Team: Hackit

Members: Mohmmad Ayaan
Shubham K. Dwivedi

AI-Powered Trust & Safety Platform

Video Link: Explanation Video

a) PROBLEM STATEMENT AND SCOPE OF INNOVATION

Problem Statement:

- Amazon faces challenges with fraudulent sellers, fake reviews, and counterfeit listings undermining customer trust.
- Manual moderation and traditional rule-based systems are not scalable or adaptive enough to deal with the sophisticated threats.

Scope of Innovation – "Proof-of-Authenticity Digital-Twin Network":

We create a **Digital-Twin** for every high-risk product (electronics, luxury, beauty) and secure its lifecycle events on a **permissioned blockchain**. A Digital twin is a virtual representation of a physical product, tracking its journey and authenticity.

Key elements:

Nano-Tag + Dynamic QR

• Cheap NFC / QR applied to products at factory.

• Each Tag's unique ID is minted(recorded) on-chain, linked to the product's SKU (Stock Keeping Unit) & lot number.

Event Oracle

• IoT scanners log key data like GPS location / time / temperature from third-party logistics(3PL) to Amazon fulfilment center (FC) to last-mile delivery. (3PL → FC → last-mile)
• Blockchain smart contract updates live authenticity score using the data.

Edge-AI Tamper Vision

• Macro-photo of tag: A driver uses mobile device to capture a close-up photo of a product tag.
• On-device CNN checks micro-pattern: CNN running on device analyses the tag's unique micro-patterns to verify its authenticity or detect tampering.

Customer "Scan-to-Verify"

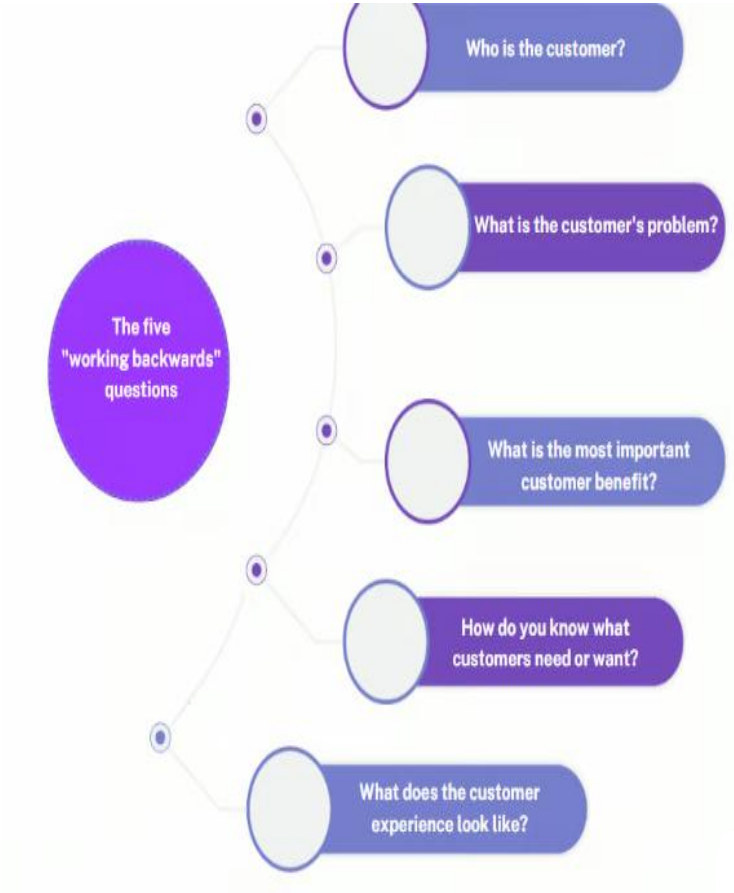
• Buyer scans QR in Amazon app: Customer scans a QR code on the product using the Amazon app.
• Views full custody chain, writes final ownership hash: The app displays the product's complete history and records the buyer's ownership on a blockchain.

Anomaly / Recall Radar

• Graph analytics spot diverging sub-chains (grey market): Graph based analytics to detect when the products deviate from expected supply chain paths.
• Auto takedown + instant recall alert : Automatically remove suspicious listings or issue recall alert.

Working backwards from the customer and define who is your customer

Customer	Pain Point	How Edge-Trust Mesh Helps
Everyday Shoppers	“Reviews are fake, can I trust this?”	Review authenticity scored on-device *before* they see it; token badge shows real-time reputation.
Honest Sellers	Fraud rivals hijack the Buy Box	A digital badge proves seller legitimacy; a trust token boosts visibility for honest sellers.
Moderation Team	Buried under report backlog	Edge filtering removes 70 % junk reports; dashboard dashboard highlights high-risk listings.



SOLUTION KEY COMPONENTS

1. Edge Review Verifier:

A 5 MB on-device lightweight AI-model (TinyBERT + MobileNet) scores every new review for authenticity and image originality before it even reaches Amazon servers.

Flags are stored locally and summarized as encrypted, differentially private gradients once/day.

2. Federated Trust Aggregator:

SageMaker Federated Hub collects gradients from millions of devices + FC scanners.

Updates a global model without seeing raw user data.

Produces “review authenticity risk” and “image originality risk” per SKU.

3. Zero-Knowledge Seller Credential (zk-Cred):

Issued by an AWS Nitro-enclave service when a seller uploads KYC + supply-chain docs.

Gives a yes/no proof of:

• Verified identity • Factory origin • No prior counterfeit strike.

Buyers and moderators can verify sellers on their phone in under 20 ms without storing personal data keeping Amazon compliant with laws like GDPR.

4. Reputation Token & Listing Badge:

ReputationToken = f(edge_risk, zkCred, return_rate, pricing_spikes)

Rendered as a live badge next to “Add to Cart”.

Recomputed every 120 s; collapses to a ‘warning sign’ if token < 0.4.

5. Continual Learning / Drift Guard:

A drift monitor auto-switches to a fresh global model if edge-risk false-positive jumps > 15 %.

Guard rails prevent malicious gradient poisoning via secure aggregation.

SUCCESS METRICS & IMPACT

Metric	12-Month Target	Impact
Authenticity Scan Rate	≥ 70 % of delivered units scanned by customers, driven by in-app prompts and incentives.	Boosts customer trust and reduces return rates.
Counterfeit Intercept %	90 % of fakes blocked before delivery	Huge reduction in A-to-Z claims
Supply-Chain Breach MTTR	< 4 hours to isolate faulty node	Faster recalls, less PR damage
Grey-Market Shrink	50 % drop in duplicate tag IDs, reducing grey-market sales that undercut MSRP pricing.	Protects MSRP pricing for brands.
Brand Adoption	1,000 vendors in Year 1, targeting high-risk categories like electronics and luxury goods first.	Scales the system, enhancing platform-wide trust.

STRATEGIC BENEFITS

- **Sustainability**: Same ledger tracks carbon footprint and cold-chain integrity, supporting Amazon's Climate Pledge and ensuring quality for perishables.

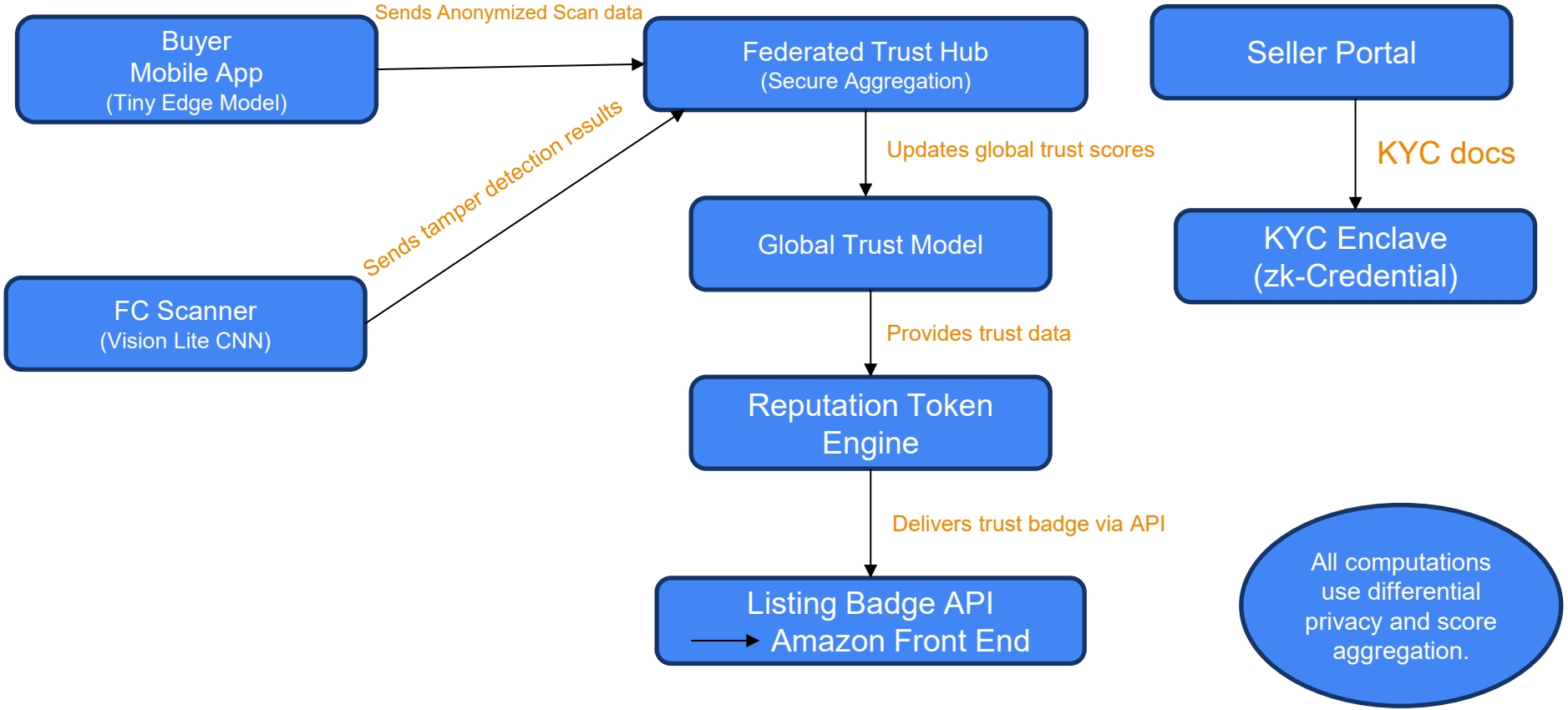
- **Buy-Back / Resale**: Future trade-in programs can instantly verify provenance, boosting trust in Amazon Renewed and supporting circular commerce.

- **Insurance Tie-In**: Offer device insurance only for products with an authenticity score ≥ 0.95 (on a 0-1 scale), ensuring low risk of fraud and creating new revenue streams.

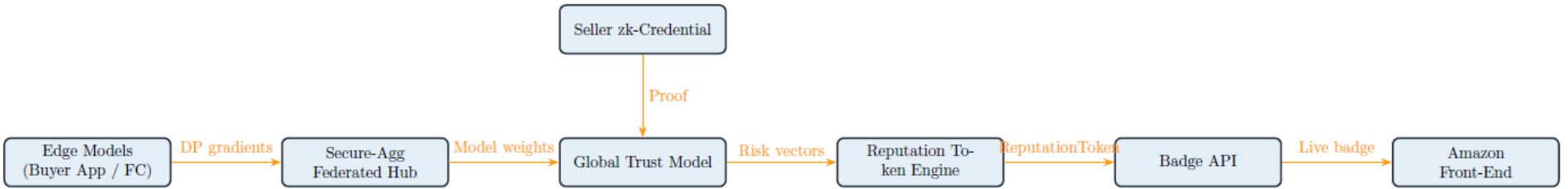
Scope for Scalability Marketplace Domain Expansion

- **Edge First → Cloud Later**: Tiny models auto-download; slower connections fall back to server-side scoring, ensuring 99% user accessibility.
- **Cross-Marketplace**: Same zk-Cred (digital badge) service can verify inventory for AWS Marketplace, Kindle eBooks, or grocery tracking.
- **International**: Privacy tools ensure compliance with global data laws, avoiding cross-border issues.
- **Category Expansion:** Easily scales to more high-risk categories like fashion, protecting more products.

Proposed Architecture



Data to Trust: Our Solution in Action



Ultimately, the buyer sees the trust badge on Amazon Front-End and scans to verify.

Component	Core Tech	Primary Function
Edge Review Verifier	TinyBERT + MobileNet (5 MB)	Scores text/images for authenticity on-device; sends DP gradients.
Federated Trust Aggregator	SageMakerSecure Aggregation	Merges encrypted gradients; updates global model without raw data.
Zero-Knowledge Seller Credential	Nitro Enclave + zk-SNARK	Issues identity/inventory proof without exposing documents.
Reputation Token Engine	Logistic fusion on edge_risk, zkCred, returns	Generates 0–1 score every 120 s; exposes live badge API.
Drift Guard	Shapley-based outlier monitor	Auto-swaps model if false-positive rate spikes $> 15\ \%$.

Table 1: Core building blocks of the Edge-Trust Mesh solution.