## **⚔️ Phantom UTXO Attack & Mitigation Matrix**

| **Phase** | **Action (Attacker)** | **System Impact** | **Detection Vector** | **Mitigation Strategy** |
| --- | --- | --- | --- | --- |
| **1. Craft Dust Input** | Generate UTXO from spoofed source with 0.00000001 BTC | Creates a valid-looking but valueless transaction | UTXO size anomaly; lack of origin tx | Implement dust-size flags in mempool validators |
| **2. Construct P2WSH** | Embed fake script hash that "redeems" a large value | Creates illusion of high-value witness script | No matching witness redemption | Force validation of redeemScript before confirming tx in mempool |
| **3. Chain Phantom TXs** | Link outputs to more fake P2WSH txs simulating internal transfers | Creates perceived transactional activity | Absence of actual BTC movement | Trace transaction ancestry; flag chains that resolve to < dust threshold |
| **4. Leverage UTXO DB** | Exploit backend wallets that auto-sync to view balances | Phantom coins show as available in viewers or wallet watchers | Backend mismatch with global state | Force backend to verify coinbase chain state against full node, not light wallets |
| **5. Disguise Origin** | Embed phantom tx in GhostBill, QR payload, physical artifact | Enables zero-electronics attack vector | Physical scan inconsistencies | Cross-verify scanned physical tx against blockchain state via hash-based confirmation |
| **6. Redeem (Optional)** | Attempt to redeem via spoofed scriptSig/witness | Could crash light wallet or redirect outputs if poorly validated | Script parsing error or fail in full nodes | Harden signature and script validation at mempool and wallet API |
| **7. Misdirection Use** | Log spoofed tx as proof-of-deposit (e.g. at Bitcoin ATM or wallet interface) | Fraudulent deposits appear temporarily valid | No matching TXID in global consensus | Validate on-chain tx before unlocking ATM actions or wallet deposits |

### **🧬 Key Takeaway:**

“This isn’t about spending Bitcoin. It’s about **making a system believe you *could*** — and leveraging that illusion at the weakest trust layer.”

Would you like me to include this in the **Threat Doctrine PDF** under **Section: Phantom UTXO Exploits**, or do you want it in a separate **“Ghost Finance” doctrine** covering ATM/QR/UTXO/Token-based fraud methods?