amazon

Smart Payment Optimization By

NKD WARRIORS

NKD Warriors

Member 1- **Anany Khare**
Member 2- **Aditya Baraskar**
Member 3- **Anurag Sharma**

THEME - Smart Payment Optimization

Q-SmartPay

Smarter Decisions. Safer Transactions. Seamless Rewards.

Problem Statement & Scope of Innovation

Secure Transaction

Theme:

Smart Payment Optimization

Title:

Q-SmartPay – Smart, Secure & Predictive Payment System for Amazon Pay

Problem Statement:

Build an AI-powered solution that enhances any aspect of the payment's ecosystem - from payment optimization and fraud detection to personalized rewards, budgeting or innovative payment experiences. The goal is to make payments smarter, more efficient and user-centric for individuals or businesses.

Q-SmartPay

Q-SmartPay introduces - a smart, secure, and offline-ready payment solution. It auto-selects the best payment method using AI to maximize savings also it works even without internet. Q-SmartPay tracks spending, offers budget insights, and uses Graph Neural Networks for real-time fraud detection. Users earn QSP tokens as on-chain rewards via Polygon smart contracts, ensuring privacy, transparency, and control. It’s the future of intelligent and rewarding digital payments.

Scope of Innovation

Q-SmartPay is an AI + cryptography-powered layer that enhances Amazon Pay by:

1. ***Suggesting the best payment method***: AI recommends the most rewarding or cost-effective payment option based on offers and history.
2. ***Enabling offline DAG-based transactions***: Securely stores and syncs offline payments using DAG to allow transactions without internet.
3. ***Predicting user budgets using LSTM***: LSTM model forecasts monthly spending and alerts users before overspending.
4. ***Providing scam/fraud detection via GNN***: GNN detects fraudulent patterns by analyzing transaction relationships and behaviors.
5. ***Automating reward validation using smart contracts***: Smart contracts verify reward eligibility and auto-credit cashback without manual checks.
6. ***Ensuring transaction privacy using FHE***: FHE allows transaction data to remain encrypted even during processing and analysis.

Need of the Hour?

Losses on ecommerce online payment fraud hit $41 million last year, in 2022 and, according to Juniper Research, the total cost of ecommerce fraud to merchants will exceed $48 billion globally this year. Of this startling figure, North America is cited as comprising 42% of fraud by value, followed by Europe at 26%. More terrifying for merchants still, it is predicted that the cumulative losses to online payment fraud globally between now and 2027 will exceed **$343 billion**.

Current reward validation systems face major loopholes like promo abuse, referral fraud, free-trial exploits and synthetic identity use-primarily due to weak identity checks and delayed fraud detection. Real-time payouts further worsen the issue, allowing fraudsters to redeem rewards instantly before systems can respond.

Meet Ayushi and Arushi – Two Smart Shoppers

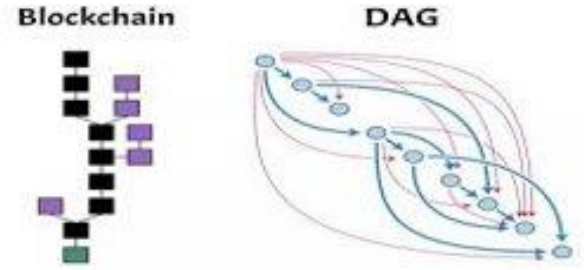
Ayushi and Arushi are college students who often shop online - from books and groceries to gadgets and cosmetics. They both recently bought smartphones worth ₹80,000 from different e-commerce platforms.

Ayushi chose a popular e-commerce site with a reward program based on loyalty coins. Arushi used a new platform powered by Q-SmartPay - a blockchain-based smart rewards system that connects to her wallet.

Little did they know, their shopping experience was about to feel very different.

The Problem &
Our DAG-Based Offline Payment Solution

When connectivity fails, so do digital payments.



The Problem – Why Offline Payments Are Needed

Meet Ravi: He tries to buy medicine via Amazon Pay UPI. Due to poor network, payment fails and order is cancelled. He loses time, trust; merchant loses the sale.

This happens in metro tunnels, rural India, and low-signal zones - thousands of times daily.

The Real Challenge: 85% of India's internet is still mobile and unstable. Current systems assume connectivity. There's no fallback mechanism to store "intent to pay."

Our Solution – A DAG-Based Offline Payment Queue

- When offline, users tap "Pay Offline." A payment node is created and linked using SHA-256, forming a secure DAG.
- Stored locally on the device → once back online, the app verifies all nodes, ensuring data integrity.
- Tampering breaks the chain → transaction is rejected.
- Orders must be completed within 24 - 48 hrs to avoid cancellation.

Enables real-time ordering even offline, preserves user intent and avoids delays.

Ayushi Faces a Glitch, Arushi Stays Ahead

A week later, both Ayushi and Arushi tried to grab another deal online - but this time, Ayushi's payment failed due to poor network at her hostel.

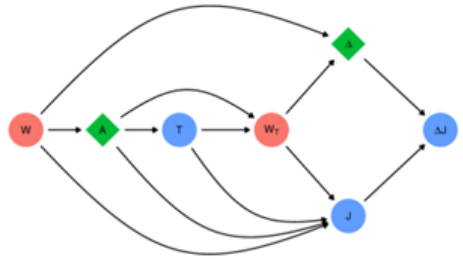
Frustrated, she had to restart the checkout later.

Arushi, on the other hand, tapped "Pay Offline".

Her order was securely saved using a DAG (Directed Acyclic Graph) structure - linking it to her previous offline actions with tamper-evident hashes.

When her device reconnected, the system verified and completed her payment - no delay, no hassle.

Why DAG & What Impact It Brings



Why Only DAG? The Structural Superiority

- Not a queue. Not a blockchain. DAG > All for this use-case.
- Each event (payment) is cryptographically linked to the previous one.
- Ensures tamper detection, clear ordering, and trust without the overhead of blockchain.

Queues/arrays lack structural integrity. DAG supports branching, retries, multi-session flows - perfect for resilient offline payments.

Key Benefits:

Blockchain-grade security without blockchain baggage. Encrypted DAG + Merkle root structure enable flexible, tamper-proof sync post reconnection.

Vision & Impact – How This Changes Payments

- UPI Lite only supports limited wallet-based offline payments.
- Our system: Stores intent to pay. Works with multiple payment methods. Verifies payment securely using DAG

“We’re not just storing offline payments - we’re proving they were real.”

The Problem &
Our AI-Based Payment Suggestion

The Problem – Why AI-Based Payment Suggestion is Required

Meet Vikram: Vikram is a regular Amazon shopper. He owns multiple UPI IDs, debit/credit cards, and wallets - but during checkout, he's confused about which one gives the maximum cashback or reward. He wants to save more, but making the right payment choice is time-consuming and often leads to missed benefits.

Core Issues and Why AI-Based Suggestion is Required

- Too Many Offers, Too Little Time - Multiple cards/wallets have different deals.
- No Unified View - There is no intelligent system that considers everything.
- Missed Savings - Users end up using fewer rewarding methods.

Our Solution – Smart AI-Based Suggestion Engine

- Q-SmartPay uses a rule-based AI engine to analyze offers, merchant type, cart value, and user preferences in real-time.
- It recommends the most rewarding payment option - helping users like Vikram maximize benefits effortlessly.

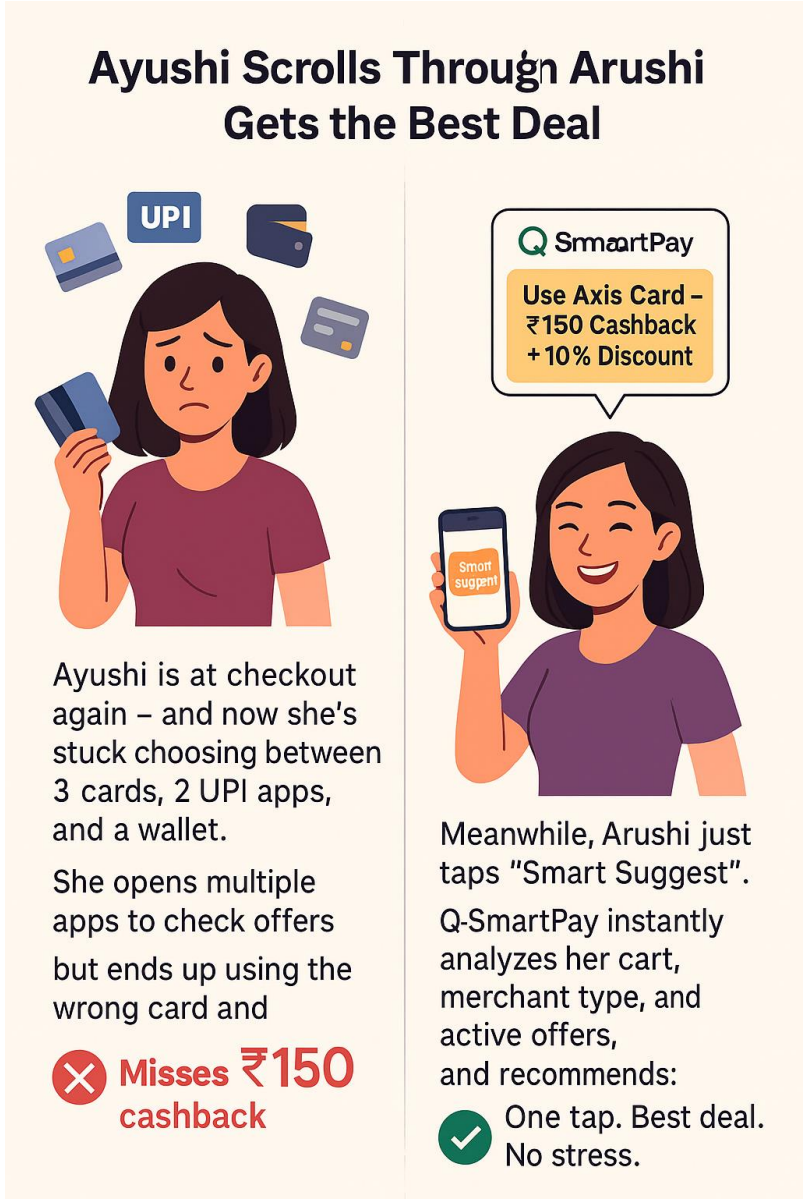
Ayushi Scrolls Through Cards, Arushi Gets the Best Deal

Ayushi is at checkout again - and now she's stuck choosing between 3 cards, 2 UPI apps, and a wallet.
She opens multiple apps to check offers… but ends up using the wrong card and misses ₹150 cashback.

Meanwhile, Arushi just taps “Smart Suggest”.

Q-SmartPay instantly analyzes her cart, merchant type, and active offers, and recommends:
“Use XYZ Card – ₹150 Cashback + 10% Discount”

She taps once. Paid. Done.
Right choice, no confusion, maximum savings.



Why Rule-Based AI + The Simplicity Impact

Why Rule-Based AI – Not Anything Else

- Our goal is to maximize offers and rewards during payments - and for this, a rule-based AI model fits best.
- It maps known conditions like merchant type, cart value, card-specific cashback, and wallet offers to simple, smart suggestions.
- This model works reliably with predictable, offer-based logic. Doesn't need deep learning or huge compute resources. Is perfect for real-time usage without delays.

Easy to Train, Easy to Trust

- Using past payment data, available card/wallet offers, and user preferences, the model can be trained quickly, deployed efficiently, optimized for maximum user benefit.
- Q-SmartPay's AI engine analyzes offers, merchant category, cart value, and user history to recommend the best payment method - ensuring maximum savings with minimum effort.
- While ML upgrades like Random Forest or Transformers can be added later for adaptability, the rule-based core ensures simplicity and clarity.

The Problem &
Our Blockchain-Based Smart Rewards Solution

Current Reward Systems Are Broken, Opaque and Underused

The Problem - Why a Reward Validation System is Needed

Meet Priya: A student makes a ₹60,000 purchase expecting big rewards. A week later, a vague, small reward appears - she's confused, can't redeem, and feels cheated.

Core Issues and Why Validation is Crucial

- Locked to one platform, non-transferable. No clarity on how rewards are calculated. Expiring coupons, poor UX, low trust. Feels gimmicky and lacks emotional value.
- Users need real-time, clear reward feedback also retailers need tamper-proof systems to verify and distribute rewards fairly. Boosts fairness, trust and usage of reward programs.

Our Solution - SmartPay: Transparent Blockchain Rewards via Amazon Pay & Prime

- QSP tokens: Instantly issued, ownable rewards stored in the user's crypto wallet.
- Tokens are redeemable for real discounts, usable across platforms, and require no extra setup.
- Integrates directly with Amazon Prime for exclusive loyalty bonuses.

Ayushi vs Arushi - A Tale of Two Reward Systems

We knew they both bought an 80k smartphone

A week after their purchases, both friends sit down in the hostel common room and open their apps to check their rewards.

Ayushi scrolls through her purchase history. She sees a reward of just **₹120 credited** as loyalty coins - confusingly split across expiry dates and limited to her next grocery order.

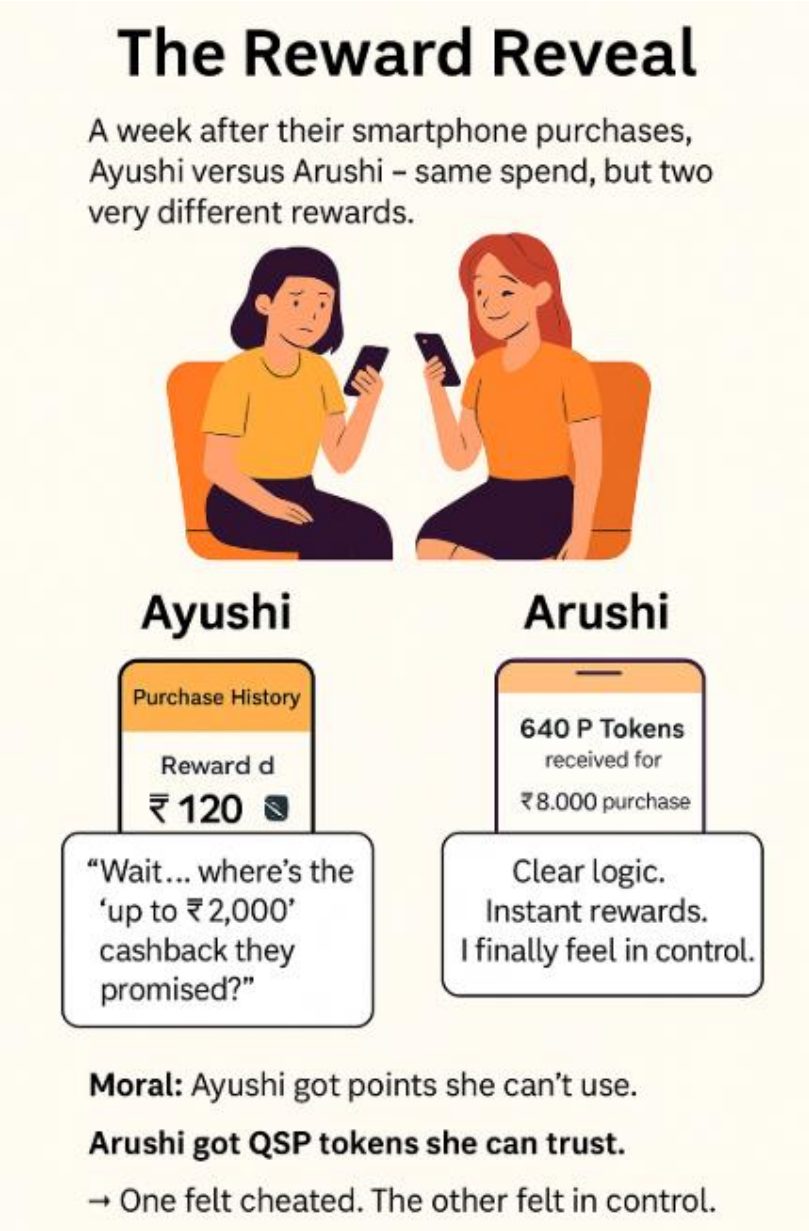
She frowns:

"Wait… where's the 'up to ₹2,000 cashback' they promised? These coins are about to expire next week!"
She reads the fine print - the offer required a special coupon code she never noticed.

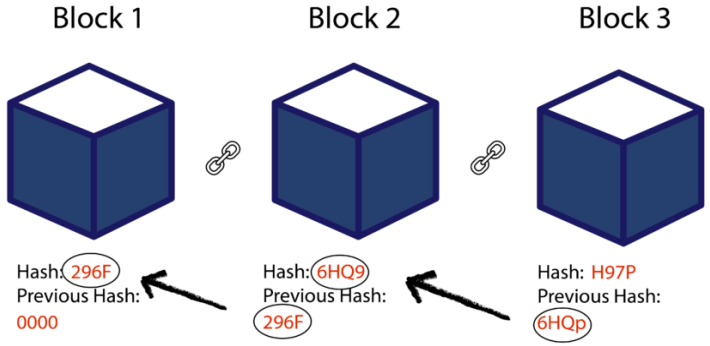
Arushi, on the other hand, opens her Q-SmartPay-integrated wallet.

Right there, she sees:

"640 QSP Tokens received for your ₹80,000 purchase."
Each token is listed with a timestamp, and a contract link shows exactly how the amount was calculated.
She smiles - these tokens can be used for groceries, streaming, even travel, across different platforms.



Why Blockchain + The Bigger Impact



Why Blockchain – Not Traditional Rewards

- Traditional systems are opaque, centralized, locked to one platform.
- Users can't verify calculations or transfer value across services.

Blockchain Advantage

- Transparent, public smart contracts verify every reward rule.
- Immutable records = fraud-proof and user-trust aligned.
- Rewards are user-owned tokens, not platform-bound points.
- Smart contracts automate eligibility checks (purchase method, amount, timing) - making rewards instant, rule-based, and tamper-proof.

Q-SmartPay: The Future of Loyalty

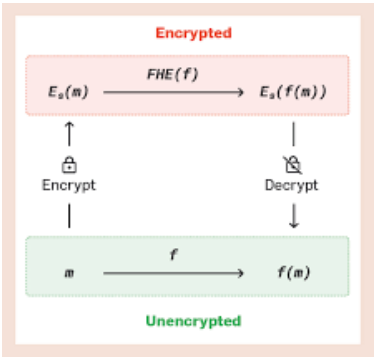
- Turns QSP into a cross-platform on-chain token, evolving every transaction into a loyalty investment.
- Seamlessly integrates with Amazon Pay, Prime, and future partners.
- 25% boost in Amazon Pay usage + increased Prime retention via exclusive reward tiers.
- Flywheel effect: More usage → More trust → More retention → Deeper loyalty.

"We're not just storing offline rewards — we're proving they were earned, transparently and securely."

The Problem &
Our Budget Prediction + FHE Privacy — Smarter, Safer Payments

The Problem – Why Budget Insights Are Needed Alongside Private Budgeting

Meet Ayesha: She frequently shops for cosmetics, books, and occasionally buys high-value medicines. But without any smart budgeting feature, she often overspends without realizing it - there's no system to alert her in advance. Worse, when she spends on sensitive items like medicines, her transaction data is exposed to the server, compromising her privacy. She has no control over her spending and no way to keep it private.



Core Issues and Why Budget Prediction & Private Budgeting Are Required

- Untracked Spending and No Personalized Alerts
- Lack of Privacy and No Control or Confidence

Our Solution – Introduction of Machine Learning

LSTM-based Budget Forecasting to predict monthly spend and alert users in real time.

Fully Homomorphic Encryption (FHE) to process spending data without eve[illegible] not even to the backend.

Ayushi Overspends, Arushi Plans Smart & Stays Private

Ayushi loves shopping during festivals.
She spends a lot across groceries, fashion, and gadgets - but has no idea she's crossing her budget until it's too late.
She ends up regretting purchases and feels stressed.

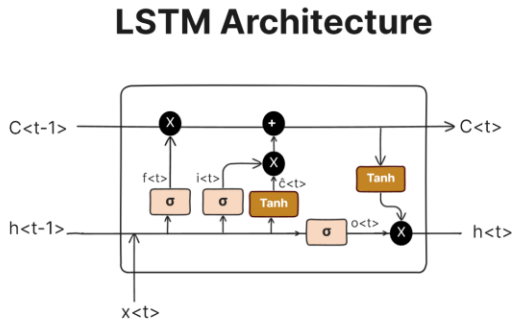
She also buys personal care products and medicines, but worries about her private spending data being visible to others in the system.

Arushi, on the other hand, uses Q-SmartPay.

- The LSTM model predicts her monthly spend and sends alerts:
  "You're close to exceeding your grocery budget this month."
- At checkout, she sees real-time insights and adjusts her cart - staying on track.
- And when buying sensitive items, her transaction data is encrypted with FHE, so:
  No raw data is exposed and she stays in control of her privacy

With Q-SmartPay, Arushi spends smarter, stays informed, and protects her privacy — all in one smooth experience.

Why LSTM + The Need for FHE



Why Only LSTM for Budget Prediction?

Q-SmartPay uses an LSTM (Long Short-Term Memory) model because:

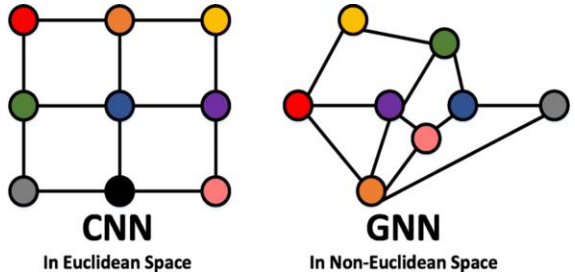
- Time-Series Power: LSTM is designed to handle sequential data, making it ideal for predicting monthly and category-wise spending patterns based on past behavior.
- Captures Spending Trends: It understands long-term dependencies - like seasonal splurges (festivals, holidays) or recurring expenses (subscriptions, groceries).
- Low Overhead, High Accuracy: Unlike heavier models, LSTM balances accuracy with speed, making it efficient for real-time predictions in a production-grade payment system.

The Need to Introduce FHE (Fully Homomorphic Encryption)

As users become more privacy-conscious, Q-SmartPay integrates FHE to build trust without compromise.

- Data Never Decrypted on Server: All processing - fraud checks, budget alerts, even reward eligibility - is done on encrypted data. The backend never sees raw values.
- Supports Sensitive Categories: For purchases like medicines, donations, or personal care, FHE ensures privacy by design - not just policy.
- User-Centric Security: Decryption happens only on the user's device, giving them full control over what they share, and when.
- Seamless + Secure: FHE enables AI features like budgeting to run without violating privacy, making Q-SmartPay future-ready and privacy-first.

The Problem & Our GNN Based Fraud Detection



The Problem – is protecting payment important

Meet Ramesh: he regularly pays using UPI for everything - food orders, recharges, local sellers. But one day, he unknowingly transfers money to a scam UPI ID involved in fraud. There was no warning, no history shown, and no red flag. He lost money and trust - and now double-checks every UPI manually, unsure who to trust.

Core Issues in Current Systems

- Scams evolve faster than rule-based systems (fake merchants, refund loops, collusion).
- No context awareness - traditional systems see payments as isolated events, not patterns.
- User is left blind - no visibility into fraud history of UPI IDs or merchants.
- False negatives - malicious behavior often slips through if it mimics normal transactions.

Our Solution - Transaction Graph AI with GNN

Q-SmartPay uses a Graph Neural Network (GNN) to analyze transaction patterns between users, merchants, and devices - detecting fraud like sudden payment bursts, refund abuse, or shared IPs.

Ayushi Falls for a Scam, Arushi Gets Alerted in Time

Ayushi is in a rush to pay a local seller via UPI.
The UPI ID looks normal, so she proceeds without thinking.
Later, she finds out it was a scam account - she loses ₹2,000 and has no way to trace it.
She wishes someone had warned her.

Arushi, on the other hand, uses Q-SmartPay.

When she tries to pay a similar UPI ID, a warning pops up: *“This UPI handle is flagged in past scam reports. Proceed with caution.”*

Behind the scenes, Q-SmartPay's Graph Neural Network (GNN) had already analyzed the connections:

The account was linked to multiple suspicious refunds and shared devices.

It was added to the Scam Registry on the blockchain.

Arushi avoids the payment.
Money saved
Trust maintained

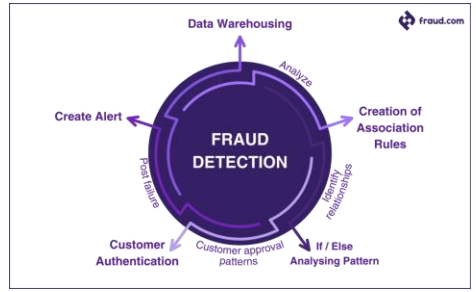
Why GNN is Built for Fraud - And Gets Smarter Over Time

Why GNN?

Traditional fraud systems treat each transaction in isolation. But fraud is relational - patterns often emerge only when connections between users, merchants, and devices are examined together.

That's where Graph Neural Networks (GNNs) come in:

- They model the entire payment ecosystem as a graph, where each user, merchant, or device is a node, and transactions are the edges connecting them.
- GNNs learn from the structure of these connections - detecting behaviors like:
  - Multiple fake merchants using the same phone or IP
  - Sudden spikes in payments or refund loops
  - Suspicious clustering around certain nodes



Unlike basic AI models, GNNs retain context, helping catch hidden fraud rings that mimic normal activity.

How It Gets Smarter Over Time

- Every flagged fraud pattern helps retrain the model - improving accuracy with more data.
- All flagged UPI handles are hashed and stored on a blockchain-based Scam Registry, building a transparent, verifiable memory of known scams.
- This enables community-driven trust, as future users are warned of suspicious accounts.
- As more transaction graphs are analyzed, the GNN detects subtle patterns, reducing both false positives and false negatives.

The result: A continuously evolving fraud detection system that grows more intelligent and more trusted with every scam it stops.

Stakeholder Impact

For End Users	For Amazon	For Fintech Ecosystem
Maximized Benefits Always get best outcome (cashback, EMI, rewards).	Higher Payment Completion Fewer drop-offs with smart suggestions.	Interoperability Unified layer for UPI, cards, BNPL, etc.
Scam Protection Warns before paying fraud UPI IDs (via GNN).	Lower Support Load Auto-reward verification = fewer queries.	Global Scalability Adapts to EU, US, Asia payment models.
Connectivity Freedom Offline payments via DAG, sync later.	Partner Loyalty Boosts use of Amazon-partnered rewards.	Privacy Standards zk-SNARKs + FHE for ethical finance.
Smarter Spending LSTM-based forecasts & savings advice.	Data Intelligence Privacy-preserving behavioral insights.	Web3 Bridge Smart contracts and on-chain reward registry.
Trust that their rewards are confirmed not maybe or later	Business Growth Personalized, secure payments = loyalty.	

Scalability Highlights

- Modular Microservices: Independent services (AI, fraud detection, smart contracts) enable easy scaling, deployment and upgrades.
- API-First Design: REST/GraphQL APIs ensure seamless integration with external apps and future third-party extensibility.
- Cloud-Hosted & Scalable: Deployed on platforms like AWS/Vercel with auto-scaling, load balancing and multi-region support.
- Lightweight Front-End SDK: JS SDK allows quick integration into merchant sites with consistent UX.
- Offline DAG Queue: Transactions stored locally in a secure DAG and synced once online, ensuring integrity in low-connectivity areas.

Marketplace Domains

- Retail (e.g., Amazon.in): Auto-applies best payment options & rewards, builds trust, and reduces cart abandonment.
- Travel & Tickets (e.g., IRCTC): DAG-based offline payments enable secure transactions in low-connectivity areas.
- Subscription Services: LSTM models forecast recurring bills, flag anomalies, and prevent fraud in auto-debits.
- Donations & Health: FHE ensures complete privacy for sensitive transactions like medical payments or donations.
- B2B / SME Payments: GNN fraud detection + smart contracts enable secure, timely vendor and bulk transactions.

Geographical Scalability

India

Built natively for the Indian fintech ecosystem, Q-SmartPay integrates seamlessly with UPI, RuPay and local wallets, aligning with NPCI regulations and Bharat Stack capabilities.

Europe (PSD2 & Open Banking)

Thanks to its modular API-first design, Q-SmartPay can easily connect to European banks via PSD2-compliant APIs. It can support smart routing of payments, budgeting and reward optimization within the Open Banking framework.

United States (ACH, Card Networks)

In the U.S., the AI and privacy-preserving features can plug into ACH systems and credit card networks, delivering reward suggestions, fraud detection and spend analysis tailored to American users.

Future Interoperability

Web3 Wallets & BNPL

Support for blockchain wallets (MetaMask, WalletConnect) and BNPL platforms (like ZestMoney or Affirm) is on the roadmap. Smart contracts ensure transparent reward disbursement, while privacy features protect user identity.

Decentralized ID (DID) Support

Future versions may incorporate DID to enable secure, self-sovereign identity in payments, allowing users to control what identity/payment info is shared across platforms.

Voice & Regional Language UX

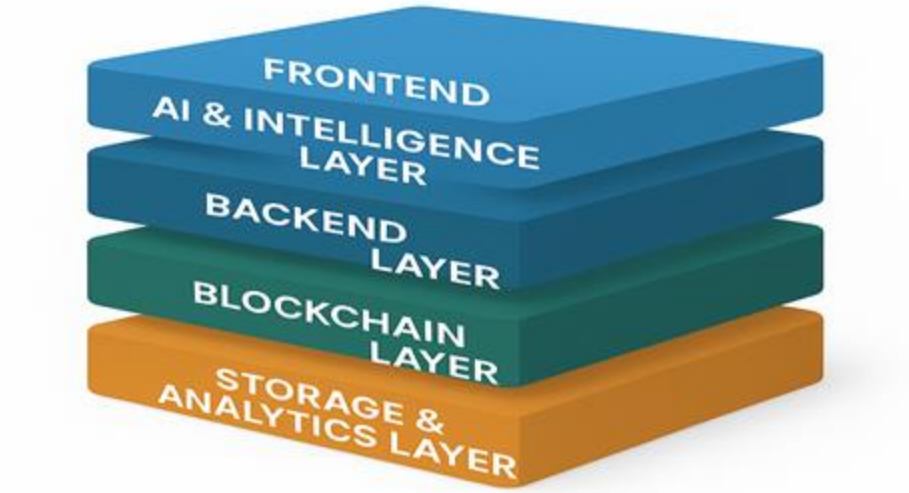
To promote digital inclusion in Tier-2 and Tier-3 cities, voice-enabled payment flows and support for vernacular languages will make smart payment features more accessible to non-tech-savvy users.

Architecture

Q-SmartPay is built on a modular, scalable, and privacy-first architecture that fuses AI, blockchain, and cryptography to deliver a smarter, safer, and more inclusive payment experience on Amazon Pay.

Features 5 main Layers :

- Frontend Layer
- AI & Intelligence Layer
- Backend Layer
- Blockchain Layer
- Storage & Analytics Layer



User Interface & Intelligence

Purpose: Seamless, smart and accessible payment experience.

User-Facing Layer

Next.js: Builds the core interface.

Budget Alerts: Real-time spend warnings (LSTM-based).

Reward Suggestions: AI- suggested payment methods with rationale.

AI & Intelligence Layer

- AI Engine (Python, scikit-learn/Transformers):
  Inputs: cart, merchant, history and offers.
  Outputs: ranked payment suggestions.
- Budget Predictor (LSTM – TensorFlow/PyTorch):
  Predicts upcoming expenses & alerts overspending.
- Fraud Detector (GNN – PyTorch Geometric):
  Flags risky behavior via transaction graph analysis.

PyTorch

Why it Matters

Enables smarter checkouts, personalized finance, and inclusive UX.

System Backbone & Trust Layer

Purpose: Ensure secure, reliable backend and decentralized trust mechanisms.

Backend Layer

- FastAPI / Flask : Hosts microservices & APIs.
- DAG Sync Engine: Stores offline transactions in DAG, syncs on connectivity.
- FHE Processor: Performs encrypted fraud/budget checks without data exposure.

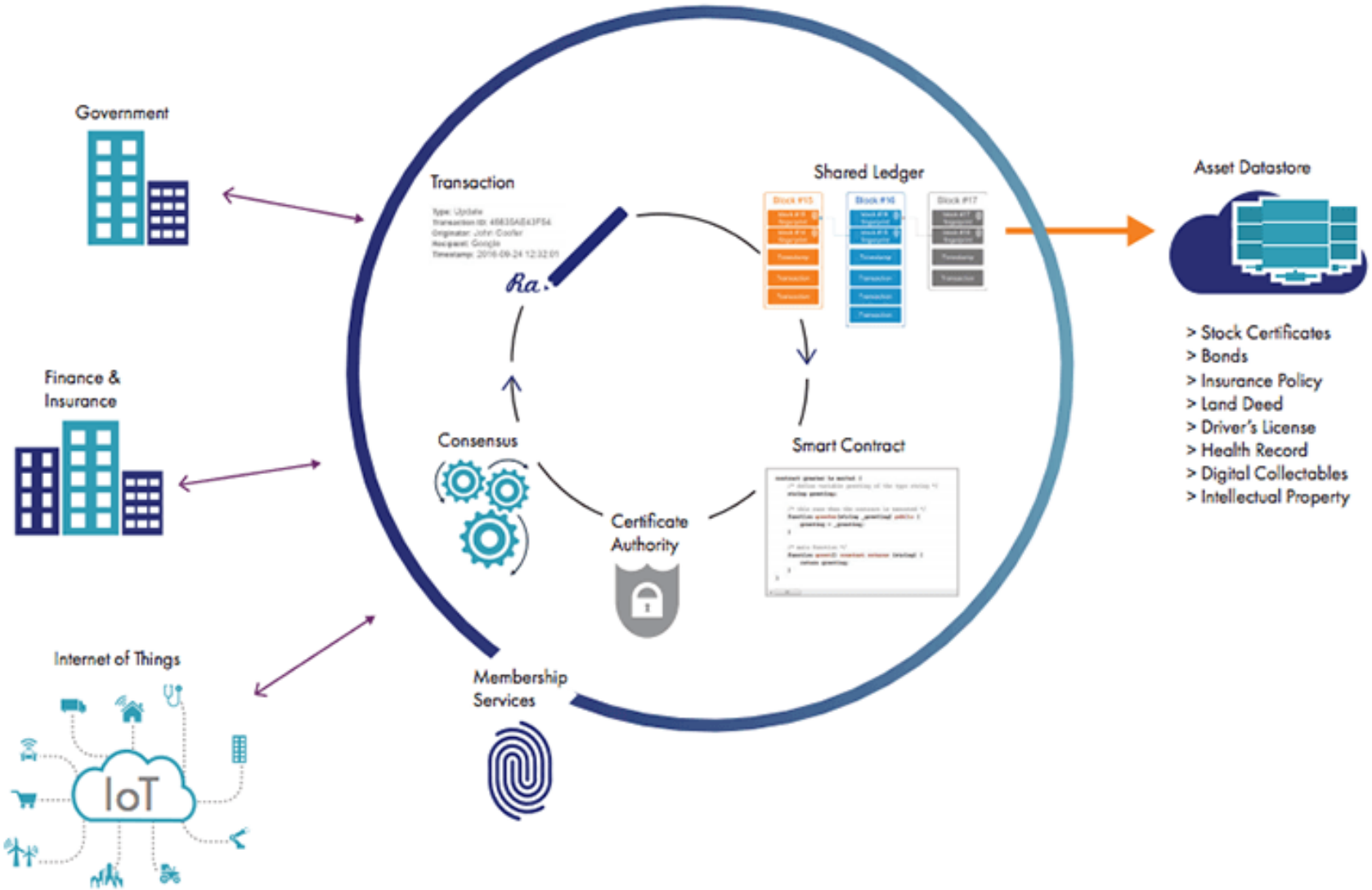
Blockchain Layer

- Smart Contracts (Solidity on Polygon): Automates rewards & scam ID validation.
- Reward Vault: Auto-credit system for verified rewards.
- Scam Hashes DB: SHA-256 hashes of flagged UPI IDs.
- Wallet Integration: MetaMask / web3.js / ethers.js for on-chain interaction

Why it Matters

Connects AI, privacy and blockchain for secure, transparent payments.

Blockchain as an Infrastructure



amazon

THANK YOU!