amazon

< HackOn >

with amazon

5.0

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.

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**.

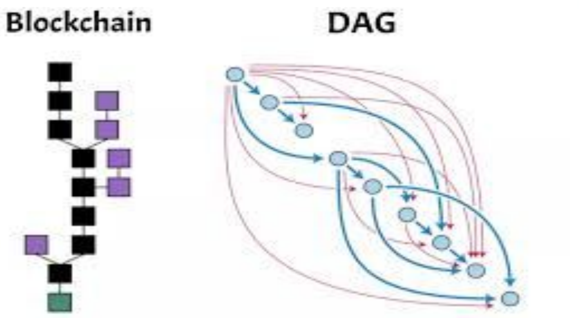
Current reward validation systems face major loopholes like promo abuse, referral fraud, free-trial exploits and synthetic identity use—primarily due to weak identity checks and delayed fraud detection. Real-time payouts further worsen the issue, allowing fraudsters to redeem rewards instantly before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

Core Features of Q-SmartPay

Q-SmartPay enhances Amazon Pay with a powerful blend of AI, cryptography and blockchain to deliver a seamless, smart and secure payment experience.

1. ***Smart Payment Suggestio***n: Recommends the most rewarding or cost-efficient payment method based on live offers and usage.
2. ***Offline Payments via DAG***: Stores transactions securely offline using DAG and syncs them reliably once the user reconnects.
3. ***Budget Prediction using LSTM***: Predicts upcoming monthly spend using LSTM and alerts users before they overspend.
4. ***Scam/Fraud Detection via GNN***: Detects suspicious UPI IDs, refund abuse, and merchant collusion through transaction graph learning.
5. ***Reward Validation via Smart Contracts***: Automates cashback and reward validation with on-chain smart contract execution.
6. ***Privacy-Preserving Computation using FHE***: Ensures that sensitive transaction data remains encrypted even during processing.

Offline Payments via DAG



Title: Enabling Reliable Offline Payments with DAG Sync

Problem: Many users in low-connectivity areas (e.g., rural zones, trains, or metro tunnels) are unable to complete payments, causing failed checkouts, user frustration, and lost revenue.

Solution: Q-SmartPay uses a Directed Acyclic Graph (DAG) structure to securely queue payments offline. Once the user reconnects, the transaction graph is verified and processed without loss or tampering.

How It Works: The steps are as follows.

1. Each offline payment becomes a node in a DAG.
2. Transactions are locally stored with partial order.
3. On reconnection, DAG is hashed and synced (Additional security measures are in place to prevent fraudulent activities or intentional misuse of offline payment capabilities).
4. Payments are validated and executed if funds/methods are still active.

Working Backwards from the Customer - Meet Priya:

Priya shops on Amazon while traveling by train. With poor internet, she enables Offline Mode. Her payments are stored securely in a DAG. When she reaches network again, they sync, verify and the items are dispatched automatically.

Customer Value:

1. Seamless experience even without internet.
2. No cart abandonment.
3. Trust and flexibility in the payment process.

Trust & Safety Measures:

1. 24-hour grace period → auto-dispatch if payment syncs (if exceed delay shipment).
2. 48-hour timeout → auto-cancel to prevent abuse.
3. Encrypted DAG + Merkle root ensures tamper-proof sync.

Budget Prediction using LSTM

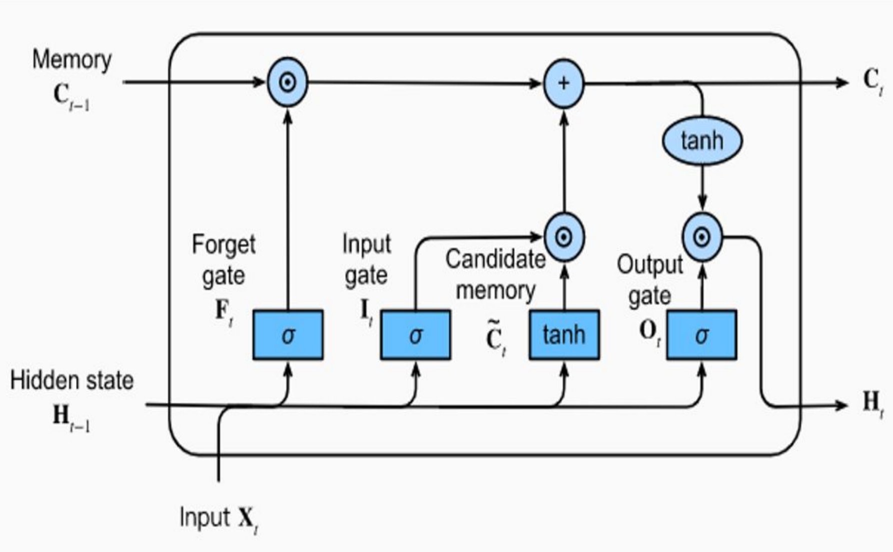
Title: Forecasting User Spending with LSTM Budget AI

Problem: Users often lose track of monthly spending and end up overspending across categories like groceries, gadgets or fashion - with no proactive system to alert them.

Solution: Q-SmartPay leverages an LSTM (Long Short-Term Memory) deep learning model to analyze transaction patterns and predict the user's upcoming monthly spending.

How It Works: The steps are as follows.

1. Model is trained on past transaction data.
2. Predicts total and category-wise spend.
3. Sends alerts when user is nearing or exceeding budget.
4. Can recommend delaying or avoiding purchases.



Working Backwards from the Customer – Meet Ayesha:

Ayesha spends frequently on cosmetics and books. Q-SmartPay warns her at checkout:

“*You’ve already spent ₹3,500 on cosmetics this month. Forecasted total: ₹5,200.”*
She adjusts her cart and stays on budget.

Customer Value:

1. Clear financial awareness.
2. Budget discipline built into Amazon Pay.
3. Alerts improve trust and shopping satisfaction.

Why It Matters:

1. Encourages responsible spending.
2. Increases user engagement with Amazon Pay dashboard.
3. Enables optional goal tracking (future scope).

AI-Based Smart Payment Suggestion

Title: Intelligent Payment Method Suggestion Using AI

Problem: Users often have multiple UPI IDs, cards and wallets - and no easy way to know which gives the maximum cashback or benefit during checkout.

Solution: 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.

How It Works: The steps are as follows.

1. Inputs: Cart value, merchant type, available payment methods.
2. Rule-based logic for MVP; upgradable to ML (Random Forest / Transformer).
3. Model ranks payment methods and explains suggestions.

Working Backwards from the Customer – Meet Gunjan:

Gunjan adds fashion items worth ₹2,499 to cart.

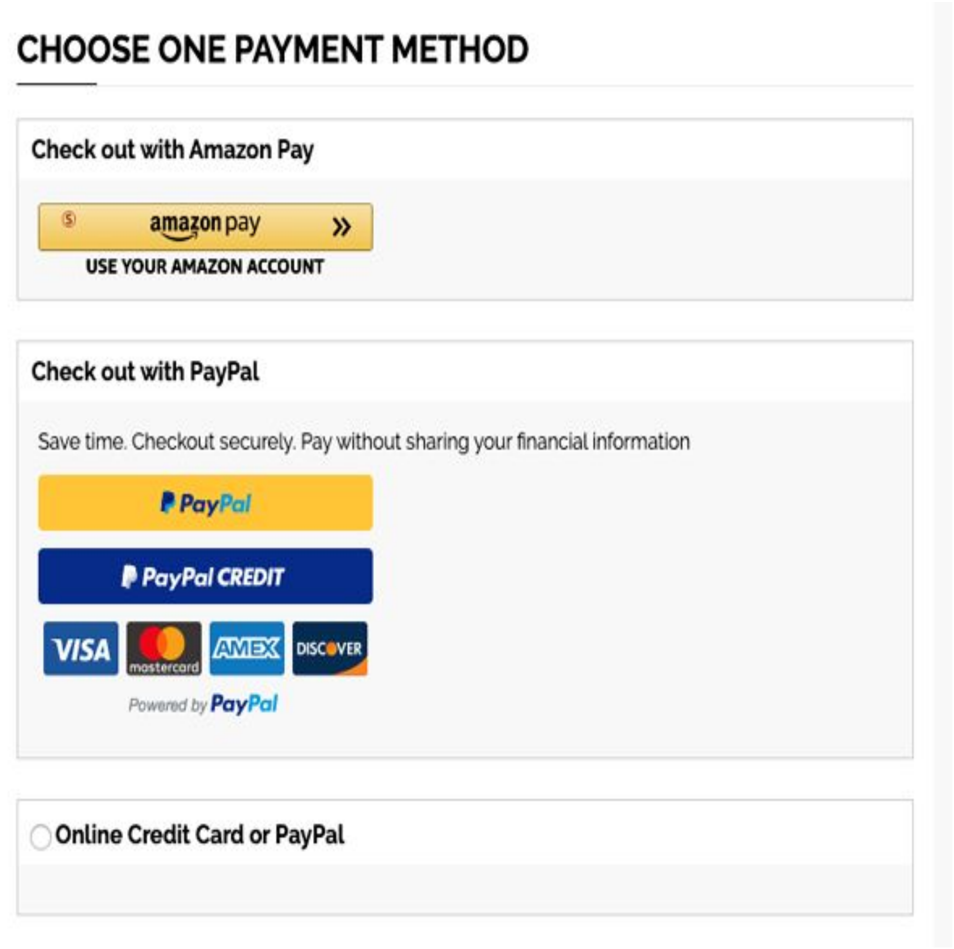
Q-SmartPay suggests: “*Use ICICI Amazon Card – ₹200 Cashback + 10% Discount*.”
Gunjan taps to confirm → payment proceeds → gets reward confirmation instantly.

Customer Value:

1. Saves time and mental effort.
2. Avoids missed offers.
3. Builds trust with transparent rationale.
4. Learns from past usage for smarter future choices

Tech Stack:

1. Frontend: React.js
2. AI: Rule-based + ML model (Python, scikit-learn)
3. Deployment: Vercel + Flask/FastAPI backend
4. Privacy: Optional federated learning (future)



CHOOSE ONE PAYMENT METHOD

Check out with Amazon Pay

Check out with PayPal

Save time. Checkout securely. Pay without sharing your financial information

○ Online Credit Card or PayPal

Reward Validation Using Smart Contracts

Title: Transparent, Instant Cashback via Blockchain

Problem: Users are often uncertain if cashback will arrive, with long delays, unclear terms, or support hassles.

Solution: Q-SmartPay uses Ethereum-compatible smart contracts to automatically validate and disburse cashback on eligible transactions - fast, fair and transparent.

How It Works: The steps are as follows.

1. Smart contract checks payment source, amount, and merchant code
2. If eligible, reward is locked and sent to user’s wallet
3. Users can auto-apply it or claim it manually
4. Reward status is visible on testnet blockchain (e.g., Polygonscan)

Working Backwards from the Customer – Meet Ayushi:

Ayushi makes a ₹5,000 payment using ICICI Amazon Pay Card.

Q-SmartPay verifies on-chain and shows:

“₹250 reward confirmed. View transaction → polygonscan_link”

Ayushi can use it for the next order or claim it to wallet.

Customer Value:

1. Eliminates reward confusion or manual follow-up.
2. Instant reward validation builds confidence.
3. Verifiable transactions → trust in Amazon ecosystem.
4. Especially valuable for high-value purchases.

Tech Stack:

1. Smart Contracts: Solidity on Polygon Testnet
2. Wallet: MetaMask + ethers.js/web3.js
3. Backend trigger: Node.js or Express API
4. UI: React + reward status/claim button
5. Explorer Integration: Polygonscan/Etherscan links

Scam & Fraud Detection using GNN (Graph Neural Network)

Title: Detecting Payment Scams & Fraud with Transaction Graph AI.

Problem: Online payments are vulnerable to scams involving fake UPI IDs, refund abuse, money laundering, and merchant collusion, which traditional fraud systems often fail to detect.

Solution: Q-SmartPay applies a Graph Neural Network (GNN) to transaction data modeled as a graph - where users, merchants, and devices are nodes and payments are edges. The system identifies abnormal, high-risk patterns and flags them in real time.

How It Works:

1. Graph built from transaction activity.
2. GNN classifies nodes/edges as risky or safe.
3. Flags suspicious behavior like: Sudden burst of payments, Refund loops, Device/IP overlaps across merchants.
4. Hashes of flagged scam UPI IDs are stored in a **blockchain-based scam registry**

Working Backwards from the Customer – Meet Ramesh:

Ramesh is about to pay a UPI handle flagged in 8 past fraud reports.

Q-SmartPay shows:

“*Warning: This UPI ID is listed in the Scam Registry. Proceed with caution.*”

Customer Value:

1. Proactively prevents payment fraud.
2. Boosts user confidence during UPI and wallet transfers.
3. Creates a transparent, community-driven fraud protection layer.
4. Helps Amazon build marketplace trust at scale.

Tech Stack:

1. AI: PyTorch Geometric, NetworkX
2. Storage: Graph DB / in-memory graph for demo
3. Registry: Smart contract on Polygon storing SHA-256 hashes
4. Frontend: React alert system at payment screen
5. Privacy: Pseudonymized analysis (no raw user data exposed)

Transaction Privacy via Fully Homomorphic Encryption (FHE)

Title: Total Privacy with Encrypted Computation using FHE

Problem: Users are increasingly privacy-conscious - but standard analytics, fraud checks, and budget predictions require their raw transaction data to be visible to the backend.

Solution: Q-SmartPay uses Fully Homomorphic Encryption (FHE) to allow processing of encrypted transaction data, ensuring that servers never see raw amounts, categories or metadata, while still performing fraud and budget analysis.

How It Works:

1. User’s transaction payload (amount, merchant, type) is encrypted on-device.
2. FHE engine runs logic like *“Is amount > ₹5,000?”* on ciphertext.
3. Result is returned in encrypted form.
4. User decrypts final output locally (e.g., reward eligibility or fraud alert).

Working Backwards from the Customer – Meet Meera:

Meera doesn’t want her ₹9,000 medicine bill visible to anyone.

Q-SmartPay runs fraud & budget checks on her encrypted data and confirms eligibility for cashback - all without decrypting the transaction.

Customer Value:

1. Privacy-first experience without sacrificing security.
2. No raw data exposure to backend or cloud.
3. Especially valuable for sensitive categories (e.g., health, personal care, donations).

Tech Stack:

1. Crypto Engine: Microsoft SEAL or TFHE
2. Client-Side: Encryption done in browser or app
3. Server-Side: Logic runs on ciphertext
4. Decryption: Done on-device by user only
5. Use Cases: Fraud check, reward validation, budget alerts

Success Metrics

Objective	Metric	Target
Smarter Payments	% of users using AI-suggested payment method	≥ 85%
Reward Effectiveness	Avg. cashback/reward increase per transaction	30%
Reward Trust & Speed	% of rewards auto-confirmed via smart contract	≥ 95%
Fraud Mitigation	% reduction in fraudulent transactions/UPI scams	≥ 40%
Offline Reliability	% of offline payments synced & validated successfully	≥ 98%
Accessibility & Inclusion	% of users engaging via voice-based UX	≥ 20%
Customer Satisfaction	NPS (Net Promoter Score)	+50+
Support Load	% drop in reward/payment-related support tickets	≥ 50%
Engagement	Increase in retention (7-day / 30-day user activity)	+15–20%

Fraud Detection using GNN

Metric	Target
Fraud detection accuracy	90% on validation set
False positive rate	< 3%
Time to decision per transaction	< 200 ms
% reduction in undetected fraud cases vs baseline	≥ 40%
% reduction in customer complaints related to false blocks	≥ 20%

Privacy Layer

Metric	Target
zk-Proof verification time	< 100 ms
% of sensitive data exposed to merchants / 3rd parties	0%
Number of users opting for privacy-preserving verification	80% adoption rate (target)
Compliance with GDPR / privacy laws	100% compliant

Real World Impact

For End Users :

Impact Area	Description
Maximized Benefits	Always get the best payment outcome — cashback, EMI, rewards — without effort.
Financial Confidence	Trust that their rewards are confirmed, not “maybe later” or “in 30 days”.
Scam Protection	GNN-powered scam detection warns them before paying a fraud UPI ID.
Connectivity Freedom	Can still complete transactions offline — sync later when connected.
Accessibility	Voice commands & regional language support make it usable for non-tech users.
Smarter Spending	LSTM budget forecasting educates users on where they spend and how to save.

For Amazon :

Impact Area	Description
Higher Payment Completion	Smart suggestions reduce drop-offs and confusion at checkout.
Lower Support Load	Auto-verified rewards = fewer customer complaints or queries.
Partner Loyalty	Optimizes usage of Amazon-partnered cards, wallets, or reward programs.
Data Intelligence	Behavioral AI models help refine future campaigns (privacy-preserving).
Business Growth	Personalized, rewarding, secure payments increase customer lifetime value.

For Fintech and Payment Ecosystem :

Impact Area	Description
Interoperability	Unified layer for cards, UPI, wallets, BNPL — with plug-in architecture.
Global Scalability	Easily localizable to EU (Open Banking), US (Card Networks), Asia (UPI/QR).
Privacy Standards	zk-SNARKs + FHE show the future of ethical fintech.
Web3 Bridge	Smart contracts + rewards registry showcase responsible DeFi in consumer tech.

Scalability Highlights

Modular Microservices Architecture

Each feature—like AI-based suggestions, fraud detection, and smart contracts—is encapsulated as a standalone service. This makes it easy to deploy, upgrade or scale individual modules without affecting the overall system.

API-First Design

Q-SmartPay’s backend is built as a set of REST/GraphQL APIs, allowing easy integration with external apps such as e-commerce sites, digital wallets, or banking systems. This also ensures future extensibility for third-party developers.

Cloud-Hosted with Horizontal Scaling

Deployed on scalable platforms like AWS, Render, or Vercel, the architecture supports automatic load balancing, stateless containers, and multi-region deployment. It handles traffic surges without performance drops.

Lightweight Front-End SDK

A React/JavaScript SDK enables easy embedding into merchant checkout pages with minimal code. This ensures rapid adoption across different platforms while offering a unified user experience.

DAG-Based Offline Transaction Queue

Even when users are offline (e.g., in transit or rural areas), transactions are stored locally in a tamper-proof DAG structure. These are securely synced and verified once connectivity is restored, maintaining transactional integrity.

Marketplace Domains

1. Retail (Amazon.in)

Q-SmartPay enhances e-commerce transactions by suggesting the most beneficial payment method, auto-applying rewards, and building trust through transparency. It reduces checkout friction and cart abandonment, especially during high-traffic sales.

2. Travel & Tickets (e.g., IRCTC, MakeMyTrip)

In connectivity-challenged scenarios like trains or rural travel, the DAG-based offline payment mechanism allows users to make secure transactions without immediate internet access, syncing later for fulfillment.

3. Subscription Services

By leveraging LSTM models, Q-SmartPay can forecast recurring spending (e.g., OTT, SaaS, utility bills) and alert users on anomalies or nearing limits. It also helps detect suspicious billing activity or fraudulent auto-debits.

4. Donations & Health

These domains require discretion. Using Fully Homomorphic Encryption (FHE), Q-SmartPay ensures sensitive transactions (e.g., medical payments, donations) are processed without revealing data to backend systems, preserving full privacy.

5. B2B / SME Payments

Bulk and vendor payments are highly susceptible to fraud or delays. The GNN-based fraud detection and smart contract-based payouts ensure secure, timely, and verifiable transactions for business partners and SMEs.

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

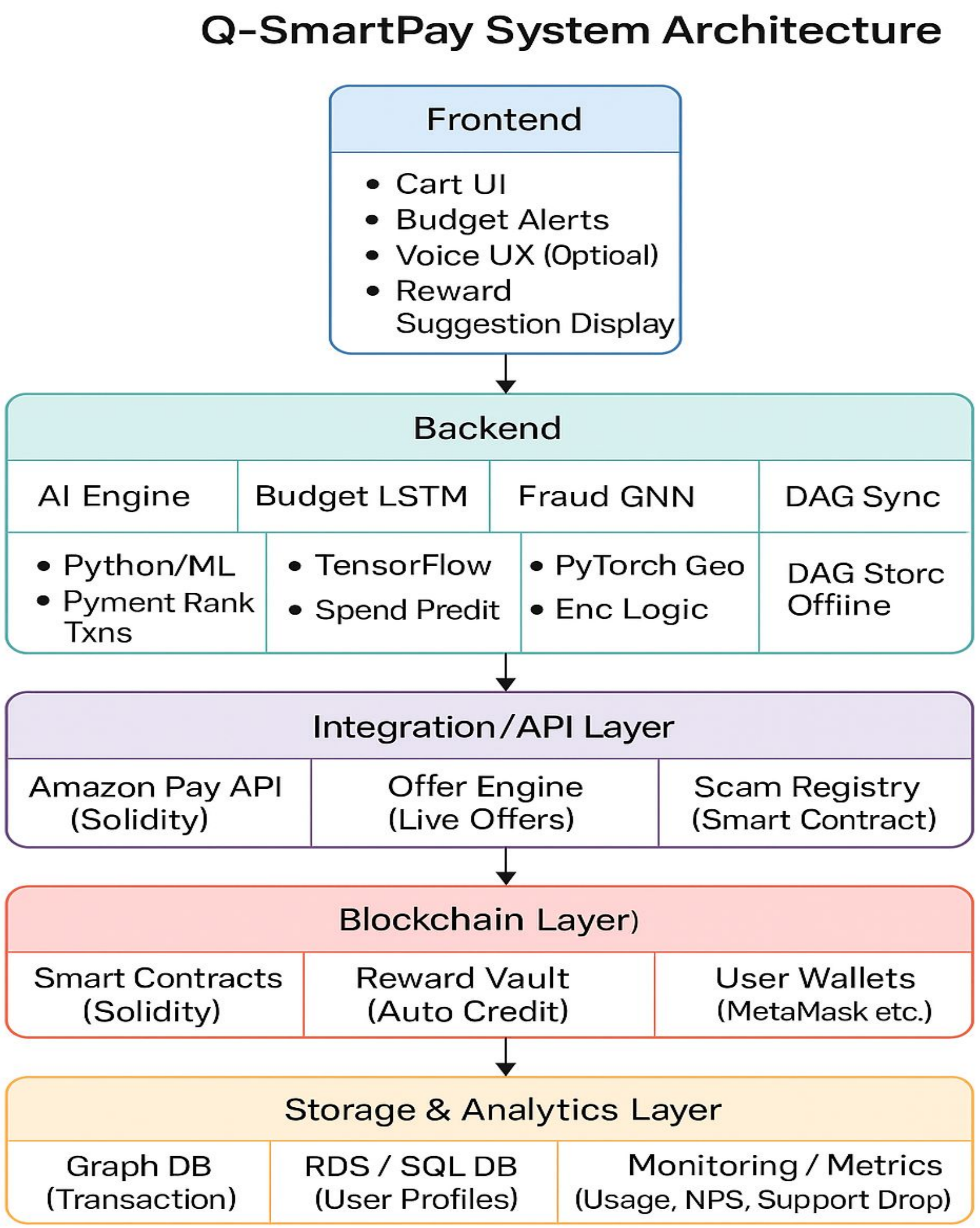
To promote digital inclusion in Tier-2 and Tier-3 cities, voice-enabled payment flows and support for vernacular languages will make smart payment features more accessible to non-tech-savvy users.

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



Q-SmartPay System Architecture

Frontend

- Cart UI
- Budget Alerts
- Voice UX (Optional)
- Reward Suggestion Display

Backend

AI Engine	Budget LSTM	Fraud GNN	DAG Sync
• Python/ML • Pyment Rank Txns	• TensorFlow • Spend Predit	• PyTorch Geo • Enc Logic	DAG Storc Offiine

Integration/API Layer

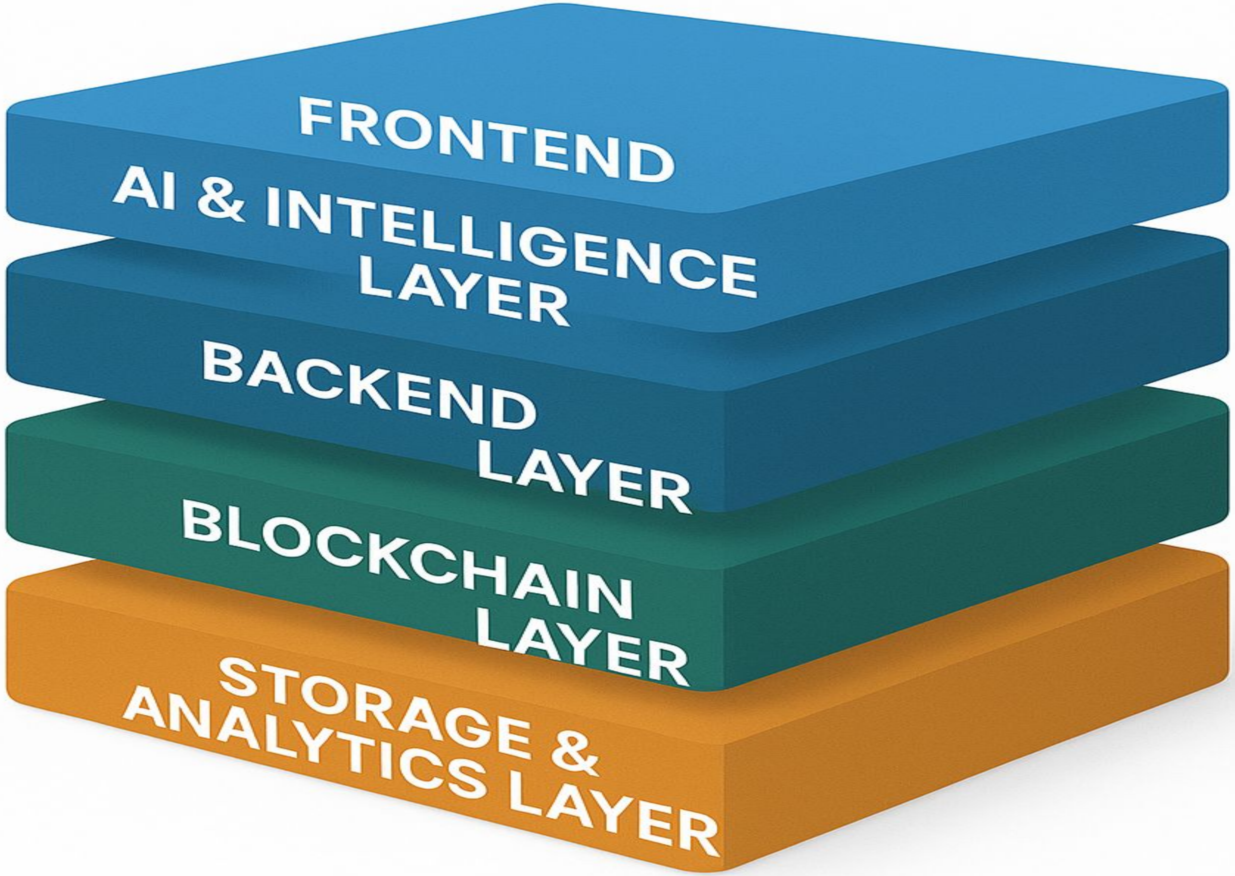
Amazon Pay API (Solidity)	Offer Engine (Live Offers)	Scam Registry (Smart Contract)

Blockchain Layer)

Smart Contracts (Solidity)	Reward Vault (Auto Credit)	User Wallets (MetaMask etc.)

Storage & Analytics Layer

Graph DB (Transaction)	RDS / SQL DB (User Profiles)	Monitoring / Metrics (Usage, NPS, Support Drop)


FRONTEND
AI & INTELLIGENCE LAYER
BACKEND LAYER
BLOCKCHAIN LAYER
STORAGE & ANALYTICS LAYER

Frontend Layer

Purpose : Provides the user-facing interface for all payment interactions.

Components:

- React.js: Core framework for building the UI.
- Voice UX: Optional voice input for accessibility and regional language support.
- Budget Alerts: Real-time spend warnings based on LSTM predictions.
- Reward Suggestions: Displays AI-suggested payment methods with rationale.

Why it Matters : Enables seamless checkout, personalized interactions and accessibility for all users.

AI & Intelligence Layer

Purpose : Drives core intelligence and personalization in payments.

Subcomponents:

- AI Engine:
  - Built in Python (scikit-learn / Transformers).
  - Input: Cart, merchant type, user history, live offers.
  - Output: Ranked payment method suggestions.
- Budget Predictor:
  - LSTM model (TensorFlow or PyTorch).
  - Predicts upcoming spending patterns and budget limits.
- Fraud Detector:
  - Graph Neural Network (PyTorch Geometric).
  - Learns risky behavior from transaction graphs and flags fraud.

Why it Matters : Delivers smarter, safer and more personalized financial experiences.

Backend Layer

Purpose : Coordinates business logic, APIs and cross-component communication.

Components:

- FastAPI / Flask / Node.js: Hosts API endpoints and microservices.
- DAG Sync Engine: Locally stores offline transactions and syncs using a directed acyclic graph when connectivity resumes.
- FHE Processor: Receives encrypted data, performs computations (fraud/budget checks) and returns encrypted results.

Why it Matters : Forms the glue connecting AI, storage, blockchain and external systems like Amazon Pay.

Blockchain Layer

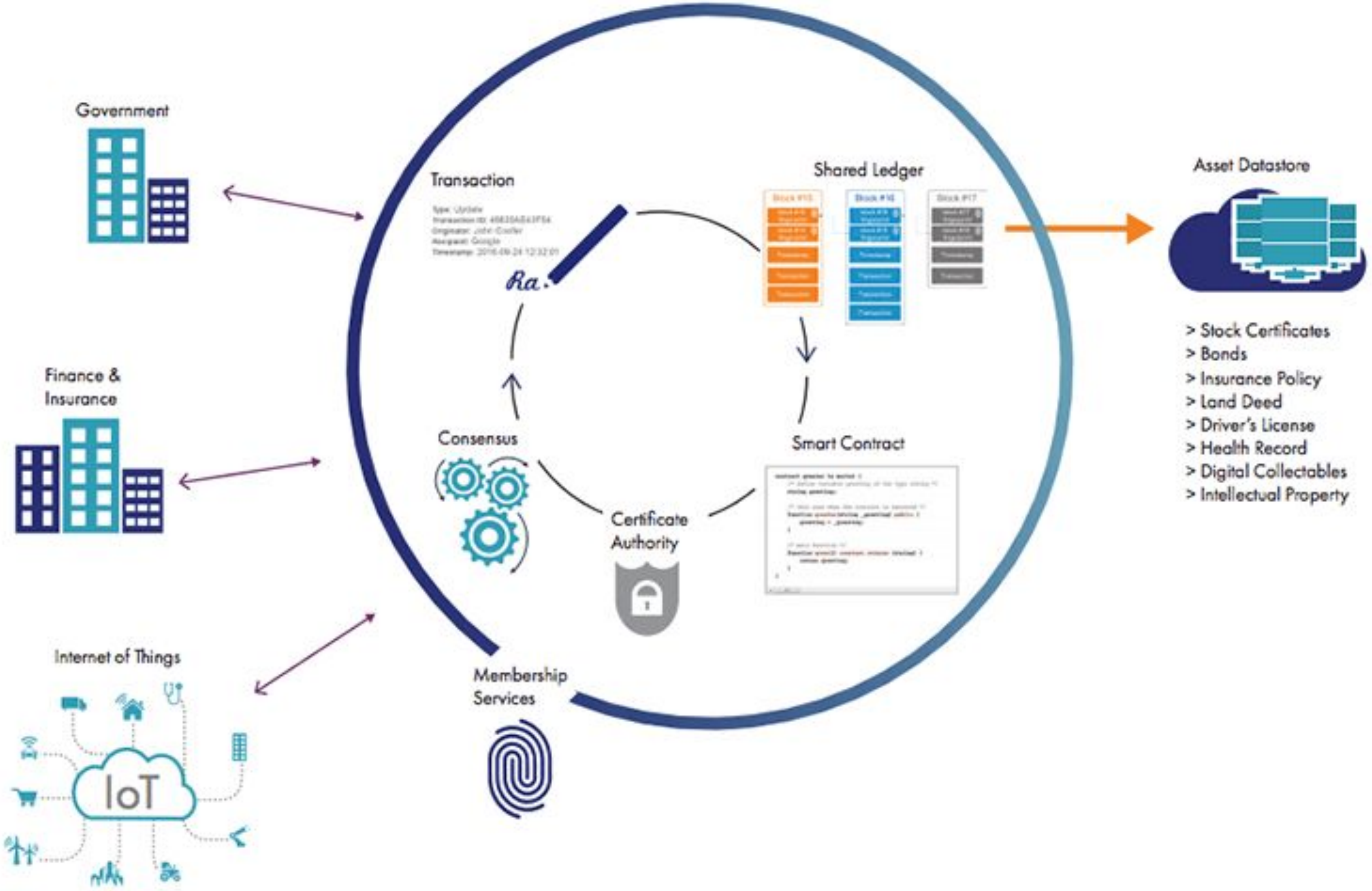
Purpose : Enables decentralized, verifiable reward validation and fraud registry.

Components:

- Smart Contracts (Solidity on Polygon):
  - For reward disbursement and scam ID hashing.
- Reward Vault:
  - Auto-credit reward system based on contract logic.
- Scam Hashes DB:
  - SHA-256 hashed UPI IDs flagged by GNN.
- User Wallet Integration:
  - MetaMask / web3.js / ethers.js.

Why it Matters : Provides trust, transparency, and automation in reward and fraud systems.

Blockchain as an Infrastructure



> Stock Certificates
> Bonds
> Insurance Policy
> Land Deed
> Driver's License
> Health Record
> Digital Collectables
> Intellectual Property

Storage & Analytics Layer

Purpose : Manages all data storage, logging and usage metrics.

Components:

- Graph DB (Neo4j or RedisGraph):
  - Stores transaction graphs for fraud detection.
- RDS/SQL DB:
  - User profiles, preferences, and transactional metadata.
- AWS S3:
  - Stores logs, offline DAG transaction files.
- Monitoring Tools:
  - Tracks success metrics like NPS, fraud rates, support ticket drop.

Why it Matters : Backbone of all analytics, fraud learning and historical trends.

THANK YOU!