future internet

MDPI

Article

CrossDeFi: A Novel Cross-Chain Communication Protocol

Shezon Saleem Mohammed Abdul *, Anup Shrestha and Jianming Yong

School of Business, University of Southern Queensland, Toowoomba, QLD 4350, Australia; anup.shrestha@usq.edu.au (A.S.); jianming.yong@unisq.edu.au (J.Y.)
* Correspondence: shezonsaleem.mohammedabdul@unisq.edu.au or shezonsaleem@protonmail.com

Abstract: Decentralized finance (DeFi) is rapidly evolving, promising to revolutionize financial services through blockchain technology. Successful integration of asset transfers across diverse DeFi platforms hinges on effective interoperability and transaction finality, ensuring security and cost efficiency. This paper introduces CrossDeFi, a novel cross-chain communication protocol tailored to address the challenges posed by heterogeneity in consensus mechanisms, smart contracts, and token systems. CrossDeFi introduces two key mechanisms: Miner and bridge selection (MBS) and improved transfer confirmation (ITC). The MBS mechanism optimizes the selection of miners and bridges based on the unique characteristics of each blockchain, significantly improving transfer accuracy, cost efficiency, and speed. Meanwhile, the ITC mechanism leverages cryptographic primitives to secure asset transfer confirmations, ensuring robust transaction finality. The protocol's effectiveness is demonstrated through detailed efficiency and security analyses, complemented by a prototype evaluation that showcases its capabilities in reducing transfer durations and costs. These findings underscore the potential of CrossDeFi to transform the DeFi ecosystem.

Keywords: DeFi (decentralized finance); cross-chain asset transfer; blockchain interoperability; finality guarantee in the blockchain; smart contract security; CrossDeFi protocol

Citation: Mohammed Abdul, S.S.; Shrestha, A.; Yong, J. CrossDeFi: A Novel Cross-Chain Communication Protocol. *Future Internet* **2024**, *16*, 314. https://doi.org/10.3390/fi16090314

Received: 3 July 2024
Revised: 12 August 2024
Accepted: 26 August 2024
Published: 29 August 2024

1. Introduction

Blockchain technology serves as a decentralized infrastructure, functioning as a distributed digital ledger that aggregates cryptographically signed transactions into blocks [1]. Often termed distributed ledger technology (DLT), it ensures transparency and security in managing digital assets through decentralization and encryption [2]. This technology enables secure peer-to-peer transactions without intermediaries [3]. Key features such as decentralization, immutability, transparency, and auditability enhance the security and tamper-resistance of transactions [4].

Smart contracts, which are scripts stored on the blockchain and automatically enforced based on predefined terms, facilitate decentralized verification and real-time access for all users within the blockchain network [5]. These contracts have elevated the blockchain from a mere ledger to a comprehensive computing platform capable of automating relationships between stakeholders through encoded logic and behavior [6]. The immutable nature of blockchains ensures that once transactions are recorded, they cannot be altered [7]. Recent advancements in blockchain technology, particularly through smart contracts, have enabled decentralized mechanisms for fulfilling contracts across various markets [8].

The financial sector, an early adopter of blockchain technology, has showcased its potential to revolutionize traditional financial systems that often suffer from inefficiencies, high costs, and delays due to intermediaries [9]. Blockchain technology has transformed financial processes, introducing new possibilities and enhancing trust and security by reducing reliance on third-party verification through consensus-based methods [10]. Additionally, the blockchain has significantly improved transparency, security, and cost-effectiveness in the financial sector [11]. By leveraging characteristics like decentralization, immutability, and transparency, financial institutions can streamline their operations, reduce costs,

and maintain transaction integrity [12]. Applications of the blockchain in cross-border payments, supply chain finance, equity financing, securities issuance, and insurance have demonstrated its versatility and effectiveness in various financial contexts [12].

In the banking industry, blockchain technology promises to transform everyday processes by making them more transparent, secure, and efficient [13]. Commercial banks are actively exploring and implementing blockchain to improve their centralized systems and enhance overall operations [14]. Blockchain-based securities trading exemplifies how the technology can foster trust and eliminate the need for third-party verification through consensus mechanisms [15]. Utilizing the blockchain, financial institutions can ensure the integrity of sustainable financial practices and promote trust among stakeholders. The immutable and traceable nature of blockchain data enhances the reliability and trustworthiness of financial processes [16].

Building on these advancements, decentralized finance (DeFi) has emerged as a groundbreaking development within blockchain technology, offering unprecedented access to financial services like lending, borrowing, and trading without traditional intermediaries [17,18]. DeFi creates a unified ecosystem where multiple protocols interact seamlessly on a blockchain infrastructure. However, the independence of different blockchain systems can undermine the core principle of decentralization and pose challenges to widespread adoption across various industries [19].

Despite continuous innovation, the DeFi ecosystem faces significant challenges, particularly with interoperability and transaction finality across diverse blockchain networks. Interoperability requires seamless interactions across different blockchains, enabling smooth data and asset transfers without third-party involvement [20,21]. Achieving interoperability within the DeFi ecosystem involves overcoming challenges related to diverse protocols and standards, security, scalability in cross-chain communications, legal compliance across jurisdictions, and the inherent complexity of the task. The primary challenge in DeFi is ensuring the mobility of digital assets without them being locked in a particular network for too long. Introducing a cross-chain DeFi communication protocol effectively addresses these issues, facilitating broader adoption and enhancing the effectiveness of cross-chain transactions [22]. Ensuring transaction finality is also crucial as it guarantees that transactions are irreversible, mitigating the risk of double-spending and ensuring immutable transaction records [23].

However, traditional cross-chain strategies often fail to provide high interoperability with multiple types of assets and a reliable finality guarantee simultaneously. They also suffer from high transaction fees, long confirmation times, and security vulnerabilities, which hinder seamless cross-chain transactions [24]. For instance, the Metronome cross-chain solution introduces new attack vectors due to the complexity of its bridging mechanism [25]. Notably, the gas fees of decentralized liquidity protocols such as Kybernetwork [26] and BTC relay [27] are expensive during peak times, deterring DeFi users from executing trades. While these cross-chain solutions are innovative and enable cross-chain interoperability, they introduce novel security concerns and high operational costs, making them impractical for real-time DeFi deployments. Moreover, they lack support for multi-asset transactions. Typically, existing protocols use different cross-chain components, such as bridges, oracles, and wrapped tokens, to facilitate interactions across different blockchains. Bridges have become adaptable within DeFi systems due to their role in asset interoperability [28]. Each DeFi system may use different bridges to transfer various assets, making it crucial to select asset-specific bridges to optimize transfer speed and security [29]. Additionally, there is no effective cross-chain solution to handle asset diversity in transfer and ensure transaction finality within a heterogeneous DeFi system.

Conventional cross-blockchain asset transfer solutions are customized and have notable design limitations, such as lacking multi-asset transfer support and faster transaction finalities, leading to real-time interoperability constraints and double-spending risks [25–27]. These limitations motivate the proposal of novel cross-chain solutions like CrossDeFi, which features asset-specific bridge selection and improved transfer confirma-

tions to provide rapid multi-asset transfer support with minimal cost and protection against double-spending in a heterogeneous DeFi environment. Given these challenges, there is an urgent need for a new cross-chain protocol specifically designed to meet the needs of the DeFi ecosystem in terms of interoperability over diversified assets and transaction finality guarantees while addressing security, speed, and cost issues. Thus, this paper proposes CrossDeFi, a novel DeFi cross-chain protocol aimed at enhancing interoperability and ensuring the finality of asset transfers while maintaining the essential features of the DeFi system.

1.1. Research Questions

The following research questions are formulated to explore the objectives of CrossDeFi:

- What are the shortcomings in the existing cross-chain approaches that motivate the proposed CrossDeFi system?
- What are the key components of CrossDeFi to improve interoperability and transaction finality under heterogeneous DeFi systems?
- How is the security analysis and experimental evaluation carried out to show the superiority of CrossDeFi?

1.2. Contributions

The primary contributions of the proposed model are as follows:

- Enhanced interoperability and transaction finality: CrossDeFi introduces significant advancements in DeFi systems' interoperability and transaction finality by integrating innovative mechanisms such as miner and bridge selection (MBS) and improved transfer confirmation (ITC).
- Miner and bridge selection (MBS): MBS enhances the selection process for miners and bridges, focusing on optimization for each specific DeFi system. This mechanism significantly reduces transaction costs and increases the speed of asset transfers.
- Improved transfer confirmation (ITC): ITC addresses the issue of asset lock-up in DeFi systems by implementing a secure and efficient asset transfer confirmation model, which guarantees the finality of transactions.
- Empirical validation: The effectiveness of CrossDeFi is demonstrated through comprehensive validation, showing improvements in heterogeneous asset transfer accuracy and transfer speeds. These results underscore the practical benefits of CrossDeFi, positioning it as a valuable addition to the field.

1.3. Paper Organization

The remainder of the paper is organized as follows. Section 2 reviews the works related to CrossDeFi, providing a background context for our contributions. Section 3 provides the necessary background information to understand the DeFi cross-chain solutions we explore. Section 4 covers the preliminaries and formulates the problems with the system and attack models for the proposed CrossDeFi. Section 5 describes the design overview of CrossDeFi, including its mechanisms. Section 6 discusses the performance efficiency and security analysis of CrossDeFi. Section 7 illustrates the practical use case of CrossDefi. Section 8 shows a prototype-based evaluation of CrossDeFi, demonstrating its evaluation results. Finally, Section 9 concludes the paper, summarizing the research and highlighting its implications.

2. Literature Survey

Cross-chain technology enables the exchange of data and assets between two relatively independent blockchain ledgers, enhancing broader interoperability within the blockchain ecosystem [30,31]. This survey categorizes the existing solutions into two main areas: those enhancing cross-chain interoperability and those ensuring transaction finality in cross-chain exchanges.

2.1. Cross-Chain Interoperability Solutions

The realm of cross-chain interoperability has various projects addressing the limitations inherent in blockchain technologies. The Metronome project [25] offers a solution limited to blockchains that support smart contracts, excluding those without this capability, and does not tackle issues related to transfer finality and confirmation. Conversely, KyberNetwork [26] provides instant trading and redemption services for digital assets on Ethereum blockchains. Further extending this concept, another project [27] leverages BTCRelay technology to facilitate cross-chain confirmations but lacks support for multi-currency transactions. Wanchain [32] is a pioneering project in blockchain cross-chain technology using intermediate chains to facilitate transactions.

Recent advancements include a blockchain scaling solution [33] focusing on computational scalability. A multi-public chain cross-chain project [34] introduces a distance-based consensus eliminating the verifier role to achieve true power decentralization. The Plasma blockchain scaling model [35] aims to regulate blockchain entities through designated rewards and penalties. Peer-to-peer heterogeneous cross-chain mechanisms are explored [36], employing the oracle machine concept to improve interoperability. BrokerFi [37] represents a significant advancement by designing a decentralized application (dApp) that enables users to manage their digital assets effectively and monetize their participation within the BrokerFi ecosystem.

Platforms like BitXHub [38], the cross-chain technology platform of Hyperchain, and WeCross [39], the cross-chain platform of WeBank, have been open-sourced, significantly advancing the development of China's domestic, independent cross-chain technology platforms. These platforms focus on interoperability of ledgers between heterogeneous consortium chains and tackle key issues in transaction capture, transmission, and verification [40]. BitXHub has achieved autonomy in consortium cross-chain interactions and supports services like unified identity management, permission control for cross-chain activities, node management, and information auditing.

In [41], the introduction of the first cross-chain Polkadot bridge enabled EVM smart contracts on Polkadot, allowing developers from Ethereum, Wanchain, and other blockchains to integrate DOT into their applications using Wanchain's decentralized blockchain interoperability solution. Moreover, Interlay launched the wrapped Bitcoin token, InterBTC (iBTC), on the Polkadot network, providing users the option to keep BTC in their Polkadot wallet [22]. The MyWish platform [42] facilitates the construction of smart contracts on the blockchain without requiring written code, supporting various blockchains like Ethereum [43] and Binance [44], and fostering high interest among users in learning about token transfers through the Wish Swap cross-chain token exchange.

However, some solutions like Cosmos [45] and wrapped bitcoin on Ethereum [46] still face challenges in providing effective bridging solutions. The work in [47] discusses multiple standards for cross-chain communication but lacks a discussion on interoperability standards compatible with different types of tokens. Additionally, a notary group-based cross-chain mechanism in [48] achieves improved interoperability across different blockchains through effective notary selection. Another approach [49] uses sidechains for fast cross-chain transfers across multiple chains but faces performance challenges as the number of chains increases.

2.2. Finality Guarantee in Cross-Chain Solutions

This segment reviews various protocols developed to ensure transaction finality in cross-chain operations, crucial for preventing issues like double-spending. The work in [50] introduces an atomic swap cross-chain protocol that relies on a hashed timelock mechanism, a foundational approach for secure asset transfers. Extending this concept, a hash-locking-based multi-party protocol in [51] aims to refine asset transfer and user settlement across blockchains, through enhanced atomic swaps.

InterTrust [52] offers an interoperable blockchain architecture that not only promises interoperability but also instills trustworthiness between diverse blockchains. It integrates

with conventional blockchains through an atomic cross-chain communication strategy known as the agnostic protocol, aimed at broad adoption. A new consensus model, multi-tokens proof-of-stake (MPoS) introduced in [53] attempts to fortify the role of token networks in cross-chain environments and significantly boost user engagement on blockchain networks. CrossLedger [54] proposes a strategy to allow more precise asset transfers across multiple blockchains, focusing on security against threats such as double-spending, liveness, and Sybil attacks. XCC [55], an extension of XCLAIM [56], reduces required collateral through periodic and time-locked commitments, allowing fractional collateralization while maintaining security. However, this approach struggles with slow transaction speeds and higher costs due to ineffective bridge strategy considerations.

Further, the work in [57] proposes a main-sub-chain architecture to enhance cross-chain protocols. A cross-chain pathfinding solution in [58] develops a structure utilizing various bridge types to streamline asset transfers. In contrast, a protocol in [59] that allows asset reusability across blockchains suffers from failure in ensuring transaction finality, leading to potential double-spending. Other innovative approaches include a proof-of-burn protocol [60], which, despite its novelty, does not address decentralized finality and transfer confirmations—key for DeFi systems. The work in [61] proposes a burn-to-claim asset transfer protocol. An AucSwap has been introduced in [62] in which an auction process is defined through a cross-blockchain token transfer protocol. Particularly, it enables asset transfer across multiple blockchains by leveraging the Vickery auction process and atomic swap technology. However, it cannot accomplish more interoperability in financial applications.

The works [63,64] introduced strategies to realize the cross-blockchain transfers among the blockchain consensus effectively. Similarly, the work in [65] verifies transaction inclusions through blockchain consensus. A notable approach in [66] employs zero-knowledge proofs for transaction verification, though its reliance on a specialized sidechain strategy raises practical implementation challenges. Despite these advancements, decentralized asset transfer mechanisms [67] still struggle with ensuring finality, an issue somewhat addressed by a new transfer confirmation model in [68], which integrates oracles to bolster transaction security, albeit at a cost. Terra once aimed to revolutionize cross-chain interoperability with its UST stablecoin, providing stable and scalable financial operations. Despite its ambitious goals, the platform faced significant challenges, leading to its collapse, as noted in [69]. Further, the transition from Bitcoin to more scalable solutions like Solana highlights innovations in blockchain architectures that significantly enhance performance for enterprise applications, as detailed in [70]. Lastly, the study in [71] offers an in-depth analysis of the Avalanche consensus protocol, which improves upon traditional consensus mechanisms by utilizing randomized processes to ensure robust and efficient cross-chain transactions.

To the best of our knowledge, the proposed work formally defines requirements, a specification, and an asset-specific bridge selection model of a cross-blockchain asset transfer protocol that takes interoperability and transfer confirmations into account with highly secure cryptography solutions under a heterogeneous DeFi system. By selecting asset-specific bridges from the bridge hub, the cross-DeFi supports a variety of asset transfers with high speed and accuracy. Unlike conventional methods that rely on external cryptography solutions, the proposed protocol does not necessitate external solutions. Moreover, it carefully integrates the cryptography solution within the interoperability layer of the blockchain by precisely analyzing its features and adaptability. Table 1 presents a comparative analysis of various cross-chain solutions based on several key parameters critical to blockchain technology's effectiveness and practical applications. These parameters include interoperability, compatibility with different blockchain technologies, scalability, the necessity of asset-locking during transactions, the ability for direct asset transfers across chains, the use of bridging or oracle solutions, overall transfer performance, guarantee of transaction finality, the complexity of the technology, and the cost of implementation.

This comparison highlights the diverse approaches and varying degrees of success these solutions have in addressing the fundamental challenges of cross-chain operations.

Table 1. Comparison of existing cross-chain works.

Cross-Chain-Solutions	Interoperability	Compatibility	Scalability	Asset Locking	Asset Transfer	Bridging Solutions	Performance	Finality	Complexity	Cost
Hash-locking	No	No	No	Yes	No	No	Low	No	High	High
Ethereum	Yes	No	No	Yes	Yes	Yes	Medium	No	Medium	High
Binance-Smart Chain	Yes	No	No	Yes	Yes	Yes	Medium	No	High	High
Polkadot	Yes	No	No	Yes	Yes	Yes	Medium	No	Low	High
Cosmos	Yes	No	No	Yes	Yes	Yes	Low	No	High	High
AucSwap	Yes	No	No	No	Yes	Yes	Medium	No	Medium	High
Zendoo	Yes	No	No	Yes	Yes	No	Medium	No	Low	High
Terra	Yes	No	No	Yes	Yes	Yes	Medium	No	High	High
Solana	Yes	No	No	Yes	Yes	Yes	Low	No	Low	High
Avalanche	Yes	No	No	Yes	Yes	Yes	Low	No	High	High
Wrapped Bitcoin on Ethereum	Yes	No	No	Yes	Yes	No	Low	No	High	High
Multi-token standards	Yes	No	No	Yes	Yes	Yes	Medium	No	High	High
Notary mechanism	Yes	No	No	Yes	Yes	No	Medium	No	Low	High
Sidechain or relay	Yes	No	No	Yes	Yes	No	Low	No	Medium	Medium
Asset transfer protocol	Yes	No	No	Yes	Yes	Yes	Medium	Yes	High	Medium

The existing cross-blockchain transfer strategies allow participants to interact among similar types of blockchains or focus on the same type of asset transfer. However, in real-time, a cross-chain protocol should be designed to permit the users to fully exploit the conventional variety of blockchains that are diverse in assets through interactions instead of allowing a single blockchain. The cross-blockchain asset transfer in CrossDeFi solves such issues and will serve as a cornerstone for the next-generation DeFi networks. Currently, a lot of cross-blockchain asset transfer solutions exist with notable limitations. They might be either tailored for specific asset transfers or lacking in providing guarantees of finality, leading to asset loss during the transfer process. Utilizing external third-party security services is the preferred solution to ensure transfer confirmation [50]. However, it is not feasible for practical DeFi scenarios. Therefore, CrossDeFi carefully designs an internal security that is incorporated with the core blockchain to carry out interoperable asset transfer transactions among various DeFi systems. The inevitable growth of diversified blockchain-enabled DeFi platforms necessitates a universal mechanism like crossDeFi for seamless asset transfer. Therefore, CrossDeFi introduces an asset-specific bridge selection model that permits any DeFi assets to be transferred among various DeFi systems.

3. Background

This section provides background information on different cross-chain solutions and components, focusing on how they support various types of tokens and assets within the DeFi ecosystem.

3.1. Cross-Chain Solutions

As the variety of blockchain assets in the DeFi system expands, numerous cross-chain networks continue to emerge. Notably, Polkadot and Cosmos are widely utilized for their robust capabilities; however, they both face challenges with transaction costs and speed, which are significant concerns for DeFi applications.

Cosmos: This platform constructs the "Internet of Blockchains", enabling diverse blockchains to share data and interact seamlessly to achieve interoperability [45]. In Cosmos, each blockchain operates independently—akin to its own universe—minimally connecting globally without cross-chain bridges. This setup reduces the need for networks to compete intensely, allowing multiple blockchains with unique characteristics and specialized use cases to coexist. Cosmos employs the Tendermint consensus protocol, which is notable for immediate transaction finality—once transactions are included in a block, they cannot

be reversed. Despite these advantages, Cosmos struggles with high transaction costs and slower speeds, impacting its effectiveness in the DeFi landscape.

Polkadot: A third-generation blockchain technology, Polkadot focuses on interoperability and scalability [41]. It facilitates seamless interoperability through a network of self-governing blockchains, known as parachains. The core of Polkadot's architecture is the relay chain, which handles transaction validation and security across all parachains, ensuring a high level of security and consistency. Polkadot also allows developers to create application-specific blockchains as parachains tailored to their specific needs. However, it does not adequately address asset-locking issues crucial for DeFi-enabled solutions.

Table 2 compares the proposed CrossDeFi solution with existing solutions from Cosmos and Polkadot across various factors like consensus type, core model, interoperability level, scalability, and more. This comparison highlights the specific areas where CrossDeFi aims to improve upon the foundations laid by Polkadot and Cosmos, particularly focusing on interoperability, finality guarantee, and optimized transaction costs and speeds within the DeFi sector.

Table 2. Comparison of Polkadot, Cosmos, and proposed CrossDeFi.

Comparison Factors	**Polkadot**	**Cosmos**	**Proposed CrossDeFi**
Consensus type	Nominated proof-of-stake (NPoS)	Tendermint (BFT)	Varies based on DeFi system
Core model	Relay chain	Bridge-hub model	Cross-chain strategy
Interoperability level	Parachains-based	IBC-based	High among disparate DeFi blockchains
Native token type	DOT	ATOM	Specific to each DeFi
Scalability	Medium (sharding, parachains)	Medium (zones, hubs)	High
Development language	Substrate (rust-based)	Cosmos SDK (golang-based)	Varies
Ecosystem	Expanding with various projects	Growing with different projects	Depends on DeFi adoption
Support for smart contract	Yes (via parachains)	Yes (via Cosmos SDK)	Varies
Security type	Shared security	Tendermint consensus security	Specific to consensus type
Cross-chain transactions	Bridges, parachains	IBC	DeFi asset-specific bridges
Governance strategy	Polkadot council, referenda	On-chain governance, validators	Varies
Upgradability	Supported	Supported	Supported
DeFi support	Scalability, interoperability	Interoperability, finality guarantee	Asset-specific interoperability
Transaction fees	High	High	Medium
Speed	Medium	Medium	High
Finality guarantee	Supported	Supported	Supported
Asset-locking	Yes	Yes	No

It is evident that existing solutions, such as Cosmos and Polkadot, primarily focus on interoperability and scalability. In contrast, the proposed CrossDeFi is specifically designed to enhance interoperability among heterogeneous DeFi platforms and ensure transaction finality within the DeFi ecosystem. An asset-specific bridge selection mechanism is integrated, which includes various characteristics related to DeFi assets and heterogeneous blockchain characteristics for seamless interoperability. This mechanism focuses on critical aspects of DeFi operations and positions CrossDeFi as a potentially transformative solution in the evolving landscape of DeFi.

3.2. Cross-Chain Components

This subsection examines the integral components of cross-chain networks—bridges, decentralized exchanges (DEXs), aggregators, wrapped tokens, and oracles. Each component plays a distinct role in enhancing the functionality and efficiency of decentralized networks. Table 3 demonstrates these roles by comparing the components across various

factors, such as their primary focus, working principles, level of centralization, interoperability, security dependence, and specific use cases within the DeFi ecosystem.

Bridges serve as critical infrastructure in cross-chain networks, facilitating the seamless transfer of assets between different blockchains while ensuring transaction finality and enhancing security. They are particularly vital in supporting the high-speed, accurate transfer of assets across heterogeneous blockchain platforms, making them indispensable for comprehensive DeFi solutions like CrossDeFi. Decentralized exchanges (DEXs) enable the trading of assets across different chains without the need for a central authority, thus supporting liquidity and lowering the risk of censorship. Aggregators play a role in optimizing transactions by pooling resources and routes across various DEXs to ensure users obtain the best possible trade executions. Wrapped tokens represent assets from one blockchain or another, allowing for the incorporation of diverse asset types into a single DeFi ecosystem without compromising the assets' native properties. Oracles bridge the gap between real-world data and blockchain networks, enabling smart contracts to execute based on inputs from outside their native chains.

Table 3. Comparative analysis of various cross-chain components.

Factors	Bridges	DEXs	Aggregators	Wrapped Tokens	Oracles
Primary focus	Facilitate cross-chain asset transfers	Enable peer-to-peer digital asset trading	Aggregate liquidity from various sources	Represent assets seamlessly across blockchains	Provide external data for smart contracts
Working principle	Transfer assets across blockchains	Match buyers and sellers for trading	Optimize trade actions by pooling liquidity	Lock native tokens and issue equivalents on target chains	Fetch and validate real-world information
Centralization	Centralized or decentralized	Decentralized	-	Centralized or decentralized	Centralized or decentralized
Interoperability	Support	Support	Support	Support	Support
Security dependence	Bridge design	Consensus and smart contracts	Secure data aggregation and trading algorithms	Decentralized collateralization	Reputation or collateralization
Tokens	Custom and bridge-specific	ERC-20, BEP-20, SPL, etc.	-	ERC-20, BEP-20, etc.	-
Examples	Interledger, Cosmos IBC, Polkadot bridges	Uniswap, SushiSwap, PancakeSwap	1inch, Paraswap, Matcha	Wrapped Ether (WETH), Wrapped Bitcoin (WBTC)	Chainlink, Band Protocol, API3
Use cases	Cross-chain asset transfers, interoperable DeFi applications	Decentralized trading, liquidity provision	Optimized trading, best price execution	Asset representation, cross-chain liquidity	Supplying data to smart contracts

Each of these components, particularly bridges, contributes uniquely to achieving interoperability among heterogeneous blockchain networks. By leveraging the capabilities of bridges, CrossDeFi can overcome current limitations associated with traditional DeFi components, thereby unlocking new opportunities for cost efficiency, speed, and broad adoption across diverse blockchain-enabled DeFi systems.

3.3. Seamless Token Representation (STR)

The CrossDeFi system is designed to provide a seamless asset representation model, enhancing the uniformity of assets across various blockchain architectures used by the DeFi system. This model uses a sophisticated tokenization platform that allows for interaction between different DeFi user groups and intermediaries, such as agents, thereby facilitating beneficial exchanges. This service not only promotes the liquidity of previously illiquid assets but also implements a trust structure based on code, rather than relying solely on intermediaries.

Tokenization within CrossDeFi helps bridge the gap between tangible and intangible assets, making both more accessible and manageable within the DeFi ecosystem. By

employing digital tokens as references to physical counterparts, CrossDeFi enhances the liquidity and speculative value of tangible assets. For intangible assets, the model provides unique representation capabilities through smart contracts, which ensure security and verifiability. Verification processes such as Know Your Customer (KYC) and Anti-Money Laundering (AML) are integral to maintaining high standards of trust and compliance in the CrossDeFi system, addressing potential concerns from users and regulatory bodies.

The functionality of STR is underpinned by a variety of token types, each serving specific roles within the DeFi ecosystem:

- Security tokens like 10SET ERC 20 represent ownership and participation rights but often suffer from high transaction fees and scalability issues.
- Utility tokens such as ETH facilitate access to services and products but face regulatory uncertainties.
- Non-fungible tokens (NFTs) like CryptoKitties provide unique asset representations but may experience excessive transaction fees and interoperability challenges.
- Governance tokens such as BAL enable participation in blockchain governance but are often limited by the scalability of their native platforms.
- Payment tokens like BTC are used for transactions but can be volatile and have high fees.
- Wrapped tokens such as WETH allow for the use of one blockchain's assets on another platform but involve risks related to centralization.
- Stablecoins like USDC aim to maintain stable values pegged to real-world assets but may face issues related to centralization and regulatory oversight.

To illustrate the variety and functionalities of different token types utilized within DeFi platforms, Table 4 provides a comparative analysis based on their primary functions, supported assets, and inherent drawbacks. This comparison highlights the diverse applications and challenges associated with each token type, offering insights into their suitability for various DeFi applications.

Table 4. Understanding of different tokens with their characteristics.

Tokens	Token Type	DeFi Asset Support	Function	Drawbacks
10SET, ERC-20, Polymath, tZero, Harbor, BCAP	Security	Tokenize assets	Ownership, participation	High fees, scalability issues
ETH, DOT, GAS, EOS	Utility	Product/services	Access protocol services	Regulatory risks
CryptoKitties, Crypto-Punks	Non-Fungible	Unique assets	Unique representation	Excessive fees, poor scalability
BAL, COMP, AAVE, CRV	Governance	Participation rights	Fuel blockchain-based voting	Limited support, scalability issues
BTC, LTC, DASH, BCH	Payments	Financial assets	Medium of exchange	Volatility, high fees
WETH, WCK, RENZEC, WMATIC	Wrapped	Cryptocurrencies	Use across blockchains	Centralization risks
USDC, TUSD, BUSD, PAX	Stablecoins	Real-world assets	Asset pegging	Centralization, regulatory concern

In DeFi, tokens are fundamental building blocks as they represent diverse assets, rights, and utilities. Analyzing various token characteristics is essential to understand their functionalities, roles, and potential risks. This analysis becomes particularly important for CrossDeFi to understand token characteristics for accomplishing seamless interoperability, ensuring finality guarantee, and optimizing asset transfer performance. Through this token characteristics analysis, CrossDeFi successfully implements asset-specific bridge selection for cross-chain interoperability and can design more efficient, robust, and secure cross-DeFi asset transfers that cater to a wide range of use cases.

4. Preliminaries

This section defines the problem handled by the proposed CrossDeFi and describes the system and attack model.

4.1. Problem Formulation

Current solutions proposed for cross-chain interoperability and finality guarantees fall short in several key areas. Primarily, existing systems struggle to handle the diversity across consensus mechanisms, token types, assets, and components effectively. There is no adaptive solution for a variety of asset transfers, resulting in poor interoperability, especially among DeFi systems with various blockchains. Moreover, many conventional cross-chain solutions rely heavily on Oracle components for asset transfers across multiple blockchains, which incurs substantial fees and implementation costs, rendering them impractical for real-time DeFi systems. To address such issues, this framework proposes a Cross DeFi, which dynamically adapts to the characteristics of different assets and blockchain platforms, ensuring seamless and secure asset transfers.

Another significant challenge is asset locking, where assets are frequently locked for extended periods on various DeFi blockchains without definitive transaction finality, posing a major issue in many existing cross-chain systems. Developing innovative asset-locking solutions is crucial to enable seamless communication and interoperability among diverse DeFi platforms. However, creating effective asset-locking solutions across different cross-chain DeFi systems is inherently complex. Delays or failures in cross-chain transactions can severely impact user experience and the overall effectiveness of DeFi services. Therefore, there is a pressing need for novel cross-chain solutions that support both interoperability and finality guarantees without compromising on speed, cost, or security across heterogeneous DeFi systems. The CrossDeFi communication protocol is designed to address these challenges, taking into account the complexities of heterogeneous blockchains and asset-locking issues.

To formulate the cross-chain asset transfer among two DeFi systems, consider the scenario where DeFi X and DeFi Y represent two different DeFi networks having assets A_X and A_Y. The problem formulation has to consider several unique blockchain characteristics, including asset pools (AP), miners (Mi), smart contracts (Smr), consensus (Con), and bridges (Bri), as defined in Table 5. Firstly, it is crucial to consider the transaction participants for DeFi X and DeFi Y: let BMi_X and BMi_Y represent the best miners selected from the mining pools of X and Y, respectively, who are responsible for facilitating the transaction process across these networks through the asset-specific bridge.

Table 5. Transaction Participants for DeFi X and DeFi Y.

Transaction Participants	DeFi X	DeFi Y
Asset pools	AP_X	AP_Y
Assets	A_X	A_Y
Initial assets	A_X^{initial}	A_Y^{initial}
Asset type	AT_X	AT_Y
Miners	Mi_X	Mi_Y
Smart contracts	Smr_X	Smr_Y
Consensus protocols	Con_X	Con_Y
Best miner from Mi to facilitate the transfer process	BMi_X	BMi_Y
Bridges	Bri_X	Bri_Y

Definition: For formulating the transaction process, it is considered that DeFi X wants to transfer A_X to DeFi Y by using the selected bridge according to AT_X, (Smr_X, Smr_Y) and (Con_X, Con_Y) of DeFi X and DeFi Y.

Asset transfer formulation: It is stated that the smart contracts, consensus, and bridges used by DeFi X and DeFi Y are $\{Smr_X, Con_X, Bri_X\}$ and $\{Smr_Y, Con_Y, Bri_Y\}$, respectively. Initially, DeFi X and DeFi Y have initial assets, referred to as A_X^{initial} and A_Y^{initial}. A miner of DeFi X, MiX, initiates the asset transfer process by analyzing the real-time asset type AT_X, asset value to be transferred, blockchain type, and transaction fees. This analysis determines the current state of the transaction process and ensures that all necessary

conditions and parameters are met before proceeding with the asset transfer. Select the optimal and suitable bridge (Bri_{suit}) for asset transfer using the following equation:

$$Bri_{\text{suit}} = \arg\max_{Bri}\{\text{Suit}(Bri, \text{current state})\} \quad (1)$$

Best miner BMi_X locks the asset $\Delta A_X^{\text{Initial}}$ in the AP_X as follows.

$$AP_X^{\text{locked}} = AP_X^{\text{Initial}} - \Delta A_X^{\text{Initial}} \quad (2)$$

Consequently, Smr_X generates the proof for the locked asset at AP_X. Select the bridge using Equation (1) by sending the proof X to DeFi Y, and the miner BMi_Y verifies whether the received information is true or not. If it is true, the locked asset valued at X is credited in the AP_Y at DeFi Y.

$$Ass(T_{X\to Y}) = \text{Bridge}(\text{DeFi } X, \text{DeFi } Y) \quad (3)$$

This formulation indicates that the selection of miners and bridges is critical in determining the level of interoperability performance and finality guarantee. The asset transfer process is defined as:

$$AP_Y^{\text{Final}} = AP_Y^{\text{Initial}} + \Delta A_X^{\text{Initial}} \quad (4)$$

Consequently, Bri generates the transaction finality proof ($TFproof$) of the successful asset transfer and reversely sends it to DeFi X for confirmation.

Interoperability and bridging solutions between any two chains typically support a diverse set of digital assets and charge differently based on their business models. Moreover, these bridges vary in liquidity depths and may appeal to different types and sizes of users and dApp transactions. All this information must be incorporated while modeling the cross-chain networks to ensure effective and efficient asset transfers from a source chain to a destination chain.

4.2. Requirements

CrossDeFi establishes fundamental requirements for transferring assets across diverse DeFi systems. These requirements serve as the foundation for defining the CrossDeFi protocol. In CrossDeFi, the DeFi system utilizes a variety of blockchains, and asset transfers are conducted through a finite set D. Each DeFi system in the set $D = \{\text{DeFi X, DeFi Y, } \dots\}$ employs its smart contracts to facilitate asset transfers. Here, any DeFi system in set D can act as either a source or a destination. Before the transfer of asset A, it must exist only on the source DeFi, and after the transfer, A must exist solely on the destination DeFi. At no point should A exist simultaneously on both the source and destination DeFi systems, as this could lead to accidental asset duplication, potentially deflating the asset's value. Therefore, a CrossDeFi A transfer is deemed successful only if A is created on the destination DeFi after being burned on the source DeFi by its owner.

Requirement 1: A user in a DeFi system must burn A on their blockchain. For example, if user UX in DeFi X wishes to transfer AX, then AX should be burned in DeFi X if $UX \subseteq$ DeFi X and $AX \subseteq AP_X$.

Requirement 2: When DeFi X needs to transfer AX, it must first burn AX from AP_X and send proof to the destination to recreate AX in the destination asset pool.

Requirement 3: It is crucial to prevent double-spending at all times. That is, if asset A is burned on the source blockchain, then A can be recreated only once at the destination DeFi.

Requirement 4: A time-bound t is established for recreating A at the destination after it has been burned at its source DeFi system. Finality should always be decentralized, with no single actor responsible for ensuring it.

Requirement 5: After a particular asset, A, is burned on the source DeFi, the source must eventually receive confirmation of the successful recreation of A on the destination within t. This transfer confirmation ensures that the source blockchain is informed about whether A has been successfully recreated at the destination or another blockchain.

4.3. System Architecture

Cross-chain technology enables seamless interoperability among various blockchain-enabled DeFi networks, facilitating asset transfers across different systems with diverse characteristics. This technology allows each blockchain within a multi-blockchain system to operate independently yet interact effectively through cross-chain strategies. These strategies permit seamless asset transfers, meeting the required specifications and thus enhancing the efficiency and performance of the combined DeFi systems. Cross-chain capabilities also allow multi-chain systems to offer greater scalability and interoperability compared to single-chain systems.

A typical novel cross-chain structure across different DeFi systems is shown in Figure 1. It illustrates how different blockchain networks within the DeFi ecosystem interact using cross-chain bridges, how cross-chain smart contracts are utilized, and how DeFi users engage with each other.

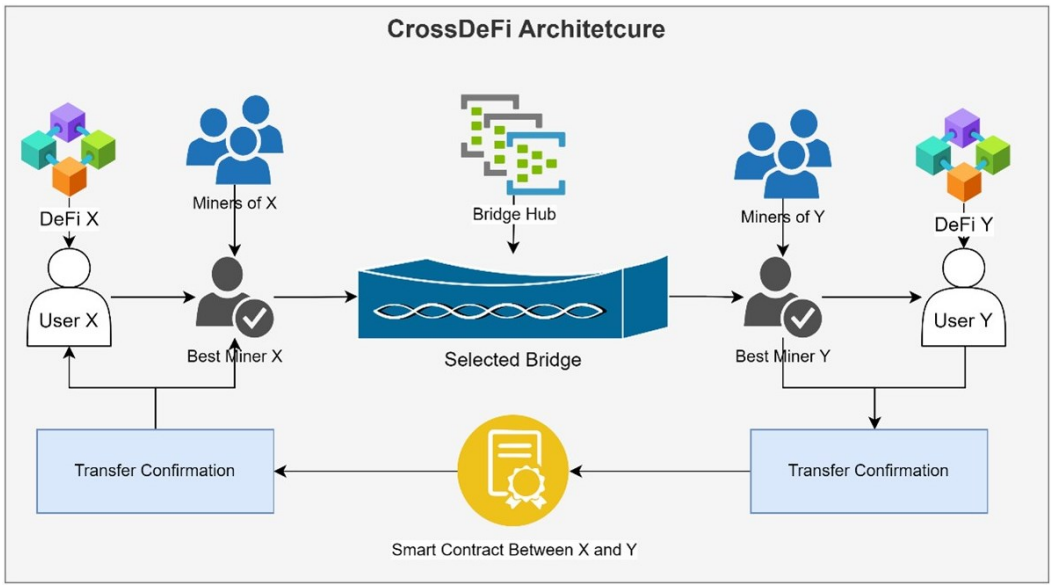

Figure 1. A typical CrossDeFi architecture.

This section effectively describes the system model of CrossDeFi. Figure 1 explains the typical process of asset transfer across two distinct DeFi systems, DeFi X and DeFi Y, which utilize different blockchain models with various characteristics. These blockchains employ various smart contracts, consensus algorithms, assets, tokens, and bridges to enable DeFi services. For instance, DeFi X may use a Bitcoin type of blockchain, while DeFi Y might utilize Ethereum or Hyperledger Fabric technologies. The CrossDeFi protocol acts as a generalized asset transfer protocol where any user can be a source or destination for asset transfer. Apart from the users of DeFi X and DeFi Y, the miners play another crucial role in the system. CrossDeFi selects specific miners from both DeFi X and DeFi Y. The cross-chain asset transfer is performed among the selected miner nodes. The miner nodes in CrossDeFi further communicate with the specific users who initiate the asset transfer process, e.g., user X (UX) and user Y (UY) in Figure 1. If the asset is successfully transferred between X and Y, the miner node confirms the asset transfer to both users, DeFi X and DeFi Y. The CrossDeFi defines the system model's main components: DeFi user, asset, miner, and asset transfer confirmation.

DeFi Users: In DeFi X and DeFi Y, users UX and UY initiate the asset transfer process. UX acts as the sender, and UY as the receiver, each belonging to different blockchains, DeFi X and DeFi Y, respectively.

Asset: This is a digital representation on a blockchain in token form that can be traded with various types of currencies across different DeFi systems.

Miners: The best miners ($BMiX$ and $BMiY$) are chosen from the miner pools of DeFi X and DeFi Y, respectively, based on consensus type and other characteristics. The best miner, $BMiX$ from DeFi X, is responsible for transferring the assets and confirming the successful asset transfer from the source to the destination. Highly trusted miners are mostly selected to participate in the transfer process.

Successful asset transfer: This is the process of delivering assets from the source, DeFi X, to the destination, DeFi Y, with appropriate transfer confirmation messages. CrossDeFi considers factors such as asset support ability, transaction fees, security features, and community reputation in miner selection and chooses the most appropriate miners for asset transfer. Additionally, the miner of DeFi Y is responsible for generating irreversible new blocks to confirm successful asset transfers.

4.4. Attack Model

In the realm of CrossDeFi-based asset transfers between distinct DeFi systems, understanding the attack model is crucial due to the high risk of malicious interventions. The presence of a malicious user (MU), defined as an actor attempting to impersonate a legitimate user or interfere with the asset transfer process, poses significant risks to system integrity and user trust. CrossDeFi establishes several assumptions to safeguard against these threats, enhancing both the security and efficiency of the system.

- Double spending: This critical threat involves an MU attempting to spend the same assets multiple times. Such actions can compromise the DeFi system's trustworthiness, potentially leading to significant financial losses and eroding user confidence.
- Sybil attack: Here, an MU may create numerous fake identities that appear legitimate to gain disproportionate influence within the system. This attack is particularly damaging as it can manipulate asset transfers, distort markets, and cause considerable financial damage.
- Liveness attack: In this attack, an MU aims to disrupt the normal functionality of the asset transfer system by intentionally delaying the confirmation of transfers. This can degrade the user experience and cause significant operational disruptions within the DeFi ecosystem.

These attack vectors highlight the need for robust security measures within the CrossDeFi design and operational protocols. By anticipating and preparing for these threats, CrossDeFi enhances the resilience of asset transfers across diverse DeFi systems, ensuring that transactions remain secure, efficient, and trustworthy.

5. Proposed Work Overview

The primary goal of this work is to introduce CrossDeFi, a novel DeFi Cross-chain communication protocol designed to enhance interoperability and ensure finality across various DeFi systems. Inspired by existing solutions such as Cosmos and Polkadot, CrossDeFi differentiates itself through unique miner and bridge selection methods, enhanced cross-chain interoperability, and a robust finality guarantee mechanism. The block diagram of the proposed CrossDeFi is shown in Figure 2.

Firstly, the proposed protocol integrates an advanced bridge hub that supports various types of bridges, enhancing cross-chain interoperability in terms of speed and reducing transaction fees. Additionally, CrossDeFi introduces novel cryptographic techniques in asset-transfer confirmation to ensure a high level of transaction finality, thus preventing financial losses and improving user experience.

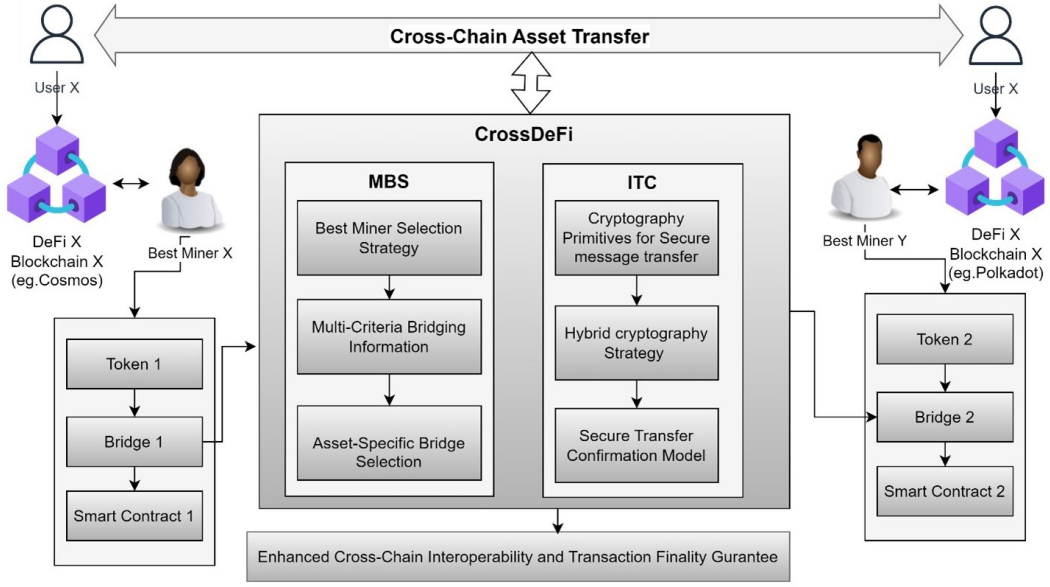

Figure 2. Design process of CrossDeFi protocol.

The CrossDeFi achieves seamless interoperability and ensures a higher level of finality guarantees by integrating two mechanisms: miner and bridge selection (MBS) and improved transfer confirmation (ITC). MBS selects optimal miners and efficient bridges based on multi-criteria information, enhancing cross-chain adaptability across different DeFi applications. ITC introduces a novel bi-directional interaction strategy that ensures asset transfer across multiple DeFi systems with minimal cost and high security.

5.1. Miner and Bridge Selection (MBS)

Bridges in DeFi systems support various types of digital assets and are critical in managing the diverse transaction fees, liquidity depths, and user capacities that characterize different blockchain environments. Effective bridge and miner selection tailored to the specific needs of a DeFi application enhances cross-chain interoperability substantially. Miner and bridge selection is crucial for ensuring secure, fast, and cost-efficient multi-asset transfer support in the CrossDeFi framework. The selection begins within a consensus pool, hosting a spectrum of miners differentiated by their transaction fee structures, liquidity provisions, network congestion handling, and reliability. Choosing the optimal miner from this pool can significantly enhance user experience by optimizing transaction costs and boosting system trustworthiness.

Traditional blockchain architectures typically restrict message transmission to a unidirectional flow. This limitation is a significant hurdle in verifying the successful receipt of assets, as the destination DeFi system cannot send confirmation back through the same channel. Addressing this, CrossDeFi implements a two-way interaction strategy that not only fortifies trust across different blockchain networks but also bridges fundamental gaps observed in traditional cross-chain communication protocols. Here, cross-chain bridges serve a dual function: they facilitate asset transfers and enable reciprocal transfer confirmation communications, thereby assuring transaction finality—a feature absent in other cross-chain components like dexes, aggregators, wrapped tokens, and oracles.

The proposed model employs a bridge-centric approach designed to boost performance across DeFi cross-chains. Selecting the right bridge is crucial; inappropriate choices could delay transactions and heighten vulnerability to attacks. CrossDeFi tackles these challenges by adopting a unique selection strategy that leverages multi-criteria evaluations of both miners and bridges, thus enhancing the robustness and reliability of the DeFi ecosystem.

Best Miner Selection (BMS)

The best miner selection (BMS) algorithm in CrossDeFi leverages the underlying consensus algorithms of the DeFi systems involved to ensure robust and efficient miner selection. For example, miners operating under a proof-of-work (PoW) system, like DeFi X, are selected based on different criteria than those under a proof-of-stake (PoS) system, such as DeFi Y.

Step 1: The BMS algorithm efficiently selects the most suitable miners, $BMiX$ and $BMiY$, from the mining pools of DeFi X and Y, respectively. This selection process is designed to ensure high integrity and trust within the network.

Step 2: The selection algorithm considers a network of k nodes $N = \{N1, N2, \ldots, Nk\}$, each responsible for generating blocks $B = \{B1, B2, \ldots, Bk\}$ linked in sequence. The miner for the next transaction, $Nk - 1$, is chosen based on its ability to maintain the security and reliability of the chain:

$$BMi\_Score = w1 \cdot R_i + w2 \cdot TF_i + w3 \cdot Lq_i + w4 \cdot SL_i \quad (5)$$

where R_i, TF_i, Lq_i, and SL_i represent the reliability, transaction fee, liquidity, and security level of node i, respectively. Weights $w1$, $w2$, $w3$, and $w4$ prioritize these factors based on current DeFi requirements, ensuring an optimal selection.

Step 3: Upon selection, a token representing the transaction details (Token X = create-Token(F_ID, T, F_H)) is generated, encapsulating the identity, timestamp, and hash value of the transaction. This token is sent by $BMiX$ to $BMiY$, initiating the asset transfer process.

This multi-step BMS algorithm, synchronized across both the source (DeFi X) and the destination (DeFi Y), enhances security, reduces costs, and improves the efficiency of cross-chain asset transfers by aligning mining operations with the specific needs and operational parameters of each involved blockchain system.

5.2. Asset-Specific Bridge Selection (ABS)

The asset-specific bridge selection (ABS) process is essential for determining the most suitable bridge or interoperability protocol for transferring specific assets between different blockchain networks within the DeFi framework. This selection is pivotal to ensure efficient, secure cross-chain transactions, minimizing risks and enhancing user experience. The most suitable bridge selection can enable quick and more effective transfer strategies, ensuring reliable and smooth asset transfers. This mechanism can minimize the attack surfaces by utilizing unique security measures tailored for particular risks. ABS considers a variety of factors including asset type, liquidity, security, and network compatibility to pinpoint the optimal bridge for each asset scenario. The purpose of using an asset-specific bridge is to optimize interoperability, enabling DeFi users to transfer specific assets securely and in a decentralized manner across diverse blockchain networks. This approach enhances the liquidity and accessibility of certain assets within the broader blockchain ecosystem.

To illustrate the diversity and capabilities of available bridges, we have compiled a comparative analysis of different bridges currently utilized within DeFi ecosystems. Table 6 offers a detailed comparison based on several key characteristics, including asset support, integration with DeFi apps, speed and efficiency, network adaptability, availability of validators, support for bi-directional transfers, security level, and transaction fees. This analysis aids stakeholders in making informed decisions by highlighting the strengths and weaknesses of each bridge, allowing for the selection of the most suitable option based on specific needs and characteristics.

Table 6. Understanding of different bridges with their characteristics.

Bridges	Asset Support	Integration with DeFi Apps	Speed and Efficiency	Network Adaptability	Validators	Bi-Directional Transfer	Security Level	Transaction Fees
Binance	Yes	No	High	Medium	Yes	Yes	Medium	Very high
Portal	Yes	Yes	High	High	Yes	Yes	Medium	High
Plenty	Yes	Yes	High	High	No	Yes	High	High
Avalanche	Yes	Yes	Medium	Very high	No	Yes	Very high	High
Stargate	Yes	No	Medium	Medium	No	Yes	Medium	High
Zeroswap	Yes	Yes	Medium	High	No	Yes	High	High
cBridge	Yes	Yes	Medium	High	No	Yes	High	High

5.2.1. Working Process of Bridges in CrossDeFi

In the CrossDeFi ecosystem, the functioning of bridges is crucial for asset transfers between different blockchain networks. As illustrated in Figure 3, the asset bridging cycle (ABC) process encompasses both "lock-and-mint" and "burn-and-release" mechanisms to ensure the stability of token distribution across chains. Specifically, when tokens are transferred from Chain A to Chain B, the bridge locks the specified number of tokens on Chain A while simultaneously minting an equivalent number of tokens on Chain B. This dual-action mechanism maintains the total number of circulating tokens but redistributes them across two chains. For example, if Chain A initially holds fifteen tokens and five are to be transferred, Chain A will lock these five tokens, effectively still displaying fifteen tokens in total by counting the locked ones. Concurrently, Chain B will increase its token count by five, reflecting the new tokens minted. These minted tokens on Chain B are controlled by their owner and can be redeemed anytime. The redemption involves burning the tokens on Chain B, which triggers the simultaneous release (unlocking) of the equivalent locked tokens on Chain A. This process ensures that the total number of tokens across both chains remains constant, thereby stabilizing the market value and providing a reliable transfer mechanism that mirrors traditional financial processes in a digital and decentralized environment.

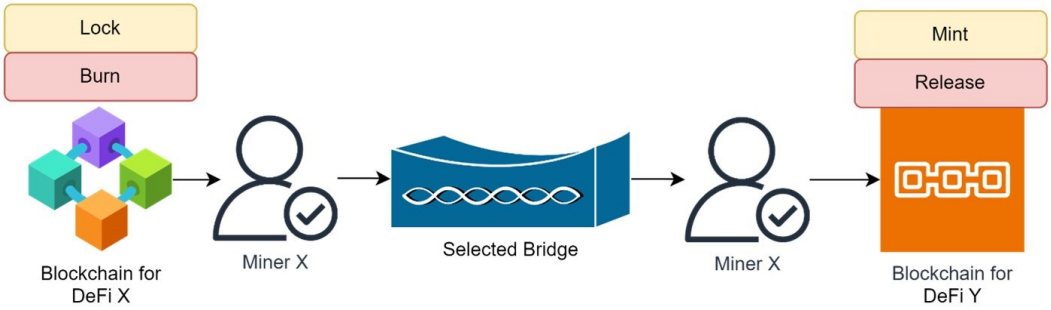

Figure 3. CrossDeFi asset transfer process.

5.2.2. Overview of Bridge Selection

The selection of an asset-specific bridge within CrossDeFi is a critical process that ensures optimized, secure, and efficient transfers of assets across different blockchain networks. This process involves several steps:

1. Identification of Transferable Assets: Identify the specific digital assets that need to be transferred across different DeFi systems, ranging from cryptocurrencies to other digital assets unique to specific networks. This step is essential for tailoring the bridge selection to these specific asset requirements.
2. Evaluation of Bridge Protocols: Evaluate various bridge protocols available within the DeFi ecosystem, assessing, for each asset, compatibility and network support.

This evaluation includes a thorough analysis of each bridge's features, capacities, and constraints, ensuring that the selected bridge aligns perfectly with the asset's transfer requirements.

3. Consideration of Liquidity: Assess the liquidity available for the asset pairs at both the source and destination networks. Adequate liquidity is crucial for handling the volume of transfers without causing market disruption or experiencing slippage, thus supporting efficient and smooth asset transitions.

By following these structured steps, CrossDeFi ensures that asset transfers are not only possible but are conducted with maximum efficiency and security, reflecting the robustness of CrossDeFi's operational framework.

5.2.3. Operational Details of Bridge Selection

The proposed CrossDeFi introduces the asset-specific bridge selection (ABS) process by modeling cross-chain communication between two distinct DeFi applications utilizing various blockchain technologies. This process is visually represented in Figure 4, which illustrates the operational flow of bridge selection. In this scenario, the source blockchain from DeFi Application 1 needs to transfer an asset to the destination blockchain in DeFi Application 2. The ABS employs oracles to gather community information from the cloud server, enhancing the security of the bridge selection process. The optimal bridge between the source and destination is chosen based on a multi-criteria decision process involving community size, asset type, liquidity depth, security level, and adaptability level, all of which aim to minimize the time required for asset transfer while ensuring maximum security and efficiency.

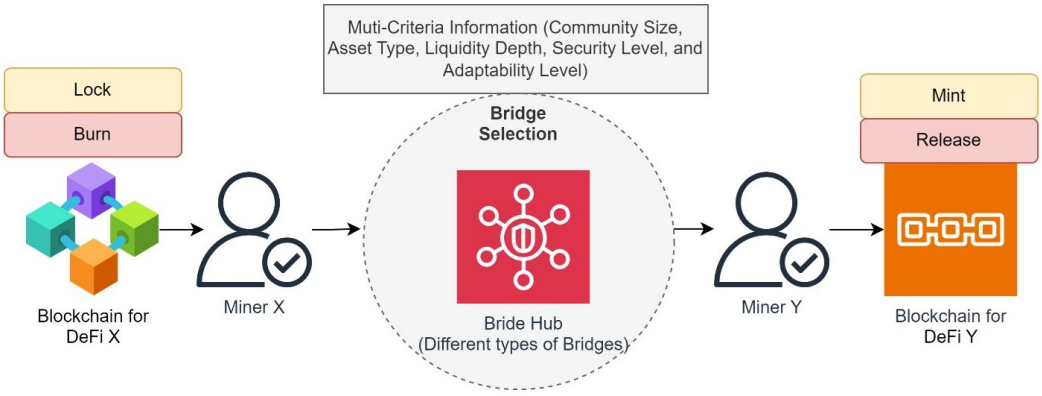

Figure 4. Operational flow of bridge selection in CrossDeFi.

The bridge hub, depicted in the figure, plays a central role in the bridge selection process. It houses various types of bridges, each evaluated based on multiple criteria. These criteria include: community size, reflecting the bridge's popularity and reliability; asset type compatibility, ensuring that the bridge can support specific DeFi transactions; liquidity depth, crucial for executing large transactions without slippage; security level, guaranteeing that asset transfers are safe from attacks; and adaptability level, assessing the bridge's ability to function efficiently across different blockchain technologies.

5.2.4. Quantifying Bridge Suitability

The ABS considers multiple criteria to select the most suitable bridge between the source and destination. A miner is involved in selecting the suitable bridge for the transactions. Multiple bridge information is stored in the bridge hub, and the miner node estimates the bridge score B_{Score} for each bridge for suitable bridge selection. Based on

the real-time DeFi characteristics, the bridge hub information is varied. This selection is quantified through the following equation:

$$B_{\text{Score}} = \alpha(C_{\text{Size}}) + \beta(A_{\text{Type}}) + \gamma(L_{\text{Depth}}) + \delta(S_{\text{level}}) + \omega(A_{\text{level}}) \quad (6)$$

The variable B_{Score} represents the bridge's score value, estimated using criteria such as community size (C_{Size}), asset type (A_{Type}), liquidity depth (L_{Depth}), security level (S_{level}) and adaptability level (A_{level}). The coefficients α, β, γ, δ, and ω are weighting factors for each criterion, summing to one.

5.2.5. Detailed Criteria Definitions

Community size (C_{Size}):

$$C_{\text{Size}} = w_1 \cdot \text{NoU} + w_2 \cdot \text{VoTT} + w_3 \cdot \text{NoUTH} \quad (7)$$

NoU denotes the number of users, VoTT is the volume of transactions over the bridge, and NoUTH is the number of unique token holders. The weighting factors are w_1, w_2, and w_3.

Asset type (A_{Type}):

$$A_{\text{Type}} = a_1 \cdot U + a_2 \cdot S + a_3 \cdot C + a_4 \cdot R \quad (8)$$

This considers usability (U), security (S), cost (C), and reliability (R) of the bridge.

Liquidity depth (L_{Depth}):

$$L_{\text{Depth}} = \sum_k B_k + \sum_k S_k \quad (9)$$

B_k and S_k denote the kth buy and sell price level of the asset quantity.

Security level (S_{level}):

$$S_{\text{level}} = A \cdot SC \cdot KM\&C \cdot NS \cdot CTR \cdot ER\&H \cdot R \quad (10)$$

The terms A, SC, KM&C, NS, CTR, ER&H, and R represent the architecture design, security level of smart contracts, key management and custody, network security level, community trust and reputation, emergency response and handling of incidents, and reliability, respectively.

Adaptability level (A_{level}):

$$A_{\text{level}} = k_1 \cdot \text{C}_{\text{DApp}} + k_2 \cdot TS + k_3 \cdot SL \quad (11)$$

C_{DApp}, TS, and SL refer to compatibility with the DeFi App, transaction speed, and scalability level, respectively. The factors k_1, k_2, and k_3 are weighting importance factors between 0 and 1.

5.2.6. Final Selection

The ABS uses this comprehensive scoring system to select a bridge that offers the best balance between these factors, ensuring the bridge is highly suitable for asset transfer. The bridge score B_{Score} is normatively scaled between 0 and 1, indicating the suitability of the bridge for the specific transfer requirements. Algorithm 1 explains the miner and bridge selection process (MBS). Only miners from the approved set of DeFi mining pools, denoted as BMi, are eligible for selection as miners (BMiX or BMiY) if they are part of this miner set. By tailoring unique miners and bridges according to the specific characteristics and requirements of various asset types, CrossDeFi can provide more efficient, highly secure, maximum speed, and user-friendly cross-chain asset transfers.

Algorithm 1 Miner and bridge selection process

Intention: Selects most suitable miner and bridges for asset transfer.
procedure MBS
    Initiate the BMS.
    Select $BMiX$ and $BMiY$ based on the consensus and Fscore.
    $BMi_{\text{Score}} = w_1 R_i + w_2 TF_i + w_3 Lq_i + w_4 SL_i$;
    for each miner $i = 1$ to k **do**
        if $BMi_{\text{Score}} \geq BMiTH$ **then**
            Miner selected.
        else
            Repeat the BMS.
        end if
    end for
end procedure
procedure ABS
    Initiate the bridge selection process.
    Estimate the B_{Score} using Equation (6).
    Apply Equations (7)–(11) in Equation (6).
    for each bridge $i = 1$ to N **do**
        if $B_{\text{Score}} = 1$ **then**
            Bridge is highly suitable.
            Select the bridge for asset transfer.
        else
            Bridge is not suitable.
            Repeat the ABS process until a suitable bridge is selected.
        end if
    end for
end procedure
The miner transfers the assets through the selected bridge.

5.3. Improved Transfer Confirmation (ITC)

The improved transfer confirmation (ITC) is a fundamental mechanism within the CrossDeFi framework, designed to ensure secure and verifiable asset transfers from a source DeFi system (DeFi X) to a destination system (DeFi Y). By tailoring the ITC, CrossDeFi enables faster and more reliable confirmations for asset transfers, significantly reducing the risk of fraudulent behaviors like double-spending, where a user spends the same asset more than once. Activated after the successful MBS process, ITC ensures that the asset ownership is singular and authenticated before initiating a transfer. Upon confirming that DeFi X possesses undisputed ownership of an asset Ass, characterized by the asset being uniquely owned at any given time and identified as Ass $\in m_{i=1}$Ass, the ITC mechanism is initiated.

As depicted in Figure 5, miner BMiY plays a critical role in communicating the successful confirmation of asset transfers to both users and miner BMiX. To secure the confidentiality and authenticity of the asset transfer between DeFi X and DeFi Y, CrossDeFi integrates a hybrid cryptographic strategy. This strategy employs elliptic curve cryptography (ECC) and secure hash algorithm (SHA-256), with the cryptographic key pairs designated as SKFX for DeFi X and SKFY for DeFi Y.

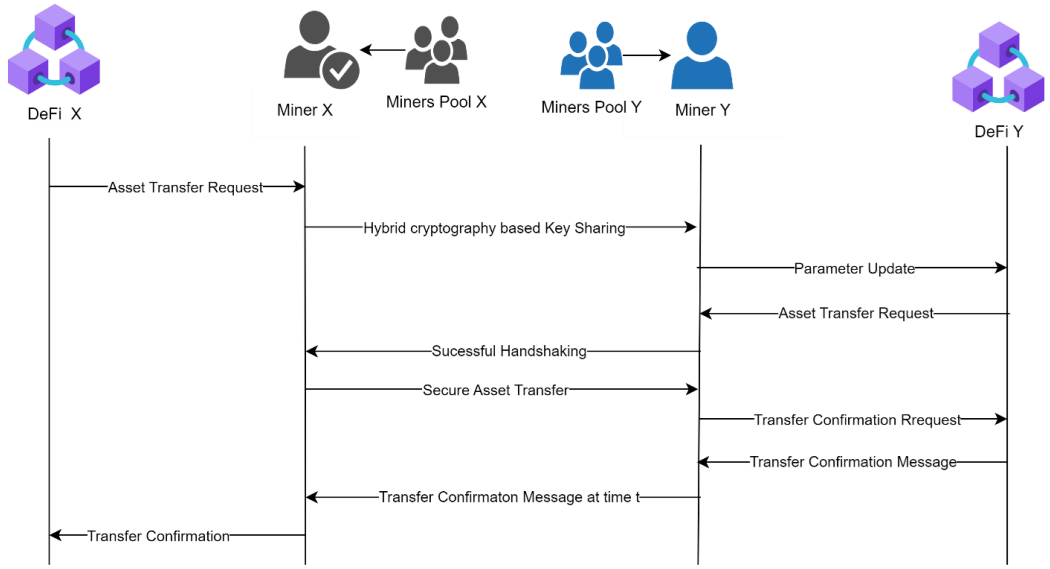

Figure 5. Asset transfer communication scenario.

The transfer process begins when a user from DeFi X initiates the transfer by sending the asset to DeFi X's blockchain. The asset is then placed into the asset transaction pool of X (ATP-X) after being recorded in the latest block by miners. Miner BMiX facilitates the transfer of the asset from ATP-X to ATP-Y using the selected bridge B(X-Y), as outlined in the MBS guidelines. Upon receipt, the blockchain of DeFi Y processes the asset from ATP-Y, with miner BMiY ensuring its integration into the DeFi Y network. If the asset is verified as legitimate, DeFi Y sends a transfer confirmation back to both BMiX and BMiY, culminating in user X receiving this confirmation. To support asset traceability, BMiX records the transaction within the latest block of blockchain X, accessible only to authorized users, ensuring data integrity and the traceability of the asset's origin.

Encryption and Confirmation Process

Step 1: BMiX, the designated miner for DeFi X, initiates the transfer by generating an asset hash H for Ass, termed Ass Hash X $= H(\text{Ass X})$. BMiX also generates a nonce from a true random number generator (TRNG) and captures the hash of the preceding block PH. Using these values, BMiX constructs a block defined as $B = B_X(\text{Ass H}, T, PH, \text{nonce})$ and securely transmits it using ECC encryption and a digital signature, denoted as send$(\sigma_{B_X}, \text{Enc}_{pK_{BMiX}}(B_X))$.

Step 2: At the destination, BMiY mirrors the actions performed by BMiX. BMiY decrypts and verifies the received block $B_X = \text{Dec}_{sK_{BMiY}}(B_X)$ and verifies $(pK_{BMiX}, B_X, \sigma_{B_X})$. Post verification, BMiY recalculates the asset hash Ass H $= H(\text{Ass X})$ and reconstructs the block as $B_X^* = B_X^*(\text{Ass H}, T, PH, \text{nonce})$. A successful verification confirming the accuracy of the transferred asset is established if B_X equals B_X^*. Algorithm 2 provides a detailed procedure for the improved transfer confirmation (ITC) process.

Moreover, ITC enables quick and reliable transfer confirmations and ensures precise finality, making CrossDeFi more effective and capable of managing massive asset transaction volumes with a higher level of user satisfaction. This process not only improves the entire user experience against double-spending but is also highly beneficial for time-sensitive DeFi operations.

Algorithm 2 Improved transfer confirmation (ITC) process

Initialize Transfer Confirmation:
1: Analyze asset: BMiX in DeFi X analyzes the asset type Ass to execute the miner and bridge selection (MBS).
2: Security measures: Employ a hybrid cryptography strategy to burn and lock Ass, where the burn is at DeFi Y, destination chain, and lock is via a smart contract at a designated address.
Initiate Asset Transfer:
3: Begin transfer: BMiX initiates the asset transfer process.
4: Transmission: BMiX transmits proof of the locked asset Ass to BMiY in DeFi Y.
Validate and Confirm Transfer:
5: Validator actions: BMiY checks the proof of asset lock and ensures transaction validity using cryptographic verification.
6: Minting and releasing: BMiY in DeFi Y initiates the asset minting and releasing process, completes the asset transfer.
Finalize and Confirm:
7: Send confirmation: BMiY sends back transfer confirmation to BMiX via the same bridge using the cryptography scheme.
8: Ensure finality: Transaction finality is ensured, confirming the successful asset transfer.

6. Analysis

This section delves into the efficiency and security aspects of the CrossDeFi system, providing an in-depth evaluation through various proof-of-characteristics and simulated attack scenarios. It aims to demonstrate the robustness of the CrossDeFi architecture against common threats and inefficiencies in decentralized finance systems, offering quantifiable metrics that highlight its performance and resilience.

6.1. Efficiency Assessment

This subsection assesses CrossDeFi's efficiency by exploring its performance across diverse decentralized finance (DeFi) applications and contrasting its proof-of-characteristics—namely interoperability and transaction finality—with those of existing protocols. The analysis highlights CrossDeFi's adaptability and effectiveness in real-world scenarios, showcasing its capacity to meet the varied demands of the DeFi landscape.

6.1.1. Different DeFi Use Cases

The proposed Cross-DeFi framework is specially designed to facilitate interoperability and seamless asset transfer among different blockchain-enabled DeFi systems while ensuring a finality guarantee. By enabling seamless cross-chain asset transfers, CrossDeFi can support a wide variety of use cases across DeFi. Exploiting the proposed CrossDeFi framework across various DeFi use cases can offer significant benefits, including seamless interoperability, increased asset transfers, improved security, and opportunities for diversified investment. However, it has to face some challenges, such as asset loss, additional transaction fees, adaptability level, finality guarantee, implementation complexity, and performance efficiency. By effectively addressing such challenges, Cross-DeFi can drive innovation and growth in DeFi, providing users with more effective, flexible, and secure financial services. Table 7 evaluates the impact of CrossDeFi on various DeFi use cases, illustrating its influence on critical factors such as asset loss, double-spending, additional fees, adaptability, finality guarantee, complexity, and performance.

Each row in the table provides insights into the specific impacts of implementing CrossDeFi within different scenarios, from trading on decentralized exchanges (DEXs) and engaging in yield farming activities to participating in decentralized autonomous organizations (DAOs). Notably, CrossDeFi enhances adaptability and guarantees finality across all listed use cases, reducing the potential for asset loss and double-spending while slightly increasing transaction fees in some instances. This aligns with the advanced

security measures and infrastructure improvements that typically accompany the deployment of such innovative solutions. The assessment underscores CrossDeFi's capacity to address the unique needs and challenges of various DeFi sectors, making it a versatile and valuable addition to the DeFi landscape. Table 7 assists in analyzing the challenges of implementing CrossDeFi across various DeFi use cases, paving the way to utilize its full potential to improve next-generation DeFi systems. By leveraging asset-specific cross-chain bridge selection and enhanced transfer confirmation within the core blockchain layer, the CrossDeFi framework enhances asset transfer efficiency and DeFi user experience. This wider support motivates the proposed approach to utilize CrossDeFi across diverse use cases and enables the growth of DeFi, making it more versatile and efficient.

Table 7. Impact of CrossDeFi on different DeFi use cases.

DeFi Use Case	User	Service Type	Asset Loss	Double-Spending	Additional Fees	Adaptability Level	Finality Guarantee	Complexity	Performance
DEXs	Buyer, trader	Asset exchange	No	No	Yes	High	Yes	Medium	High
Yield farming	Liquidity providers and yield farmers	Asset transfer	No	No	Yes	High	Yes	High	Very high
Lending and borrowing	Buyer, trader	Asset transfer	No	No	No	High	Yes	Medium	Very high
Online gaming	Investors, players, traders	Asset transfer, exchange	No	No	Yes	High	Yes	High	Very high
DAO	Liquidity providers and token holders	Asset transfer, token transfer	No	No	Yes	High	Yes	High	High

6.1.2. Proof-of-Characteristics with Existing Cross-Chains

Traditional mechanisms, such as hash-locking, multi-token standards, notary services, and sidechains typically achieve only low to medium interoperability and often lack robust finality guarantees. This comparison underscores the advanced capabilities of CrossDeFi, particularly in its unique approach to ensuring transaction finality. Table 8 provides a comparative analysis of the proposed CrossDeFi with existing cross-chain solutions using a comprehensive set of parameters.

Table 8. Comparative analysis of CrossDeFi with conventional solutions.

Cross-Chain Solutions	Interoperability	Asset-Locking	Transfer Confirmation	Cross-Chain Asset transfer	Finality Guarantee	Double-Spending Prevention	Bridging or Oracle Solutions	Transfer Performance	Speed	Security Level	Adaptability	Applicability	Scalability	Complexity	Difficulty to Achieve	Regulatory Complexity
Hash locking	N	Y	N	N	N	N	N	L	L	M	M	M	L	H	N	Y
Multi-token standards	Y	Y	N	N	N	N	Y	M	L	M	L	H	M	H	Y	Y
Notary mechanism	Y	Y	N	N	N	N	Y	M	M	L	M	L	M	H	Y	Y
Sidechain or relay	Y	Y	N	N	N	N	Y	H	L	H	L	M	M	H	N	Y
Asset transfer protocol	Y	N	Y	Y	Y	Y	Y	H	M	L	M	L	M	M	Y	Y
Proposed CrossDeFi	Y	N	Y	Y	Y	Y	Y	H	H	H	H	H	H	H	Y	Y

Y—Yes, N—No, H—High, L—Low, M—Medium.

CrossDeFi distinguishes itself by employing a transfer confirmation strategy that is integral to its design, ensuring a higher level of finality guarantee compared to existing solutions. Unlike traditional models that often rely on simplistic asset-locking mechanisms, which do not prevent asset loss or double-spending effectively, CrossDeFi incorporates an asset-specific bridge selection model. This model leverages multi-criteria information to enhance bridge selection, significantly improving the system's performance, speed, and cost-efficiency.

The asset-specific bridge selection (ABS) mechanism of CrossDeFi assigns significant weight to crucial parameters such as security, speed, cost, and adaptability, which greatly enhances the accuracy and efficiency of cross-chain asset transfers. This strategic focus not only reduces potential bottlenecks associated with bridge performance but also aligns with the diverse requirements of various DeFi applications, facilitating tailored solutions for different use cases.

Despite its complexity, the implementation of CrossDeFi offers substantial improvements over existing systems by eliminating issues associated with asset-locking and double-spending. This makes it exceptionally suitable for various DeFi applications, from decentralized exchanges (DEXs) to complex financial products involving lending, borrowing, and yield farming. The system's design, centered around its unique bridge selection and transfer confirmation processes, ensures that CrossDeFi can adapt to and effectively support a broad spectrum of DeFi activities, thereby enhancing overall user experience and system reliability.

6.2. Security Analysis

This section delivers a detailed security analysis of CrossDeFi, highlighting its robust defenses against well-known vulnerabilities within cross-chain DeFi environments.

6.2.1. Lemma 1 for Double-Spending Attack

Double-spending in CrossDeFi occurs when an asset is illicitly spent more than once by the same user. This lemma explores two potential scenarios for a double-spending attack within the CrossDeFi environment.

Case 1: Concurrent Spending on Multiple Users

Proof. Consider a scenario within CrossDeFi where a user, UX from DeFi X, attempts to spend the same asset, Ass, concurrently on two different users, UY in DeFi Y and UZ in DeFi Z. The success probability of double spending is expressed in the following equation:

$$(ATC_n)_{\text{DeFi\_X}} = (ATC_n)_{\text{DeFi\_Y}} \tag{12}$$

In this case, the ATC (asset transfer confirmation) numbers received by the miners in both DeFi X and DeFi Y are the same. According to Requirement 3, an asset is recreated at DeFi Y after receiving proof for asset burning at DeFi X, preventing the double-spending attack against malicious users.

CrossDeFi secures against such attacks by ensuring immediate transfer confirmation from the recipient DeFi chain back to the sender. Consider n as the number of nodes in each blockchain within CrossDeFi. Each miner Mi from each DeFi blockchain sends an ATC message in the opposite direction to the sender's blockchain network, fostering trust among parties. This process involves each miner securing n verifications to validate the legitimacy of the miners and build trust across the network. CrossDeFi employs a traceable ring signature to sign the ATC message.

If the verification count $\text{VC}(\text{Msg}_{\text{ATC}}) = n$, the miner's status is trusted, and it is deemed valid. If BMiX from DeFi X receives n verifications from DeFi Y, and BMiY from DeFi Y receives n verifications from DeFi X, trust is effectively established. This arrangement significantly enhances the security against double-spending attacks within CrossDeFi. □

Case 2: Duplicate Asset Spending

Proof. Consider a scenario where a malicious user (MU) in DeFi X attempts to send duplicate or conflicting assets to the same user, UX in DeFi X. If MU $\notin \sum_{i=1}^{n}$ attempts to spend asset Ass X and its duplicate, Ass X*, then CrossDeFi performs a check to verify asset ownership to confirm that a single user holds the asset. Through efficient asset representation policies, CrossDeFi ensures that each asset can only be owned by one user at a time, thereby preventing the possibility of double-spending. □

This rigorous approach to security in the CrossDeFi framework not only prevents the occurrence of double-spending but also establishes a trust mechanism that supports the integrity of transactions across multiple DeFi platforms.

6.2.2. Lemma 2 for Sybil Attack

In CrossDeFi, the Sybil attack poses a significant threat, where a malicious user (MU) may create multiple duplicate miners or fraudulent accounts to manipulate transactions for personal gain. This section outlines two potential cases where a Sybil attack could be executed within CrossDeFi.

Case 1: Fraudulent Account Creation When an MU creates multiple fake accounts attempting to transfer assets illegitimately claimed as their own.
Case 2: Fake Node Creation When an MU establishes a counterfeit node purporting to be a legitimate miner.

Proof for Case 1. In CrossDeFi, assets are uniquely tied to their owners, ensuring that each asset is associated with a single user at any given time. Suppose user UX, UY $\in \sum_{i=1}^{n} U$ and user UX legitimately owns asset Ass X $\in \sum_{i=1}^{m}$. If an MU from DeFi X attempts to transfer AssX, the transfer is only valid if UX is the unequivocal owner of AssX. The system checks Owner(MU, Ass X), ensuring that the MU $\notin \sum_{i=1}^{n} U$ and therefore cannot initiate the transfer. This mechanism ensures that before and after the transfer, AssX is owned by UX and subsequently UY, with both users being validated members of their respective DeFi systems. □

Proof for Case 2. This scenario involves an MU attempting to pose as a legitimate miner. CrossDeFi's miner and bridge selection (MBS) process is designed to select trustworthy miner nodes based on their historical performance and contributions to the blockchain.

For example, consider three miners M1, M2, and M3, mining blocks B1, B2, and B3, respectively, with the blocks ordered as $B1 \leftarrow B2 \leftarrow B3$. Here, B3 is the latest block mined by M3, and B2 is its parent block mined by M2. In this setup, M2 is selected as the miner for its proven reliability and the absence of any malicious activity in its past block mining efforts. This selection process reduces the load on M3 and leverages M2's established trustworthiness, thereby mitigating the risk of a Sybil attack. If an MU falsely claims to be a miner, CrossDeFi evaluates the miner's reliability before designation, ensuring that only legitimate miners are tasked with critical roles. □

Through these proofs, CrossDeFi demonstrates robust defenses against the Sybil attack, leveraging stringent asset ownership verification and meticulous miner selection to maintain the integrity and security of asset transfers within its ecosystem.

6.2.3. Lemma 3 for Liveness Attack

A liveness attack in the context of CrossDeFi involves a malicious user (MU) attempting to delay the communication of messages within the network, thereby degrading user experience. This type of attack focuses on interrupting the normal operation and responsiveness of the system.

Proof. Consider the following scenario where BMiX, a miner from the blockchain of DeFi X, sends an asset transfer confirmation (ATC) message to the blockchain of DeFi Y. Similarly, BMiY from DeFi Y sends an ATC message back to DeFi X.

To ensure the integrity and timeliness of these messages, CrossDeFi employs a hybrid cryptography scheme that includes the use of traceable ring signatures (TRS). This method not only secures the message but also ensures its traceability back to the sender, thus preventing anonymity from being exploited to delay the transmission. The system sets a threshold timeframe for receiving these ATC messages. Suppose BMiX receives the required number of verifications n from BMiY within this predefined period, and reciprocally, BMiY from DeFi Y also confirms the reception of n verifications from BMiX. In that case, the transfer is validated, and trust between the two chains is established. Any ATC messages received within this timeframe are considered successful, confirming the asset transfer effectively. Conversely, messages that fail to meet the deadline are automatically deemed unsuccessful.

This strategic approach enables CrossDeFi to diminish the potential impacts of liveness attacks, ensuring that asset transfers are not only secure but also timely. By setting strict timeframes for confirmations and employing advanced cryptographic techniques, CrossDeFi enhances transaction finality and maintains a high level of user satisfaction within its network. □

7. DeFi Lending and Borrowing Use Case

For a clear understanding of the design of CrossDeFi, this section explores a use case involving DeFi lending and borrowing. This use case enables users to lend and borrow crypto-assets across two DeFi networks. The CrossDeFi framework can enhance lending and borrowing by permitting users to exchange their assets across various blockchain networks, thereby achieving seamless interoperability.

Consider a real-world lending scenario in which two DeFi networks, DeFi X and DeFi Y, are available. DeFi X utilizes the Cosmos network, and DeFi Y uses the Polkadot network, as illustrated in Figure 6.

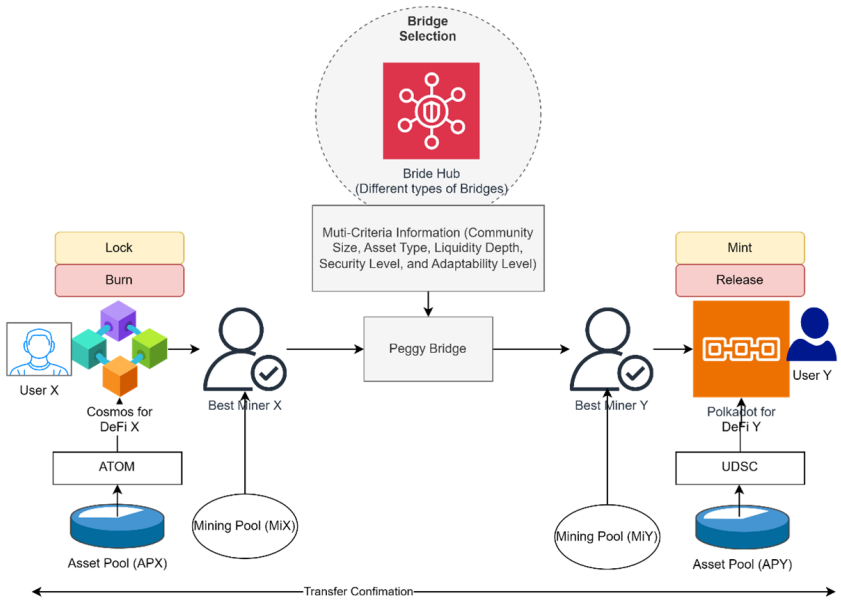

Figure 6. Illustration of the lending scenario between DeFi X and DeFi Y.

The user in DeFi X holds ATOM tokens within the Cosmos network and wants to obtain USDC tokens based on the Polkadot network. The first step involves burning the ATOM tokens in the Cosmos network and recreating them in the Polkadot network as USDC. The CrossDeFi framework facilitates this cross-chain transaction by ensuring

security, speed, and cost-efficiency. Here, both DeFi X and DeFi Y are heterogeneous, utilizing various blockchains with different tokens and assets.

Initially, the user in DeFi X initiates a borrowing request. As per the CrossDeFi design, the following steps are followed:

1. The user in DeFi X initiates the transfer process by defining the amount according to the ATOM value.
2. CrossDeFi selects one miner from the MiX using Equation (5). Consider that the reliability, transaction fees, liquidity depth, and security level of a miner in a mining pool are 99%, \$0.20, \$750 million, and 1, respectively. BMiX has a high reliability value of 99%, based on its historical performance. The Polkadot network charges \$0.20 transaction fees for ATOM transfers, and its liquidity pool value is \$750 million. The security level assumption is made in the system model. Applying these values and using Algorithm 1, CrossDeFi selects the best miner node BMiX.
3. The miner sends the burning information of asset A as proof through the cross-chain bridge. It performs a bridge selection process using Equation (6). The bridge hub in CrossDeFi includes the following bridges: Acala, Snowfork, Peggy, Interlay or InterBTC, Darwinia, Thorchain, Multichain, Renbridge, Chainbridge, and Gravity Bridge. By applying the bridge-related parameters, BMiX selects the Peggy bridge as the most suitable bridge for asset A transfer.
4. In this step, BMiX forwards the asset through the Peggy Bridge to the Polkadot system. The Polkadot network converts the ATOM into USDC through a collateral process. The asset A is recreated as USDC in the Polkadot-enabled receiver DeFi. Further, the miner BMiY sends a transfer confirmation proof via smart contracts to DeFi X.

The CrossDeFi framework streamlines the lending process across heterogeneous DeFi networks that employ Cosmos and Polkadot by leveraging different strategies. By dynamically choosing the best nodes as miners and selecting the most suitable cross-chain bridges for asset transfer, CrossDeFi enhances the overall functionality and user experience in DeFi lending and borrowing scenarios.

8. Evaluation

This section presents the evaluation of the proposed CrossDeFi within a prototype model, conducting a quantitative analysis to assess asset transfer efficiency and speed. The prototype and evaluation scripts were utilized to derive the results. According to the prototype-based evaluation, transactions such as lock and burn are initiated at the source DeFi X, while claim and release transactions are executed at the destination DeFi Y. These transactions are repeated within the experiment to measure the efficiency and speed of asset transfer. It is assumed that transaction fees are kept low to maintain simplicity in the evaluation process.

To precisely validate the robustness of the experimental results, a statistical tool known as the confidence interval is exploited. This tool quantifies the uncertainty and variability in the experimental outcomes by estimating a range of confidence for the key metrics used in the evaluation. CrossDeFi's evaluation includes several independent runs under identical conditions, generating diverse results across these runs. By calculating the mean and standard deviation of these multiple runs, CrossDeFi estimates the confidence interval at the 95% level. The confidence interval results provide a range that indicates the true results with minimal uncertainty and error rates. A narrow confidence interval suggests precise estimates, while a wider interval indicates that the results are more variable and uncertain. By applying confidence intervals to the experimental results, CrossDeFi offers a statistical measure to evaluate the robustness and reliability of its estimates.

There are thriving open-source tools, languages, and scripts available for reproducibility in blockchain technology, particularly in Cosmos and Polkadot ecosystems. The proposed CrossDeFi utilizes open-source tools, languages, and scripts such as Cosmos SDK and Polkadot.js for its prototype evaluation, ensuring the reproducibility of the CrossDeFi framework.

8.1. Experimental Setup

The experimental analysis of CrossDeFi is performed between two different DeFi-based test networks: Cosmos and Polkadot. Cosmos employs the inter-blockchain communication (IBC) protocol, while Polkadot uses the cross-chain message passing (XCMP) protocol for enabled cross-chain communication. Both test networks feature interoperability layers configured to closely simulate real-world scenarios, enabling cross-chain asset transfers between DeFi X and DeFi Y.

Cosmos utilizes CosmWasm for smart contract execution across different blockchains, facilitating a wide range of DeFi asset transfer functionalities. In Polkadot, the relay chain does not natively support smart contracts, although its parachains can. The relay chain is the heart of Polkadot, providing security, consensus, and interoperability. The parachains are independent blockchains connected to the relay chain, leveraging interoperability and security features while maintaining Polkadot's unique functionalities. Notably, Moonbeam and Astar are platforms within Polkadot that support smart contracts. This evaluation utilizes various test networks to provide sufficient transaction execution time computation and gas usage estimation on both Cosmos and Polkadot.

CrossDeFi conducts tests in intervals of 10×5 times, totaling 50 asset transfers of one ATOM from DeFi X on the Cosmos network to DeFi Y on the Polkadot network. The evaluation is performed on a computer powered by the Ubuntu 18.02 LTS operating system, equipped with a multi-core Intel i7 CPU, 64 GB of RAM, and 512GB SSD storage, ensuring a reliable internet connection.

8.2. Performance Metrics

The effectiveness of the proposed CrossDeFi system is quantified through two primary metrics: asset transfer accuracy (ATA) and transfer delay (TD).

Asset transfer accuracy (ATA): This metric evaluates the integrity of the asset transfer process by ensuring that the full value of assets is transferred from source DeFi X to destination DeFi Y without any losses or incomplete transfers. Losses may occur due to suboptimal transfer strategies or potential attack vectors. The ATA is defined mathematically as:

$$\text{ATA} = \frac{\text{Ass}^{*}_{\text{DeFi\_Y}_t}}{\text{Ass}_{\text{DeFi\_X}}} \times 100\% \tag{13}$$

where $\text{Ass}_{\text{DeFi\_X}}$ and $\text{Ass}^{*}_{\text{DeFi\_Y}}$ represent the total amount of assets sent by DeFi X and received by DeFi Y at time t, respectively. The expression $\text{Ass}_{\text{DeFi\_X}} = \text{Ass}^{*}_{\text{DeFi\_Y}_t}$ defines that the asset transfer is completed without any loss or delay. If $\text{Ass}_{\text{DeFi\_X}} = \text{Ass}^{*}_{\text{DeFi\_Y}_t}$, all assets are successfully transferred from DeFi X to DeFi Y. Otherwise, there is some loss. For instance, if 1000 asset transfers are performed from DeFi X to DeFi Y over a period t, and the successful asset transfers amount to 960, then the ATA is 96%. Likewise, CrossDeFi estimates ATA for each cross-chain strategy compared with the proposed model.

Transfer delay (TD): This metric measures the total time required for the asset transfer process and the subsequent confirmation from DeFi Y back to DeFi X. It includes the time taken to transfer the assets from DeFi X to DeFi Y and the time to send the transfer confirmation back to the source DeFi X from the destination DeFi Y:

$$\text{TD} = \text{Time}_{\text{AT(DeFi X}\rightarrow\text{DeFi Y)}} + \text{Time}_{\text{NC(DeFi X}\rightarrow\text{DeFi Y)}} \tag{14}$$

8.3. Experimental Evaluation

The asset transfer efficiency of the CrossDeFi system is influenced by network conditions and the specific blockchain technologies employed. This subsection compares the asset transfer accuracy (ATA) and transfer delay (TD) metrics of CrossDeFi (CD) with several existing cross-chain solutions, including Polkadot (Pol) [41], Cosmos (CoS) [45], hash-locking (HL) [51], notary mechanism (NM) [48], sidechain or relay (SR) [49], and asset transfer protocol (AT) [50].

Figure 7 and Table 9 illustrate the ATA results for seven cross-chain solutions, including CrossDeFi, with the number of users varying from 20 to 100. As the number of users increases, CrossDeFi exhibits a decrease in ATA due to potential errors or delays caused by strained network conditions. Although CrossDeFi prevents asset loss due to security breaches, some losses occur due to network congestion. Asset transfers might fail owing to insufficient gas fees, or they might be significantly delayed during periods of high network congestion. For example, ATA rates for CrossDeFi are 99.6% with 20 users and decrease to 96% with 100 users. Here, the asset transfer loss is 0.4% and 4%, respectively. Despite this decline, CrossDeFi achieves notably higher ATA compared to the six other solutions. This superior performance is attributed to CrossDeFi's unique miner and bridge selection mechanisms, which incorporate multiple criteria based on blockchain type and network conditions. These mechanisms enhance asset transfer accuracy without adversely affecting speed, transaction fees, user experience, or security. Notably, CrossDeFi improves ATA by 4.1%, 5.3%, 8.6%, 7.3%, 9.6%, and 5.6% compared to Pol, CoS, HL, NM, SR, and ATP, respectively.

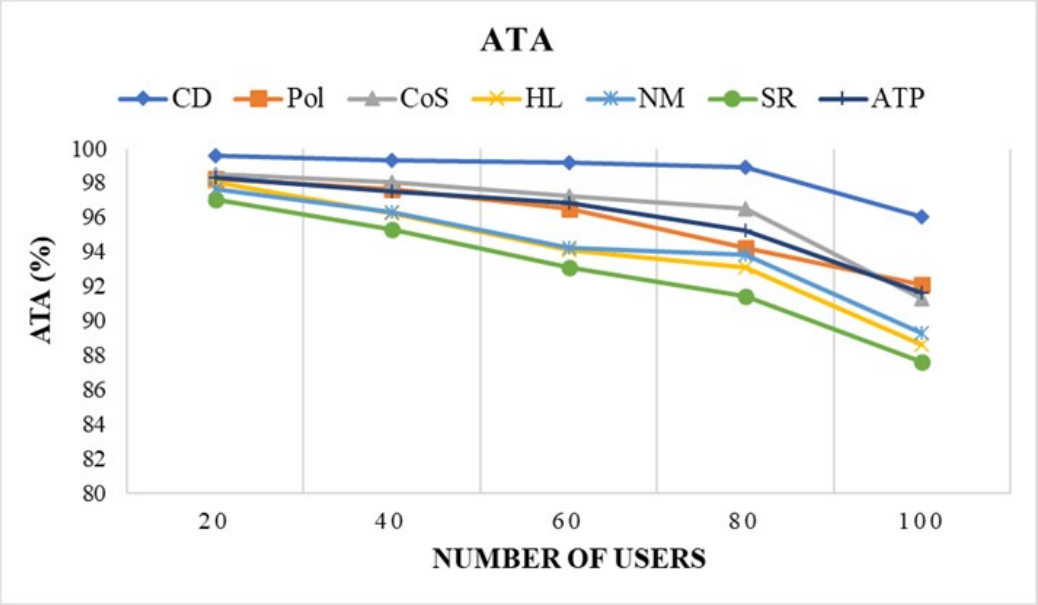

Figure 7. ATA across various cross-chain solutions as a function of user count.

Table 9. Asset transfer accuracy (ATA) across different networks with varying numbers of users.

Number of Users	ATA (%)						
	CD	Pol	CoS	HL	NM	SR	ATP
20	99.6	98.2	98.5	98	97.6	97	98.3
40	99.3	97.6	98	96.2	96.3	95.3	97.5
60	99.15	96.5	97.2	94.1	94.2	93.1	96.8
80	98.9	94.2	96.5	93.1	93.8	91.4	95.2
100	96	92.1	91.3	88.6	89.3	87.6	91.6

Figure 8 and Table 10 compare TD across the same set of cross-chain solutions as user numbers increase. This TD is estimated by the summation of both transfer time and transfer confirmation time. CrossDeFi shows an incremental delay from 25.6 s with 20 users to 72.5 s with 100 users. Despite this increase, CrossDeFi consistently maintains lower delays compared to its competitors. This efficiency is largely due to its optimized miner and asset-specific bridge selection algorithms, which effectively reduce delays and transaction fees while enhancing security. The asset-specific bridges selected by CrossDeFi significantly boost transfer speeds and ensure timely delivery of transfer confirmation messages, leading

to improved asset transfer rates. For instance, delays observed for CrossDeFi, Pol, CoS, HL, NM, SR, and ATP are 72.5 s, 102.6 s, 145.7 s, 160.1 s, 170.9 s, 165.8 s, and 140.4 s, respectively, for scenarios with 100 users.

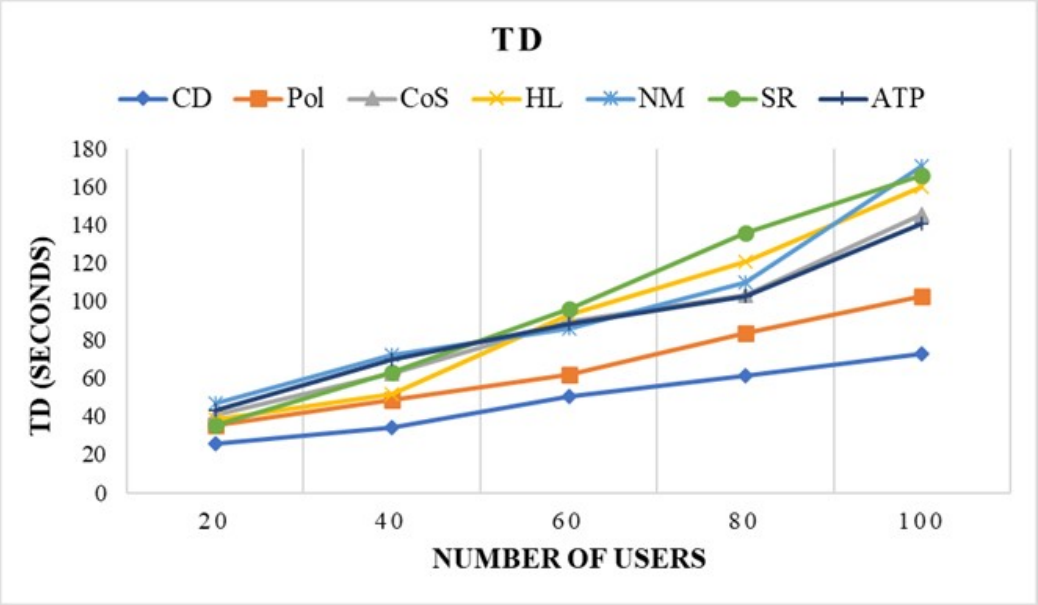

Figure 8. Impact of user load on transfer delay across multiple cross-chain protocols.

Table 10. TD (transaction duration) comparison of CrossDeFi with existing protocols in seconds.

Number of Users	TD in Seconds						
	CD	Pol	CoS	HL	NM	SR	ATP
20	25.6	35.2	40.6	38.1	46.8	35.3	42.9
40	33.8	48.7	62.2	51.7	72.3	62.9	69.8
60	50.2	61.8	89.7	93.3	85.9	95.8	88.3
80	61.4	83.2	103.6	120.9	110.2	135.9	102.7
100	72.5	102.6	145.7	160.1	170.9	165.8	140.4

In conclusion, the experimental evaluation of CrossDeFi illustrates its superior performance in terms of asset transfer accuracy and transfer delay compared to established cross-chain solutions. The system's unique selection mechanisms for miners and bridges, tailored to specific blockchain conditions and network demands, enhance its operational efficiency and interoperability of diversified assets. These results underscore CrossDeFi's potential to significantly improve cross-chain asset transfers in real-world DeFi applications, promising enhanced user experiences and heightened security.

9. Conclusions

In this paper, a novel DeFi cross-chain protocol, CrossDeFi, was proposed with the objective of enhancing interoperability and transaction finality guarantees in asset transfers across heterogeneous DeFi systems. CrossDeFi incorporates the miner and bridge selection (MBS) and improved transfer confirmation (ITC) mechanisms to achieve these goals. Initially, the MBS mechanism enhances interoperability by optimizing speed, transaction fees, and transfer accuracy through the selection of the most suitable miners and asset-specific bridges. By dynamically selecting the best nodes as miners and leveraging highly suitable cross-chain bridges for asset transfers, CrossDeFi maximizes overall efficiency and user experience in DeFi. Furthermore, by utilizing multiple pieces of information related to blockchain type and network conditions, CrossDeFi effectively addresses cross-chain asset transfer challenges and maximizes efficiency.

The ITC strategy assures a transaction finality guarantee for asset transfers by integrating an efficient and secure transfer confirmation process using cryptographic primitives between the involved DeFi systems. This approach not only secures the transfer but also ensures the integrity and finality of transactions, which is critical in financial applications. The prototype-based experimental evaluation demonstrates the performance efficiency of the proposed CrossDeFi in terms of asset transfer accuracy and speed. The asset-specific bridge selection and transfer confirmations in CrossDeFi assist in achieving an asset transfer accuracy of 96% with a reduced delay of 72.5 s even when the network comprises a high number of users. The results clearly indicate that CrossDeFi outperforms existing cross-chain solutions in terms of transfer accuracy and delay under all scenarios without compromising security levels. By providing seamless interoperability and finality guarantees across heterogeneous DeFi networks, CrossDeFi ensures precise and timely asset transfers, thereby enhancing the user experience.

Looking forward, while CrossDeFi has shown significant promise, it has some potential limitations related to privacy and universal bridge design. Enhancing the security features of CrossDeFi can protect asset transfers against a broader range of attacks. The evolving landscape of blockchain technologies presents opportunities for further enhancements of CrossDeFi in the future. Future work could explore scaling solutions to support an even broader range of transactions, extend the applicability of CrossDeFi to additional blockchain platforms, and enhance privacy measures without compromising the security and integrity of asset transfers. Instead of selecting the most suitable bridges, future work aims to design a universal bridge that supports any asset transfer across heterogeneous DeFi systems.

In conclusion, CrossDeFi represents a significant advancement in the field of decentralized finance, offering a robust framework for secure, efficient, and interoperable asset transfers across diverse blockchain systems. As the DeFi ecosystem continues to evolve, the methodologies and insights from this study will undoubtedly contribute to the development of more sophisticated and reliable financial platforms.

Author Contributions: Conceptualization, S.S.M.A.; formal analysis, S.S.M.A.; investigation, S.S.M.A.; methodology, S.S.M.A.; supervision, A.S. and J.Y.; validation, A.S. and J.Y.; writing—original draft, S.S.M.A.; writing—review and editing, S.S.M.A., A.S., and J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by an Australian Government Research Training Program (RTP) scholarship.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Popchev, I.; Radeva, I.; Doukovska, L. Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange. *Electronics* **2023**, *12*, 2244. [CrossRef]
2. Maheshwari, V.; Mani, P. Vulnerabilities and attacks on the blockchain software engineering landscape. *Appl. Comput. Eng.* **2023**, *6*, 422–427. [CrossRef]
3. Renu, S.; Banik, B. Implementation of a secure ride-sharing dapp using smart contracts on ethereum blockchain. *Int. J. Saf. Secur. Eng.* **2021**, *11*, 167–173. [CrossRef]
4. Chen, S.; Li, Q.; Wang, W.; Yang, Y.; Jiang, J. Application of blockchain in the cluster of unmanned aerial vehicles. *IET Blockchain* **2021**, *1*, 33–40. [CrossRef]
5. Zulkepli, M. Leveraging blockchain-based smart contract in Islamic financial institutions: issue and relevant solution. *Int. J. Islam. Econ. Financ. Res.* **2023**, *6*, 18–28. [CrossRef]
6. Dustdar, S.; Fernández, P.; García, J.; Ruiz-Cortés, A. Elastic smart contracts in blockchains. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1901–1912. [CrossRef]
7. Kushwaha, S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H. Ethereum smart contract analysis tools: A systematic review. *IEEE Access* **2022**, *10*, 57037–57062. [CrossRef]
8. Honari, K. Smart contract design in distributed energy systems: a systematic review. *Energies* **2023**, *16*, 4797. [CrossRef]

9. Mohammed Abdul, S.S. Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance. *Blockchains* **2024**, *2*, 265–298. [CrossRef]
10. Renduchintala, T.; Alfauri, H.; Yang, Z.; Pietro, R.; Jain, R. A survey of blockchain applications in the fintech sector. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 185. [CrossRef]
11. Ali, O.; Ally, M.; Dwivedi, Y. The state of play of blockchain technology in the financial services sector: a systematic literature review. *Int. J. Inf. Manag.* **2020**, *54*, 102199. [CrossRef]
12. Wang, X. Research on the application of blockchain technology and smart contracts in the financial industry. *Front. Bus. Econ. Manag.* **2024**, *15*, 392–395. [CrossRef]
13. Mishra, R.; Singh, R.; Kumar, S.; Mangla, S.; Kumar, V. Critical success factors of blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment. *Electron. Commer. Res.* **2023**. [CrossRef]
14. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees. *Technol. Forecast. Soc. Chang.* **2020**, *158*, 120166. [CrossRef]
15. Wu, H. Blockchain for finance: A survey. *IET Blockchain* **2024**, *4*, 101–123. [CrossRef]
16. Lin, Y. Blockchain-driven framework for financing credit in small and medium-sized real estate enterprises. *J. Enterp. Inf. Manag.* **2024**, *37*, 201–229. [CrossRef]
17. Ozili, P.K. Decentralized finance research and developments around the world. *J. Bank. Financ. Technol.* **2022**, *6*, 117–133. [CrossRef]
18. Gramlich, V.; Guggenberger, T.; Principato, M.; Schellinger, B.; Urbach, N. A multivocal literature review of decentralized finance: Current knowledge and future research avenues. *Electron. Mark.* **2023**, *33*, 11. [CrossRef]
19. Abou Jaoude, J.; George Saade, R. Blockchain Applications—Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. [CrossRef]
20. Robinson, P. Survey of crosschain communications protocols. *Comput. Netw.* **2021**, *200*, 108488. [CrossRef]
21. Ou, W.; Huang, S.; Zheng, J.; Zhang, Q.; Zeng, G.; Han, W. An overview on cross-chain: Mechanism, platforms, challenges and advances. *Comput. Netw.* **2022**, *218*, 109378. [CrossRef]
22. Tsepeleva, R.; Korkhov, V. Building DeFi Applications Using Cross-Blockchain Interaction on the Wish Swap Platform. *Computers* **2022**, *11*, 99. [CrossRef]
23. Darshan, M.; Amet, M.; Srivastava, G.; Crichigno, J. An Architecture That Enables Cross-Chain Interoperability for Next-Gen Blockchain Systems. *IEEE Internet Things J.* **2023**, *10*, 18282–18291. [CrossRef]
24. Zhao, Y.; Kang, X.; Li, T.; Chu, C.K.; Wang, H. Toward Trustworthy DeFi Oracles: Past, Present, and Future. *IEEE Access* **2022**, *10*, 60914–60928. [CrossRef]
25. Metronome. DeFi's Leading Synthetic Protocol. 2024. Available online: https://metronome.io/ (accessed on 11 February 2024).
26. Luu, L.; Velner, Y. A Trustless Decentralized Exchange and Payment Service. 2017. Available online: https://whitepaper.io/document/43/kyber-network-whitepaper (accessed on 11 February 2024).
27. Ethereum Foundation. BTC Relay. 2024. Available online: https://github.com/ethereum/btcrelay (accessed on 8 June 2024).
28. Harris, C.G. Cross-Chain Technologies: Challenges and Opportunities for Blockchain Interoperability. In Proceedings of the 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Berlin, Germany, 23–25 July 2023; pp. 1–6. [CrossRef]
29. Zilnieks, V.; Erins, I. Cross-Chain Bridges: A Potential Solution to Standardising Distributed Ledger Technology in Payment Systems. *Inf. Technol. Manag. Sci.* **2023**, *26*, 27–34. [CrossRef]
30. Han, P.; Yan, Z.; Ding, W.; Fei, S.; Wan, Z. A Survey on Cross-chain Technologies. *Distrib. Ledger Technol. Res. Pract.* **2023**, *2*, 15. [CrossRef]
31. Velloso, P.B.; Morales, D.C.; Nguyen, M.T.; Pujolle, G. State of the art: Cross chain communications. In Proceedings of the 2021 5th Cyber Security in Networking Conference (CSNet), Abu Dhabi, United Arab Emirates, 12–14 October 2021; pp. 76–81. [CrossRef]
32. Li, L.; Wu, J.; Cui, W. A review of blockchain cross-chain technology. *IET Blockchain* **2023**, *3*, 149–158. [CrossRef]
33. Alzhrani, F.; Saeedi, K.; Zhao, L. Architectural Patterns for Blockchain Systems and Application Design. *Appl. Sci.* **2023**, *13*, 11533. [CrossRef]
34. Qasse, I.A.; Abu Talib, M.; Nasir, Q. Inter Blockchain Communication: A Survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, 7–9 March 2019; pp. 1–6. [CrossRef]
35. Siris, V.A.; Nikander, P.; Voulgaris, S.; Fotiou, N.; Lagutin, D.; Polyzos, G.C. Interledger Approaches. *IEEE Access* **2019**, *7*, 89948–89966. [CrossRef]
36. Gao, Z.; Li, H.; Xiao, K.; Wang, Q. Cross-chain Oracle Based Data Migration Mechanism in Heterogeneous Blockchains. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, 29 November–1 December 2020; pp. 1263–1268. [CrossRef]
37. Zheng, J.; Chen, Q.; Su, C.; Huang, H. BrokerFi: A DeFi dApp Built upon Broker-based Blockchain. In Proceedings of the 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), Ocean Flower Island, China, 17–21 December 2023; pp. 1817–1825. [CrossRef]
38. Ye, S.; Wang, X.Y.; Xu, C.; Sun, J. BitXHub:Side-relay Chain Based Heterogeneous Blockchain Interoperable Platform. *Comput. Sci.* **2020**, *47*, 294–302. [CrossRef]

39. WeCross: Blockchain Cross-Chain Collaboration Platform. 2020. Available online: https://wecross.readthedocs.io (accessed on 10 February 2024).
40. Buterin, V. Minimal Viable Plasma. 2018. Available online: https://ethresear.ch/t/minimal-viable-plasma/426 (accessed on 30 January 2024).
41. Abbas, H.; Caprolu, M.; Di Pietro, R. Analysis of Polkadot: Architecture, Internals, and Contradictions. *arXiv* **2022**, arXiv:2207.14128. [CrossRef]
42. MyWish Crosschain Swap Service. Available online: https://bridge.mywish.io/ (accessed on 11 March 2024).
43. Ethereum. Available online: https://ethereum.org/en/ (accessed on 11 March 2024).
44. BNB Chain: An Ecosystem of Blockchains. Available online: https://docs.bnbchain.org/ (accessed on 11 March 2024).
45. Han, J.; Kim, J.; Youn, A.; Lee, J.; Chun, Y.; Woo, J.; Hong, J.W.K. Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain. In Proceedings of the 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Tainan, Taiwan, 8–10 September 2021; pp. 303–308. [CrossRef]
46. Barbara, F.; Schifanella, C. BxTB: Cross-chain exchanges of bitcoins for all Bitcoin wrapped tokens. In Proceedings of the 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA, 5–7 September 2022; pp. 143–150. [CrossRef]
47. Marin, O.; Cioara, T.; Anghel, I. Blockchain Solution for Buildings' Multi-Energy Flexibility Trading Using Multi-Token Standards. *Future Internet* **2023**, *15*, 177. [CrossRef]
48. Xiong, A.; Liu, G.; Zhu, Q.; Jing, A.; Loke, S.W. A notary group-based cross-chain mechanism. *Digit. Commun. Netw.* **2022**, *8*, 1059–1067. [CrossRef]
49. Yin, L.; Xu, J.; Tang, Q. Sidechains With Fast Cross-Chain Transfers. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 3925–3940. [CrossRef]
50. Herlihy, M. Atomic Cross-Chain Swaps. In Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham, UK, 23–27 July 2018; pp. 245–254. [CrossRef]
51. Shadab, N.; Houshmand, F.; Lesani, M. Cross-chain Transactions. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–9. [CrossRef]
52. Wang, G.; Nixon, M. InterTrust: Towards an Efficient Blockchain Interoperability Architecture with Trusted Services. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; pp. 150–159. [CrossRef]
53. Pang, Y. A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access* **2020**, *8*, 153719–153730. [CrossRef]
54. Vishwakarma, L.; Kumar, A.; Das, D. CrossLedger: A Pioneer Cross-chain Asset Transfer Protocol. In Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Bangalore, India, 1–4 May 2023; pp. 568–578. [CrossRef]
55. Bugnet, T.; Zamyatin, A. XCC: Theft-Resilient and Collateral-Optimized Cryptocurrency-Backed Assets. Cryptology ePrint Archive, Paper 2022/113. 2022. Available online: https://eprint.iacr.org/2022/113 (accessed on 25 August 2024).
56. Zamyatin, A.; Harz, D.; Lind, J.; Panayiotou, P.; Gervais, A.; Knottenbelt, W. XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 193–210. [CrossRef]
57. Pang, X.; Kong, N.; Chen, Z. AbitBridge: A cross-chain protocol based on main-sub-chain architecture. In Proceedings of the 2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 23–25 September 2022; pp. 99–104. [CrossRef]
58. Muhammad, A.; Kristensen, J. On Cross-chain Pathfinding and Bridge Selection for Decentralized Finance. Available online: https://www.researchgate.net/publication/374950963_On_Cross-chain_Pathfinding_and_Bridge_Selection_for_Decentralized_Finance (accessed on 25 August 2024).
59. Tian, H.; Xue, K.; Luo, X.; Li, S.; Xu, J.; Liu, J.; Zhao, J.; Wei, D.S.L. Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3928–3941. [CrossRef]
60. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-Burn. In *Financial Cryptography and Data Security*; Bonneau, J., Heninger, N., Eds.; Series Title: Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12059, pp. 523–540. [CrossRef]
61. Pillai, B.; Biswas, K.; Hou, Z.; Muthukkumarasamy, V. The Burn-to-Claim cross-blockchain asset transfer protocol. In Proceedings of the 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS), Singapore, 28–31 October 2020; pp. 119–124. [CrossRef]
62. Liu, W.; Wu, H.; Meng, T.; Wang, R.; Wang, Y.; Xu, C.Z. AucSwap: A Vickrey auction modeled decentralized cross-blockchain asset transfer protocol. *J. Syst. Archit.* **2021**, *117*, 102102. [CrossRef]
63. Kiayias, A.; Zindros, D. Proof-of-Work Sidechains. In *Financial Cryptography and Data Security*; Bracciali, A., Clark, J., Pintore, F., Rønne, P.B., Sala, M., Eds.; Series Title: Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 11599, pp. 21–34. [CrossRef]
64. Gaži, P.; Kiayias, A.; Zindros, D. Proof-of-Stake Sidechains. Cryptology ePrint Archive, Paper 2018/1239. 2018. Available online: https://eprint.iacr.org/2018/1239 (accessed on 25 August 2024).

65. Kiayias, A.; Miller, A.; Zindros, D. Non-interactive Proofs of Proof-of-Work. In *Financial Cryptography and Data Security*; Bonneau, J., Heninger, N., Eds.; Series Title: Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12059, pp. 505–522. [CrossRef]
66. Garoffolo, A.; Kaidalov, D.; Oliynykov, R. Zendoo: A zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. *arXiv* **2020**, arXiv:2002.01847. [CrossRef]
67. Sigwart, M.; Frauenthaler, P.; Spanring, C.; Sober, M.; Schulte, S. Decentralized Cross-Blockchain Asset Transfers. *arXiv* **2021**, arXiv:2004.10488. [CrossRef]
68. Sober, M.; Sigwart, M.; Frauenthaler, P.; Spanring, C.; Kobelt, M.; Schulte, S. Decentralized cross-blockchain asset transfers with transfer confirmation. *Clust. Comput.* **2023**, *26*, 2129–2146. [CrossRef]
69. Terra: UST and Terra: Revolutionizing Cross Chain Interoperability. 2024. Available online: https://fastercapital.com/content/Terra--UST-and-Terra--Revolutionizing-Cross-Chain-Interoperability.html (accessed on 5 March 2024).
70. Li, X.; Wang, X.; Kong, T.; Zheng, J.; Luo, M. From Bitcoin to Solana—Innovating Blockchain towards Enterprise Applications. In *Blockchain—ICBC 2021*; Lee, K., Zhang, L.J., Eds.; Series Title: Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2022; Volume 12991, pp. 74–100. [CrossRef]
71. Amores-Sesar, I.; Cachin, C.; Schneider, P. An Analysis of Avalanche Consensus. *arXiv* **2024**, arXiv:2401.02811. [CrossRef]