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 asset transfers across different blockchain networks, Altverse addresses the critical challenge of secure 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 fluid 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 distinct blockchain economies and integrating with native DEXes on each chain, Altverse increases market efficiency and accessibility while supporting a wide range of token standards (ERC20, SPL, etc.) across EVM L1s, L2s, and other networks. This bridging of diverse blockchain systems and native liquidity sources facilitates frictionless asset movement, deepening overall market liquidity through both protocol-owned and DEX-aggregated pools. Consequently, Altverse contributes to a more unified decentralized finance landscape, fostering the development of interoperable decentralized applications.

Beyond its technical capabilities, Altverse represents a potential link between traditional and decentralized finance. Through its trustless and efficient cross-chain operations, it enables centralized exchanges (CEXes) and other markets to tap into cross-chain liquidity while unlocking sophisticated arbitrage opportunities through parallel routing and multi-hop execution. This architectural approach could establish new paradigms for market unification, create unprecedented opportunities for capital efficiency, and reshape how we think about value transfer across the entire financial landscape.

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. Users can redeem their assets if no confirmation is received within the set timeframe.

While existing cross-chain solutions face challenges due to centralization and vulnerable components that have been exploited, Altverse achieves true trustless cross-chain transfers by relying only on simple messages relayed using Wormhole between smart contracts on different chains. These messages are unforgeable by design - Wormhole's implementation ensures that relayers can only pass messages between chains but cannot modify or forge their contents, as the message content is verified directly between the source and destination chain contracts.

Each transaction is secured by an escrow on the source chain, released only upon cryptographic proof of completion on the destination chain. This design, with timeouts and user-initiated claims, provides multiple layers of security through Wormhole's unforgeable messages. The system ensures users can either complete their cross-chain transfer or recover their assets, regardless of network conditions. Through this architecture, no third party ever has custody of user funds, and a security compromise on one chain cannot affect 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 cross-chain swaps across a diverse ecosystem of blockchain networks. Unlike traditional sequential single-path transfers, Altverse introduces parallel execution capabilities that allow multiple simultaneous routes within a single cross-chain hop - enabling transactions to be split and recombined at the destination. Integration with native DEXes, combined with parallelized routes and multi-hop strategies, unlocks new cross-chain DeFi primitives previously impossible in siloed networks. Through established stablecoin on/off ramps, this infrastructure can extend beyond blockchain networks, positioning Altverse to potentially capture value across both decentralized and traditional financial markets.

4 Liquidity and Rewards

The prototype implementation leverages Uniswap V2 liquidity pool mechanics and rewards as a proof of concept. Currently, liquidity on the supported testnets is provided via testnet ERC20 tokens. While the price curve is defined by $x \cdot y = k$, 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. The reward mechanism for liquidity providers is defined as:

$$R = \alpha V \frac{l}{L}(1 + \tau t) \tag{1}$$

where α is the base reward rate (e.g., 0.15% per trade), V is the pool's trading volume, l is the provider's contributed liquidity, L is the total pool liquidity, τ is the time multiplier coefficient (e.g., 0.1 per month), and t is the duration of liquidity provision.

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, τ 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 Altcoin 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 τ_{from}, τ_{to} are source/destination tokens, α is initial token amount, $\alpha_{alt}, \alpha_{dest}$ are Altcoin and destination token amounts, $\chi_{target}, \chi_{source}$ are target/source chains, u is user address, ε_{id} is escrow ID, μ is the message, H is a hash function, and τ is the escrow timeout period.

7 Advanced Market Making and Cross-Chain Value Extraction

Altverse's architecture is designed to seamlessly integrate DEXes and oracle services across connected chains, creating a uniquely powerful ecosystem for trustless cross-chain value transfer. The protocol enables a novel optimization by allowing single cross-chain hops to be split into multiple parallel routes and recombined at the destination - a capability previously unexplored in traditional cross-chain systems. Through the aggregation of deep liquidity pools and oracle price feeds, combined with parallelized routes within each hop and multi-hop opportunities, the protocol delivers superior execution prices for users while unlocking new forms of arbitrage opportunities and enhanced market efficiency mechanisms.

7.1 DEX and Oracle Integration

Integration with multiple DEXes and oracles optimizes price discovery and liquidity depth, enabling users to access better execution prices through intelligent routing while providing enhanced yield opportunities for liquidity providers. The optimal price selection from weighted oracle network can be expressed as:

$$P_{best} = \min_{i=1}^{n}(w_i O_i + \lambda \frac{Q}{D_i}) \tag{4}$$

where w_i is the reliability weight of oracle i, O_i is the price from oracle i, λ is the liquidity impact coefficient, Q is the proposed transaction quantity, and D_i is the market depth/liquidity at source i. For each liquidity provider, the reward R for a given LP position follows reward functions specific to its DEX - as mentioned earlier, one example is:

$$R = \alpha V \frac{l}{L}(1 + \tau t) \tag{5}$$

7.2 Parallel Route and Multi-Hop Arbitrage

The protocol introduces sophisticated arbitrage capabilities by enabling parallel routes within cross-chain hops - allowing transactions to be split, executed simultaneously, and recombined at the destination. This architecture, combined with multi-hop strategies like triangular arbitrage, creates new value capture opportunities across chains. The maximal arbitrage opportunity across an optimal hop sequence can be expressed as:

$$A_{total} = \max_{H}(\sum_{h=1}^{H}(1 - c_h)(\sum_{i=1}^{m_h} a_i(1 - c_i))) \tag{6}$$

where H represents the number of hops that maximizes total value, m_h is the number of parallel routes in hop h, a_i represents a parallel route's opportunity, c_h is a cross-chain hop's execution cost ratio, and c_i is a route's execution cost ratio. For an individual hop, parallel route optimization can be expressed as:

$$a_i(v, r) = \max_{P_i \in \mathcal{P}}((P_{i,dest} - P_{i,source}) \cdot v + \max_{0 \le k \le r} \sum_{j=i+1}^{m} a_j(v_j, r - k)) \mid v \le \min(v_i, r) \tag{7}$$

This dynamic programming expression represents an algorithm for optimizing value across parallel routes. The function $a_i(v, r)$ calculates the maximum value that can be captured from route i onwards, when allocating volume v to the current route with remaining volume r to be distributed among subsequent routes. where $\mathcal{P}$ is the ordered set of route prices, sorted by descending price differential $(P_{i,dest} - P_{i,source})$. The price differential $(P_{i,dest} - P_{i,source})$ represents the potential profit per unit on the current route i, multiplied by the volume v allocated to this route. The second term $\max_{0 \le k \le r} \sum_{j=i+1}^{m} a_j(v_j, r - k)$ recursively calculates the optimal value obtainable from the remaining routes ($i + 1$ to m), considering the residual volume $r - k$. The constraint $v \le \min(v_i, r)$ ensures we neither exceed the route's capacity v_i nor the total remaining volume r. This allows the algorithm to make optimal local decisions while considering their impact on future route allocations, ultimately finding the global optimum for value distribution across all parallel routes.

7.3 Total Value Capture Potential of Cross-Chain Swap Market

The total value capture potential within the cross-chain swap market combines optimal arbitrage opportunities with comprehensive liquidity provision rewards across the protocol ecosystem:

$$V_{total} = A_{total} + \sum_{d=1}^{D} \sum_{p=1}^{P_d} R_p \tag{8}$$

where A_{total} is the maximal arbitrage opportunity across multi-hop strategies as defined above, D is the number of integrated DEX protocols across all chains, P_d is the number of liquidity pools in DEX d, and R_p represents liquidity provider rewards which may follow different reward functions depending on the specific DEX implementation and chain.

7.4 Addressable Market Landscape

Altverse's trustless cross-chain execution creates pathways to the broader traditional financial ecosystem, with opportunities in the global forex market ($6T+ daily volume), derivatives market ($1Q+ valuation), amongst others. Leveraging established stablecoins like USDC as a portal between traditional finance and digital assets, the protocol can seamlessly bridge these markets through existing fiat on/off ramps. Both centralized exchanges (CEXes) and traditional financial institutions can integrate with Altverse to tap into deeper cross-chain liquidity and enhanced price discovery, enabling their users to access optimal execution prices across previously siloed blockchain networks. The protocol's parallel routing capabilities can help all participants - from retail traders to institutional players - reduce spreads and slippage by automatically splitting large orders across multiple DEX venues and chains, while its multi-hop functionality provides a unified, configurable interface for executing sophisticated arbitrage strategies across different market venues. Through future protocol integrations and advanced trading primitives, Altverse can interface with securities lending, fixed income products, and institutional liquidity pools. The protocol's architecture therefore enables streamlined integration between DeFi protocols and traditional financial infrastructure, positioning it as a candidate for the foundational infrastructure layer of institutional adoption and bridging the TradFi-DeFi divide while enhancing market efficiency through unified price discovery and optimized routing across centralized, decentralized, and traditional financial venues.

8 Future Milestones

1. **Ecosystem Expansion:**
   - Integration with multiple additional Wormhole-supporting networks
   - Integration with other ecosystems other than EVM-based networks (Solana, Cosmos, NEAR, etc.)
2. **Advanced AMM and DEX Integration:**
   - Integration of improvements and alternative pricing models from various AMM designs
   - Refinement of pricing mechanisms and internal routing to enhance swap efficiency, reduce slippage, etc.
   - 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.
3. **Security and User Control Enhancements:**
   - Implementation of fine-grained control over slippage and other trade parameters
   - Liquidity protection of LP pool token shares using zero-knowledge proofs (ZKPs)
   - Development of Account Abstraction (AA) mechanisms for secure LP token management
4. **USDC Integration:**
   - Integration of native USDC liquidity across supported chains
   - Integration of USDC's Cross-Chain Transfer Protocol (CCTP)
5. **Governance and Tokenomics:**
   - Design and implementation of a governance token for community-driven decision making
   - Development of a staking mechanism for Altcoin holders to participate in protocol governance
6. **Advanced Trading Features:**
   - Implementation of limit orders and advanced slippage controls for cross-chain swaps
   - Integration of parallelized routing and multi-hop strategies
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. **Enhanced Security:** The trustless nature of the protocol and its escrow mechanism provide robust security for cross-chain operations. With no centralized bridges or intermediaries, users and protocols can conduct cross-chain transactions with significantly reduced risk compared to traditional solutions.
2. **Advanced Arbitrage:** The system enables sophisticated arbitrage strategies through both parallelized routes within each hop and multi-hop combinations. Multiple value capture paths can be executed simultaneously through parallel routes within each hop, while supporting sophisticated multi-hop arbitrage strategies, creating deeper and

more efficient markets across blockchain ecosystems.

3. **Universal Liquidity and Capital Efficiency:** By enabling seamless asset transfers between different blockchain ecosystems, Altverse creates a universal liquidity layer that enables more efficient capital allocation across the DeFi landscape. This unified liquidity infrastructure addresses one of the biggest challenges in the fragmented blockchain ecosystem, potentially unlocking new levels of capital efficiency.
4. **Cross-Chain Protocol Development:** By providing a standardized interface for cross-chain operations, Altverse simplifies the development of truly trustless chain-agnostic protocols. This enables developers to build sophisticated cross-chain applications while abstracting away the complexity of cross-chain messaging and execution.
5. **Financial Market Unification:** The protocol's architecture establishes it as a potential cornerstone for institutional financial infrastructure, bridging traditional markets, CEXes, and DeFi ecosystems. This enables access to substantial traditional markets including global forex ($6T+ daily volume), derivatives ($1Q+ valuation), and institutional lending, unlocking unprecedented opportunities for cross-market arbitrage and liquidity provision.
6. **Enhanced User Experience:** Users can perform instant cross-chain swaps in a single transaction and with just one click, blurring the distinction between cross-chain and single-chain operations. This significant simplification from most current multi-step processes could lower the barrier to entry for new users and increase overall adoption of DeFi.

10 Conclusion

Altverse represents a significant advancement in cross-chain trading through its trustless, bridge-free architecture. 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, while creating natural pathways to traditional finance markets including centralized exchanges, forex, derivatives, and institutional lending.

As the protocol evolves and integrates with more chains and DEXes, it will 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 financial ecosystem – one that seamlessly connects both traditional and decentralized finance – positions it as a candidate for the foundational infrastructure layer of the future for global finance.