TRON Drainer Infrastructure Analysis

Smart Contract, Revenue Sharing and Backend Fund Flows

Prepared by

Valdevies Simone
Founder — Chainradar
Independent Blockchain
Intelligence

1. Executive Summary

This report documents the technical and financial analysis of a TRON-based drainer infrastructure operating through a deterministic revenue-sharing architecture. The investigation focused on the smart contract identified as **TZ4jr**********TrBfte**, with specific emphasis placed on backend fund aggregation behavior, embedded payout logic, downstream redistribution patterns, and interaction with exchange-linked infrastructure.

On-chain evidence demonstrates that the analyzed infrastructure operates according to a fixed two-recipient payout model, where approximately 70% of extracted funds are distributed to execution-layer operator wallets while 30% is consistently routed toward a centralized backend aggregation wallet.

Subsequent tracing identified additional downstream treasury behavior and exposure to custodial or exchange-related infrastructure, including interactions associated with HitBTC and ChangeNOW-linked deposit addresses.

2. Scope & Methodology

The investigation was conducted using publicly available blockchain intelligence and transaction reconstruction methodologies. Primary analytical sources included Arkham Intelligence and TRONSCAN. Analysis steps included:

- Smart contract ABI interpretation
- Bytecode behavioral reconstruction
- Internal transaction tracing
- Fund flow graph analysis
- Revenue split verification
- Backend wallet clustering analysis
- Downstream redistribution assessment
- Exchange exposure identification

3. Smart Contract Technical Analysis

The analyzed infrastructure centers around the smart contract address:

TZ4jr**********TrBfte

ABI review identified multiple functions operationally consistent with a malicious extraction and redistribution framework. Observed capabilities include:

- Dynamic execution through execute()
- Native TRX withdrawal routing
- Multi-recipient payout distribution
- TRC20 withdrawal support
- Operator-controlled execution gating
- Centralized payout orchestration

The contract contains withdrawal functionality capable of distributing funds to multiple recipients during a single execution path, enabling deterministic revenue allocation between operational affiliates and backend infrastructure.

4. Bytecode Behavioral Findings

Behavioral reconstruction of the deployed bytecode identified multiple characteristics commonly associated with drainer-as-a-service (DaaS) infrastructure rather than conventional treasury or payment management contracts.

- Hardcoded operator validation logic
- Internal redistribution routines
- Dynamic external call execution
- Multi-recipient payout processing
- TRC20 token draining support
- Execution-layer access control

Observed execution paths strongly suggest that the infrastructure was intentionally designed for coordinated extraction and downstream redistribution of victim-controlled assets.

5. Revenue Sharing Verification

Transaction reconstruction confirmed the existence of a deterministic 70/30 revenue-sharing model embedded within the payout logic of the smart contract.

```
Transaction Hash:
142461ec043534703b6bb7c534881a2714d511dbb453184ecc274a89300a5d06
```

Recipient	Amount	Observed Share
TAUdT**********3GdEr	11.60001 TRX	30%
TB9KA**********QJGi	27.06669 TRX	70%

The proportional payout distribution was observed directly within the internal execution path of the contract, confirming that backend revenue allocation is enforced programmatically rather than through manual post-processing.

6. Backend Infrastructure Wallet Analysis

On-chain tracing identified the wallet **TAUdT**********3GdEr** as the recurring downstream recipient of the backend infrastructure share across observed contract executions.

A total of repeated internal transfers originating from the drainer contract were observed routing toward this address, demonstrating consistent backend revenue aggregation behavior.

Observed characteristics include:

- Recurring receipt of approximately 30% of distributed funds
- Deterministic downstream routing
- Aggregation of extracted TRX proceeds
- Redistribution toward secondary treasury infrastructure
- Interaction with exchange-linked infrastructure

7. Treasury / Staging Wallet Assessment

Further tracing identified the wallet **TTwLB**********xKhhF** as a likely treasury or staging node within the broader infrastructure.

Observed Transfer	Amount
Transfer 1	26,000 TRX
Transfer 2	16,666 TRX
Transfer 3	7,000 TRX
Transfer 4	3,600 TRX
Transfer 5	2,400 TRX

At the time of analysis, the wallet retained approximately 55,666 TRX, representing an estimated balance of roughly USD 20,000 equivalent. The observed behavior is operationally consistent with a

treasury accumulation layer or temporary staging node prior to downstream redistribution or cash-out.

8. Cash-Out Exposure & Investigative Considerations

Downstream tracing identified outbound interactions with exchange-linked or custodial infrastructure, including exposure to services associated with HitBTC and ChangeNOW.

Observed Service Exposure	Infrastructure Type
HitBTC-linked deposit address	Centralized Exchange
ChangeNOW-linked deposit address	Instant Swap / Exchange Service

The presence of interactions with custodial or exchange-linked infrastructure introduces potential attribution opportunities through legal process, compliance cooperation, account metadata, or transactional retention policies, subject to jurisdictional constraints and platform-specific retention standards.

9. Indicators of Compromise (IOC)

Indicator Type	Observed Value
Drainer Contract	TZ4jr**********TrBfte
Backend Aggregation Wallet	TAUdT**********3GdEr
Treasury / Staging Wallet	TTwLB**********xKhhF
Observed Exchange Exposure	HitBTC-linked infrastructure
Observed Exchange Exposure	ChangeNOW-linked infrastructure

10. Conclusion

The analyzed infrastructure demonstrates characteristics strongly consistent with a professionally operated Drainer-as-a-Service ecosystem deployed on the TRON network.

Observed evidence confirms the existence of deterministic backend revenue allocation, centralized aggregation behavior, treasury-layer staging, and downstream interaction with exchange-linked infrastructure.

The combined smart contract architecture, fund distribution logic, and downstream transactional behavior collectively support a high-confidence assessment that the analyzed wallet cluster represents operational backend infrastructure associated with a coordinated drainer ecosystem.