**CONFIDENTIAL CERN BRIEF** **GhostCore Threat Intelligence Division** **Title:** Phantom UTXO Exploit Vector and Blockchain Manipulation  
 **Classification:** RED - EYES ONLY

**Summary:** This document provides a technical summary of a proof-of-concept exploit that leverages the Bitcoin UTXO (Unspent Transaction Output) model to simulate fraudulent but seemingly legitimate transactions. The attack manipulates "dust" transactions (UTXOs too small to be spent economically) and witness validation layers to create phantom transactions that mislead nodes and block explorers into confirming fake funds. This has the potential to undermine the trust mechanism of blockchain-based financial systems.

**Exploit Name:** Phantom UTXO Chain Injection  
 **Category:** Blockchain Protocol Exploit / Transaction Forgery  
 **Status:** Prototype Complete / Controlled Lab Testing

**Core Attack Logic:**

1. **UTXO Dust Aggregation:**
   * Aggregate thousands of dust-level UTXOs from unrelated addresses.
   * Combine into a transaction structure via a rogue node or tampered wallet software.
2. **Ghost Wallet Insertion:**
   * Use custom-crafted witness scripts to point to a target wallet as the destination.
   * Simulate legitimacy via temporal confirmation spoofing and self-referential validation.
3. **Phantom Broadcast:**
   * Inject transaction into the mempool with delay triggers or cloaked propagation logic.
   * Chain multiple phantom transactions to simulate high value transfers.
4. **Synthetic Confirmation:**
   * Leverage 100s of dummy wallets under attacker control to "confirm" the phantom transaction.
   * Use fake miners or timestamped block insertions for public-facing explorers.
5. **Finalization:**
   * Exchange phantom-confirmed funds at exchanges before detection.
   * Use mixers and burn wallets to wipe traces.

**Visual Payload:**

* Transaction Payload contains valid header, hash structure, and Merkle root signatures.
* UTXOs used are traceable on-chain but falsely bundled.
* Destination address appears funded.

**Potential Impacts:**

* False wallet funding visible on-chain.
* Undetected asset laundering.
* Use in ransomware and terrorist financing.
* Undermining of blockchain immutability perception.

**Mitigation Recommendations:**

1. **Witness Chain Cross-Validation:** Enforce multi-source validation across unique consensus nodes.
2. **Dust Monitoring:** Automated flagging for mass aggregation of dust UTXOs.
3. **Self-Referential Watchdogs:** Identify recursive spending or self-validating transactions.
4. **Exchange-side Deep Verification:** Require multisig and high-confirmation thresholds for large fund transfers.

**CERT/CERN Coordination Path:**

* This brief is intended for private CERT review under controlled disclosure.
* GhostCore recommends independent verification and patch strategy development with blockchain core dev teams.

**Prepared By:** GhostCore Division  
 "Reality is not verified by eyes, but by the ledger of unseen truth."

**End of Document**