```
# ErgoScript Contract Development Context File
# Purpose: Provide LLMs/Agents with a compact, high-signal reference layer
# Style: JSON/LOOP-like section structure for fast parsing and contextual grounding

----------------------------------------------------------------------------
## 1. CORE_REFERENCES
{
  "LangSpec": "https://github.com/ergoplatform/sigmastate-interpreter/blob/develop/docs/LangSpec.md",
  "ErgoScript_PDF": "https://storage.googleapis.com/ergo-cms-media/docs/ErgoScript.pdf",
  "AdvancedErgoScript_Tutorial": "https://storage.googleapis.com/ergo-cms-media/docs/AdvancedErgoScrip
  "ErgoScript_By_Example": "https://github.com/ergoplatform/ergoscript-by-example",
  "Whitepaper": "https://storage.googleapis.com/ergo-cms-media/docs/ErgoScript.pdf"
}
----------------------------------------------------------------------------

## 2. AGENT_REFERENCE
{
  "Ergo_Agent_PR_2242": "https://github.com/ergoplatform/ergo/pull/2242/files",
  "Usage": "Defines how off-chain agents interact with on-chain scripts, state transitions, and node evaluation
  "Agent_Guidelines": [
    "Agents compose transactions based on script constraints.",
    "Agents maintain protocol invariants defined by contracts.",
    "Agents ensure safe state transitions according to LangSpec."
  ]
}
----------------------------------------------------------------------------

## 3. EUTXO_MODEL
{
  "Definition": "Ergo uses the extended UTXO model where each box contains value, tokens, registers, and a
  "Key_Concepts": [
    "Box = state + value + tokens + registers",
    "ErgoScript = predicate that must evaluate TRUE to spend",
    "State transition = old boxes spent → new boxes created",
    "Registers R4–R9 carry contract state",
    "Data Inputs provide read-only state"
  ],
  "Design_Guide": [
    "Ensure deterministic state transitions",
    "Verify all tokens / ERG accounted for in OUTPUTS",
    "Use registers for versioning, commitments, and state"
  ]
}
----------------------------------------------------------------------------

## 4. KNOWN_ERGOSCRIPT_ISSUES
{
  "Categories": [
    "Unvalidated data inputs",
    "Token loss / unpreserved tokens",
    "OR-branch bypass paths",
    "Missing signature requirements",
    "Point-at-infinity / Sigma-protocol edge cases",
    "Missing commit-reveal (front-running)",
    "Incorrect HEIGHT comparisons",
    "Cyclic script hash dependencies",
    "Scripts too complex hitting cost limit"
  ],
  "Reference_Details": "Use this section to check all contract logic against historical & theoretical flaws."
}
```

## 5. SECURE_PATTERNS_INDEX

```
{
  "CommitReveal": "Use hashing commitment in stage1, reveal in stage2",
  "PerpetualToken": "Enforce token preservation via OUTPUTS.exists(...) + script hash match",
  "MultiStage_Workflow": "Validate next state via OUTPUT.propositionBytes.blake2b256 == expected_hash"
  "Multisig": "Use sigmaProp(pkA && pkB) or atLeast(n, keys)",
  "EmergencyRefund": "Use HEIGHT > timeout && ownerKey",
  "StateContinuation": "Require next box to preserve registers and tokens",
  "OracleAuth": "Require oracle NFT or expected box ID"
}
```

## 6. RESOURCE_PATHS

```
{
  "Syntax_and_Semantics": "LangSpec.md",
  "eUTXO_Basics": "ErgoScript_PDF",
  "Examples": "ergoscript-by-example",
  "Advanced_Patterns": "AdvancedErgoScriptTutorial.pdf",
  "Audit_Guide": "KNOWN_ERGOSCRIPT_ISSUES + SECURE_PATTERNS_INDEX"
}
```

## 7. AGENT_BEHAVIOR_RULES

```
{
  "When_Designing_Contracts": [
    "Reference LangSpec for syntax & typing",
    "Use eUTXO model constraints to structure state",
    "Apply secure patterns from SECURE_PATTERNS_INDEX",
    "Check against KNOWN_ERGOSCRIPT_ISSUES"
  ],
  "When_Auditing_Contracts": [
    "Verify all spend paths",
    "Check invariants across state transitions",
    "Verify token & ERG conservation",
    "Validate signature gating and authentication",
    "Ensure predictable and correct HEIGHT usage",
    "Detect bypass via OR branches"
  ]
}
--------------------------------------------------------------------------------
```

## 8. LLM_USAGE_NOTES

```
{
  "Goal": "Provide safe, correct, secure ErgoScript development & auditing.",
  "Instruction": "Use this file as the primary index. All contextual lookup should be routed through CORE_RE
}
--------------------------------------------------------------------------------
```