ClenFi Protocol - Complete Master Documentation v2.0

Executive Summary

Mission Statement

ClenFi revolutionizes DeFi lending by eliminating over-collateralization requirements through Zero-Knowledge proof identity verification, enabling billions of users to access credit based on their proven unique identity and on-chain credit history rather than locked capital.

Core Innovation Matrix

Problem	Traditional DeFi Solution	ClenFi Innovation
Capital Inefficiency	150% over-collateralization	Zero collateral required
Identity Verification	Wallet-based pseudonymity	ZK-proof of PAN (privacy-preserved)
Credit Assessment	None (collateral-only)	On-chain credit scoring (300-900)
Governance	Token-based voting (plutocratic)	Proof of Trust (7-of-11 multisig)
User Rewards	Liquidity mining (inflationary)	Dual-layer sustainable rewards

Key Metrics

- **Target Market**: 1.4B Indians with PAN cards (expanding globally)
- **Credit Multiplier**: 1.5x-3x based on credit score
- **APR Range**: 9-24% (tier-based)
- **Default Target**: <3%
- **Revenue Model**: 1.5% transaction fee + interest spread
- **6-Month Revenue Projection**: $74,880 (conservative)

---

1. System Architecture

1.1 Multi-Chain Strategy

Chain	Purpose	Contracts	Why
Ethereum	Identity anchoring	Registry, ProofOfTrust	Maximum security, decentralization
Arbitrum	Daily transactions	All core contracts	Low gas costs (~$0.50/tx)
Base	AI & rewards	ScoreEngine, RewardsHub	Coinbase ecosystem, fast finality

1.2 Smart Contract Architecture

```
graph TD
    A[User] --> B[Registry - Identity]
    B --> C[CreditNFT]
    C --> D[Spender]
    D --> E[Uniswap V3]
    D --> F[DebtNFT]
    F --> G[Repay]
    G --> H[ScoreEngine]
    H --> C
    I[ProofOfTrust] --> J[RiskParams]
    J --> D
    J --> G
    K[OracleHub] --> D
    L[Emergency] --> ALL[All Contracts]
    G --> M[RewardsHub]
    M --> N[CT Points]
    M --> O[CLEN Token]
```

1.3 Core Components Table

Component	Contract	Purpose	Key Innovation
Identity	Registry	ZK-PAN verification	One-human-one-identity
Credit Line	CreditNFT	Credit representation	Dormant upgrades (no burn)
Debt Tracking	DebtNFT	Loan management	Lot-based accounting
Spending	Spender	Token conversion	Uniswap V3 integration
Repayment	Repay	Payment processing	Multi-token support

Scoring	ScoreEngine	Credit evaluation	Deterministic on-chain
Governance	ProofOfTrust	Parameter control	7-of-11 multisig
Rewards	RewardsHub	Incentive distribution	Dual-token system
Risk	RiskParams	Configuration store	Real-time updates
Price Feeds	OracleHub	Oracle aggregation	Multi-source validation
Safety	Emergency	Circuit breakers	Automatic triggers

---

2. Identity System (ZK-PAN)

2.1 Zero-Knowledge Architecture

User Input:
├── PAN Number (private)
├── Salt (random)
└── Secret (user-chosen)

ZK Circuit Output:
├── Commitment: H(PAN || salt)
├── Nullifier: H(PAN || secret)
└── Proof: SNARK proof of validity

On-Chain Storage:
├── Nullifier (prevents duplicates)
├── Commitment (identity anchor)
└── IdentityId: H(nullifier)

2.2 Privacy Guarantees

Data Type	Storage Location	Visibility	Reversibility
PAN Number	Never stored	Never visible	Impossible
Personal Info	Never stored	Never visible	Impossible
Salt/Secret	User's device only	User only	N/A
Nullifier	On-chain (hashed)	Protocol only	Computationally infeasible

Commitment	On-chain (hashed)	Protocol only	Computationally infeasible
Wallet Addresses	On-chain	Public	N/A
Credit Score	On-chain	Public	N/A

2.3 Registration Flow

```
// Step 1: User generates proof off-chain
proof = generateZKProof(PAN, salt, secret)

// Step 2: Submit to Registry contract
Registry.registerZK(proof, nullifier, commitment)
// Gas cost: ~$10 on Arbitrum

// Step 3: Bind wallet
Registry.bindWallet(wallet, signature)

// Result: One identity, multiple wallets OK
```

---

3. Credit System

3.1 Credit NFT Mechanics

Property	Description	Range	Update Method
Face Value	Purchase amount	$100-$25,000	Fixed at mint
Spending Capacity	Face value × multiplier	$150-$75,000	Tier-based
Validity Period	Active duration	365 days	Renewable
APR	Interest rate	9-24%	Score-based
Version	Metadata version	1+	Dormant upgrade

3.2 Credit Lifecycle State Machine

[None] → [Issued] → [Active] → [Multiple Paths]:

```
├→ [Frozen] → [Active] (payment cure)
├→ [Expired] → [Renewed]
└→ [Defaulted] → [Burned]
```

3.3 Spending Power Formula

spendingPower = faceValue × tierMultiplier × protocolHealthFactor

where:
- tierMultiplier: 1.5x (Bronze) to 3.0x (Diamond)
- protocolHealthFactor: 0.5x to 1.0x (based on global risk)

---

4. Credit Scoring System

4.1 Score Calculation (300-900 Range)

```
// Base Score
baseScore = 300

// Performance Components
repaymentScore = (onTimePayments / totalPayments) × 350  // 35% weight
utilizationScore = (1 - currentUtilization) × 200         // 20% weight
tenureScore = min(accountAge / 365, 1) × 150              // 15% weight
diversityScore = (uniqueTokensUsed / 5) × 100             // 10% weight

// Penalties
penalties = daysLate30to60 × 10 +
            daysLate60to90 × 25 +
            daysLateOver90 × 50

// Final Calculation
finalScore = baseScore + repaymentScore + utilizationScore +
             tenureScore + diversityScore - penalties

// Protocol Stress Adjustment
adjustedScore = finalScore × (1 - protocolStressLevel)
```

4.2 Tier System

Score Range	Tier	Multiplier	APR	Max Credit	Benefits
300-450	Bronze	1.5x	24%	$1,000	Basic access
451-550	Silver	1.75x	18%	$2,500	Lower APR
551-650	Gold	2.0x	15%	$5,000	Higher limits
651-750	Platinum	2.5x	12%	$10,000	Premium features
751-900	Diamond	3.0x	9%	$25,000	VIP treatment

---

5. Rewards System (Dual-Token)

5.1 CT Points (Credit Tokens)

Nature: Non-transferable reward points for good behavior

Earning Formula:

```
CT_earned = min(UserCap, EpochCap,
  interestPaid × baseEarnRate × tierMultiplier × scoreFactor ×
  (1 + earlyBonus) × (1 + streakBonus) × (1 + sCLENBoost))
```

Variable Definitions:

- `baseEarnRate`: 0.50 CT per $1 interest paid
- `tierMultiplier`: 0.8x (Bronze) to 1.8x (Diamond)
- `scoreFactor`: Linear 300→0.5x to 900→1.5x
- `earlyBonus`: +10% if paid ≥3 days early
- `streakBonus`: +10/20/30% at 3/6/12 consecutive on-time
- `sCLENBoost`: +0-30% based on CLEN staking duration

Usage:

1. **Primary**: Reduce interest at repayment (up to 50%)
2. **Secondary**: Redeem coupon NFTs from partners

5.2 CLEN Token

Nature: ERC-20 utility token (1B max supply)

Token Distribution:

Allocation	Amount	Vesting	Purpose
Liquidity Pool	50-100M	Immediate	DEX seeding
Rewards Pool	200-300M	Epoch drip	User incentives
Team/Founders	100M	3-4 years	Alignment
Investors	100-150M	2-3 years	Funding
Treasury Reserve	450-550M	PoT controlled	Future ops

Utility Functions:

1. **Staking**: Lock CLEN → sCLEN for CT boost (up to +30%)
2. **Fee Discounts**: Pay fees in CLEN for up to 25% discount
3. **Premium Access**: Exclusive coupons and partner perks
4. **Governance**: Non-binding Snapshot polls

5.3 Economic Sustainability

Funding Sources:

- 30% of transaction fees → Rewards Pool
- 5% of liquidation penalties → Rewards Pool
- Unspent campaign budgets roll over

Controls:

- Hard caps per user per epoch
- PoT controls emission rates
- Automatic circuit breakers if unsustainable

---

6. Debt Management & Liquidation

6.1 Debt NFT Structure

struct DebtNFT {

```
    uint256 creditNFTId;      // Associated credit line
    uint256 principal;        // Outstanding amount
    uint256 accruedInterest;  // Accumulated interest
    bytes32[] lots;           // Individual spending episodes
    uint256 dueDate;          // Next payment deadline
    uint8 delinquencyState;   // Current status
    Payment[] history;        // Repayment records
}
```

6.2 Delinquency Timeline

Days Late	Status	Actions	Score Impact	Reversible
0-7	Grace Period	Reminders only	None	N/A
8-14	Early Warning	2% late fee	-10 points	Yes
15-29	Soft Freeze	+5% APR, spending blocked	-25 points	Yes
30-60	Hard Freeze	NFT non-transferable	-50 points	Yes
61-89	Pre-Liquidation	Debt offered at 30% discount	-100 points	Partial
90+	Default	NFT burned, permanent record	-200 points	No

6.3 Liquidation Mechanism

For Liquidators:

```
Example: $1,000 debt, 90 days late
├── Outstanding with fees: $1,100
├── Offered at: $770 (30% discount)
├── Liquidator buys: $770
├── Collects from user: $950 (negotiated)
└── Profit: $180 (23% return)
```

Revenue Split:

- Liquidator: 50% of penalty
- Treasury: 50% of penalty

---

7. Governance (Proof of Trust)

7.1 Approver Composition

Role	Count	Expertise	Compensation
Founders/Core	3	Protocol knowledge	$5,000/month
Risk Experts	2	TradFi credit	$3,000/month
Technical Experts	2	Smart contracts	$3,000/month
Community Leaders	2	DeFi reputation	$2,000/month
Legal Advisor	1	Compliance	$2,000/month
Financial Advisor	1	Treasury mgmt	$2,000/month

7.2 Decision Framework

Decision Type	Quorum	Timelock	Examples
Normal	7/11	48 hours	Parameter updates
Emergency	9/11	Immediate	Circuit breakers
Critical	11/11	72 hours	Protocol upgrades

7.3 Governance Parameters

// Core Risk Parameters
baseAPR: 1200 bps (0-5000 range)
spendMultiplier: 2.0x (1.5x-3.0x range)
gracePeriodDays: 7 (3-14 range)
maxUserExposure: $10,000 ($1k-$100k range)
maxProtocolExposure: $10M ($1M-$100M range)

// Update Frequencies
- Daily: Protocol exposure limits
- Weekly: User limits, oracle feeds
- Monthly: APR, multipliers, fees
- Quarterly: Score weights, grace periods

---

8. Technical Implementation

8.1 Contract Specifications

Contract	Gas Cost (avg)	Storage Slots	Upgrade Pattern
Registry	150k	20	UUPS
ProofOfTrust	80k	15	UUPS
CreditNFT	200k	25	UUPS + Dormant
DebtNFT	180k	30	UUPS
ScoreEngine	100k	18	UUPS
Spender	250k	22	UUPS
Repay	120k	20	UUPS
RewardsHub	150k	35	UUPS
OracleHub	60k	12	UUPS
Emergency	40k	10	UUPS

8.2 Security Architecture

Access Control:

DEFAULT_ADMIN_ROLE: Protocol owner
UPGRADER_ROLE: Upgrade contracts
PAUSER_ROLE: Emergency pause
RISK_ROLE: Risk parameters
POT_APPROVER_ROLE: Governance
ORACLE_ROLE: Price feeds
ATTESTER_ROLE: Score updates

Security Measures:

- Reentrancy guards on all external calls
- Integer overflow protection (Solidity 0.8.x)
- Timelock delays (48-72 hours)

- Multi-signature requirements
- Circuit breakers (automatic + manual)
- 50-slot storage gaps for upgrades

8.3 Oracle Architecture

Primary: Chainlink (every block)
↓ (if stale/unavailable)
Secondary: Uniswap V3 TWAP (10-min window)
↓ (if manipulation detected)
Emergency: PoT Manual Feed (requires 7/11)

---

9. DEX Integration (Uniswap V3)

9.1 Spending Flow

```
function spend(uint256 creditNFTId, address tokenOut, uint256 amount) {
    // 1. Validation
    require(ownerOf(creditNFTId) == msg.sender);
    require(!isFrozen(creditNFTId));
    require(availableCapacity >= amount);

    // 2. Quote from Uniswap
    (uint256 amountOut, uint256[] memory fees) = quoter.quoteExactInput(
        abi.encodePacked(CREDIT_TOKEN, poolFee, tokenOut),
        amount
    );

    // 3. Slippage protection
    uint256 minAmountOut = amountOut * (10000 - maxSlippageBps) / 10000;

    // 4. Execute swap
    uint256 actualOut = router.exactInput(SwapParams({
        path: abi.encodePacked(CREDIT_TOKEN, poolFee, tokenOut),
        recipient: msg.sender,
        deadline: block.timestamp + 300,
        amountIn: amount,
        amountOutMinimum: minAmountOut
    }));

    // 5. Create/update debt
    debtNFT.addLot(creditNFTId, amount, apr);
```

```
    // 6. Update score
    scoreEngine.recompute(getIdentity(msg.sender));
}
```

9.2 Supported Tokens & Pools

Token Pair	Pool Fee	Min Liquidity	Max Slippage
USDC/USDT	0.05%	$500k	0.5%
USDC/DAI	0.05%	$500k	0.5%
USDC/WETH	0.3%	$1M	1.0%
USDC/WBTC	0.3%	$1M	1.0%

---

10. Risk Management

10.1 Risk Controls Matrix

Control Type	User Level	Protocol Level	Circuit Breaker
Exposure Limits	$10k default	$10M total	>20% breach
Daily Velocity	50 tx/day	10k tx/day	>200% normal
Default Rate	N/A	3% target	>5% trigger
Price Deviation	5% slippage	10% oracle	>15% halt
Gas Price	N/A	500 gwei max	>1000 gwei

10.2 Circuit Breaker Logic

```
if (defaultRate > 5%) {
    pauseNewCredits();
    increaseRequiredScores();
    notifyPoT();
}

if (priceDeviation > 10%) {
```

```
    pauseSwaps();
    switchToManualOracle();
}

if (protocolTVL.dropped(20%, 1 hours)) {
    globalPause();
    emergencyPoTMeeting();
}
```

---

11. Economics & Revenue Model

11.1 Fee Structure

Fee Type	Rate	Distribution	Example ($1000 spend)
Transaction	1.5%	70% Treasury, 30% Rewards	$15
Interest	9-24% APR	80% Treasury, 20% Rewards	$7.50-20/month
Late Payment	2%	100% Treasury	$20
Liquidation	10%	50% Liquidator, 50% Treasury	$100

11.2 6-Month Financial Projection

Conservative Scenario:

Assumptions:
- Starting users: 100
- Growth rate: 50% monthly
- Average credit: $2,000
- Utilization: 60%
- Average APR: 18%
- Default rate: 3%

Month 1: 100 users × $2,000 × 60% × 1.5% = $1,800 fees
Month 2: 150 users × $2,000 × 60% × 1.5% = $2,700 fees
Month 3: 225 users × $2,000 × 60% × 1.5% = $4,050 fees
Month 4: 338 users × $2,000 × 60% × 1.5% = $6,084 fees
Month 5: 507 users × $2,000 × 60% × 1.5% = $9,126 fees
Month 6: 760 users × $2,000 × 60% × 1.5% = $13,680 fees

Plus interest income (18% APR on outstanding):
Month 1-6 cumulative: ~$37,440

Total 6-month revenue: $74,880

11.3 Treasury Allocation

Total Revenue: $74,880
├── Operations (40%): $29,952
├── Founder 1 (30%): $22,464
├── Founder 2 (20%): $14,976
└── Strategic Partner (10%): $7,488

---

12. User Experience Examples

12.1 New User Journey (Raj - Retail Trader)

Day 1: Registration
├── Submit ZK proof of PAN ($10 gas)
├── Purchase $500 Credit NFT
└── Receive $750 spending power (Bronze 1.5x)

Week 1: First Transaction
├── Buy 0.3 ETH for NFT purchase
├── Debt NFT created: $750 @ 24% APR
└── Monthly payment: $765 (principal + interest)

Month 1: First Repayment
├── Pay $100 on time
├── Earn 50 CT points (0.5 × $100)
└── Score increases to 460 (+10 points)

Month 6: Established User
├── Score: 650 (Gold tier achieved)
├── New credit line: $5,000
├── APR reduced: 15% (from 24%)
├── Total savings: $450 in interest
└── CT points accumulated: 500

12.2 Power User Strategy (Sarah - Arbitrageur)

Optimization Strategy:
├── Maintain 50-60% utilization (optimal score)
├── Pay 5 days early (earlyBonus +10%)
├── Diversify across 5+ tokens (diversity score)
├── Stake 10,000 CLEN for 6 months (+20% CT boost)
└── Refer 5 users (referral rewards)

Results Timeline:
├── Month 1: Bronze → Silver (Score 450→520)
├── Month 3: Silver → Gold (Score 520→620)
├── Month 6: Gold → Platinum (Score 620→750)
└── Benefits: 2.5x multiplier, 12% APR, $10,000 limit

Monthly Operations:
├── Credit line: $10,000 → $25,000 spending power
├── Arbitrage volume: $200,000
├── Gross profit: $20,000 (10% margin)
├── Protocol fees: $3,000 (1.5%)
├── Interest cost: $100 (12% APR)
└── Net profit: $16,900

12.3 Business Use Case (Alice - NFT Gallery)

Business Setup:
├── Register business wallet with ZK-PAN
├── Purchase $10,000 Credit NFT
├── Receive $20,000 spending power (Gold 2.0x)
└── APR: 15%

Daily Operations:
├── Spot purchases at NFT launches
├── Instant liquidity for deals
├── No collateral locked
└── Flexible repayment terms

Monthly Performance:
├── NFT purchases: $200,000
├── Sales revenue: $240,000
├── Protocol fees: $3,000
├── Interest cost: $250
├── Traditional loan cost avoided: $2,000
└── Net benefit: $1,750/month saved

---

13. Deployment & Launch Strategy

13.1 Deployment Phases

Phase	Timeline	Milestone	Success Criteria
Alpha	Month 1	Testnet deployment	100 test users
Beta	Month 2-3	Mainnet soft launch	1,000 users, <1% bugs
Launch	Month 4	Public release	5,000 users
Growth	Month 5-6	Scaling	10,000 users
Expansion	Month 7+	Multi-region	50,000 users

13.2 Initial Configuration

```
// Deployment Order
1. Deploy Registry (Ethereum)
2. Deploy ProofOfTrust (Ethereum)
3. Deploy all contracts (Arbitrum)
4. Deploy RewardsHub (Base)
5. Configure parameters via PoT
6. Seed CLEN liquidity pool
7. Enable circuit breakers
8. Open registration

// Initial Parameters
baseAPR = 1200; // 12% base
spendMultiplier = 200; // 2.0x
gracePeriodDays = 7;
maxUserExposure = 10000e18; // $10,000
protocolCap = 10000000e18; // $10M
defaultRateTarget = 300; // 3%

// CLEN Token Launch
Total Supply: 1,000,000,000 CLEN
Initial LP: 50M CLEN + $1M USDC
Initial Price: $0.02
```

Market Cap at Launch: $20M (FDV)

---

14. Compliance & Regulatory

14.1 Compliance Framework

Requirement	Implementation	Verification
KYC/AML	ZK-PAN proof	On-chain verifiable
GDPR	Data minimization, right to forget	Nullifier revocation
Securities	No investment contract	Howey test compliant
Lending Laws	Jurisdiction-specific terms	PoT governance

14.2 Regulatory Strategy

1. **India Focus**: Launch with PAN (1.4B addressable)
2. **Regulatory Sandbox**: Apply for RBI sandbox
3. **Global Expansion**: Add SSN (US), NIN (UK), etc.
4. **Compliance Partners**: Legal advisors in each region

---

15. Risk Disclosure

15.1 Protocol Risks

Risk Type	Severity	Mitigation
Smart Contract	High	Audits, bug bounties, insurance
Oracle Manipulation	Medium	Multi-source validation
Governance Capture	Low	7/11 multisig, timelock
Regulatory	Medium	Compliance framework
Market Risk	High	Circuit breakers, limits

15.2 User Risks

- **No Collateral Recovery**: Unsecured loans mean no asset seizure
- **Credit Score Impact**: Poor repayment affects future access
- **Smart Contract Risk**: Potential bugs or exploits
- **Market Volatility**: Token price fluctuations

---

16. Future Roadmap

Phase 1: Foundation (Months 1-6) ✓

- [x] Core protocol development
- [x] ZK-PAN implementation
- [x] Uniswap V3 integration
- [x] Basic scoring system
- [x] PoT governance
- [x] Rewards system design

Phase 2: Enhancement (Months 7-12)

- [ ] AI-powered scoring (GPT integration)
- [ ] Multi-country identity support
- [ ] Mobile app launch
- [ ] Institutional partnerships
- [ ] Advanced analytics dashboard
- [ ] Cross-chain bridges

Phase 3: Expansion (Year 2)

- [ ] Global identity framework
- [ ] B2B credit lines
- [ ] Crypto credit cards
- [ ] DeFi credit bureau
- [ ] Regulatory licenses
- [ ] $1B TVL target

Phase 4: Maturity (Year 3+)

- [ ] Full DAO transition (optional)
- [ ] Protocol token (if needed)
- [ ] Traditional finance integration
- [ ] Credit derivatives

- [ ] Global standard for DeFi credit

Appendices

Appendix A: Contract Interfaces

[Detailed function signatures for all 11 contracts - see Technical Specification document for complete listing]

Appendix B: Error Codes

Code	Error	Description
E001	INVALID_PROOF	ZK proof verification failed
E002	DUPLICATE_IDENTITY	Nullifier already used
E003	INSUFFICIENT_CAPACITY	Spending limit exceeded
E004	NFT_FROZEN	Credit line suspended
E005	ORACLE_STALE	Price data outdated
E006	CIRCUIT_BREAKER_TRIGGERED	Emergency pause activated

Appendix C: Events

Event	Emitted By	Parameters
IdentityRegistered	Registry	(nullifier, commitment, wallet)
CreditIssued	CreditNFT	(tokenId, owner, faceValue)
SpendExecuted	Spender	(creditId, amount, token)
RepaymentMade	Repay	(debtId, amount, remaining)
ScoreUpdated	ScoreEngine	(identity, oldScore, newScore)
ProposalApproved	ProofOfTrust	(proposalId, attesters)

Glossary

Term	Definition
APR	Annual Percentage Rate - yearly interest rate
cNFT	Credit NFT - represents user's credit line
CLEN	Protocol utility token for rewards and governance polls
CT Points	Credit Tokens - non-transferable reward points
dNFT	Debt NFT - tracks outstanding loans
Nullifier	Unique identifier preventing double registration
PAN	Permanent Account Number (Indian tax ID)
PoT	Proof of Trust - 7-of-11 governance mechanism
sCLEN	Staked CLEN tokens with time lock
TWAP	Time-Weighted Average Price
UUPS	Universal Upgradeable Proxy Standard
ZK	Zero-Knowledge proof

Contact & Resources

- **Documentation**: docs.clenfi.com
- **GitHub**: github.com/clenfi/protocol
- **Discord**: discord.gg/clenfi
- **Twitter**: @ClenFiProtocol
- **Email**: team@clenfi.com
- **Bug Bounty**: immunefi.com/bounty/clenfi

Legal Disclaimer

This documentation is for informational purposes only and does not constitute financial advice, an offer to sell, or a solicitation to buy any tokens or use any services. The ClenFi protocol is experimental software that carries significant risks. Users should conduct their own research and consult professional advisors before participating. The protocol is provided "as is" without warranties of any kind.

Document Information

- **Version**: 2.0.0
- **Status**: Complete Master Documentation
- **Created by**: The Honoured Ones