REMITTIX (RTX)

Risk Analysis Report v1.0

Prepared: 2026-02-18

Prepared by RedFlag Analytics – Independent Blockchain Risk Reports

Legal Disclaimer (Read First)

This document is an independent analytical and forensic risk assessment based solely on publicly available information, user-supplied screenshots of project communications, and blockchain transaction data observed via block explorers at the time of analysis. It does not constitute financial advice, investment advice, or legal advice, and it does not assert criminal misconduct. Where uncertainty exists, it is explicitly stated. All probability ranges are analytical estimates intended to quantify uncertainty and risk—NOT factual determinations.

Executive Summary

Remittix presents itself as a PayFi / cross-border payments solution intended to enable crypto-to-fiat transfers that settle into bank accounts. The project has been promoted via an extended presale period (reported starting in December 2024 and continuing into 2026) and high-intensity bonus campaigns (e.g., 300% bonus messaging). A platform launch date of February 9, 2026 was publicly communicated.

This v1.0 report consolidates: (1) public narrative claims, (2) documented marketing and communication patterns, (3) contract/address inconsistencies, and (4) blockchain-level forensic observations from identified presale-related wallets. The key forensic outcome is

that, for the wallets observed, we did not identify a clear immediate multi-hop draining pattern; however, we did identify structured capital segmentation and rapid redistribution behaviors that materially reduce transparency and increase execution and custody risk.

Bottom-Line Classification

Overall classification (RedFlag Analytics): HIGH to EXTREME RISK (context-dependent).

Reason: multiple high-severity structural red flags (extended presale duration, aggressive incentive structure, launch communication ambiguity, limited public governance transparency, and unresolved canonical contract/address clarity), plus a presale flow model that relies on identifiable receiving wallets rather than fully transparent escrow-style contracts.

Methodology & Evidence Standards

This report follows a strict evidence chain:

• Claim → Evidence source → Interpretation → Stated uncertainty → Severity rating.

Evidence types used:

A) Public sources (project website/docs, third-party listings, press releases).

B) User-supplied screenshots (X/Twitter posts, wallet prompts, Wert receipts, Etherscan views).

C) On-chain observations (wallet balances, ERC-20 transfer logs, transaction patterns).

Important: User-supplied screenshots are treated as documentary evidence of what was shown to a user at a specific time, but may not capture full context. On-chain data is treated as primary technical evidence for fund-flow claims.

1. What Remittix Is (Stated Purpose) & What It Promises

Stated purpose: a payments layer bridging cryptocurrency and real-world banking, enabling a user to pay in crypto while the recipient receives fiat into a bank account (crypto → fiat → bank settlement).

Operational reality check: a crypto-to-bank off-ramp requires regulated partners, AML/KYC enforcement, banking rails, jurisdiction-by-jurisdiction restrictions, and ongoing compliance operations. This significantly increases delivery risk compared to purely on-chain token projects.

2. Timeline Reconstruction (Observed / Reported)

Key timeline points consolidated from public narrative and observed communications:

• Presale reportedly began in Dec 2024 and continued into 2026 (extended presale).

• Platform launch date publicly communicated: Feb 9, 2026.

• Bonus incentive campaigns observed: 300% bonus windows and extension messaging.

• Community/user commentary observed questioning whether the launch delivered the promised scope; project responses included 'stay tuned' / announcement-pending style replies (as shown in screenshots).

Interpretation: Extended presale + launch ambiguity increases uncertainty about product readiness, runway, and delivery alignment.

3. Publicly Verifiable Components (What Exists)

The following components have been observed as existing in public view:

• Website + presale interface (web purchase flow).

• Documentation describing tokenomics and contract details.

• Third-party security/audit listing presence (badges/claims).

• Public social communications (launch countdown, bonus marketing, milestone messaging).

• iOS wallet application listing (public app store presence).

Limitations: existence of a website/app/listing does not prove that the full off-ramp/bank settlement capability is operational at scale.

4. Canonical Contract / Address Clarity (Critical Technical Risk)

Observed issue: multiple distinct Ethereum addresses have been presented or interpreted publicly as 'Remittix (RTX) contract' or 'token address'. Two addresses repeatedly surfaced during analysis:

A) 0xe7654694ec16F3163084eC559193e10c7ABA17CB (appears in project-facing contract references and an Etherscan 'Contract' view).

B) 0xc7f59c4bD6927996186696A0A9cF95dD1727b54E (appears in some third-party/security listing contexts and as an address with an ERC-20 tracker view and multiple transactions).

Forensic interpretation (honest): At least one of these addresses is clearly an ERC-20 token contract (0xe765… based on the Etherscan contract view). The other address (0xc7f59…) may be a contract or an address used for token tracking; the evidence available here does not conclusively establish it as the canonical token contract. Therefore, canonical contract identity remains unresolved within this report.

Severity Assessment: CRITICAL (5/5)

Why this is critical: canonical contract ambiguity is one of the highest-risk factors in presales because it enables accidental purchase of the wrong asset, supports clone-token confusion, and undermines transparent verification of tokenomics and holder distribution.

5. Incentive & Marketing Structure (300%+ Bonus)

Observed: high-percentage bonus campaigns with urgency messaging (e.g., 24-hour 300% bonus, 'extended' messaging). Such incentives can materially distort distribution and increase post-listing sell pressure.

Severity Assessment: HIGH (4/5)

Risk mechanism: aggressive bonus structures attract momentum capital, accelerate fundraising, and can create a larger immediate liquid supply at claim/TGE—which increases volatility risk for retail participants.

6. Launch Communications & Delivery Clarity

Observed: a Feb 9, 2026 launch date was publicly communicated. User-supplied screenshots show community questioning whether the launch occurred or whether it delivered the promised scope, with project responses indicating that announcements/updates were pending.

Severity Assessment: HIGH (4/5)

Interpretation: this creates 'moving goalposts' risk—where the milestone is declared/marketed but the externally verifiable functional scope remains unclear.

7. Governance & Team Transparency

Observed: limited public executive transparency (anonymity/limited doxxing), paired with claims of third-party verification badges. In payment and remittance verticals, public accountability and regulatory posture are central trust variables.

Severity Assessment: HIGH (4/5)

8. Regulatory & Off-Ramp Execution Complexity

Crypto-to-bank settlement requires licensed partners, AML/KYC controls, jurisdictional compliance, and strong operational risk management. Even legitimate projects frequently fail or delay here due to compliance, banking partner fragility, or geographic restrictions.

Severity Assessment: HIGH (4/5)

9. Blockchain Forensics – Presale Flow Model (Evidence-Based)

9.1 Identified Presale-Related Receiving Wallet (Wert receipts)

User-supplied Wert receipts show card/Google Pay purchases routed to an Ethereum wallet address:

Primary presale receiving wallet: 0x1443583B03C1A2079c1F33D3f574237463D864EA

Interpretation: this indicates a presale architecture using a direct receiving wallet (custodial treasury model) rather than a fully transparent escrow-style smart contract sale.

9.2 Primary Wallet Observations (0x144358…)

Observed on-chain (Etherscan screenshots provided): • Total transactions observed: 94. • ETH balance observed at the time of capture: ~0.02078 ETH (~$41). • Token holdings displayed: ~$61k across ~93 tokens (snapshot).

ERC-20 transfer behavior (key observation): the wallet receives multiple USDT inflows (varying amounts such as ~223, ~474, ~139, ~47, ~48 USDT) from a small set of repeating source addresses consistent with payment processing aggregation. The wallet then sends structured outbound transfers in consistent increments (notably 650 units repeated many times) to multiple recipient addresses.

Interpretation: this is a capital segmentation / redistribution model. It is not, by itself, proof of wrongdoing. However, it reduces transparency because it breaks direct linkage between incoming contributions and final treasury custody without a public treasury policy.

Treasury Transparency Assessment (primary wallet behavior): MODERATE–HIGH RISK (3–4/5)

9.3 Secondary Wallet Case Study (0x070AE8…)

One key recipient address identified from the primary wallet's outbound transfers:

Secondary wallet: 0x070AE8c9f7ef4CB3a101F451C325b1297b3eE3F0

Observed: the secondary wallet receives multiple inbound transfers of 650 units from the primary wallet. The Transactions tab shows no normal ETH transactions and no outgoing transfers at the time of capture; activity is limited to inbound ERC-20 transfers.

Interpretation: within the evidence available, this recipient wallet behaves like a storage/segmentation wallet rather than a pass-through laundering node. This reduces support for a 'multi-hop drain' hypothesis for this specific branch of the flow.

9.4 DApp Prompt & Direct ETH Send (connection.remittix.io)

User-supplied wallet UI screenshots show that the buy flow can trigger a direct ETH transfer confirmation to an address displayed as 0x9Dd8…95d via the domain connection.remittix.io. The full destination address was not captured in the evidence available in this report, so further on-chain tracing for that specific address branch remains pending.

Risk note: presale architectures that rely on direct transfers to addresses (rather than contract calls) create custody and reversibility risk, even if the operator is legitimate. This increases retail risk.

10. Evidence Log (What Was Actually Observed)

Evidence items referenced in this report include:

• User-supplied X/Twitter screenshots: 300% bonus messaging, raised/milestone messaging, launch-related community questions and project replies.

• User-supplied Wert receipts: multiple card/Google Pay purchases mapping to wallet 0x144358…864EA.

• User-supplied Etherscan screenshots: overview + transactions for 0x144358…864EA; ERC-20 transfer table showing inflows and structured outbound transfers; secondary wallet 0x070AE8…E3F0 showing inbound-only ERC-20 transfers and no outgoing transactions.

Important: full forensic certainty requires exporting full transaction CSVs and mapping all recipient wallets. This report documents the evidence available at the time of analysis.

11. Red Flag Register (Detailed)

Red Flag	What We Observed / Why It Matters	Severity
RF-01 Canonical Contract / Address Ambiguity	Multiple addresses appear as 'RTX contract/token' across materials; canonical contract not conclusively established here.	CRITICAL (5/5)
RF-02 Extended Presale Duration (Dec 2024 → 2026)	Multi-year presale increases runway uncertainty and fundraising-delivery misalignment risk.	HIGH (4/5)
RF-03 Aggressive Bonus Incentives (300%+)	High bonus alters distribution, increases volatility and sell pressure risks.	HIGH (4/5)
RF-04 Launch/Delivery Ambiguity	Externally verifiable scope at launch remains unclear; communications indicate delays/announcements pending.	HIGH (4/5)
RF-05 Limited Public Governance Transparency	Anonymity/limited public accountability is risky for regulated payment rails.	HIGH (4/5)
RF-06 Off-Ramp Regulatory Complexity	Bank rails and compliance dependencies materially elevate delivery failure risk.	HIGH (4/5)
RF-07 Treasury Transparency & Segmentation	Direct receiving wallet + structured redistribution reduces transparency absent a public treasury policy.	MODERATE–HIGH (3–4/5)

12. Probability Modeling (Revised, Evidence-Constrained)

These ranges quantify uncertainty given the combined red flags and forensic observations. They are NOT claims of wrongdoing.

A) Intentional Fraud Risk (analytical estimate): 45–65%

B) Execution / Delivery Failure Risk (analytical estimate): 70–85%

C) Retail Participant Significant Loss Risk (analytical estimate): 80–90%

Rationale for adjustment: Forensic evidence reviewed did not show a clear immediate multi-hop drain for the wallets analyzed; however, structural and governance risks remain severe, and execution risk remains high due to off-ramp complexity and extended presale behavior.

13. What Would Make This Conclusive (Next Forensic Steps)

To elevate this dossier from 'high-confidence risk analysis' to 'near-conclusive forensic mapping', the following are required:

• Export full CSV transaction history for the primary wallet and map ALL outbound recipients (cluster analysis).

• Trace each outbound recipient wallet for onward transfers to exchanges/bridges/mixers (if any).

• Identify canonical token contract via authoritative project announcement + third-party listings + on-chain verification.

• Capture full destination address for the connection.remittix.io direct-send branch (0x9Dd8…95d) and trace it.

• Perform holder distribution analysis on the canonical contract once confirmed.

14. Conclusion

Based on the evidence available, Remittix exhibits multiple high-severity red flags and remains a high-to-extreme risk presale project. The forensic review identified a direct receiving wallet model and structured redistribution into at least one inbound-only secondary wallet. This does not, by itself, prove wrongdoing; however, it materially reduces transparency and increases custody risk. Execution risk remains high due to the inherent complexity of delivering crypto-to-bank settlement at scale, especially alongside extended presale behavior.

RedFlag Analytics – Independent Blockchain Risk Reports

ADDENDUM A (Post-Confirmation Forensic Updates)

Addendum date: 2026-02-18

Purpose: This addendum appends verified findings obtained after the initial v1.0 COMPLETE compilation. No prior content is removed. Where these findings refine or supersede earlier uncertainty, the update is stated explicitly.

A1. Canonical Contract Clarification (Two RTX ERC-20 Trackers Observed)

New evidence shows two separate Etherscan token tracker pages both labeled "Remittix (RTX)" with the same reported max total supply of 1,500,000,000 RTX, but different contract addresses:

• Contract A: 0xc7f59c4bD6927996186696A0A9cF95dD1727b54E

• Contract B: 0xe7654694ec16F3163084eC559193e10c7ABA17CB

Implication: The presence of two ERC-20 trackers with the same ticker/name and supply indicates either (a) a migration/redeployment scenario or (b) parallel contracts. Within the evidence available, a definitive 'canonical' contract cannot be declared without an authoritative project announcement explicitly stating which contract is the valid live token and whether migration occurred.

Severity impact: Canonical ambiguity remains CRITICAL (5/5).

A2. Token Distribution Status Audit (Holders = 1 on Both Trackers)

Verified observation from Etherscan token tracker views:

• Both Contract A and Contract B show: Max total supply = 1,500,000,000 RTX

• Both show: Holders = 1 (single holder controls 100.0000% of supply at time of capture).

Interpretation (evidence-constrained): On-chain public distribution to presale participants is not visible at this time. This is consistent with an off-chain allocation model where contributions are accepted prior to on-chain distribution/claim, or with a staged distribution plan not yet executed. This is not proof of wrongdoing; it is a structural custody and execution risk.

Severity assessment: EXTREME centralization risk until distribution occurs (5/5).

A3. Execution Risk Implications of 'Single-Holder Supply'

A single-holder supply structure creates the following non-accusatory but material risks:

1) Distribution Event Risk: a future mass distribution/claim event can introduce high volatility and sell pressure.

2) Governance/Custody Risk: full supply control remains with one entity until verifiable distribution occurs.

3) Transparency Risk: presale buyers cannot independently verify allocations on-chain until distribution is executed.

4) Listing/LP Risk: any market listing would require liquidity provisioning and/or transfers from the single holder.

These risks are structural and exist regardless of intent.

A4. Capital Flow Forensics – Reaffirmed Findings & Quantification Limits

Reaffirmed (from prior evidence): Primary presale receiving wallet 0x1443583B03C1A2079c1F33D3f574237463D864EA shows USDT inflows consistent with payment processing aggregation and structured outbound ERC-20 transfers (e.g., repeated 650-unit increments) to multiple recipients, including 0x070AE8c9f7ef4CB3a101F451C325b1297b3eE3F0.

Clarification: The reviewed recipient wallet 0x070AE8c9…E3F0 showed inbound-only ERC-20 transfers and no outgoing ETH transactions at time of capture, which weakens the specific hypothesis of immediate multi-hop draining for that branch.

Quantification limits: Exact totals (aggregate USDT received, aggregate USDT/asset outflows, and recipient concentration ranking) require exporting full transaction histories (CSV) for the primary wallet and mapping all outbound recipients. This addendum does not invent totals.

A5. Updated Red Flag Register – New/Refined Items

Red Flag	Evidence / What We Observed	Severity
RF-08 Dual RTX Token Trackers (Same Name/Ticker, Different Contracts)	Two Etherscan token tracker pages labeled Remittix (RTX) with different contracts: 0xc7f59… and 0xe765…	CRITICAL (5/5)
RF-09 Single-Holder Supply on Both Trackers	Both trackers show holders=1 and 100% supply held by one address at time of capture.	CRITICAL (5/5)

A6. Updated Probability Modeling (Data-Anchored Revision)

This revision reflects the newly verified 'holders=1' status on both token trackers and the continued canonical ambiguity. It preserves the earlier forensic conclusion that immediate multi-hop drain was not observed for the analyzed branch.

Intentional Fraud Risk (analytical estimate): 45–70%

Execution / Delivery Failure Risk (analytical estimate): 80–92%

Retail Participant Significant Loss Risk (analytical estimate): 85–95%

Rationale: Execution and retail loss risks increase materially when (a) the token supply is fully centralized with a single holder and (b) on-chain distribution to buyers is not verifiable at the time of analysis. Intentional fraud risk is not increased solely by centralization, but uncertainty rises due to canonical ambiguity and prolonged presale dynamics.

ADDENDUM B – Raised Amount Verification & Transparency Gap Analysis

Addendum date: 2026-02-18

The presale interface publicly displays a raised amount exceeding $29 million USD. However, blockchain-level analysis of the identified primary presale receiving wallet (0x1443583B03C1A2079c1F33D3f574237463D864EA) shows total observable USDT inflow of 1,166.9465 USDT and negligible ETH inflow at the time of forensic capture.

This creates a Verification Gap between the publicly displayed fundraising total and the on-chain balances visible within the analyzed treasury wallet.

Possible Explanations (Non-Accusatory)

1) Funds may be partially retained within payment processor custody (e.g., Wert) prior to on-chain settlement.
2) Funds may be distributed across multiple treasury wallets not yet identified.
3) Portions of funds may remain in fiat accounts before crypto conversion.
4) The displayed raised amount may represent cumulative accounting across phases rather than a single wallet balance.

At the time of analysis, no single Ethereum wallet with balances approaching the publicly stated total has been identified within the reviewed wallet cluster.

Token Centralization Alert

Both observed ERC-20 Remittix (RTX) token trackers show:

- Total Supply: 1,500,000,000 RTX
- Holders: 1
- 100% of supply controlled by a single address

This indicates that no public on-chain distribution of tokens to presale participants has occurred at the time of review. Until token distribution or claim events are verifiable on-chain, all supply remains centrally controlled.

Implications of Single-Holder Supply

- Full control over minting, distribution, and liquidity remains centralized.
- Any future distribution event may introduce extreme volatility.
- Retail participants cannot independently verify allocation integrity until distribution is executed.
- Liquidity provisioning will require transfers from the single controlling address.

Limitations of On-Chain Verification

This report analyzes observable Ethereum blockchain data only. If funds are held within custodial processors, centralized exchanges, or fiat banking rails, such balances are not directly visible on-chain. Therefore, absence of multi-million dollar balances in reviewed

wallets does not conclusively disprove fundraising claims, but it materially increases transparency uncertainty.

Final Risk Positioning (v1.0 Polished)

After integrating all available forensic observations, the project remains classified as HIGH to EXTREME RISK based on structural centralization, canonical ambiguity, extended presale duration, incentive intensity, and raised-amount verification gaps.

No conclusive evidence of immediate treasury draining was observed in the analyzed wallet branch. However, transparency limitations and centralized supply control materially elevate execution and retail risk.

RedFlag Analytics – Finalized v1.0 Release

Addendum A – Community Governance & Telegram Risk Analysis (v1.1)

1. Telegram Onboarding & Pinned Messaging Analysis

Within the official Remittix Telegram channels (including the portal link referenced in the whitepaper), new users are presented with pinned onboarding messages referencing wallet verification, KYC requirements, and claim eligibility checks via external domains.

2. External Domain Observed: app.remittixcheck.live

The domain app.remittixcheck.live is presented as a wallet eligibility checker. The domain naming structure differs from the primary domain remittix.io and was not previously referenced in canonical materials reviewed earlier in the report.

Observed Risk Indicators:

- Domain structure inconsistent with primary brand domain
- Wallet eligibility verification requiring user interaction
- Inconsistent eligibility result when testing known project-linked wallet addresses
- User confusion reported within Telegram channels

3. Governance Risk Consideration

Two primary interpretations are possible:

A) Official subdomain deployed by project operators without sufficient transparency
B) Malicious phishing infrastructure surfaced within official channels due to bot misconfiguration or moderation failure

If scenario A: Risk relates to poor security design and unclear wallet handling practices.

If scenario B: Risk relates to governance and moderation failure allowing malicious infrastructure exposure.

4. Severity Classification

Risk Layer: Community & Interaction Layer
Severity: HIGH (user interaction risk present)
Reason: Wallet-level interaction prompts combined with inconsistent domain architecture may increase exposure to phishing-style exploits.

This addendum does not conclude malicious intent. It documents structural inconsistencies and observable risk signals for forensic completeness.