.co.uk/about-santander/media-centre/press-releases/santander-launches-the-first-blockchain-based-international-money-transfer-service-across-four

[52] Reuters (2018) Special Report: Inside the Bangladesh Bank Cyber Heist.

[53] Deloitte (2021) Deloitte's 2021 Global Blockchain Survey. https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf

[54] Australian Securities Exchange (2021) CHESS Replacement. https://www2.asx.com.au/markets/clearing-and-settlement-services/chess-replacement

[55] PYMNTS (2020) 64 Pct of Businesses Cite Payment Traceability as Cross-Border Pain Point.

[56] IBM (2019) IBM Blockchain World Wire. https://www.ibm.com/blockchain/solutions/world-wire

[57] SWIFT (2022) SWIFT FIN Traffic & Figures. https://www.swift.com/about-us/swift-fin-traffic-figures

[58] Zamani, M., Movahedi, M. and Raykova, M. (2018) RapidChain: Scaling Blockchain via Full Sharding. *Proceedings of the* 2018 *ACM SIGSAC Conference on Computer and Communications Security*, Toronto, 15-19 October 2018, 931-948. https://doi.org/10.1145/3243734.3243853

[59] Bitcoin (2022) Bitcoin Transaction Rate. https://www.blochain.com/charts/transactions-per-second

[60] Ethereum (2022) Ethereum Transaction Rate. https://etherscan.io/chart/tx

[61] Bank for International Settlements (2020) Central Bank Digital Currencies: Foundational Principles and Core Features. https://www.bis.org/publ/othp33.pdf

[62] Thomas, S. and Schwartz, E. (2019) A Protocol for Interledger Payments. https://interledger.org/interledger.pdf

[63] Digiconomist (2022) Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption

[64] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., *et al*. (2017) A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 *IEEE International Conference on Software Architecture* (*ICSA*), Gothenburg, 3-7 April 2017, 243-252. https://doi.org/10.1109/icsa.2017.33

[65] Arner, D.W., Buckley, R.P., Zetzsche, D.A. and Veidt, R. (2020) Sustainability, Fintech and Financial Inclusion. *European Business Organization Law Review*, **21**, 7-35. https://doi.org/10.1007/s40804-020-00183-y

[66] Garaus, M. and Treiblmaier, H. (2021) The Influence of Blockchain-Based Food Traceability on Retailer Choice: The Mediating Role of Trust. *Food Control*, **129**, Article 108082. https://doi.org/10.1016/j.foodcont.2021.108082

[67] Bass, F.M. (1969) A New Product Growth for Model Consumer Durables. *Management Science*, **15**, 215-227. https://doi.org/10.1287/mnsc.15.5.215