TRUSTFY V4.2

Product Requirements Document (PRD)

Product: Trustfy
Version: V4.2
Scope: Non-custodial, smart-contract-powered P2P escrow marketplace
Target networks: EVM-compatible chains
Audience: Engineering, Security Audit, Compliance, Product, Indexer, UI

---

1. Product Vision

Trustfy is a **non-custodial P2P escrow platform** where:

- Funds are locked before trade execution
- Economic commitment replaces reputation systems
- Disputes resolve by facts, not authority
- Platform fees pay for service, not dispute outcomes
- No central party holds user funds

All critical economic rules are enforced by smart contracts.

---

2. Design Principles

1. **Funds first, intent second**
   Trades begin only after capital commitment.
2. **Economic seriousness over trust**
   Bonds filter spam, fraud, and unserious actors.
3. **Deterministic outcomes**
   Every terminal state produces predictable balance changes.
4. **Minimal custody surface**
   Credits exist as ledger entries, not discretionary custody.
5. **Clear separation of concerns**
   Ads, credits, and escrow remain modular.

---

3. System Architecture Overview

On-chain modules

Module	Responsibility
TrustfyCreditVault	Unified credit wallet per user per token
TrustfyAdBondManager	Ad bond locking, slashing, ad state control
TrustfyEscrow	Trade execution, fees, bonds, disputes

Off-chain modules

- UI and intent builder
- Indexer and event processor
- Fiat settlement and messaging
- Evidence collection for disputes

---

4. Asset Model

TokenKey definition

- `tokenKey = address(0)` → native coin
- `tokenKey = ERC20 address` → ERC20 token

All balances, pools, and credits are tracked per `tokenKey`.

---

5. Unified Credit Wallet (V4.2 Core Change)

5.1 Definition

Each user has **one unified credit wallet per token**:

```
credits[user][tokenKey]
```

This wallet is shared across:

- Ad bonds
- Seller bonds
- Buyer dispute bonds
- Bond refunds

- Fee refunds

5.2 Credit funding sources

Credits increase only by:

1. Wallet deposits (native or ERC20)
2. Contract-granted credits from:
   - bond refunds
   - fee refunds
   - trade refunds

5.3 Credit usage

Credits are spent only by:

- AdBondManager
- Escrow contract

Direct user spending is not permitted.

5.4 Withdrawals

Rules:

- User must hold sufficient credit
- Credit balance must meet `withdrawThreshold`
- Withdrawals send funds directly to user wallet
- Threshold exists to reduce micro-withdraw spam and gas waste

---

6. Fee Model (V4.2 Clarified)

6.1 Fee types

- Maker fee
- Taker fee

Both fees:

- Exist only in crypto
- Are paid upfront by seller
- Are reimbursed off-chain in fiat by buyer

6.2 Fee settlement rules

Trade outcome	Platform fee
Happy path	Collected
Dispute buyer-wins	Collected
Dispute seller-wins	Refunded to seller credits

Fees are **payment for platform service**, not penalties.

---

7. Bond System

7.1 Bond types

Bond	Purpose
Ad bond	Spam prevention
Seller bond	Seller honesty enforcement
Buyer bond	Buyer honesty enforcement

7.2 Bond rules

- Bonds are locked before progress
- Winner bond is refunded
- Loser bond is forfeited to platform bond revenue

---

8. Ad Lifecycle and Enforcement (V4.2 Core Change)

8.1 Ad bond requirement

Before an ad becomes visible:

- Ad bond must be locked
- Funding source: credit wallet or Web3 wallet

8.2 Ad states

State	Meaning
POSTED	Editable, cancelable
IN_PROGRESS	Trade started, locked
CLOSED	Closed without penalty
CANCELLED_SLASHED	Bond forfeited

8.3 Editing rules

- Editing allowed only in POSTED
- Editing blocked in IN_PROGRESS

8.4 Cancellation rules

- Cancel in POSTED → ad bond forfeited
- Cancel in IN_PROGRESS → blocked

This rule enforces spam resistance on-chain.

---

9. Trade Lifecycle

9.1 On-chain trade states

State	Meaning
CREATED	Seller listed trade
TAKEN	Buyer accepted
FUNDED	Seller locked funds
PAYMENT_CONFIRMED	Buyer locked bond
DISPUTED	Arbitration active
RESOLVED	Terminal success
CANCELLED	Terminal refund

9.2 Trade flow

1. Seller creates trade
2. Buyer takes trade
3. Seller locks amount + fee + seller bond
4. Buyer confirms payment and locks buyer bond
5. Seller releases funds or dispute begins

10. Timeout Rules

Scenario	Action
Buyer fails to confirm	Seller refunds after window
Seller fails to release	Buyer opens dispute

Timeouts protect capital and prevent hostage scenarios.

11. Dispute System (V4.2 Final Logic)

11.1 Dispute initiation

- Allowed after release window expires
- Either party may initiate

11.2 Dispute outcomes

Buyer wins

- Buyer receives trade amount
- Buyer bond refunded
- Seller bond forfeited to platform
- Platform fee collected

Seller wins

- Seller receives trade amount back
- Seller bond refunded
- Buyer bond forfeited to platform
- Platform fee refunded to seller credits

This rule enforces fairness without rent extraction.

12. Platform Revenue Accounting

12.1 Pools

Pool	Source
platformFeePool	Collected fees
platformBondRevenue	Forfeited trade bonds
adBondRevenue	Slashed ad bonds

All pools are tracked per tokenKey.

12.2 Withdrawals

- Admin withdraws to feeRecipient
- No direct user access
- Transparent on-chain accounting

13. Security Constraints

- Reentrancy protection on all transfers
- No `transfer()` usage
- Strict tokenKey validation
- Fee basis points capped on-chain
- Role-based access control enforced

14. Off-chain Responsibilities

Area	Responsibility
UI	Intent building, quotes, approvals
Indexer	Event indexing, state mirroring
Messaging	Fiat coordination
Dispute evidence	Off-chain storage

Off-chain logic never moves funds.

---

15. Compliance Positioning

- No custody of user funds
- No KYC enforced on-chain
- Smart contract enforces fairness
- Arbitrator role limited to dispute resolution

---

16. Audit Expectations

Auditors should verify:

- Deterministic balance changes
- No ambiguous fee paths
- Bond symmetry
- No admin fund seizure paths
- No silent state changes

---

17. Non-Goals

Trustfy does not:

- Guarantee fiat settlement
- Reverse on-chain outcomes
- Enforce off-chain evidence formats
- Act as counterparty

---

18. V4.2 Acceptance Criteria

- Every PRD rule maps to on-chain logic
- All terminal states produce exact balance deltas
- Ad spam economically discouraged
- Seller-wins dispute refunds fees
- Buyer-wins dispute charges fees
- Unified credit wallet operational

---

19. Summary

Trustfy V4.2 is a **deterministic, economically enforced escrow system**.

Trust is replaced by locked capital.
Authority is replaced by code.
Fairness is enforced by math.