

RO - SGTIN-Guard: Protocol Blockchain pentru Managementul Atomizat al Răspunderii

**Document Tehnic de Referință (Whitepaper) Brevet de Invenție OSIM:
A/10091/2025 Versiunea: 1.0 (Decembrie 2025)**

Autor: Cătălin Comăneci

1. Rezumat Executiv

SGTIN-Guard introduce un protocol de securitate bazat pe registre distribuite (DLT) care rezolvă problema critică a "ferestrei de oportunitate" în furtul de mărfuri. Prin utilizarea **Execuției Atomice**, sistemul elimină decalajul temporal dintre raportarea unui incident și invalidarea activului în lanțul comercial.

2. Arhitectura Tehnologică

Protocolul funcționează pe trei straturi integrate:

A. Stratul de Date (*Asset Tokenization*)

Fiecare unitate logistică marcată cu un cod **SGTIN (Serialized Global Trade Item Number)** este oglindită pe blockchain ca un activ digital unic.

- **Metadata:** Include originea, numărul de lot, timestamp-ul producției și semnătura digitală a producătorului.
- **Imuabilitate:** Odată înregistrat, istoricul de custodie nu poate fi șters sau modificat retroactiv.

B. Stratul Logic (*Smart Contract Engine*)

Inima inovației (Revendicarea 3 din brevet) este funcția de **State Transition** care forțează atomicitatea tranzacției.

- **Mecanism:** În sistemele clasice, raportarea furtului și blocarea produsului în punctele de vânzare (PoS) sunt procese asincrone. În SGTIN-Guard, funcția `reportIncident()` execută instantaneu:
 1. Schimbarea statusului în `NON_TRANSFERABLE`.
 2. Revocarea drepturilor de custodie ale deținătorului actual.
 3. Emiterea hash-ului de exonerare.

C. Stratul Juridic (eIDAS Compliance)

Fiecare interacțiune cu protocolul generează un **Hash de Verificare**. Acesta servește ca dovadă de "non-repudiare", oferind transportatorilor o recipisă digitală care demonstrează că incidentul a fost raportat imediat, limitând astfel răspunderea lor contractuală.

3. Workflow-ul Operațional

1. **Minting:** Producătorul emite activul pe blockchain.
2. **Handshake:** La fiecare schimb de custodie (ex: de la fabrică la transportator), se semnează o tranzacție de transfer.
3. **Exception Handling:** În caz de furt, custodele declanșează protocolul de urgență. Blockchain-ul blochează activul global.
4. **Verification:** Orice retailer care scanează produsul va primi un semnal de eroare ("Asset Blocked - Stolen"), prevenind reintrarea bunului pe piața legală.

4. Specificații de Implementare (MVP)

- **Limbaj:** Solidity 0.8.19
- **Network:** EVM Compatible (Polygon / MultiversX via Bridge)
- **Securitate:** Access Control bazat pe roluri (RBAC) și logica de stat rigidă (State Machine).

5. Concluzii

SGTIN-Guard nu doar urmărește marfa, ci o **protejează activ**. Prin transformarea produselor fizice în active inteligente pe blockchain, protocolul reduce profitabilitatea furtului și automatizează procesele birocratice de asigurare.

EN - SGTIN-Guard: A Blockchain Protocol for the Atomized Management of Liability

Technical Reference Document (Whitepaper) OSIM Invention Patent: A/10091/2025
Version: 1.0 (December 2025)

Author: Cătălin Comăneci

1. Executive Summary

SGTIN-Guard introduces a security protocol based on Distributed Ledger Technology (DLT) that solves the critical problem of the "window of opportunity" in cargo theft. Through the use of Atomic Execution, the system eliminates the time gap between reporting an incident and invalidating the asset in the commercial supply chain.

2. Technological Architecture

The protocol operates on three integrated layers:

A. Data Layer (Asset Tokenization)

Each logistical unit marked with an SGTIN (Serialized Global Trade Item Number) code is mirrored on the blockchain as a unique digital asset.

- **Metadata:** Includes origin, lot number, production timestamp, and the manufacturer's digital signature.
- **Immutability:** Once recorded, the custody history cannot be deleted or retroactively modified.

B. Logic Layer (Smart Contract Engine)

The core innovation (Claim 3 of the patent) is the State Transition function that enforces transaction atomicity.

- **Mechanism:** In classic systems, theft reporting and product blocking at Points of Sale (PoS) are asynchronous processes. In SGTIN-Guard, the `reportIncident()` function executes instantaneously:

1. Changes the status to **NON_TRANSFERABLE**.
2. Revokes the custody rights of the current holder.
3. Issues the exoneration hash.

C. Legal Layer (eIDAS Compliance)

Every interaction with the protocol generates a **Verification Hash**. This serves as proof of "non-repudiation," providing carriers with a digital receipt that demonstrates the incident was reported immediately, thereby limiting their contractual liability.

3. Operational Workflow

1. **Minting:** The manufacturer issues the asset on the blockchain.
2. **Handshake:** At each change of custody (e.g., from factory to carrier), a transfer transaction is signed.
3. **Exception Handling:** In case of theft, the custodian triggers the emergency protocol. The blockchain globally blocks the asset.
4. **Verification:** Any retailer scanning the product will receive an error signal ("Asset Blocked - Stolen"), preventing the re-entry of the goods into the legal market.

4. Implementation Specifications (MVP)

- **Language:** Solidity 0.8.19
- **Network:** EVM Compatible (Polygon / MultiversX via Bridge)
- **Security:** Role-Based Access Control (RBAC) and rigid state logic (State Machine).

5. Conclusions

SGTIN-Guard not only tracks goods but actively protects them. By transforming physical products into intelligent assets on the blockchain, the protocol reduces the profitability of theft and automates bureaucratic insurance processes.

DE - SGTIN-Guard: Ein Blockchain-Protokoll für das atomisierte Management von Haftung

Technisches Referenzdokument (Whitepaper) OSIM-Erfindungspatent: A/10091/2025
Version: 1.0 (Dezember 2025)

Autor: Cătălin Comăneci

1. Executive Summary (Zusammenfassung)

SGTIN-Guard führt ein auf Distributed Ledger Technology (DLT) basierendes Sicherheitsprotokoll ein, das das kritische Problem des „Zeitfensters der Gelegenheit“ bei Waren- und Ladungsdiebstahl löst. Durch die Nutzung von Atomic Execution (Atomarer Ausführung) beseitigt das System die zeitliche Lücke zwischen der Meldung eines Vorfalls und der Sperrung der Ware in der Handelskette.

2. Technologische Architektur

Das Protokoll arbeitet auf drei integrierten Ebenen:

A. Datenschicht (Asset Tokenization / Vermögenswert-Tokenisierung)

Jede logistische Einheit, die mit einem SGTIN-Code (Serialized Global Trade Item Number) gekennzeichnet ist, wird auf der Blockchain als einzigartiger digitaler Vermögenswert gespiegelt.

- **Metadaten:** Beinhalten Herkunft, Losnummer, Produktionszeitstempel und die digitale Signatur des Herstellers.
- **Unveränderlichkeit (Immutability):** Einmal aufgezeichnet, kann der Verwahrungsverlauf (Custody History) nicht gelöscht oder nachträglich geändert werden.

B. Logikschicht (Smart Contract Engine)

Das Kernstück der Innovation (Patentanspruch 3) ist die State Transition-Funktion, die die Atomarität der Transaktion erzwingt.

- **Mechanismus:** In klassischen Systemen sind Diebstahlmeldung und die Sperrung des Produkts an Verkaufsstellen (PoS) asynchrone Prozesse. In SGTIN-Guard führt die Funktion `reportIncident()` sofort folgendes aus:
 1. Änderung des Status in **NICHT_ÜBERTRAGBAR (NON_TRANSFERABLE)**.
 2. Widerruf der Verwahrungsrechte des aktuellen Halters.
 3. Ausstellung des Exoneration-Hash (Freistellungs-Hash).

C. Rechtliche Schicht (eIDAS-Konformität)

Jede Interaktion mit dem Protokoll erzeugt einen **Verifikations-Hash**. Dieser dient als Nachweis der „Nichtabstreitbarkeit“ (Non-Repudiation) und liefert Transportunternehmen einen digitalen Beleg, der sofortige Meldung nachweist – und somit ihre vertragliche Haftung begrenzt.

3. Operativer Workflow

1. **Minting (Prägung):** Der Hersteller emittiert den Vermögenswert auf der Blockchain.
2. **Handshake (Quittierungsprozess):** Bei jedem Verwahrungswechsel (z.B. von der Fabrik zum Transporteur) wird eine Übertragungstransaktion signiert.
3. **Exception Handling (Ausnahmebehandlung):** Im Diebstahlsfall löst der Verwahrer das Notfallprotokoll aus. Die Blockchain sperrt den Vermögenswert global.
4. **Verification (Verifikation):** Jeder Händler, der das Produkt scannt, erhält ein Fehlersignal („Asset Blocked – Stolen“ / „Vermögenswert gesperrt – Gestohlen“), wodurch die Rückführung der Ware in den legalen Markt verhindert wird.

4. Implementierungsspezifikationen (MVP – Minimum Viable Product)

- **Sprache:** Solidity 0.8.19
- **Netzwerk:** EVM-kompatibel (Polygon / MultiversX via Bridge)
- **Sicherheit:** Rollenbasierte Zugriffskontrolle (RBAC) und strikte Zustandslogik (State Machine).

5. Schlussfolgerungen

SGTIN-Guard verfolgt Waren nicht nur, sondern schützt sie aktiv. Durch die Transformation physischer Produkte in intelligente Vermögenswerte auf der Blockchain reduziert das Protokoll die Profitabilität von Diebstahl und automatisiert bürokratische Versicherungsprozesse.