# WHITE PAPER
# AUSDT 2.0 (USDT 2.0)
# A Central Bank Digital Currency (CBDC)


## Abstract

*AUSDT is a stablecoin issued on the ALLTRA SmartChain, designed to maintain a 1:1 parity with the US Dollar (USD). Each AUSDT token is fully backed by USD held in reserve and re-insured by an equivalent amount of USD in a separate insurance reserve. This two-tiered backing ensures that the token consistently retains its value and provides users with a secure and stable digital currency for transactions, payments, and decentralized finance (DeFi) applications.*


## Overview

*AUSDT 2.0 (USDT2.0) is a purpose-built ACR-20 token deployed on the EVM-compatible ALLTRA SmartChain, developed to serve as a secure and compliant payment asset across the ALLTRA financial ecosystem. Designed with MiCA-aligned architecture and future-proof security controls, AUSDT 2.0 empowers digital commerce with administrative recovery, compliance, and modular integration.*

## Secure, Compliant, and Recoverable Digital Payments on ALLTRA SmartChain

***Token Address**: https://alltra.global/token/0x015B1897Ed5279930bC2Be46F661894d219292A6*
***Network**: ALLTRA SmartChain (ALL MAINNET) – EVM Compatible*
***Token Standard**: ACR-20*

*AUSDT leverages the security and transparency of blockchain technology, combined with robust financial backing, to create a reliable stablecoin that users can trust for everyday financial transactions, trading, remittances, and as a store of value.*

## Core Security & Compliance Features

**MiCA-Ready & Upgradable**

- Architected for **Markets in Crypto-Assets (MiCA)** compliance.
- **Upgradeable smart contract** structure enables alignment with evolving regulations and technical improvements.

### Administrative Controls with Granular IAM

- **Access Manager System** handles all restricted administrative functions with **granular role-based permissions**, enabling secure operational delegation.
    - Example: A designated account may trigger an **emergency pause**, but **only the super admin** can resume transfers.
- Ensures **internal access control and security separation** for core functions.

### Token Lifecycle Management

- **Pause / Unpause** capability for end-of-life or emergency intervention.
- **Blacklist Functionality** to block transfers **to and from** compromised or sanctioned addresses.
- **Admin Mint & Burn** to or from **any account**.
- **Administrative Transfers** can override blacklist checks, enabling **recovery of stolen or lost tokens** securely and legally.

### Interoperable Access Management

The **centralized Access Manager** is designed to be reusable across future smart contracts, forming the backbone of a **chain-wide on-chain Identity and Access Management (IAM)** framework. This modular design enables other contracts to plug into the same IAM system, ensuring consistent, secure role governance throughout the Alltra ecosystem.

### Utility & Use Case

AUSDT 2.0 is the foundational token for transaction, payment, and merchant systems across ALLTRA's ecosystem, supporting:

- **Instant settlement**
- **Gateway and financial integrations**
- **DeFi modules with enforced compliance**
- **Core-banking and smart finance solutions**

## Settlement, Mechanics, Transaction Flow and Integration

### Fiat Backed Digital Token System

The foundational purpose of this system is to create a **digital token** that is a 1:1 representation of real-world fiat currency (such as USD, AUD, etc.). The value of each token is guaranteed by a corresponding unit of **reserve currency** held in a secure bank account. This design ensures that the token's value is stable and predictable, distinguishing it from unbacked cryptocurrencies.

Users of the system can perform three primary actions: minting, transferring, or redeeming tokens. These tokens are designed to be both fungible (interchangeable) and portable. The system's operational integrity is secured by a set of core principles:

- **Circulation = Reserve**: The total number of tokens in circulation must never exceed the value of the fiat currency held in reserve.

- **Minting Requires Reserve**: New tokens can only be created if an equivalent amount of fiat is first deposited into the reserve.
- **Burning Redeems Fiat**: Destroying or "burning" a token triggers the release of the corresponding fiat from the reserve to the user's bank account.
- **Transfers Are Internal**: Moving tokens between user wallets is a purely internal ledger update that does not interact with the reserve or external banking systems.
- **Immutable Ledger**: Every transaction is permanently recorded in a secure, tamper-proof ledger for auditing and transparency.
- **Security Layer**: Robust security measures, including authentication, cryptographic signatures, timestamps, and idempotency keys, are in place to prevent fraud and unauthorized access.

## Background and Classification

The Stable Token System (STS) can be classified as a Centralized Digital Currency or a Fiat- Backed Stablecoin. It is a centralized system because a single entity controls the ledger and the underlying fiat reserve. This differs from decentralized cryptocurrencies like Bitcoin, which rely on a distributed network. The STS's primary function is to serve as a high-speed, low-cost medium of exchange for digital payments and transactions, leveraging existing banking infrastructure while offering the speed and programmability of a digital asset. The system is designed to seamlessly integrate with global financial systems by handling foreign exchange (FX) conversions internally.

## Core Components and Mechanics

The STS's operation is orchestrated through a RESTful API that serves as the primary interface for all user actions.

## JSON Payload Structure

All requests are initiated by sending a JSON payload via a HTTP POST request. The payload is a structured data object containing the following required fields:

- **Wallet ID**: A string identifying the user's unique wallet.
- **Amount**: A numerical value representing the number of tokens to be processed.
- **Currency**: A string (e.g., "USD" or "AUD") specifying the currency type for the transaction.
- **Idempotency Key**: A unique, one-time identifier for each request. This is a critical security feature that prevents a request from being processed more than once, guarding against network timeouts or accidental retries.
- **Timestamp**: An ISO 8601 formatted UTC timestamp of the request. The server uses this to prevent replay attacks, where a malicious party resends a valid request.
- **Signature:** A cryptographic hash that verifies the authenticity and integrity of the payload. The signature is generated using a shared secret key and is a HMAC-SHA256 of the concatenated payload data and the timestamp. The secret key is stored securely on the server and is never transmitted in the payload.

## Transaction Flow and Backend Integration

Once a signed JSON payload is received by the API endpoint (e.g., /mint, /transfer, /redeem), the system proceeds through a series of automated steps:

- **API Validation:** The system first validates the request's authenticity by checking the Authorization header (containing a Bearer token) and independently recalculating the HMAC signature to ensure it matches the one in the payload. It also checks the Idempotency key against a record of past requests.

- **Backend Processing:** The API routes the request to the appropriate backend systems. For example, the core banking platform could be Mifos that manages the central ledger, while Alltraloop handles wallet and payment processing.
- **Reserve Interaction:** For mint and redeem actions, the system interacts with the fiat reserve, which is held in a bank account. Minting locks a corresponding amount of fiat in the reserve, while redeeming releases it. Transfers only update balances on the internal ledger, as no fiat changes hands.
- **FX Conversion:** If a redemption is requested in a currency different from the reserve's currency (e.g., redeeming AUD from a USD reserve), the system uses live market exchange rates from a trusted third-party provider to perform the conversion. A small spread or fee may be applied.
- **Response**: The API returns a JSON response indicating the transaction's success or failure, along with relevant details like a transaction ID, updated balance, security and/or specific error codes.

### Applications and Scope

This token system is designed for any application requiring stable, fast, and auditable digital transactions. Its primary use cases include:

- **Cross-border Payments:** Facilitating low-cost international transfers by leveraging the system's internal FX conversion capabilities.
- Digital Wallets and P2P Transfers: Enabling instant, peer-to-peer token transfers without the delays and fees associated with traditional bank transfers.
- E-commerce: Providing a stable payment method that is not subject to the volatility of

unbacked cryptocurrencies. The system's robust security model and clear separation between environments (sandbox vs. production) allow for safe and reliable development. Initial testing must always be conducted in the sandbox environment using fake wallets and non-monetary transactions to prevent
irreversible mistakes.

## Conclusion

The Stable Token System represents a robust and secure framework for a fiat-backed digital currency. By leveraging established financial protocols and integrating with existing banking infrastructure, it provides the stability of traditional money with the efficiency of a digital asset. The system's reliance on a well-defined API, secure JSON payloads, and an auditable ledger ensures transparency, security, and integrity, making it a viable solution for modern digital finance applications. This structured approach, which clearly separates user actions from backend processes and reserves, is crucial for maintaining the 1:1 token-to-fiat backing and for ensuring the platform's long-term reliability.