# AltVerse: Trustless, Instant Cross-Chain Swaps

## 1 Introduction

AltVerse is a protocol designed to facilitate instant, trustless, and fully decentralized cross-chain asset transfers. By enabling seamless movement of assets between different blockchain networks, AltVerse addresses the critical challenge of interoperability in the fragmented blockchain ecosystem.

> ”For the Imperium, Spice is used by the navigators of the Spacing Guild to find safe paths between the stars. Without Spice, interstellar travel is impossible... making it, by far, the most valuable substance in the universe.”

Just as Spice facilitates interstellar travel in the Dune universe, Altcoin (ALT) aims to enable seamless navigation across the blockchain multiverse. Pegged to a basket of approved stablecoins, Altcoin serves as the crucial intermediary for cross-chain transactions in the AltVerse ecosystem. Currently functioning as a stand-in for USDC and its Cross-Chain Transfer Protocol (CCTP), Altcoin paves the way for secure and efficient value transfer between disparate blockchain networks.

AltVerse enhances the DeFi ecosystem through its approach to cross-chain interactions. The protocol offers cross-chain swaps with a fail-safe design and auto-refunds, improving user security and experience. By connecting previously isolated blockchain economies, AltVerse increases market efficiency and accessibility while supporting a wide range of ERC20 tokens across L1, L2, and other compatible networks. This bridging of diverse blockchain systems facilitates more fluid asset movement, potentially increasing overall market liquidity. Consequently, AltVerse contributes to a more integrated decentralized finance landscape, fostering the development of interoperable decentralized applications.

Beyond its technical capabilities, AltVerse represents a shift in how we conceptualize blockchain interactions. By demonstrating the feasibility of trustless, efficient cross-chain operations, it challenges the notion of blockchain isolation and encourages a more holistic view of the crypto ecosystem. This paradigm shift could lead to new research directions in blockchain interoperability, influence the design of future cryptocurrencies, and potentially reshape regulatory approaches to cross-chain transactions. As such, AltVerse not only contributes to the technical advancement of DeFi but also plays a role in expanding the philosophical and practical boundaries of decentralized technologies.

## 2 Security and Decentralization

AltVerse operates without middlemen or vulnerable bridges, ensuring complete decentralization with all operations conducted on-chain. The platform is secured by trustless escrows and timeouts, eliminating the need to trust any third party. If no confirmation is received within a set timeframe, users can redeem their assets from the escrow, protecting against unexpected failures.

While solutions like the Wormhole foundation or Multichain foundation have advanced cross-chain interoperability, they may face challenges related to centralization. AltVerse aims to avoid possible attack vectors that have been exploited in past incidents by using a combination of on-chain escrows, cryptographic proofs, and decentralized consensus mechanisms to ensure the security of cross-chain transfers across all supported chains.

Each transaction is secured by an escrow on the source chain, which is only released upon cryptographic proof of completion on the destination chain. This design, along with timeouts and user-initiated claim functions, provides multiple layers of security, allowing users to recover their assets in case of network failures or attacks, and ensuring that a compromise on one chain doesn’t affect the security of assets on other chains.

## 3 Cross-Chain Compatibility

AltVerse can integrate with any Layer 1, Layer 2, or other blockchain network that supports Wormhole. This wide compatibility ensures that AltVerse can facilitate cross-chain swaps across a diverse ecosystem of blockchain networks.

## 4 Liquidity and Rewards

This prototype leverages Uniswap V2 liquidity pool mechanics and rewards as a proof of concept. Currently, liquidity on the testnets is provided via testnet ERC20 tokens. While the price curve is defined by x * y = k, where x and y represent the quantities of the two tokens in the liquidity pool and k is a constant, the focus is on the overall functionality of the cross-chain swaps. Liquidity providers can earn rewards by contributing to liquidity pools on any supported chain. The reward mechanism is defined as:

$$R = f(L, V, T, P) \tag{1}$$

Where $R$ is the reward, $L$ is the liquidity provided, $V$ is the trading volume, $T$ is the time period, and $P$ represents the specific parameters of the liquidity pool in use. The function $f$ depends on the liquidity pool mechanism (currently Uniswap V2) and may evolve as more advanced AMMs are integrated.

# 5 Escrow Mechanism

The escrow system ensures the security of cross-chain swaps. It can be represented as:

$$E(u, a, \tau) = H(u \parallel a \parallel \tau) \tag{2}$$

$E$ is the escrow ID, $H$ is a hash function, $u$ is the user's address, $a$ is the escrowed amount, $\tau$ is the timeout period. The escrow is created when a user initiates a swap and is released under two conditions:

$$\text{Claim} = \begin{cases} \text{Release to contract} & \mid \text{if confirmation received} \\ \text{Return to user} & \mid \text{if timeout reached without confirmation} \end{cases} \tag{3}$$

In the first case, the escrowed tokens are released to the contract and processed according to the swap protocol. In the second case, the user can claim their escrowed tokens back, ensuring they don't lose funds due to network failures or other issues. Users can claim their escrowed tokens by calling a specific function on the contract after the timeout period, providing the escrow ID as proof of ownership.

# 6 Protocol Mechanics

AltVerse facilitates trustless cross-chain swaps using ALT as an intermediary. The core mechanics can be represented in the following pseudocode:

**Algorithm 1** AltVerse Cross-Chain Swap

```
function crossChainSwap($\tau_{from}, \tau_{to}, \alpha, \chi_{target}$)
    $\alpha_{alt} \leftarrow$ swapTokenForALT($\tau_{from}, \alpha$)
    $\varepsilon_{id} \leftarrow H(u \parallel \alpha_{alt} \parallel \tau)$
    $E \leftarrow$ createEscrow($u, \alpha_{alt}, \tau$)
    $\mu \leftarrow$ createSwapMessage($\tau_{from}, \tau_{to}, \alpha_{alt}, u, \varepsilon_{id}$)
    sendWormholeMessage($\chi_{target}, \mu$)
end function
function receiveWormholeMessage($\chi_{source}, \mu$)
    if $\mu$.isSwapMessage then
        $\alpha_{dest} \leftarrow$ swapALTForToken($\mu.\alpha_{alt}, \mu.\tau_{to}$)
        transfer($\mu.u, \mu.\tau_{to}, \alpha_{dest}$)
        $\mu_{conf} \leftarrow$ createConfirmationMessage($\mu.\varepsilon_{id}$)
        sendWormholeMessage($\chi_{source}, \mu_{conf}$)
    else
        processEscrow($\mu.\varepsilon_{id}$)
    end if
end function
function processEscrow($\varepsilon_{id}$)
    $E \leftarrow$ getEscrow($\varepsilon_{id}$)
    burnALT($E.\alpha_{alt}$)
    deactivateEscrow($\varepsilon_{id}$)
end function
function claimTimedOutEscrow($\varepsilon_{id}$)
    $E \leftarrow$ getEscrow($\varepsilon_{id}$)
    validateEscrowTimeout($E$)
    transfer($u, E.\alpha_{alt}$)
    deactivateEscrow($\varepsilon_{id}$)
end function
```

Where $\tau_{from}, \tau_{to}$ are source/destination tokens, $\alpha$ is initial token amount, $\alpha_{alt}, \alpha_{dest}$ are ALT and destination token amounts, $\chi_{target}, \chi_{source}$ are target/source chains, $u$ is user address, $\varepsilon_{id}$ is escrow ID, $\mu$ is the message, $H$ is a hash function, and $\tau$ is the escrow timeout period.

# 7 DEX Integration, Oracle Services, and Cross-Chain Arbitrage

AltVerse is designed to seamlessly integrate with Decentralized Exchanges (DEXes) and oracle services on connected chains. This integration, combined with AltVerse's cross-chain capabilities, creates significant opportunities for arbitrage and enhances overall market efficiency.

## 7.1 DEX and Oracle Integration

The integration with DEXes and oracles allows for:

- Accurate price discovery: $P = f(O_1, O_2, ..., O_n)$
- Enhanced liquidity: $L = \sum_{i=1}^{n} l_i$
- Arbitrage opportunities: $A = |P_1 - P_2|$

Where $P$ is the asset price, $O_i$ are oracle inputs, $L$ is total liquidity, $l_i$ are individual liquidity sources, and $A$ is the absolute value of the price difference between two markets, representing the arbitrage opportunity.

## 7.2 Cross-Chain Arbitrage

The arbitrage potential between two chains can be represented as:

$$A_{ij} = \max(P_i - P_j, 0) \tag{4}$$

Where $A_{ij}$ represents the arbitrage opportunity between chains $i$ and $j$, and $P_i$ and $P_j$ are the prices of the same asset on chains $i$ and $j$ respectively.

For multi-hop arbitrage across multiple chains, the total arbitrage opportunity can be calculated as:

$$A_{total} = \sum_{i=1}^{n-1} A_{i,i+1} \tag{5}$$

Where $n$ is the number of chains in the arbitrage path.

## 7.3 Compounded Multi-Hop and Multi-Oracle Opportunities

For more complex arbitrage strategies involving multiple hops and multiple oracles, we can extend our model:

$$A_{compound} = \prod_{i=1}^{n}(1 + A_i) - 1 \tag{6}$$

Where $A_i$ represents the arbitrage opportunity at each hop, considering the best price from multiple oracles:

$$A_i = \max_j\left(\frac{P_{i+1,j}}{P_{i,j}} - 1\right) \tag{7}$$

Here, $P_{i,j}$ represents the price of the asset on chain $i$ according to oracle $j$. The reward function $R$ introduced earlier represents the incentives for liquidity providers. We can incorporate this into our model to represent the total value capture potential:

$$V_{total} = A_{compound} + \sum_{i=1}^{n} R_i \tag{8}$$

Where $V_{total}$ represents the total value capture potential, combining both arbitrage opportunities ($A_{compound}$) and liquidity provision rewards ($\sum_{i=1}^{n} R_i$). This model allows market participants to identify and exploit complex price discrepancies across different chains and DEXes, while also considering the rewards for providing liquidity. Arbitrageurs can focus on maximizing $A_{compound}$, while liquidity providers can optimize for $R_i$. As these actors pursue these opportunities, they collectively help to balance prices and enhance liquidity across different blockchain ecosystems, leading to more efficient and integrated markets.

# 8 Future Milestones

1. **Ecosystem Expansion:**
    - Integration with multiple popular Wormhole-supporting networks
    - Integration with other ecosystems other than EVM-based networks (Solana, Cosmos, NEAR, etc.)
2. **Advanced AMM and DEX Integration:**
    - Integration of potential improvements or alternative pricing models from various AMM designs
    - Refinement of pricing mechanisms to enhance swap efficiency and reduce slippage
    - Development of DEX routing capabilities for optimized swaps within each supported chain through integration with generalized oracle services and specific DEX oracles (e.g., UniswapV2Oracle), etc.
    - Implementation of internal routing to efficiently manage liquidity across multiple pools and optimize returns
3. **USDC Integration:**
    - Integration of native USDC liquidity across supported chains
    - Integration of USDC's Cross-Chain Transfer Protocol (CCTP)
4. **Security and User Control Enhancements:**
    - Implementation of fine-grained control over slippage, escrow, and trade parameters
    - Liquidity protection of LP pool token shares using zero-knowledge proofs
    - Development of account abstraction mechanisms for secure LP token management
5. **Governance and Tokenomics:**
    - Design and implementation of a governance token for community-driven decision making
    - Development of a staking mechanism for ALT holders to participate in protocol governance
6. **Advanced Trading Features:**
    - Implementation of limit orders for cross-chain swaps
    - Development of a cross-chain yield aggregator
7. **Security and Auditing:**
    - Conducting comprehensive security audits by reputable firms and bug bounties
    - Development of a formal verification framework for critical smart contract components

# 9 Value Proposition and Market Impact

AltVerse brings several significant advantages to the DeFi ecosystem:

1. **Universal Liquidity Layer:** By enabling seamless asset transfers between different blockchain ecosystems, AltVerse has the potential to create a universal liquidity layer across multiple blockchains. This solves one of the biggest challenges in the fragmented blockchain ecosystem.
2. **Capital Efficiency:** The ability to quickly and easily transfer assets across chains leads to more efficient capital allocation across the DeFi ecosystem. This could potentially unlock new levels of capital efficiency in DeFi.
3. **DeFi Unification:** AltVerse has the potential to unify disparate DeFi ecosystems, creating a more cohesive and interoperable DeFi landscape. This could lead to new synergies and use cases that were previously impossible due to the siloed nature of different blockchain networks.
4. **Enhanced User Experience:** Users can perform cross-chain swaps in a single transaction and with just one click, which is significantly more user-friendly than most current multi-step processes. This simplification could lower the barrier to entry for new users and increase overall adoption of DeFi.
5. **New Arbitrage Opportunities:** The system creates new arbitrage opportunities across chains, which not only benefits traders but also contributes to more balanced and efficient markets across different blockchain ecosystems.
6. **Cross-Chain Yield Farming:** AltVerse could enable new strategies for yield farming across different chains, potentially leading to more efficient markets and higher yields for liquidity providers.
7. **Simplified Cross-Chain dApp Development:** By providing a robust infrastructure for cross-chain asset transfers, AltVerse could make it easier for developers to create truly cross-chain decentralized applications. This could spur innovation and lead to a new generation of DeFi applications.
8. **Enhanced Security:** The lack of centralization and the trustless nature of the protocol significantly improve

security when bridging tokens across chains. With an escrow mechanism guaranteeing asset protection, users, organizations, and future protocols can engage in cross-chain transactions with confidence, mitigating risks associated with centralized solutions.

## 10 Conclusion

AltVerse represents a significant advancement in cross-chain trading, offering functionality similar to a cross-chain version of Uniswap or 1inch, but with the crucial difference of being completely trustless and bridge-free. By facilitating seamless asset transfers between different blockchain ecosystems, AltVerse has the potential to unlock new opportunities for arbitrage, liquidity provision, and decentralized finance applications.

As the protocol evolves and integrates with more chains and DEXes, it could play a crucial role in bridging isolated blockchain economies, enhancing overall market efficiency and accessibility in the rapidly growing DeFi landscape. The potential for AltVerse to create a more unified, efficient, and accessible DeFi ecosystem makes it a project with significant implications for the future of decentralized finance.