GURUFIN

Next Generation Layer-1 Hybrid Mainnet

v 1.0.4

JUL 2023

TABLE OF CONTENTS

1. OVERVIEW

Since the launch of the Bitcoin Network in 2009, many projects have proposed innovations to counter challenges facing the new industry. Current limitations of blockchain technology make broad application impractical and can be encapsulated into five main factors:

- Energy Consumption

Consensus mechanisms and the number of nodes required to operate and maintain the network can require a significant amount of computational power, which in turn consumes a large amount of energy.

- Security and Scalability

The design and implementation of algorithms, mechanisms, and degrees of decentralization dictate network reliability. As a blockchain network grows, the network can become congested which leads to slower transaction processing, performance degradation, and higher fees. Without scaling, a network is likely to experience network outage and is more vulnerable to data breaches that may result in irrevocable loss of digital assets.

- Transaction Processing Speed

Block size, consensus algorithm, and network latency can determine the transaction processing speed. Larger block sizes can increase the number of transactions processed in each block, while faster consensus algorithms can reduce the time between block creation. Lower network latency can reduce transaction time but may require additional network infrastructure. Blockchain networks struggle to support large-scale transactions with the reliability and speed that traditional financial institutions provide.

- Decentralization

Decentralization tends to offer better security with slower transaction processing. Contrariwise, centralization tends to be faster with lower security due to a single point of failure. Asynchrony or consensus discrepancy may cause fragmentation, or the creation of uncle blocks that compromise security and efficiency.

- Cost

The degree of decentralization may result in higher energy consumption, utility expenditures, and fees, or require more maintenance infrastructure. Less secure networks may lead to substantial recovery expenditures in the event of an attack.

The architecture of a blockchain may have significant trade-offs to meet the objective of its project and intended users.

NEXT GENERATION LAYER-1 HYBRID MAINNET

The GURUFIN Project presents its technology and concepts to provide a blockchain network alternative that is suitable for general use and encourages mass adoption and participation by addressing the constraints listed above. GuruFin Chain aims to facilitate countless services and business models by converging blockchain technology and traditional payment systems for the real economy and Web 3.0 environment.

1. Blockchain Type
   - Hybrid (Governance Chain, Compliance Chain)
2. Network Scalability
   - Interoperability between Zones (Station Feature)
   - Token Swap Pool
   - ITMT Processing System
3. Fast Speed (10,000+ TPS)
   - Adjustable 1-3 Second Block Creation Time
   - TBFT & DPoS Consensus Algorithms
   - TBFT & PoC Consensus Algorithms
4. ITMT (Inter-Transaction Multi-Transfer) Processing System
   - Generate real-time block records by batching multiple transactions for collective processing
   - Traditional finance integration (e.g., banks, central banks)
5. DARK (Divided Authority and Recovery Key) Security System
   - Patent-pending mnemonic-based multi-signature security recovery system
6. Machine Learning
   - Metadata analysis for personalized recommendation using AI

2. HYBRID BLOCKCHAIN

2.1. Definition

The GuruFin Mainnet constitutes a hybrid blockchain infrastructure that operates through the dualization of the Governance and Compliance Chains. This establishes a comprehensive and robust framework that facilitates efficient governance processing while operating compliance measures that are above current industry standards.

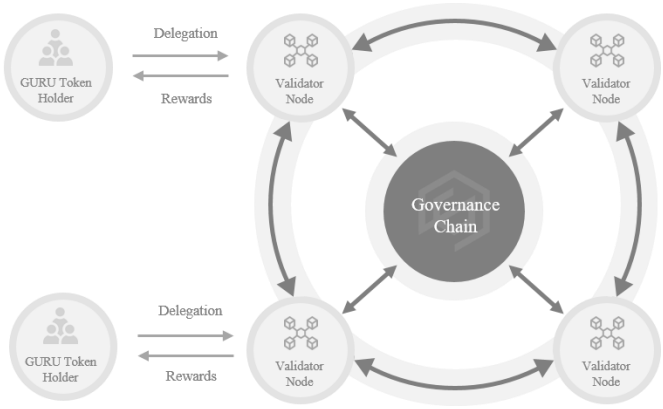
GURU and MU native token conversion is designed to expand the token economy.
Each chain possesses distinct token trading capabilities (refer to 4. Scalability).

2.2 Governance Chain

2.2.1. Definition

The Governance Chain uses the Tendermint Byzantine Fault Tolerance (BFT) and Delegated Proof-of-Stake (DPoS) consensus algorithm. GURU native token is issued to play a central role in creating a decentralized and democratic governance structure to meet user demands. Token holders delegate GURU to vote on proposals and decisions that affect the future development and direction of the network, share rewards with validators, and monitor validator integrity. External entities are encouraged to participate in node operation.

Refer to 3.1. Criteria. Qualified and interested applications can email help@gurufin.com to initiate the process.



[Governance Chain Network Configuration]

2.2.2. Technical Specifications

Consensus Algorithms	Tendermint BFT & DPoS(Delegated Proof-of-Stake)
Native Token	GURU
Block Generation	1-3 Seconds Setting
Gas Limit	∞
TPS	10,000+
Max. Gas Fee	0.013 GURU
Max. Validator Node Operation	100
Memory Pool Size	10,000 Transactions

Max. Transaction Size	3 GB

2.3 Compliance Chain

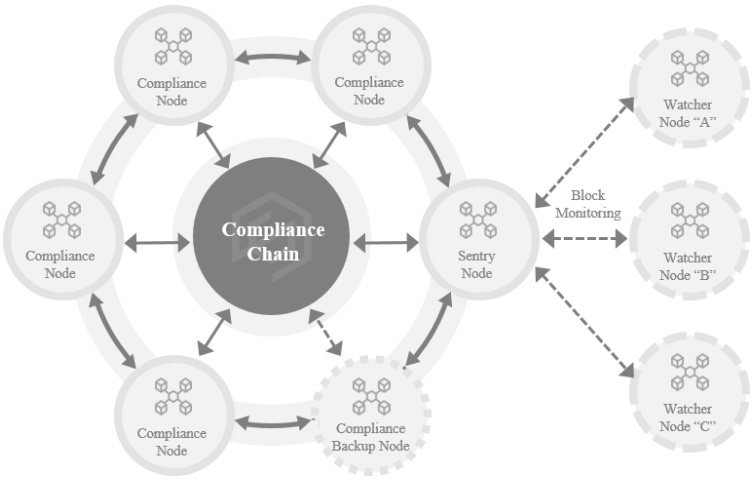
2.3.1 Definition

The Compliance Chain functions as a semi-private chain whereby GuruFin operates the Compliance and Sentry Nodes while the operation and delegation of Watcher Nodes are open to external entities. By employing the Tendermint BFT and Proof-of-Compliance (PoC) consensus algorithms, the network achieves streamlined transaction processing with remarkably low gas fees.

Upon receiving a transaction request, Compliance Nodes assume the responsibility of generating and validating blocks. Blocks are added to the Compliance Chain and monitored by Sentry Nodes for data integrity and potential corruption. Sentry Nodes share information with Watcher Nodes, upholding safeguards against potential threats.

Furthermore, the Compliance Chain provides a conducive environment for decentralized applications (dApps) and smart contracts by integrating the Ethereum Virtual Machine (EVM). This integration allows for seamless deployment and execution of smart contracts written in Turing-complete programming languages, facilitating effortless migration to the Compliance Chain without requiring code modifications.

One notable feature of the Compliance Chain is the issuance of the MU native fiat-backed stable token, which maintains a 1 MU : 1 USD peg and undergoes real-time auditing. The MU token serves as a utility token, bridging the gap between traditional finance and the broader GuruFin Ecosystem. It provides investors with a stable store of value and enables users to mitigate risks associated with cryptocurrency volatility. In addition to the MU token, the Compliance Chain also supports the issuance of ERC-20 and ERC-721 tokens.



[Compliance Chain Network Configuration]

2.3.2. Node Types

- **Compliance Node**

The Compliance Node is the core entity responsible for operating the network and adhering to Compliance regulations. It performs the role of generating and verifying blocks through the Tendermint BFT and PoC consensus algorithm among Compliance Nodes to process trusted transactions. There are four active Compliance Nodes and one safeguard backup node.

- **Sentry Node**

The Sentry Node acts as a buffer for the Compliance Nodes from external attacks and transmits data to the Watcher Node. It supports the monitoring and verification of the Compliance Chain through synchronized block data.

- **Watcher Node**

The Watcher Node is located on an external network and performs the role of supervising Compliance Node operations. Working in conjunction with the Sentry Node, it oversees block integrity and data corruption generated by Compliance Nodes. GURU is rewarded for participating as a monitor in the Compliance Network. Refer to 3.1 for the Watcher Node Operation Criteria. Qualified and interested applications can email help@gurufin.com to initiate the process.

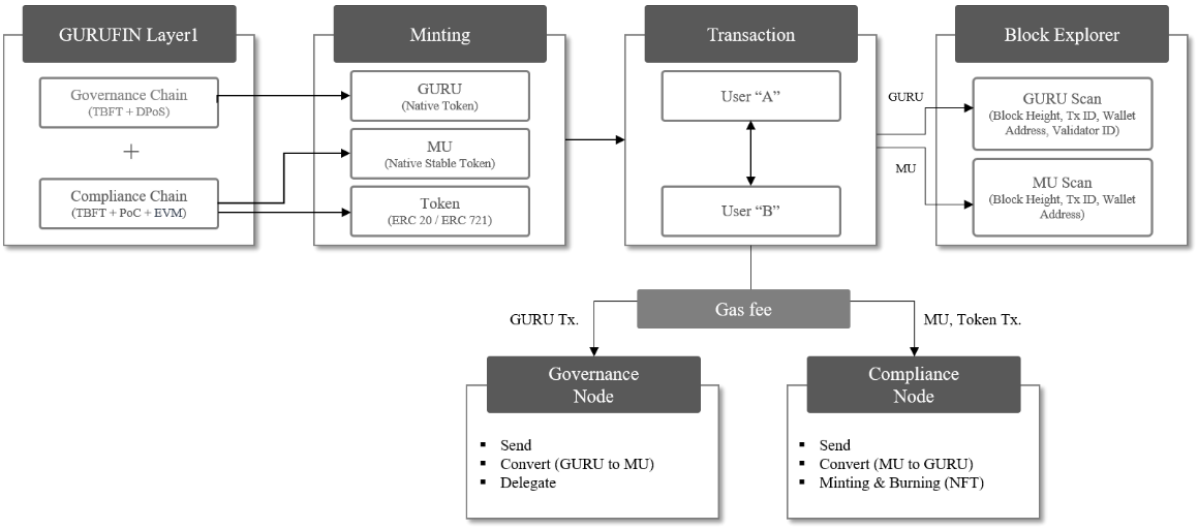
2.3.3. Technical Specifications

Consensus Algorithms	Tendermint BFT, PoC(Proof-of-Compliance)
Native Stable Token	MU
Block Generation	1-3 Seconds Setting
Gas Limit	∞
TPS	10,000+
Min. Gas Fee	0.000032 MU
Max. Planned Node Operations	5 Compliance 3+ Sentry ∞ Watcher
Memory Pool Size	10,000 Transactions
Max. Transaction Size	3 GB

2.4 Transactions

A block is generated and recorded on the blockchain network when a transaction occurs.

- Issuance / Minting
  - Governance Chain: GURU
  - Compliance Chain: MU / ERC-20 / ERC-721
- Conversions
  - GURU ⇔ MU ⇔ ERC-20
  - GURU ⇔ ERC-20
- Gas Fee
  - Fees incurred during transactions are deducted from the sender's fungible token balance.
  - ERC-20 and ERC-721 token transactions use MU for gas fees.



[Transaction Process]

Guru Scan is the GuruFin Governance Chain block explorer and Mu Scan is the GuruFin Compliance Chain block explorer. These block explorers display transaction details, checks the current state of the network, and shows other relevant information. Users can search for specific transactions, addresses, or blocks within the blockchain.

3. VALIDATORS

Elected Validator Nodes are rewarded for participating in the consensus protocol by providing cryptographic signatures or votes to commit new blocks on the blockchain. The voting power of a validator is directly proportional to the amount of GURU Tokens delegated to them. A limit of 100 active validators is elected to partake in the consensus process. If the number of active validators surpasses this threshold, the selection of

elected validators occurs based on their voting power. Active validators not elected are placed in a queue and can replace jailed validators or increase their delegated GURU Token to move up the queue.

3.1 Criteria

	Governance Chain	Compliance Chain
GENERAL	• Node Name: Validator Node • Officially registered with GuruFin Foundation • Min. 3,000,000 GURU delegated • Maintain a stable internet connection	• Node Name: Compliance Node • Officially registered with GuruFin Foundation • Min. 300,000 GURU delegated • Maintain a stable internet connection
HARDWARE	• 4+ CPU cores • Min. 500GB of SSD disk storage • Min. 16GB of memory (RAM) • Min. 100 mbps network bandwidth	• 8+ CPU cores • Min. 500GB of SSD disk storage • Min. 16GB of memory (RAM) • Min. 100 mbps network bandwidth
SOFTWARE	• Darwin/arm64 • Darwin/x86_64 • Linux/arm64 • Linux/ard64 • Windows/x86_64	

3.2 Penalty

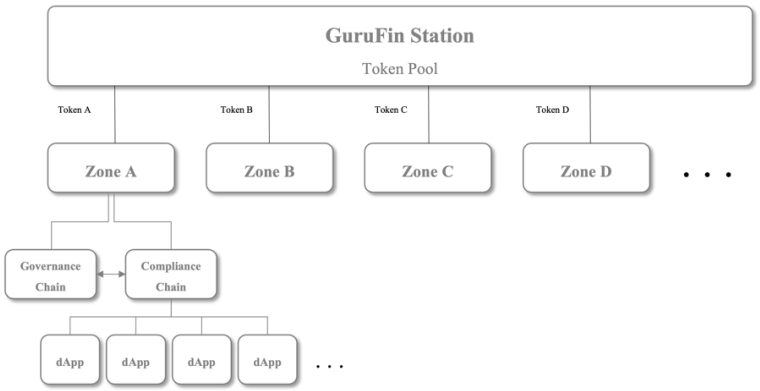
Penalties are enforced on validators deviating from the approved network protocol. An elected validator is jailed and suffers fund deductions if it does not commit votes for at least $500/10{,}000$ blocks or double signs a block. Regardless of the number of elected or jailed validators, there is a consistent ratio for network operation due to the TBFT consensus.

$$(Elected - Jailed)\ 2/3 = \text{Network Operation}$$
$$(Elected - Jailed)\ 1/3 = \text{Network Failure}$$

Jailed validators can formally petition for reactivation. Queued validators are not subject to penalties if they fail to meet the predetermined criteria.

4. SCALABILITY

Projects can leverage the GuruFin SDK to create independent chains (or 'Zones'). Zones have the autonomy to create unique ecosystems, protocols, and tokens within the broader GuruFin Ecosystem. By having control over the token infrastructure, projects can design and implement custom tokenomics models that align with their business models and ecosystem dynamics. APIs are provided for interoperability, allowing communication between Zones through the Station. GuruFin plans to expand the ecosystem by opening IBC channels to communicate between GuruFin Station and Cosmos Hub.



The GuruFin Station is designed to add networks horizontally for indefinite ecosystem expansion and participants are encouraged to leverage shared resources and capabilities.

The Station has a Token Pool managed by smart contracts. Tokens issued by different Zones can be exchanged with GURU and vice versa. This feature uses the Target Price Market Maker (TPMM) model to maintain a target price for listed tokens in the pool, rather than a constant ratio or sum. Entities that have issued unlisted tokens can participate in the Token Pool if approved by the GuruFin Foundation. Each Zone can integrate one or both hybrid chains, which come with several benefits.

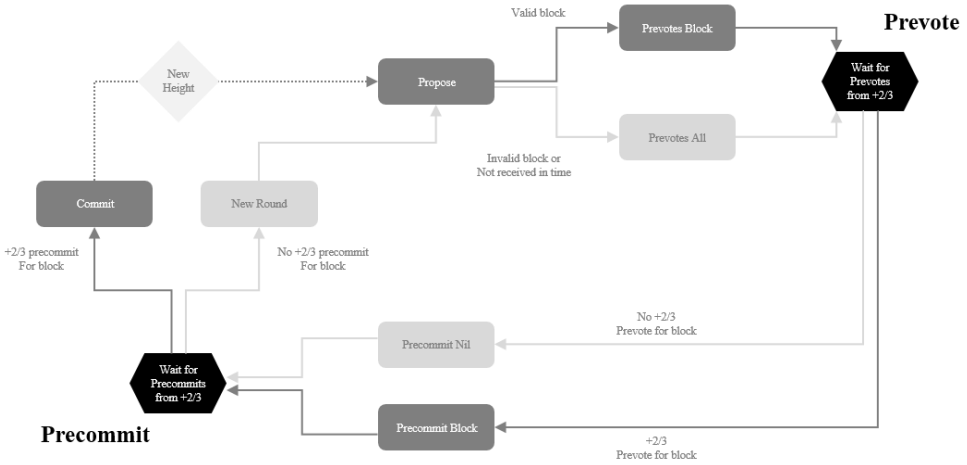
The Governance Chain issues the GURU native token, which serve as a fundamental currency utilized across the core GuruFin dApps. By accepting transactions in GURU, users can conveniently transact within the ecosystem without the need for token exchanges or conversions. This streamlined process enhances user experience and reduces friction in conducting financial activities.

The Compliance Chain fulfills the pivotal role of issuing MU, as well as tokens compliant with the ERC-20 and ERC-721 standards. This issuance occurs through the implementation of smart contracts for security and integrity in the token issuance and transaction processes. Projects can deposit 1 USD : 1 MU to use MU token in its ecosystem. The linking value provides users with the stability and transparency that GuruFin Chain offers.

Projects have the flexibility to create a business model that benefits its users, developers, and stakeholders.

5. CONSENSUS ALGORITHM

The Tendermint BFT consensus algorithm provides high throughput and low latency. Each process mandates votes from at least two-thirds of the validators to proceed to the next stage. This allows up to one-thirds of the validators to simultaneously fail or behave maliciously without network failure or delays. Majority consensus enhances the network's defense, stable block creation, and transaction finality to minimize the generation of uncle blocks.



[Consensus Algorithm Process]

PROCESS

1. Proposal
   A validator initiates a block proposal that contains transaction data.
2. Prevote
   Other validators receive the proposal then broadcast their prevote messages, indicating the assessment of the block's validity.
3. Precommit
   Once the validator has received prevotes from at least two-thirds of the validators, a precommit message is broadcasted to confirm the validation of the proposed block.
4. Commit
   Once two-thirds of validators have precommitted to the proposal, the block is committed to the blockchain. Validators apply the state transitions from the committed block.
5. Validation
   Validators continuously check the blockchain for validity. If an invalid block is detected, they can vote to slash the stake of the validator who proposed the invalid block.

The next validator to propose a block is determined by a weighted round-robin algorithm.

6. OPTIMIZATION

6.1 Block Generation

Tendermint block generation time is adjustable and applicable to the hybrid chain within a network. The process involves prevote and precommit timeouts set at 1 second, while the final block commit time can be adjusted between 1 to 3 seconds. Below is the formula to calculate the annual block generation time:

$$Uint64(60 \times 60 \times 8766\ )\ per\ Second$$

10,519,200 to 31,557,600 Blocks Generated Annually

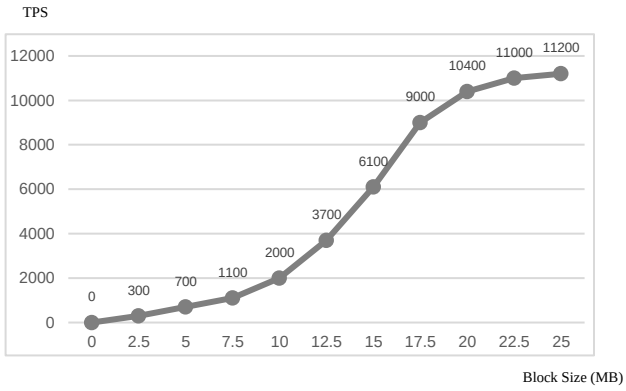
However, the drawback of a shorter generation time is the increase in empty block creations, which demands high energy consumption for nodes to synchronize block data. It is recommended to adjust the block generation time in relation to the TPS necessary to optimize the node operation of a network.

6.2 Transactions

Tendermint P2P (peer-to-peer) protocol offers adjustable parameters that can be customized to suit specific requirements. The message payload size is set to 10,240 bytes and transmits 5,120,000 packet bytes. Each validator receives transaction processing requests and is responsible for loading these transactions into its own memory pool for further processing. The number of transactions processed per second can be increased by modifying the memory pool size of each node to 10,000 transactions and controlling the maximum block size to 22,020,096 bytes. Operating multiple trusted nodes contributes to the scalability of the network and process large transaction volumes.

6.3 Performance Criteria and Indicators

Node Operation	5 Nodes
Total Memory Pool	3GB
Block Size	22M
Assumed Transaction Size of 2K	(10,000 +) TPS



7. SYSTEM ARCHITECTURE

dApp Services

- ITMT Processing System
  - Airdrop
  - Simultaneous Execution of Multi-Transactions to Multi-Recipients
- Proof-of-Content
  - NFT Metadata
- Certification of Ownership
  - NFT+
- Payment Service Provider (PSP)
  - Credit Card
  - Carrier Billing
  - MU Native Fiat-backed Stable Token

Core Platform

- GuruFin Wallet
  - GURU Wallet for GURU Token
  - MU Wallet for MU, ERC-20, ERC-721
- Blockchain Explorers
  - Guru Scan for Governance Chain
  - Mu Scan for Compliance Chain
- NFTs
  - Digigooz B2C Storefront
  - Digigooz C2C Marketplace
  - Gamegooz Game Item NFTs
  - Musicgooz Music-related NFTs
- FTO / DAO
  - Linktory Web 3.0 FTO Community

Data Security

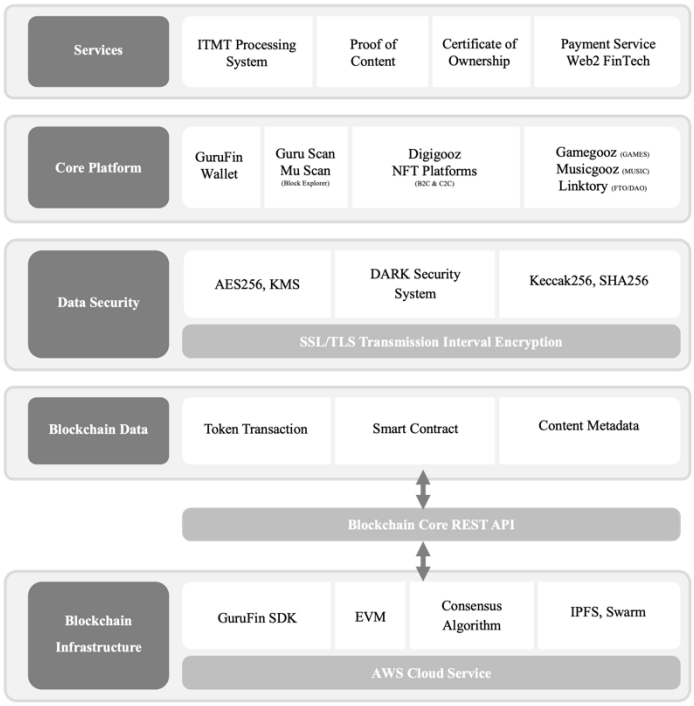
- AES256, KMS
  - AES256 encryption algorithm for strong cryptographic protection
  - KMS for secure generation, storage, and management of encryption keys
- DARK Security System
  - Mnemonic-based multi-signature system
  - Dual-seed or key-splitting process
- Keccak256, SHA256
  - Cryptographic hash functions that produce fixed-size outputs

Block Data

- Token Transactions
- Smart Contract
- Metadata
  - NFT Content
  - User Profile
  - User Behavior

Blockchain Infrastructure

- GuruFin SDK
- EVM Integration
- Consensus Algorithms
- IPFS/Swarm, AWS Cloud Service
- Decentralized, distributed file storage



8. GURUFIN WALLET

8.1 Introduction

GuruFin Wallet consists of two separate digital wallets that allow its users to securely store and manage GURU, ERC-20, and ERC-721 tokens.

GURU Wallet:

Register as a GuruFin Wallet member and pass the KYC verification to create a GURU Wallet. Choose a mnemonic word required to make GURU transactions (refer to Section 9).

MU Wallet:

Register as a GuruFin Wallet member to create a MU Wallet. ERC-20 tokens issued through a Compliance Chain can be registered on the wallet to trade for GURU or MU. NFTs issued through GuruFin Chain can be managed and transferred through the wallet or traded on the GuruFin native Digigooz Web2 and Web3 Storefront or NFT marketplace platform.

8.2 Features

Function	GURU	MU	NFT	Notes
Wallet Address	O	O	X	Requires a MU Wallet
Transfer	O	O	O	
Convert	O	O	X	GURU and MU Trading Optional
Buy	O	O	X	
Delegation	O	X	X	
Vote	O	X	X	
Rewards	O	X	X	
WalletConnect	X	O		

8.3 Platform Security and Advantages

The platform applies the DARK Security System and multi-factor authentication (MFA) to elevate the standard of wallet security and user experience.

DARK Security System:

Other hierarchical deterministic wallets store private keys as a mnemonic phrase, where users must import 12 to 24 words in a specific array. A data breach or neglect to manage the mnemonic phrase may result in permanent loss of access to wallets and funds. With GuruFin Wallet's DARK System, private keys store 23 words and can only be recovered with one mnemonic word. This heightens wallet security and user recollection.

MFA:

Members can access their wallets on any compatible device, even if the original login device is lost due to the security measures in place. To prevent unauthorized access, only one device may be logged in at one time.

GuruFin Wallet: General Access

- Login Credentials
  - Email ID
  - Password

GURU Wallet: GURU Token Transactions

- Mnemonic Word

MU Wallet: MU, ERC-20, ERC-721 Token Transactions

- Passcode

Membership Benefits:

- Purchase GURU and MU with fiat currency
- Receive rewards through node delegation
- Exchange tokens issued on GuruFin Chain
- Confirm transactions, including ERC-721 tokens purchased from Digigooz

9. DARK (Divided Authority and Recovery Key) SECURITY SYSTEM

9.1 Background

All transaction information on the blockchain is recorded in blocks requiring a signature performed by a valid digital key. Digital keys consist of a pair of public and private keys, of which the latter is typically stored in a digital wallet.

Non-deterministic wallets are collections of random private keys that its users must generate each use. Users are left to manage, back up, and import each key to access their wallets and the funds they control. On the contrary, a hierarchical deterministic (HD) wallet has related private keys that originate from the same key (or the 'seed'). This mechanism creates a tree structure by allowing the parent key to derive the sequence of child keys, each of which can then derive the sequence of grandchild keys. This structure was proposed and defined by the BIP32 standard and improved in BIP44.

- BIP44 Tree Structure

  m / purpose'/ coin_type'/ account'/ change/ address_index

Level-1 (purpose): Set to 44

Level-2 (coin_type): Specifies the type of cryptocurrency

The standard document SLIP0044 defines several currencies, and each currency allows for its own sub-tree of wallets. E.g., Ethereum is m/44'/60' and the testnet for all currencies is m/44'/1'.

Level-3 (account): Allows users to further subdivide wallets into separate sub-accounts or 'multi-accounts'

E.g., An HD wallet can contain two Bitcoin accounts such as m/44'/0'/0' and m/44'/0'/1'. Each account is the root of its own sub-tree.

Level-4 (change): Specifies between a normal and change account

BIP44 contains a quirk unrelated to Ethereum. HD wallets have two sub-trees, deposit and change. However, Ethereum does not require a change level, always using the 'deposit' path which is 0. While the previous levels used hardened derivation, this level uses non-hardened derivation to export extended public keys at the account level for use in non-secure environments.

Level-5 (address_index): Creates available address indexes

E.g., The third deposit address for Ethereum payments is the primary account m/44’/60’/0’/0/2. This is the child of the Level-4 derivation in the HD wallet.

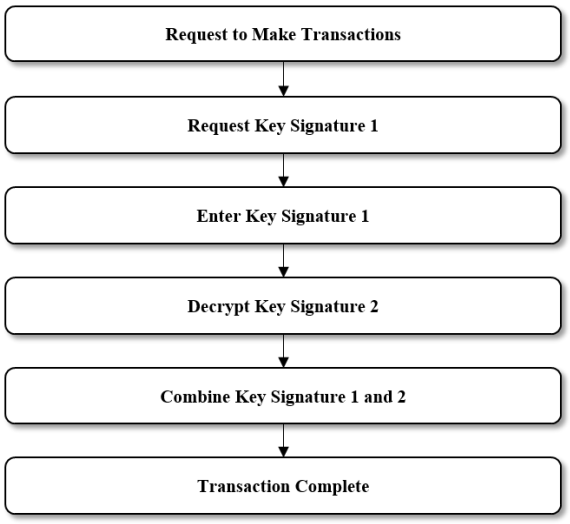
There are several advantages to using an HD compared to a non-deterministic wallet. The tree structure can express structural meaning by assigning different branches for deposits, withdrawals, departments, subsidiaries, or accounting. Users can generate a sequence of public keys to use the wallet on insecure servers or as view and receive-only. However, users are required to generate a private key and memorize a mnemonic phrase of 12 to 24 words in a specific array to access the wallet and move funds.

GuruFin presents its solution: DARK (Divided Authority and Recovery Key) Security System.

9.2 Definition

DARK is patent-pending technology that applies a mnemonic-based multi-signature authentication method to the GURU Wallet. Users are prompted to choose **one** of the randomly generated 24 words to create and encrypt their mnemonic.
The chosen word (or ‘mnemonic word’) generates the first signature key and is stored by the user. The remaining 23 words are generated as the second signature key and stored in the system. This is referred to as the dual-seed (or ‘key-splitting’) process.

Traditional mnemonics phrases encrypt a 12-to-24-word sequence with a single centralized encryption key, which heightens the chance of being hacked and its assets stolen. Furthermore, users have the disadvantage of having to remember the number and array of words in the sequence. Forgotten mnemonics result in irrevocable loss of assets.



9.3 Mnemonic Generation Process

Step S10: Entropy Generation
Entropy is a randomly generated digital code that is difficult to recognize or record.

Step S20: Binary Code Conversion
One character of entropy is converted to a four-digital binary number resulting in a dataset of 256 bits.

Step S30: Hashing
Entropy can be hashed using the SHA256 algorithm, then added as a checksum at the end of a binary code. An 8-digit binary value of the hash value can be added to the end of the binary code as a binary code. The subset of data added to the end can serve as a checksum.
Step S40: Decimal Conversion
A binary code with the added checksum can be converted to decimal.
E.g., A 264-digit binary code with an added checksum can be divided into 24 groups of 11 bits and converted to decimal.

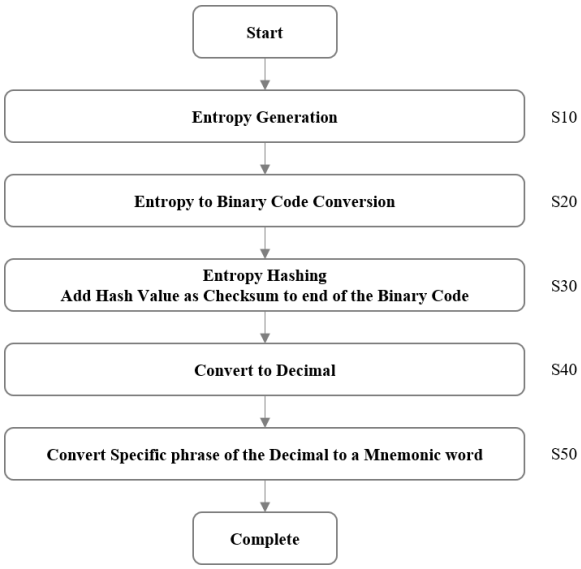
Step S50: Mnemonic Word Conversion
A particular syntax of the converted decimal can be converted into a word. Each word corresponds to a number in the converted decimal that can be replaced with one of the 2048 words in the mnemonic word list. Words included in the list may be predetermined words in compliance with the Bitcoin Improvement Proposals (BIPs).

A digital wallet will generate random words to present to the user. The user chooses a mnemonic word to create and encrypt the mnemonic.

The ideal mnemonic word list should be encoded in UTF-8 using NFKD
(Normalization Form Compatibility Decomposition) and have the following characteristics:

(1) Clearly identifiable by entering the first four characters
Similar words should be avoided.
E.g., Word pairs such as “build” and “built,” “woman” and “women,” and “quick” and “quickly” are difficult to remember and more prone to errors.

(2) Sorted for efficient search of words
E.g., If implemented as programming codes, binary search has the advantage of being available over linear search.



10. PERSONALIZATION

10.1 Overview and Process

Up to Depth 10 of metadata can be extracted from NFTs, user profile, and user behavior for in-depth analysis and insight on NFT transactions and user engagement. By employing advanced analytics techniques, patterns and trends can be identified to personalize and optimize marketing strategies. This analysis is conducted with the goal of enhancing the overall user experience and ultimately driving revenue of NFT-related projects.

Through data mining, marketers can gain valuable insight into user preferences, interests, and behaviors. This information enables the creation of tailored marketing campaigns that resonate with the target audience, increasing the likelihood of user engagement and conversion. By personalizing marketing efforts, users are more likely to discover NFTs and projects that align with their interests, fostering a stronger connection between users and the NFT ecosystem.

GuruFin adhere to strict privacy guidelines and regulations such as the General Data Protection Regulation (GDPR) in the European Union regarding data management. Data is anonymized to ensure the protection of individual identities to maintain user privacy. Compliance with GDPR safeguards against potential misuse or unauthorized access to personal information.

Categories		Properties			
Collection	Item Name	Game	Genre	Color	Clothing
		Sports	Grade	Skin	Body
		Collectable	Characteristics	Vibe	Face
		Goods	Shape	Situation	Hands
		Arts	Country of origin	Artist	Leg
		Music	Manufacturing date	Hair	Etc.

Data of user Profiles	Age	Data of user action	Purchase History
	Gender		Keywords of interest
	Region		Shopping basket info.
	Mobile		Etc.
	Email		

[Extracted Metadata]

Data Collection and Machine Learning Process:

Step 1: Collect user profile data generated on the NFT platform.
Step 2: The data is preprocessed and converted to a key-value pair format. Data mining removes missing values and outliers, and categorical data is converted to numeric data through encoding.
Step 3: Machine and deep learning is applied to the preprocessed data to develop a hybrid model that combines collaborative and content-based filtering. Deep learning models such as Multilayer Perceptron, Convolutional Neural Network, and Recurrent Neural Network are used to personalized recommendations.
Step 4: Personalization and optimization is evaluated using precision, recall, and F1- score metrics. The model structure, hyperparameter, or preprocessing method may be adjusted for necessary improvements.
Step 5: User profile data identifies user preference to provide personalized advertisements.

10.2 Features

GuruFin aims to provide a personalized advertising experience while prioritizing personal data security:

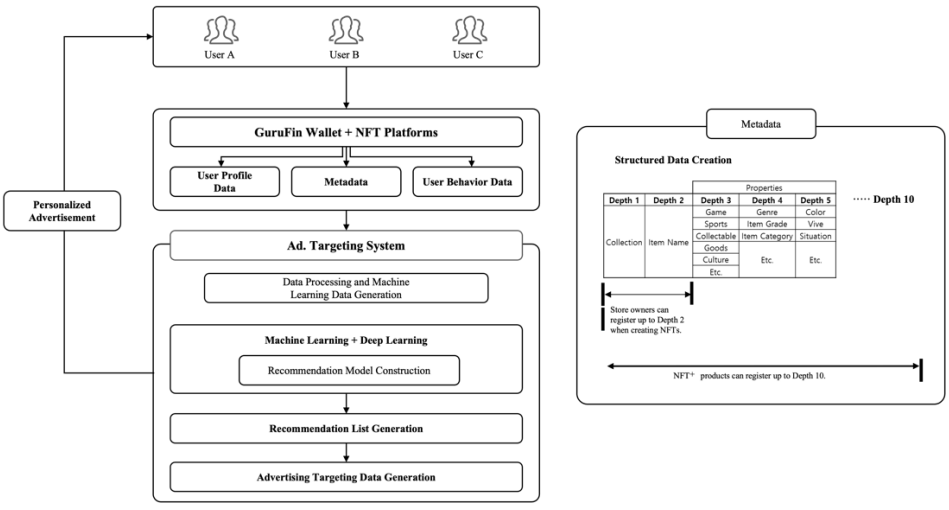
- Data Mining
  - Analyze up to Depth 10 of extracted metadata from NFT transactions, user profiles, and user behavior
  - Insight into user preferences, interests, and behaviors
  - Tailored advertisements for more relevant and engaging advertising experience

- Deep Learning-based Recommendation Algorithm
  - Process extracted metadata to generate accurate and personalized user recommendations
- Personal Data Security
  - Processing Policy
    - Agree to the collection and use of personal data in accordance with the GuruFin Privacy Policy to use the GuruFin Network
  - Data Encryption

    Data used for personalization is encrypted and stored in adherence to the General Data Protection Regulation (GDPR) in EU law. Personal data is **anonymized** to prevent sensitive information leakage.
  - Updates

    Continuous monitoring of security vulnerabilities and potential threats is conducted to improve security maintenance and updates.
  - Audit Logs

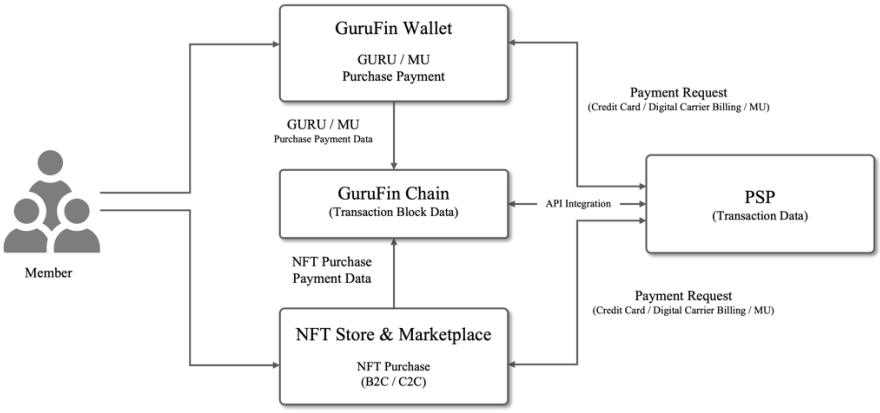
    User and administrator activity is recorded to detect illegal access and tampering.



[Personalized Recommendation System Processing]

11. PAYMENT SYSTEM

The integration of a traditional Payment Service Provider (PSP) into the GuruFin System brings seamless purchasing capabilities to consumers within the Web 3.0 environment. This integration allows users to conveniently acquire GURU, MU, ERC-20, and ERC-721 tokens using various payment methods for fiat currency transactions. The availability of fiat currency transactions enables users to purchase tokens directly, eliminating the need for additional steps such as downloading decentralized finance (DeFi) applications or converting fiat to cryptocurrency before engaging with the Web 3.0 ecosystem. By accepting payment instruments such as cards and carrier billing, the system simplifies the purchasing process and reduces the entry barrier for individuals who may be interested in Web 3.0 but feel intimidated by its complexities.
By incorporating a real economy PSP, the GuruFin System ensures a secure and reliable payment process. Users can confidently transact knowing that their payment information is handled by a trusted and regulated PSP, adhering to industry standards and security protocols. Furthermore, the integration with the blockchain ensures that every purchase, along with its details, is recorded for a verifiable and auditable history of transactions.



[PSP Integration and Payment System Structure]

12. ITMT (Inter-Transaction Multi-Transfer) PROCESSING SYSTEM

12.1 Background

Traditional finance provides countless remittance services by means of banks, money transfer operators, and payment processors through an extensive network of agents, correspondent banks, and regulatory frameworks that facilitate smooth flow of funds across borders. The experience and established relationship with regulatory bodies help navigate compliance requirements and ensure secure execution of transactions. However, the existing banking system incurs high fees and significant security costs to cope with data integrity and tampering during inter-bank fund transfers. Also, there are communication and network participation costs to connect to inter-bank transaction networks. In order to maintain the system, complex system development and configuration are necessary, leading to ongoing expensive operational costs. As a result, blockchain technology is piquing the interest in the traditional finance sector.

Blockchains can provide transparent and immutable transaction records that minimize the risk of fraud and improve accountability, with lower transaction fees. The reluctance of widespread adoption and acceptance of decentralized finance is due to its nascence, which poses challenges regarding interoperability and scalability with existing financial networks. For example, the volume of remittance transactions corresponds with the time consumed for block creation and transaction signature recording. Even if the block creation time takes 1 second, 100,000 transactions would require approximately 27 hours and 27 minutes to complete. Many blockchains have a block creation time ranging from 5 to 30 seconds, making decentralized finance a nonviable option for remittance processing.

Bridging the Gap: Integrating GuruFin Technology into Traditional Finance

GuruFin’s patent-pending Inter-Transaction Multi-Transfer (ITMT) Processing System addresses these issues by enabling simultaneous transfers to multiple payees. The ITMT Processing System records multiple transaction lists in a smart contract of an entire node system in advance and generates transactions for remittances simultaneously when the predefined conditions are met. This reduces the processing time and costs for large volumes and amounts of remittance transactions normally seen in traditional finance and airdrops.

GuruFin has also designed a comprehensive remittance system that works in tandem with blockchain technology to meet the standard of approval in the traditional banking industry, expanding the benefits of the ITMT Processing System into the traditional finance sector. The combination of

PoC and ITMT technology increases transparency and reduce vulnerabilities to fraud in banking systems through the adoption of blockchain technology devised for partial or complete transition to decentralization.

12.2 Traditional Bank Transfer Methods

Bank transfers can be categorized into two main types: bulk and fast transfers. Bulk transfers are primarily used to handle large-scale transactions, including interbank transfers, international transactions, and government-related transactions. This is typically facilitated through central entities like central banks or clearinghouses.

Fast transfer methods enable nearly real-time payment and settlement services, available round the clock. This ensures that payment instructions from the payer and the receipt of funds by the payee occur almost instantly. Fast transfers can be further classified into Deferred Net Settlement (DNS) and Real-Time Gross Settlement (RTGS) methods.
DNS involves accumulating multiple transactions at a clearinghouse for process in regular intervals at designated times. While DNS can help save system resources and costs, it may result in payment delays due to the lack of real-time processing. As a result, DNS is excluded from the scope of applications requiring real-time processing. RTGS processes transactions as occurs. Each transaction is individually processed in real-time, leading to faster transaction processing for swift fund transfers but with higher costs and resources. Private institution and central bank operations apply this method.

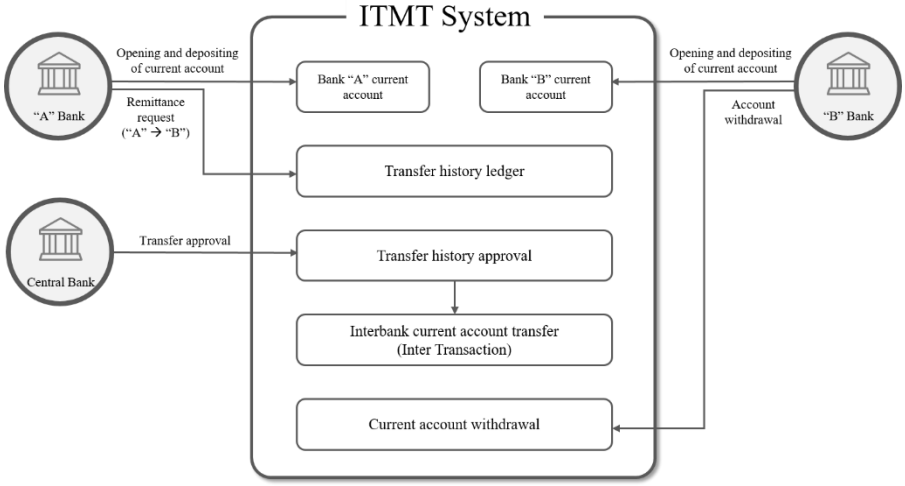
12.3 GURUFIN'S ITMT (Inter-Transaction Multi-Transfer) System

GuruFin's ITMT technology securely records transaction data on the blockchain using contract-based technology, with approved functionalities and conditions required by banking institutions for remittance services. This design leverages blockchain technology to enhance transparency in transaction management and vulnerabilities mitigation to fraud present in traditional finance. Extensive analysis of existing money transfer system has been used to design the framework.

The PoC and ITMT mechanisms have been applied to the RTGS method to ensure both the speed and stability of transaction processing while striking a balance in the degree of decentralization. PoC serves as an authentication algorithm that adhere to financial regulatory requirements. If regulatory requirements are not met, transactions are not processed. ITMT is a technology that enables the simultaneous processing of single and multiple transactions, allowing for the cost-effective technology capable of handling a large volume of transactions.

ITMT Processing System employs a ledger-based bookkeeping structure to record bulk transactions. It maps the ledger status data and constructs a key list array encompassing the entire list of payees, enabling cyclic remittance. Funds are transferred in a cycle between multiple parties for efficient and automated distribution of funds among a group of recipients. Each payee entry undergoes validation of their address and corresponding amount. Subsequently, an entry is created to encompass the total amount and information of each payee.

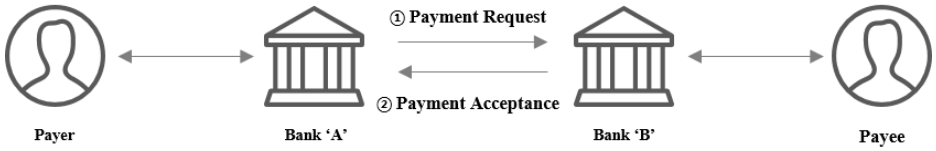
Once the construction of remittance entries is finalized, the approval process for remittance can be verified during the external audit period. The circular transfer between bank accounts commences for the entire remittance. Following the predetermined order within the entry, the system continuously transfers funds, flagging any failed remittance values separately. Ultimately, the total remittance amount is calculated and recorded on the blockchain. After remittance completion, each bank can synchronize its accounts with the existing bank system through their individual account withdrawal processes.



[Diagram 1: ITMT Process]

Bank ‘A’ receives a transfer request from the Payer ‘A’. This request is recorded in a ledger as state data within a mapping structure. A key list array of all payees is constructed to facilitate the implementation of cyclical transfers. When a new Payee is added to the list, the Bank ‘A’ conducts verification to ensure the validity of the Payee’s address, confirming the ability to receive funds. Subsequently, the Payee’s address and corresponding amount are recorded to generate the Payee entry. Furthermore, an entry is created to capture the total amount, relevant information, and individual amounts for each Payee.

Once the entry construction is finalized, Bank ‘A’ initiates the transfer by sending the entire transaction, following the order of the entries, to Bank ‘B’. This transfer request is made using the "① Payment Request." Subsequently, Bank ‘B’ approves the contract conditions received from Bank ‘A’ and finalizes the transfer by issuing a "② Payment Acceptance" request. In cases where any transfers fail, the respective values are added to the entry, and the final block is generated as a GuruFin block, concluding the process [Diagram 2].



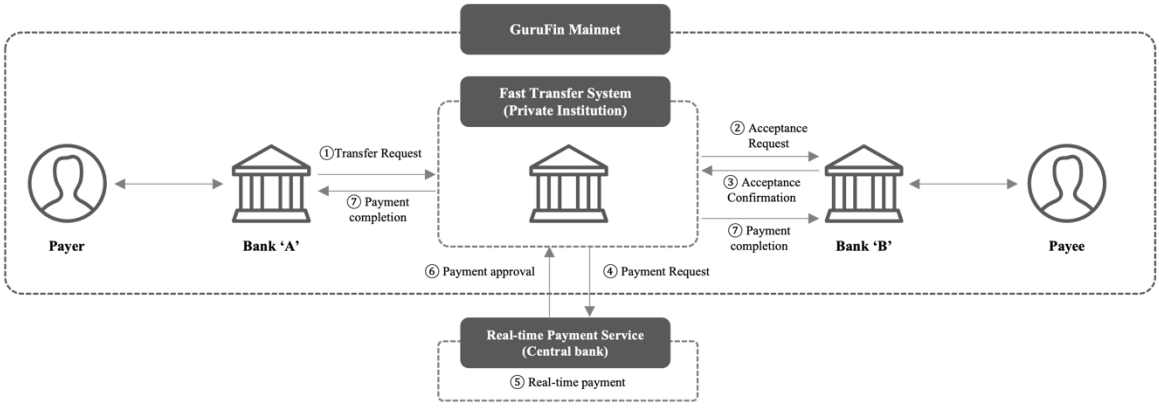
[Diagram 2: GuruFin Mainnet and Interbank Transactions]

12.3.1. Partial Decentralization through Private Institutions

[Diagram 3] and [Diagram 4] present two methods for notifying interbank transfers through a private institution.

[Diagram 3] Bank ‘A’ and ‘B’ are exempt from central bank protocol for payment completion notifications. Compliance lies solely in requirements set by the private institution. While this approach offers advantages in terms of management and cost, the central bank does not directly transmit payment completion notifications to individual banks. Instead, the central bank sends notifications to the private institution, which is then forwarded to the respective banks. This process ensures a comprehensive conclusion with an additional step.

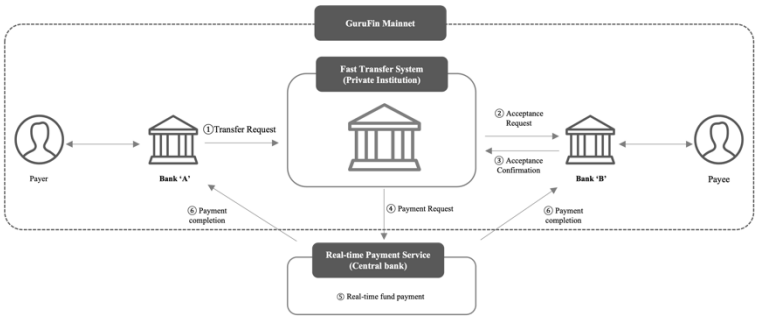
[Diagram 4] The central bank does not need to modify the transmission protocol. This allows for a straightforward adoption process with private institutions and banks in a country with different operation agreements.
In both diagrams, when the Payer initiates a payment request, Bank ‘A’ processes the first and second transactions using the same method as the direct interbank transfers by utilizing the ITMT System. Once the entire transfer entry is finalized, Bank ‘A’ sends a "① Transfer Request" message to Bank ‘B’ through the private institution to indicate the completion of the overall transfer. The private institution follows a sequential mapping process of the payment ledger based on the predefined order received from Bank ‘A.’ It then reconfigures the mapping structure as ledger state data for each bank. Then the private institution sends a "② Acceptance Request" to each bank. Once the private institution receives the "③ Acceptance Confirmation" from Bank ‘B’, the contract conditions are approved, and the transaction is considered complete.



[Diagram 3: GuruFin Mainnet and Private Institutions and Banks – Case 1]

In this scenario, steps ④, ⑤, and ⑥ follow the central bank protocol, as depicted in [Diagram 1]. If a "⑦ Payment Completion" is issued through a private bank, the private institution forwards a "④ Payment Request" to the central bank. The central bank then handles the "⑤ Real-Time Payment" process and sends a "⑥ Payment Approval" back to the private institution. Upon receiving this notification, the private institution proceeds to send a "⑦ Completion Notification" to both Bank ‘A’ and ‘B’, signifying the finalization of the contract conditions. The total

transferred funds are calculated, and any unsuccessful transfer values are incorporated into the entry to generate the conclusive GuruFin block. In this scenario, steps ④, ⑤, and ⑥ follow the central bank protocol, as depicted in the accompanying diagram.



[Diagram 4: GuruFin Mainnet to Private institutions and Banks – Case 2]

In this scenario, steps ④, ⑤, and ⑥ adhere to the existing central bank protocol, as depicted in [Diagram 4]. When the central bank directly issues a "⑥ Payment Completion", the private institution sends a "④ Payment Request" to the central bank first. The central bank then facilitates the "⑤ Real-Time Payment" process and subsequently transmits a "⑥ Payment Completion" to both Bank 'A' and 'B'. Upon receipt of this notification, the final contract conditions are considered complete. The total amount of transferred funds is calculated, and any unsuccessful transfer values are incorporated into the entry to generate the ultimate GuruFin block.

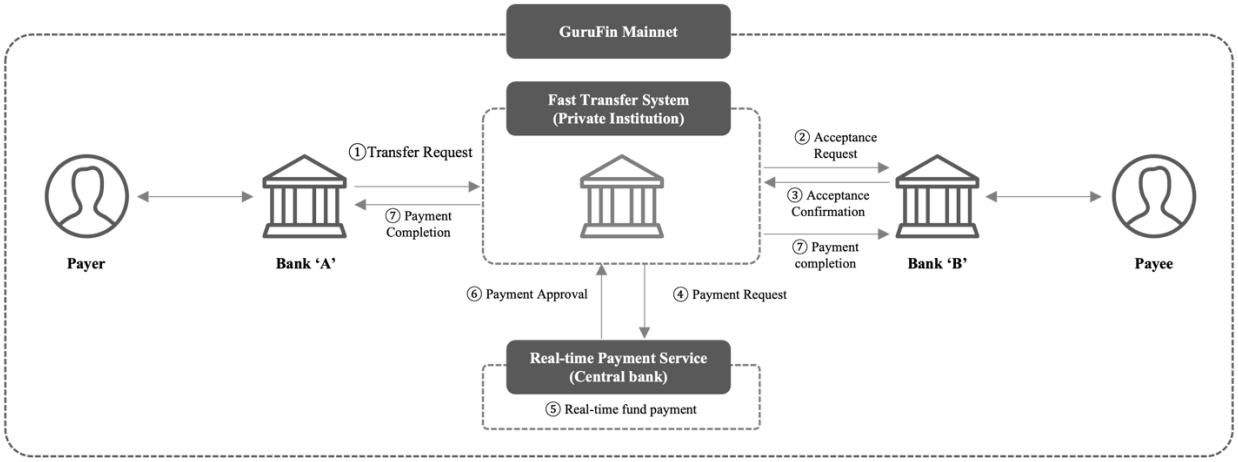
12.3.2. Decentralized Configuration

GuruFin Mainnet presents a framework to establish a comprehensive network comprising the central bank, private institutions, and banks. This integration aims to enhance security measures against tampering attempts and ensure the integrity of data. The existing structure of the Real-Time Gross Settlement (RTGS) system can be effectively utilized within this structure, providing a solid foundation for the network's construction and operation.

1) Private Institution Operations

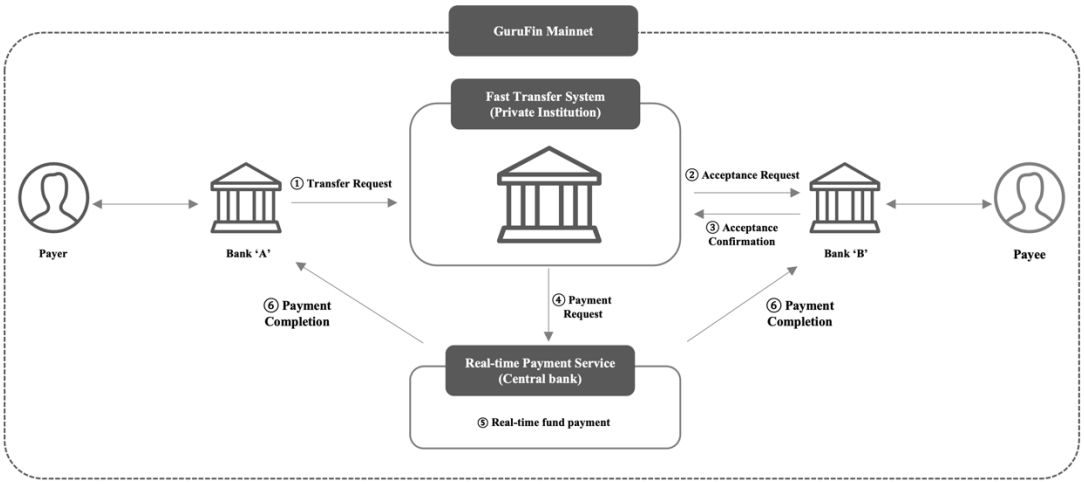
When a Payer initiates a payment request, [Diagram 3] and [Diagram 4] follow the same process until "③ Acceptance Confirmation" is reached.

CASE 1 - [Diagram 5] If a "⑦ Payment Completion " is received through a private bank, the private institution proceeds by sequentially modifying the mapping structure of the remittance ledger, following the order specified in the entry received from Bank 'A'. This restructuring entails transforming the entry into ledger state data, mirroring the actions of Bank 'A'. Subsequently, the private institution sends a "④ Payment Request" to the central bank. The central bank processes the "⑤ Real-Time Payment" and notifies the private institution of the "⑥ Payment Approval." Once received, the private institution transmits the "⑦ Payment Completion" to both Bank 'A' and 'B', thereby fulfilling the final contractual conditions. The total amount of transferred funds is then calculated, and any unsuccessful transfer values are incorporated into the entry, culminating in the creation of the final block on the GuruFin blockchain.



[Diagram 5: Central Bank, Private Institutions, and Banks – Case 1]

CASE 2 - [Diagram 6] When the "⑥ Payment Completion" is issued by the central bank, the private institution follows a similar process. It sequentially modifies the mapping structure of the remittance ledger based on the predetermined order specified in the entry received from Bank ‘B’, replicating the ledger state data transformation performed by Bank ‘A’. Subsequently, the private institution submits a "④ Payment Request" to the central bank. The central bank processes the "⑤ Real-Time Payment" and notifies both Bank ‘A’ and ‘B’ of the "⑥ Payment Completion." Once all the final contractual conditions are satisfied, the total amount of transferred funds is calculated, and any unsuccessful transfer values are integrated into the entry, resulting in the creation of the final block on the GuruFin blockchain.



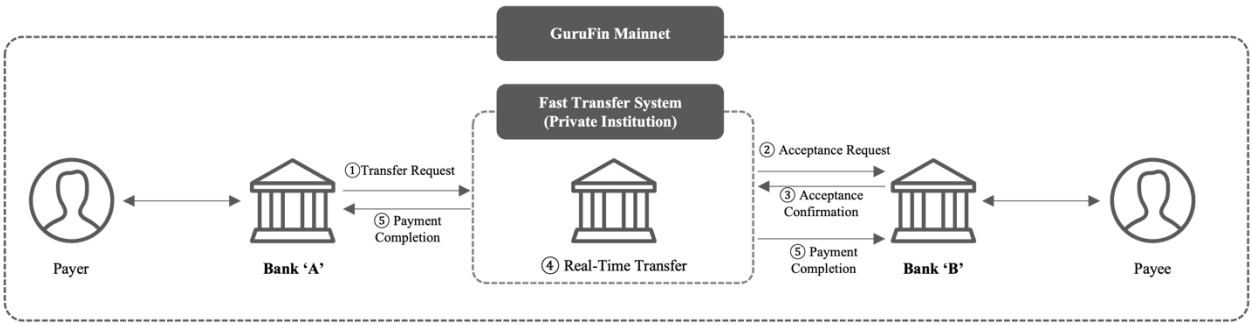
[Diagram 6: Central Bank, Private Institutions, and Banks – Case 2]

2) Central Bank Operations

[Diagram 2] The Payer initiates a payment request. Both the first and second parties of Bank ‘A’ follow a similar process. Once the construction of the remittance entry is finalized, the central bank facilitates the process by issuing a "① Transfer Request" to Bank ‘B’ through its own channels, encompassing the entirety of the transfer.

The central bank performs a restructuring of the remittance ledger in a mapping structure, following the order specified in the entry received from Bank ‘A’. This restructuring is done in a manner similar to how Bank ‘A’ handles ledger state data. Subsequently, the central bank proceeds to send a "② Acceptance Request" to Bank ‘B’. Upon receiving the "③ Acceptance Confirmation" from Bank ‘B’, the contract conditions are duly approved.

Once the central bank obtains the "③ Acceptance Confirmation," it proceeds with the "④ Real-Time Transfer" process and issues a "⑥ Payment Completion " to both the Bank ‘A’ and ‘B’. This notification marks the completion of the final contract conditions. The total amount transferred is calculated and incorporated into the entry, encompassing the value of any failed transfers. Ultimately, this leads to the generation of the final block on the GuruFin Mainnet.



[Diagram 7: Configuration of GuruFin Mainnet Application for Central Bank and Banks]

13. The GURUFIN Project: Core dApps

- **DIGIGOOZ (NFT Platform)**
  Digigooz provides a B2C Web2 & Web3 Storefront and C2C NFT platforms. NFT creators can mint and sell, and users can buy and trade physical goods and digital assets. Users can sell, buy, list, trade, and bid NFTs in the marketplace with credit card, digital carrier billing, or stable tokens. NFT creators receive payment in fiat currency or stable token per sale. Issuing and trading NFTs has been made more accessible with low minting cost and close-to-zero gas fees. NFTs can be in various file formats (e.g., jpg, 3D, video). Companies can open and independently operate the stores free-of-charge. Customers can sign up with an existing Google account or through GuruFin Wallet for a simple and effortless user experience.

- **GAMEGOOZ (Web3 Gaming Platform)**
  Gamegooz is a platform that provides blockchain technology to Web2 and Web3 game projects while allowing games to maintain their existing gameplay mechanics. Projects can use Gamegooz as a bridge into the ecosystem to leverage shared resources and capabilities of the community.

- **MUSICGOOZ (Web3 Music Platform)**
  MUSICGOOZ is a Web3 music platform that offers a dynamic range of music content in the form of NFTs. Listeners can collect rare and meaningful music content from their favorite musicians and enjoy their favorite music content through streaming at any time.

- **LINKTORY (Web3 Fan Community Platform)**
  Linktory is a Web3 Fan Community Platform that operates based on Fan Tokens. Fan Token holders can actively participate in various events such as content creation through voting. This allows content creators and fandom to grow together and enjoy the results.

- **DIMPLE (Metaverse Platform)**
  dimple is a 3D web-based metaverse platform with no downloading required. NFTs are integrated with interactive features for a truly immersive experience.

14. GURU & MU TOKENOMICS

The GuruFin Layer-1 Mainnet Network serves as a pioneering hybrid chain, incorporating both a Governance Chain and a Compliance Chain. This innovative dual-chain system supports two distinctive native coins: GURU, derived from the Governance Chain, and MU, a stablecoin linked to the Compliance Chain.

MU stablecoin is fully collateralized on a 1:1 basis by traditional fiat currencies such as the US dollar, Japanese yen, euro, Philippine peso, among others. Each MU is supported by its dedicated Layer-1 Mainnet (the Compliance Chain), which ensures heightened security, rapid transaction speeds, energy efficiency, and near-zero gas fees ($0.000032) – prerequisites for widespread adoption. Its inherent stability positions MU as a preferred option for minting operations and assorted transactional fees.

GURU, on the other hand, acts as a multi-faceted token, encompassing governance, staking, and utility roles. The application of GURU extends to:

1. Governance: GURU enables users to participate in GuruFin's decentralized decision-making processes.

2. Staking: Network nodes can stake GURU and earn rewards for their involvement in network maintenance and operation.

3. Utility: GURU functions as the network usage fee across all platforms on the MU chains:

A. Various versions of GuruFin's stablecoin MU (USMU, PHMU, JPMU, and more) will be applied to a multitude of transactions, including NFT minting, P2P remittances, and retail payments across the world. The stable nature of MU fosters a predictable, fixed-price fee structure that will promote widespread blockchain adoption for consumers and businesses alike. Subsequently, the network will convert a portion of collected MU fees to GURU for reward distribution amongst participating nodes and for token burning purposes.

B. GURU will serve as a common fee denomination across the GuruFin network. Digital wallets on the network, like Surge Pay in the Philippines, will impose fees, including conversion and FX fees, payable in GURU. However, to maintain seamless user experiences, these fees will be initially levied in MU and then converted into GURU.

C. Financial institutions using the GuruFin network and its proprietary technology, such as Inter-Transaction Multi-Transfer (ITMT), will pay transaction fees in GURU. MU conversions across a spectrum of global financial institutions will also incur a GURU fee.

D. In cross-border transactions, merchants who wish to utilize the MU system for credit card, Direct Carrier Billing (DCB), or Alternative Payment Methods (APMs) will be required to secure and deposit GURU as a Security Merchant Deposit, drawing from the non-circulated reserve of 65 billion GURU tokens.

E. Following the integration of the GuruFin point system, users can convert a variety of accumulated points, earned from sources such as airlines or hotels, into GURU at the current market rate. This further broadens GURU token utility, providing a broad spectrum of use-cases throughout the GuruFin ecosystem. The impending GuruFin Merchant Application will facilitate payments in GURU, MUs, and other major cryptocurrencies, with GURU being the principal token used for conversion fees in all these instances.

15. Members & Advisors

15.1. Members

Dr Jae S. Jeong
Technology

Marcus Ko
Business Development

Liam Lee
Finance

Ralph Simon FRSA
Founder, Mobilium Global

Ray Anderson
Founder, Bango

Ryan Jeon
Strategy

Oliver Kwon
Blockchain Development

Danny Park
MCN/Marketing

Jonathan Lizarondo
Web2 & Web3 Fintech

Charles David Inducil
Web3 Blockchain/Game

Bryan Lim
Web 3 Digital Ownership

Xavier Yoon
Web3 Fan Platform **Erica Jeong**
KYC/AML

Rosendo III Lizarondo
Community Relations

Lloyd Kang
Platforms Dev

Mansu Jung
Web3 Game Platform

Alexander Rausa
UI / UX

YH Bae
Web2 & Web3 Payment Service/PG

SY Park
Cyber Security

Quentin Behem
Operation

Amelia Kim
Project Management

Francis Jimenez
Digital Marketing

Suk-Jin Chon
Attorney, Sangyung

Seo-In Kim
Partner Attorney, SIA Law

Erica Jeong
KYC/AML

Cheol-Hyun Yoo
Managing Partner / Co-Founder, BLT Patent and Law Firm

15.2. Advisors

BLT Patent & Law Firm

LEE & KIM Law Firm

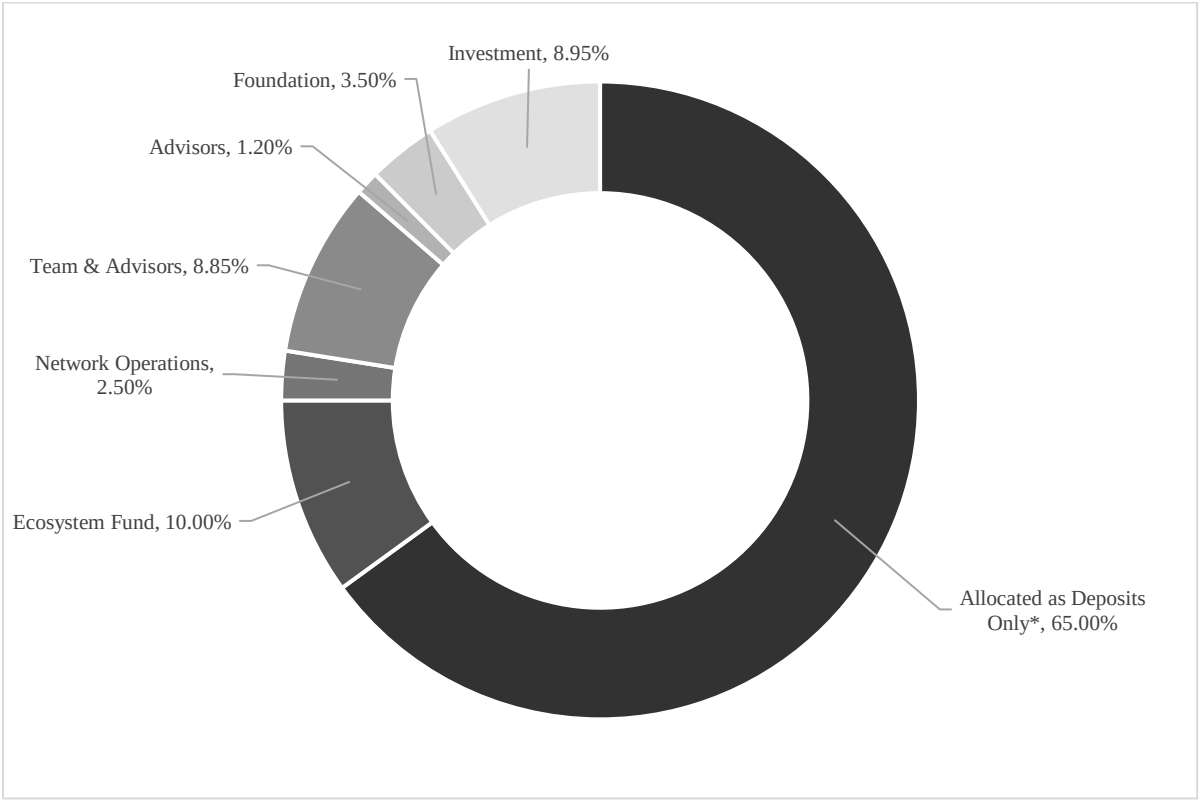
SIA Law Firm

Yool-Hyun Tax

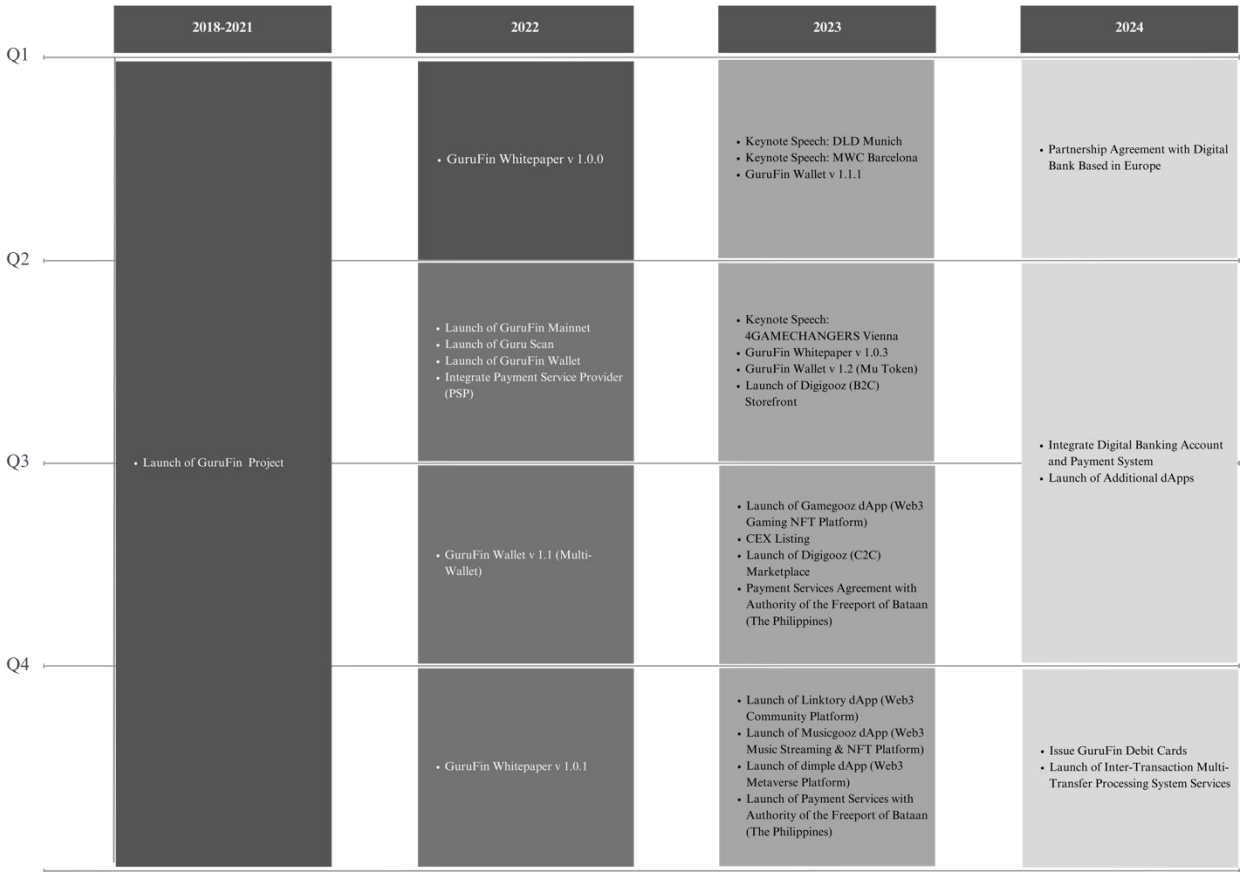
16. Token Allocation

No.	Category		Allocated Token	Ratio	Lock-up Period
1	Allocated as Security Deposits Only* Not to be circulated in market*		65,000,000,000	65.000%	Perpetual Lock
2	Ecosystem Fund		10,000,000,000	10.000%	TGE (1/60 per month)
3	Network Operations		2,500,000,000	2.500%	3% Unlock per month from TGE
4	Team & Developers		8,850,000,000	8.850%	1year, 1/60 per month
5	Advisors		1,200,000,000	1.200%	1year, 1/60 per month
6	Foundation/Holdings		3,500,000,000	3.500%	1 year, 1/120 per month
7	Investment	Seed/Private Sale	2,750,000,000	2.750%	7.5% Unlock per month from TGE
		Strategic Round	1,700,000,000	1.700%	5% Unlock per month from TGE
		Presale	1,500,000,000	1.500%	3% Unlock per month from TGE
		Liquidity	3,000,000,000	3.000%	Unlock
Total			100,000,000,000	100.000%	

*Allocated as Security Deposits for businesses and dApps that want to use GuruFin Project's real economy payment transactions such as credit card and carrier billing. Not to be circulated in the market therefore not included in Total Market Circulating Supply.



17. Roadmap



This white paper has been distributed for reference purposes only. Nothing in this document should be understood as an offer to sell, a solicitation to purchase, or interpreted as a guarantee of how the GuruFin Blockchain will develop, be utilized, or accrue value. Possession of GURU coins shall not be acknowledged, interpreted, or treated as an opportunity to receive or participate in return, payment, or profit in relation to GuruFin and its related projects and products.

GuruFin only outlines its current vision and mission, with the success of which will depend on various factors outside of its control. Forecasting statements do not guarantee future results, performances, or achievements. GuruFin Foundation undertakes no obligations to update its plans. Information in this document is subject to change at the sole discretion of GuruFin.

CONTACT US

info@gurufin.io