Picule Protocol Whitepaper

1. Abstract

Picule Protocol introduces a revolutionary trustless crowdfunding system that merges NFT and ERC-20 token launches into a unified, rug-pull-resistant ecosystem. By permanently locking LP tokens within NFTs while maintaining their earning potential, the protocol creates intrinsically valuable NFTs and eliminates developer exit scam risks.

2. Introduction

The current crypto landscape suffers from fragmented launch processes, valueless NFTs, and widespread rug pull scams. Picule Protocol addresses these issues through a novel approach: combining ICO crowdfunding with automated liquidity provision and NFT-based LP token locking, creating a trustless system where code guarantees replace reputation-based trust.

3. System Architecture

3.1 Core Components

The protocol consists of six interconnected smart contracts:

- **ICO Contract**: Manages contribution collection and goal verification
- **Token Launch Manager**: Factory contract creating verified ERC-20, ERC-721, and Funds Manager instances
- **Funds Manager**: Handles LP token locking and commission distribution via checkpoint system
- **Pair Contract**: Standard AMM pool with integrated commission tracking for locked liquidity
- **Router Contract**: Facilitates token swaps and liquidity operations
- **Marketplace**: Lists only verified assets created through the Token Launch Manager

3.2 Contract Interaction Flow

```
Investor → ICO Contract → Funds Manager → Pair Contract → NFT (LP Tokens)
                        ↓
                 Token Distribution
```

4. ICO Mechanism

4.1 Contribution Process

The ICO follows a time-bounded crowdfunding model using MON as the base currency:

1. **Project Creation**: Token Launch Manager deploys project-specific contracts
2. **Contribution Period**: Investors contribute MON within the deadline
3. **Success Condition**: Goal must be reached before deadline
4. **Automatic Execution**: Upon success, funds flow to Funds Manager for liquidity creation

4.2 Contribution Validation

The system enforces several constraints:

- Minimum contribution threshold
- Maximum total not exceeding target
- Deadline enforcement
- Contributor tracking for token distribution

4.3 Refund Mechanism

If the ICO fails to reach its target within the deadline:

- All contributor funds remain in the ICO contract
- Individual refunds can be claimed manually
- No tokens are distributed
- No liquidity pools are created

5. Liquidity Locking Innovation

5.1 LP Token Locking Process

Upon successful ICO completion:

1. Funds Manager receives all contributed MON
2. ERC-20 tokens are minted (10,000,000 × 10^18 total supply)
3. Liquidity is added to the AMM pool using equal value ratios
4. **Single NFT is minted** containing 100% of initial LP tokens
5. LP tokens are permanently locked but remain active in pool calculations

5.2 LP Token Structure

```
struct NFTData {
    address user;                    // NFT owner
    uint256 checkpointClaimed;       // Last claimed checkpoint
    uint256 _numOfAdd;               // Number of LP additions
    mapping(uint => uint256) checkpointLp;  // LP amount per checkpoint
    uint256 totalLpLockedByUser;     // Total LP tokens locked
}
```

6. Commission Distribution System

6.1 Commission Calculation

Trading fees are distributed to locked LP token holders based on their proportional share:

Locked Share Formula:

```
LS = (LLP × 10^18) / TS
```

Commission Share Formula:

```
S_i = (F_i × LS) / 10^18
```

Where:

- `LS` = Locked share ratio
- `LLP` = Total locked LP tokens
- `TS` = Total LP token supply
- `F_i` = Fee collected for asset i
- `S_i` = Commission share for asset i

6.2 Binary Commission Tracking

The pair contract tracks accumulated commissions using packed storage for gas optimization:

```
// Commission calculation in pair contract
lockedShare = (totalLockedLp × 10^18) / totalSupply
share0 = (fee0 × lockedShare) / 10^18
share1 = (fee1 × lockedShare) / 10^18

// Unpack stored binary commission
oldCommission0 = binaryCommission >> 128          // Left part (upper 128 bits)
oldCommission1 = binaryCommission & 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  // Right part (lower 128 bits)

// Add new shares to old commissions
newCommission0 = oldCommission0 + share0
newCommission1 = oldCommission1 + share1

// Pack back into single storage slot
binaryCommission = (newCommission0 << 128) | newCommission1
```

Trading Fee Structure: The pool collects a flat 0.3% fee on all swaps regardless of direction, distributed proportionally between the two assets in the pair.

7. Checkpoint System

7.1 Checkpoint Creation

Checkpoints are created whenever:

- New LP tokens are locked to an NFT
- Commission rewards are updated
- Manual checkpoint updates are triggered

7.2 Tokens Per Share Calculation

For each checkpoint, the system calculates tokens per share:

```
TPS_i = ((C_i + T_i) - O_i) / L × 10^18
```

Where:

- `TPS_i` = Tokens per share for commission flow i
- `C_i` = Current commission for asset i
- `T_i` = Total claimed commission for asset i
- `O_i` = Old total commission for asset i
- `L` = Total LP tokens locked

7.3 Reward Distribution

NFT holders can claim accumulated rewards by:

1. Calculating unclaimed checkpoints since last claim
2. Iterating through checkpoint history
3. Applying appropriate LP token amounts per checkpoint
4. Transferring proportional commission shares

8. Economic Model Example

8.1 Initial Setup

- ICO Target: 5,000 MON
- Token Supply: 10,000,000 tokens
- Initial Liquidity: 5,000 MON + 10,000,000 tokens
- LP Tokens Created: 100% locked in NFT (all initial LP tokens)
- Trading Fee: 0.3% collected on all swaps

8.2 Commission Calculation Example

Given:

- All LP Tokens: 100% locked in NFT (complete initial supply)
- Trading Volume: 10 MON (swap direction)

Calculation:

```
Locked Share: LS = (100% locked LP) = 1.0 × 10^18

Total Fee Collected: F = 10 × 0.003 = 0.03 MON

Commission for locked LP: S = (0.03 × 1.0 × 10^18) / 10^18 = 0.03 MON
```

Multi-Asset Distribution: The 0.03 MON commission is distributed proportionally between both pool assets based on current pool composition. If the pool is 50/50 MON/ERC-20:

- MON commission: 0.015 MON
- ERC-20 commission: equivalent value in ERC-20 tokens

Total Commission Earnings: NFT owner receives commission from all trading activity in both directions (MON→ERC-20 and ERC-20→MON swaps), with final payout calculated based on their share of locked LP tokens relative to total pool LP supply.

9. Additional LP Token Locking

9.1 User-Initiated Locking

Any user holding LP tokens can lock them to create or enhance NFTs:

1. **New NFT Creation**: Users with no existing NFT can lock LP tokens to mint one
2. **LP Addition**: Existing NFT owners can add more LP tokens to their NFT

3. **Checkpoint Updates**: Each addition triggers a new checkpoint for fair reward distribution

9.2 Multi-Addition Tracking

The system tracks multiple LP additions per NFT:

- Each addition creates a new checkpoint entry
- Historical LP amounts are preserved for accurate reward calculations
- Users can add LP tokens over time while maintaining fair distribution

10. Manager Claims and Token Economics

10.1 Three-Phase Manager Reward System

The protocol implements a sophisticated three-phase reward system designed to incentivize long-term value creation while increasing NFT utility:

Phase 1: Pre-Mint Phase (Token Supply Not Fully Minted)

- **MON Distribution**: 50% of earned MON fees are used for automatic liquidity addition
- **Token Minting**: ERC-20 tokens are minted on-demand to match added MON liquidity
- **ERC-20 Rewards**: All earned ERC-20 tokens from fees are sent directly to the manager
- **Pool Growth**: This phase naturally grows the liquidity pool and increases trading depth

Phase 2: Burn Phase (All Tokens Minted, Burning Active)

- **MON Rewards**: 100% of earned MON fees are transferred directly to the manager
- **Token Burning**: 50% of earned ERC-20 tokens are permanently burned
- **Value Appreciation**: Burning reduces total supply, potentially increasing per-token value
- **Deflationary Mechanism**: Creates upward pressure on token price

Phase 3: Full Distribution Phase (All Operations Complete)

- **Complete Rewards**: 100% of all fees (both MON and ERC-20) go directly to the manager
- **Maximum Utility**: NFT reaches peak earning potential
- **Stable Economics**: Token supply and pool composition are finalized

10.2 Economic Impact Analysis

Phase 1 Benefits:

- Increases pool depth and reduces slippage
- Creates buying pressure for ERC-20 tokens through minting demand
- Compounds LP token value through larger pool size

Phase 2 Benefits:

- Deflationary pressure increases scarcity value
- Manager receives full MON benefits while contributing to token appreciation
- Burn mechanism benefits all token holders

Phase 3 Benefits:

- Maximum revenue generation for NFT holders
- Stable, predictable fee distribution
- Full value realization of the NFT asset

10.3 Burn Limit Controls

To prevent economic manipulation and ensure system stability:

- Burn operations are governed by smart contract limits
- Maximum burn percentage per transaction is enforced
- Burn history is transparently tracked on-chain
- Emergency pause mechanisms protect against malicious burning

11. Marketplace Integration

11.1 Verification Requirements

The integrated marketplace enforces strict standards:

- Only tokens created via Token Launch Manager are listed
- All NFTs must contain locked LP tokens
- External LP positions are not permitted
- Contracts are deployed through verified factory patterns ensuring consistency

11.2 Trading Mechanics

NFT trading on the marketplace transfers:

- Ownership of locked LP tokens
- Rights to future commission claims
- All unclaimed rewards up to the sale point

12. Security Considerations

12.1 Immutable LP Locking

- LP tokens locked in NFTs can never be withdrawn
- No admin functions exist to unlock LP tokens
- Smart contracts are designed without upgrade mechanisms for core locking logic

12.2 ICO Refund Safety

- Failed ICOs require manual refund claims
- No automatic refund mechanisms to prevent MEV attacks
- Contributors maintain full control over their refund timing

12.3 Permissioned Architecture

- Pair creation is restricted to verified Funds Manager contracts only
- Token Launch Manager creates trusted contract instances during project deployment
- Factory contracts validate all component integrations through whitelist system

13. Risk Analysis

13.1 Smart Contract Risks

- All contracts operate under strict protocol control with immutable core logic
- Function calls are restricted to trusted contracts through permissioned architecture
- Internal contract interactions follow predetermined patterns to ensure system integrity

13.2 Economic Risks

- LP token value depends on underlying asset performance
- Commission earnings rely on trading volume
- Market adoption affects overall system value

13.3 Regulatory and Disclaimer Considerations

Data Transparency: All protocol data will be publicly accessible through subgraph systems, ensuring complete transparency of operations, transactions, and token movements.

Financial Disclaimer:

- Picule Protocol is an experimental DeFi system designed for educational and technological demonstration purposes
- All participants engage with smart contracts at their own risk
- No guarantees are made regarding token value, NFT appreciation, or commission earnings
- This protocol should be considered similar to other crypto, NFT, and memecoin projects in terms of speculative nature
- Users should only participate with funds they can afford to lose entirely
- The protocol creator assumes no financial responsibility for user losses or system performance

Regulatory Status:

- The protocol operates as a decentralized system without central control after deployment

- All operations are governed by immutable smart contracts
- Users are responsible for compliance with their local regulations regarding digital asset ownership and trading

14. Future Development

14.1 Planned Enhancements

- **Uniswap V3 System Integration**: Potential Protocol V2 development with concentrated liquidity model (not migration of existing pools due to immutable contracts)
- **Advanced Marketplace Features**: Enhanced NFT trading mechanics and analytics
- **Subgraph Integration**: Complete on-chain data accessibility through The Graph protocol

14.2 Governance Considerations

- **Protocol Evolution**: Careful development of new features while maintaining core security principles
- **Community Feedback Integration**: Development priorities based on user adoption and community interest

15. Conclusion

Picule Protocol represents a fundamental innovation in combining NFTs, token launches, and liquidity provision. By permanently locking LP tokens within NFTs while preserving their earning potential, the protocol creates a trustless system that eliminates rug pull risks while providing intrinsic value to NFTs.

The checkpoint-based commission distribution ensures fair reward allocation, while the integrated marketplace creates a complete ecosystem for verified, value-backed digital assets. This one-man project demonstrates that innovative solutions can emerge from identifying and solving real problems in the crypto space.

As the first ICO featuring the MPC token launches, Picule Protocol will prove its model and open the platform to other creators, democratizing access to trustless fundraising while maintaining the highest security standards.

Picule Protocol - Trustless Innovation in Digital Asset Creation
Conceived and Developed in 2024