Whitepaper: Mixer Multichain – Ensuring Privacy Across EVM Blockchains

Abstract

Mixer Multichain is a decentralized protocol designed to provide privacy and anonymity for users across multiple Ethereum Virtual Machine (EVM) compatible blockchains. Supporting networks like Ethereum, Avalanche, Arbitrum, Lukso, Optimism, Binance, and Polygon, this innovative platform enables users to mix their funds in a pool, breaking the traceability between deposit and withdrawal addresses. By leveraging advanced cryptographic techniques, **Mixer Multichain** ensures that transactions remain private and secure.

Table of Contents

1. Introduction

Privacy in financial transactions is a fundamental right, yet public blockchains expose user activities to unwanted scrutiny. **Mixer Multichain** addresses this issue by offering a platform where users can anonymize their funds across multiple EVM-based blockchains. By mixing deposits in a shared pool, the protocol ensures that the link between deposit and withdrawal addresses is severed, protecting users’ identities.

Mixer Multichain supports the following blockchains: Ethereum, Avalanche, Arbitrum, Lukso, Optimism, Binance, and Polygon. Its multichain compatibility and flexible architecture make it a powerful tool for privacy-conscious users across the blockchain ecosystem.

---

2. Problem

Public blockchains, while transparent and secure, expose the transactions of users to potential surveillance and tracking. This lack of privacy can be detrimental for those who need to keep their financial transactions confidential. Additionally, current cryptocurrency mixers often operate on a single chain, limiting their ability to provide privacy across multiple blockchains.

Challenges:

- **Transaction Traceability**: Public exposure of blockchain addresses allows observers to link deposits with withdrawals.
- **Limited Privacy**: Existing mixers lack multichain support, restricting users from fully anonymizing their activities across multiple networks.

---

3. Solution

Mixer Multichain solves these problems by enabling users to mix their funds in a pool shared with other users, effectively breaking any link between the deposited and withdrawn funds. The protocol relies on the generation of three cryptographically secure codes:

- **Commitment**: A unique hash that is recorded on-chain and linked to the deposit.
- **Secret**: A private code used to authorize the withdrawal of funds.
- **Nullifier**: Ensures that each Commitment is used only once for withdrawals.

These codes are cryptographically linked but irreversible, meaning the **Secret** and **Nullifier** cannot be derived from the **Commitment**. This guarantees the security and anonymity of users when making transactions.

Flowchart of the Solution:

```
[Off-chain Generation] ----> [Commitment (Hash of Secret + Nullifier)]
       |                                  |
   [Private]                         [Public on blockchain]
```

4. Cryptographic Architecture

At the core of **Mixer Multichain** is its cryptographic architecture. Users generate the **Commitment**, **Secret**, and **Nullifier** off-chain. Only the **Commitment** is recorded on the blockchain, while the **Secret** and **Nullifier** remain private.

This process ensures that:

1. The **Commitment** is a cryptographic hash derived from the **Secret** and **Nullifier**.
2. The **Commitment** is recorded on-chain when the user deposits their funds.
3. To withdraw, the user must provide the **Secret** and **Nullifier**, making it impossible to link the withdrawal to the original deposit address.

Diagram of Cryptographic Flow:

```
[Commitment Generated] --> [Recorded on-chain]
[Secret + Nullifier] --> [Used for withdrawal privately]
```

5. Deposit and Withdrawal Process

Step 1: Wallet Connection

The user connects to the protocol via **Metamask** or a similar wallet.

Step 2: Code Generation

The dApp generates three cryptographic codes: **Commitment**, **Secret**, and **Nullifier** off-chain. Only the **Commitment** is shared publicly.

Step 3: Deposit

The user deposits their native blockchain currency using the **Commitment**, which is stored on-chain. This deposit is mixed with others in the shared pool.

Step 4: Withdrawal

The user switches to a different wallet and uses the **Secret** and **Nullifier** to withdraw funds to a third wallet, ensuring complete anonymity between the deposit and withdrawal.

Flowchart of Deposit and Withdrawal:

```
1. [Wallet 1] --(Commitment)--> [Deposit in pool]
2. [Funds mixed in pool]
3. [Wallet 2] --(Secret + Nullifier)--> [Withdrawal to Wallet 3]
```

6. Token Economy and Fees

The protocol charges a **5% fee** on every deposit made into the pool. This fee is used to ensure the long-term sustainability of the project and maintain liquidity within the pool. Users can withdraw their funds at any time, as long as they meet the waiting period and deposit conditions.

The **pool balance** is maintained to ensure that sufficient funds are always available for user withdrawals.

7. Tokenomics and DAO

DAO Launch

Mixer Multichain will launch a DAO, allowing the community to govern key aspects of the protocol. Users will be able to vote on decisions such as fee structure, future blockchain expansions, and privacy improvements.

Governance Token

The governance token will be launched on Binance Smart Chain (BSC) with a total supply of **18 million tokens**. Token holders will have voting rights and influence over the protocol’s evolution.

Token Distribution:

- **50%** will be distributed to the community through a **fair launch**.
- **25%** will be allocated to the DAO treasury for future development.
- **15%** will be reserved for the founding team.
- **10%** will be allocated for liquidity incentives and relayer development.

Tokenomics Chart:

```
[50%] Community (Fair Launch)
[25%] DAO Treasury
[15%] Founding Team
[10%] Incentives and Relayer Development
```

8. Use Cases

For Traders:

Traders can use **Mixer Multichain** to hide their strategies and movements between wallets, ensuring that their activities remain private.

For Organizations:

Companies that need to make private transactions across multiple blockchains can use the protocol to hide the origin of their funds.

For Individual Users:

Everyday users looking to keep their daily transactions private can benefit from the anonymity provided by **Mixer Multichain**, ensuring no link between their deposit and withdrawal activities.

9. Privacy and Security

Mixer Multichain implements advanced security measures:

1. **Irreversibility of Cryptographic Hashes**: The hashes generated are irreversible, ensuring that no one can derive the **Secret** or **Nullifier** from the **Commitment** recorded on-chain.
2. **Reentrancy Protection**: The contract uses `ReentrancyGuard` to prevent reentrancy attacks.
3. **Withdrawal Security**: The **Nullifier** ensures that each **Commitment** can only be used once, protecting against double withdrawal attempts.

---

10. Roadmap

Phase 1 (Completed):

- Deployment of contracts on **Ethereum, Avalanche, Arbitrum, Lukso, Optimism, Binance, and Polygon**.
- Launch of the **frontend** and social media channels.

Phase 2 (Upcoming):

- Launch of the **DAO** and **governance token** on Binance Smart Chain.
- Development of an **exclusive relayer** to enhance the anonymity of transactions.

Phase 3:

- Expansion to other EVM-compatible blockchains.
- Integration of **zk-SNARKs** for enhanced privacy.

Roadmap Chart:

```
[Phase 1] -> [Contracts and Frontend Launched]
[Phase 2] -> [DAO and Token Launch]
[Phase 3] -> [Relayer + zk-SNARKs Integration]
```

---

11. Conclusion

Mixer Multichain provides a robust solution for ensuring privacy in cryptocurrency transactions, leveraging the power of multichain compatibility and advanced cryptographic techniques. With its community-driven governance and strong commitment to user privacy, the protocol is positioned to become a key player in the future of anonymous transactions on the blockchain.