

Hackathon Challenge: Payments Innovation

Welcome to an immersive hackathon experience designed to push the boundaries of payments technology. Over the course of this event, you'll tackle two real-world scenarios that address critical challenges in the rapidly evolving fintech landscape: stablecoin-powered cross-border payments and AI-driven fraud prevention.

These scenarios aren't just theoretical exercises—they reflect genuine market needs where innovation can create meaningful impact. Your mission is to demonstrate strategic thinking, creative problem-solving, and the ability to design solutions that balance technical feasibility with user experience, regulatory compliance, and business viability.

We're looking for teams that can think holistically about complex payment ecosystems, considering everything from technical architecture to human-centered design. Your presentations should showcase not just what you'd build, but why it matters and how it would work in the real world.

Scenario 1: Global Stablecoin Payment Relay

Revolutionizing Cross-Border Remittances for the Unbanked



The global remittance market represents both enormous opportunity and persistent challenges. With \$690 billion flowing annually to developing countries—yet burdened by average fees around 5%—there's a clear need for innovation. Meanwhile, stablecoin transaction volume has surged to \$4 trillion in 2025, marking an 83% increase and signaling strong market adoption.

The stablecoin market has matured significantly, with over \$300 billion in market capitalization. Regulatory frameworks are taking shape globally, from the EU's MiCA regulations to the U.S. GENIUS Act, creating clearer pathways for compliant innovation.



Multi-Chain Liquidity

Design interoperability across multiple stablecoins and blockchains, optimizing liquidity routing to minimize slippage and maximize cost efficiency for cross-border transfers.



Alternative Identity

Develop verification methods beyond traditional social logins—biometrics, community attestation, progressive KYC—enabling access for users without formal banking relationships.



Low-Bandwidth Access

Create solutions for offline or intermittent connectivity environments, including USSD protocols, SMS-based transactions, and local caching mechanisms for rural areas.

Dynamic Compliance

Build adaptive AML/KYC systems that adjust requirements based on geography, transaction size, and risk profile while maintaining regulatory compliance across jurisdictions.

Fraud vs. Volatility Protection

Balance fraud detection with volatility management—protect users from both malicious actors and market swings through smart contract safeguards and threshold mechanisms.

Transparent Fee Structure

Design clear pricing models with upfront disclosure, no hidden charges, and efficient dispute resolution processes that build trust with vulnerable user populations.

Expected Deliverables: Your solution should include detailed user journey maps for sender and recipient experiences, comprehensive ecosystem mapping showing all stakeholders and value flows, a compliance matrix addressing regional regulatory requirements, a fraud prevention strategy with risk scoring, and a scalable business model demonstrating unit economics and path to profitability.

Scenario 2: AI-Driven Fraud Detection

Building Customer Trust Through Intelligent Security

Financial fraud has reached crisis levels. In 2024, 79% of firms reported fraud attempts, and projections estimate global losses will exceed \$40 billion by 2027. Yet there's hope: AI-powered fraud detection systems have already reduced credit card fraud by 60% in early adopter organizations. The challenge isn't just detecting fraud—it's doing so without creating friction that erodes customer trust and experience.

Your mission is to design a real-time fraud detection system that adapts to increasingly sophisticated threats while maintaining seamless user experiences. This requires balancing competing priorities: security versus convenience, privacy versus data analysis, automation versus human oversight, and speed versus accuracy.

01	02	03
AI Risk Scoring Architecture Design machine learning models for dynamic risk assessment that operate in real-time, analyzing behavioral patterns, transaction context, device fingerprinting, and network effects while maintaining strict privacy compliance with GDPR, CCPA, and emerging regulations.	Adaptive Friction Framework Create tiered authentication systems that apply appropriate friction based on risk levels—seamless approval for low-risk transactions, step-up authentication for medium risk, and enhanced verification for high-risk scenarios without frustrating legitimate customers.	Intelligence Sharing Ecosystem Develop frameworks for cross-industry fraud intelligence sharing that preserve competitive boundaries while enabling collective defense against sophisticated fraud rings operating across multiple platforms and institutions.
04	05	
Trust & Transparency Layer Build customer communication strategies and dispute flows that explain security decisions clearly, provide rapid resolution pathways, and turn security measures into trust-building opportunities rather than points of frustration.	Continuous Learning Loop Establish feedback mechanisms where AI models continuously adapt to emerging threats, incorporating analyst insights, false positive analysis, and successful fraud patterns to stay ahead of evolving attack vectors.	

What You'll Deliver

- **Technical Architecture:** End-to-end fraud detection system design with AI model specifications, data pipelines, and integration points
- **Privacy Framework:** Comprehensive approach to data governance, encryption, anonymization, and regulatory compliance
- **Risk-Tiered Journeys:** User flow diagrams showing customer experiences across different risk scenarios and authentication requirements
- **Collaboration Blueprint:** Strategy for fraud intelligence sharing with clear governance, legal frameworks, and participation incentives
- **Customer Education Plan:** Communication strategies that build security awareness and trust while reducing support burden

