Global Payment Security: Navigating Compliance Across Borders

Dharshan Shanthamurthy

Founder & CEO
SISA

The Great Shift – From Cash to Digital

The future of money is in motion!

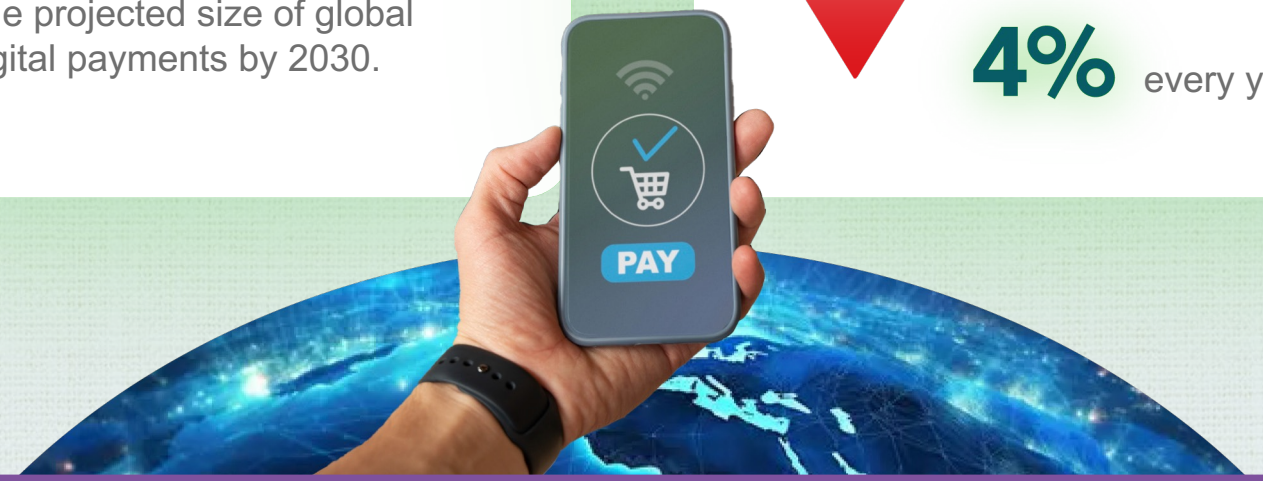
$33.5 trillion

The projected size of global digital payments by 2030.

80%

Cash use has dropped to 80% of 2019 levels - and keeps falling by

4% every year



"This isn't a regional trend - it's a global pivot. And it's reshaping everything."

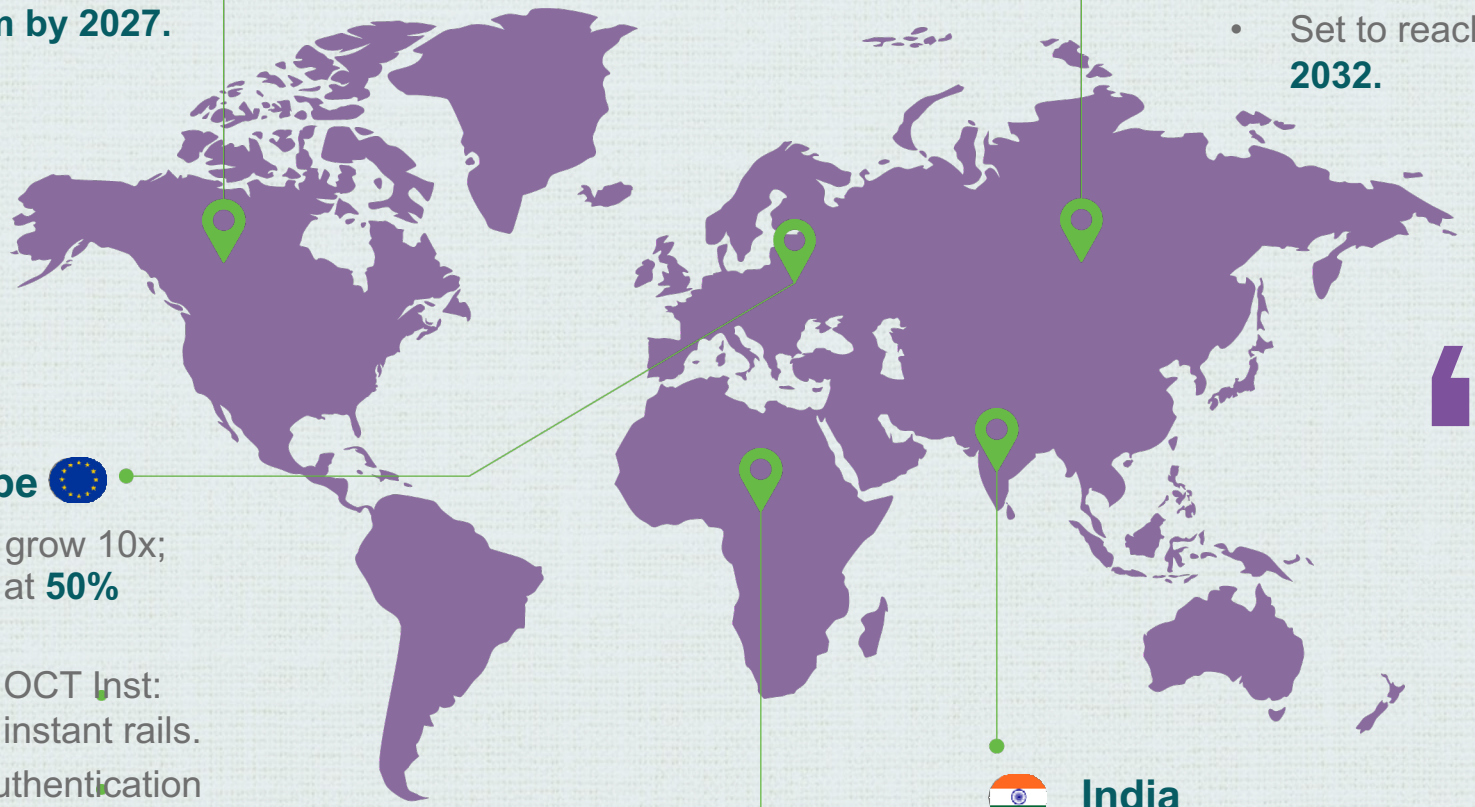
A World Rewriting the Rules of Money

North America

Digital wallets to reach **52% of US eCom by 2027.**

Asia

- QR codes and instant payments dominate.
- Set to reach **$23.8tn in 2032.**



Europe

- Instant payments to grow 10x; Open Banking, A2A at **50% CAGR.**
- EPI's Wero wallet + OCT Inst: new cross-currency instant rails.
- PSD3: Tightening authentication and third-party access.

> *Real-time finance is the new reality.*

India

Cash share down to **<10% by 2028;** UPI leading remittance innovations.

Africa & LATAM

- Cross-border payments is projected to triple to **USD 1Tr by 2035**.
- Mobile money, PIX, real-time rails drive financial inclusion.

Inclusion at Scale – CBDCs and Stablecoins

01 CBDCs: Explosive Growth Potential

90%+
of central banks are piloting or exploring CBDCs.

CBDC transaction volumes projected to surge 2,430% by 2031, hitting 7.8 billion transactions.

China's e-CNY, Nigeria's e-naira, India & Brazil's inclusion pilots, EU's digital euro, UK's digital pound blueprint and Korea's retail pilot with 100,000 people.

Stablecoins Become Mainstream 02

- Now an integral crypto asset class with ~28% annual supply growth.
- Stablecoin market could grow from $250 billion today to $1.6–$3.7 trillion by 2030
- Major banks jumping in: JPMorgan Chase, Citigroup, PayPal, Bank of America, Stripe, are all launching or planning stablecoins.
- Emerging use cases for B2B and supply chain financing.
- The GENIUS Act a federal framework for regulation of stablecoins, will encourage their adoption among fintech startups in Asia.

> **"The emergence of programmable digital money is expanding global access, reducing costs, and bridging financial ecosystems**

The Quantum Countdown – Disruption at a Cryptographic Level

01

2025

UN's International Year of Quantum Science & Technology

02

Fault-tolerant quantum computers by end of decade (Icons: Google Willow chip, Microsoft Majorana-1, IBM, Quantinuum)

03

RSA 2048-bit key
10 seconds (Quantum)
vs. **300 trillion years (Classical)**

04

"Shor's algorithm makes RSA, DSA, ECDSA obsolete"

05

AES needs larger keys (AES-256+) to stay resilient.

06

"Harvest Now, Decrypt Later" means sensitive data today is exposed tomorrow.

07

Sectors like finance, government, and automotive are already at risk.

"Security built for today won't survive tomorrow. Financial systems must begin the shift to quantum-safe protocols - before it's too late."

The New Reality – A Multi-Rail, Multi-Risk Ecosystem

Coexistence Brings Complexity

01

Cards Networks

Still dominant, but evolving with tap-to-pay, tokenization, blockchain pilots.

02

Banks & Fintechs

Open Banking, Pay-by-Bank, real-time payment rails..

03

Blockchain & Stablecoins

Real-time, programmable, borderless value transfer..

04

Quantum Computing

The disruptor rail that will break current cryptographic rails like RSA and DSA.

$15 trillion

Every new rail is an opportunity - for fraudsters and threat actors too.

Current Threats — Exploiting the Multi-Rail Reality

The financial sector has experienced more operational losses of approximately USD 12 billion in the last 20 years

Social Engineering & Credential Theft

AI-powered phishing, deepfakes, and chatbot scams are targeting people, not just systems.

Supply Chain & Third-Party Breaches

Vendors, software updates, and open-source code are frequent attack vectors.

Ransomware & Insider Abuse

Attackers target core banking systems and leverage insider knowledge.

Identity Attacks

MFA bypass and executive impersonation exploit weak identity controls.

API & Cloud Vulnerabilities

Weak API security and misconfigured cloud services widen the attack surface.

IoT Blind Spots

ATMs, kiosks, and wearables add invisible, often unmanaged vulnerabilities.

Attackers are innovating just as fast as the ecosystem, making real-time, end-to-end cybersecurity critical.

Tomorrow’s Threats - The Next Wave of Complexity

Here’s what’s coming next as digitization accelerates:

Deepfake & AI-Generated Attacks

Hyper-personalized, believable fraud will test even mature security controls.

Malicious Libraries & Supply Chain Risks

Fake or poisoned open-source packages will multiply.

Prompt Hacking & Adversarial LLMs

New rails mean new exploits - attackers will use generative AI against financial services.

Quantum Disruption

Existing encryption at risk - quantum-safe practices will become essential.

Cryptocurrency & Stablecoin Exploits

Digital assets and wallets are lucrative, borderless targets.

IoT Everywhere

More embedded devices, more hidden vulnerabilities

The future threat landscape is not linear - it’s exponential. Security must match the pace of payment innovation!

Security as Strategy: What Payments Must Prioritize Now!

Security is no longer a backend function; it's now the bedrock of innovation, consumer trust, and competitive edge in digital payments.

Real-time threat detection is foundational, integrating cybersecurity intel with fraud monitoring

As real-time payments expand, fraud use cases are shifting. Legacy card frameworks aren't enough; adaptive fraud models must evolve in parallel.

GenAI is a double-edged sword & while it's enabling hyper-accurate fraud detection, it also demands explainability, governance & ethical guardrails.

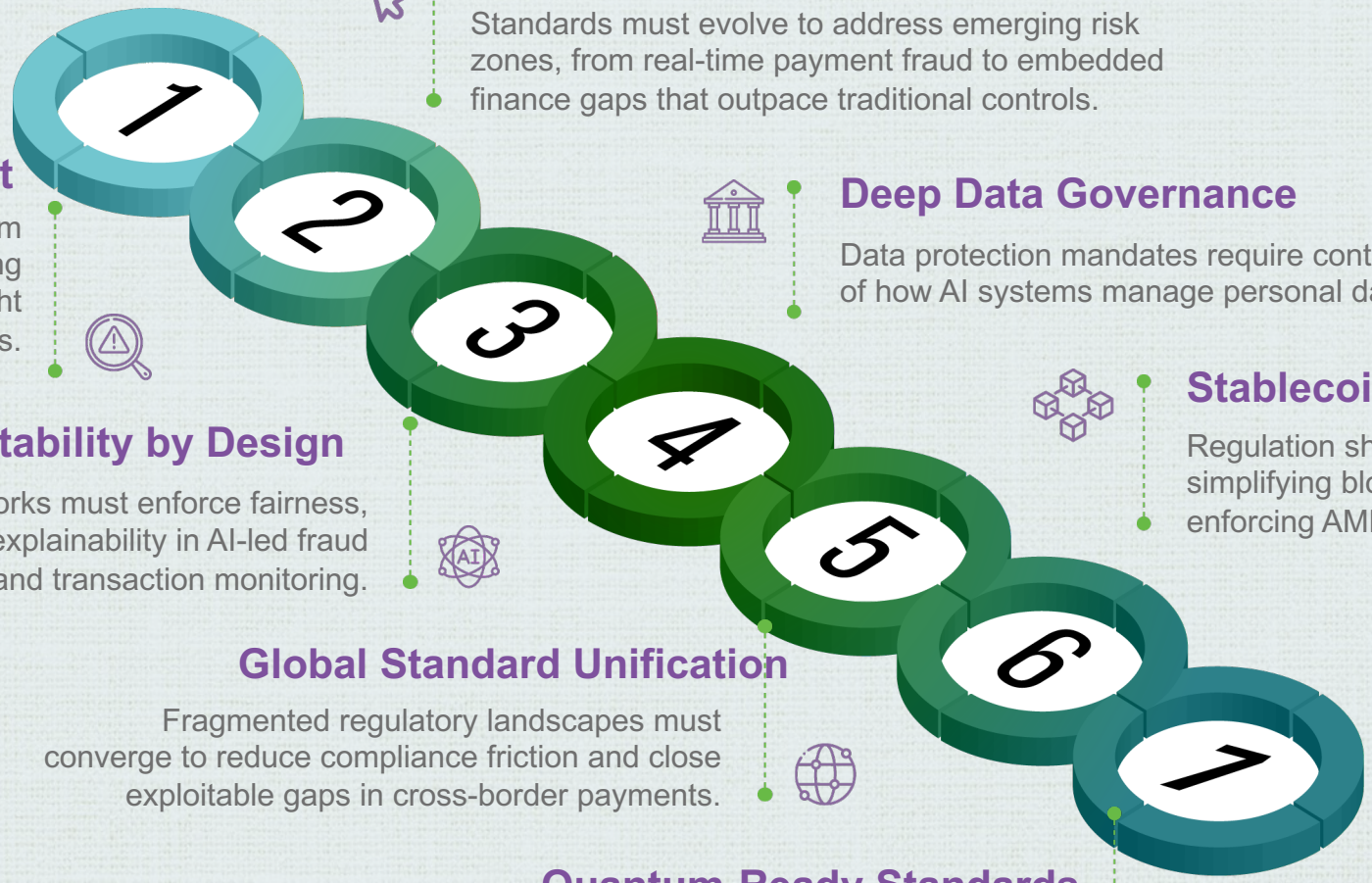
Cloud-native payments need cloud-native security. Encryption, access control, and real-time monitoring must be embedded

Data privacy is no longer just regulatory. Anonymization, consent-based AI usage, and compliance with global privacy laws are core to customer loyalty.

The threat of quantum decryption is real. Hence organizations must now architect crypto-agility into their core infrastructure.

Detection alone won't suffice. Instant response and recovery capabilities are a strategic necessity in always-on, borderless ecosystems.

Regulators and Industry Must Build the Future Together



1 Reinforcing the Weakest Links

Standards must evolve to address emerging risk zones, from real-time payment fraud to embedded finance gaps that outpace traditional controls.

2 Real-Time Risk Management

Regulation must shift from retrospective enforcement to enabling real-time, intelligence-led oversight across all payment rails.

3 Deep Data Governance

Data protection mandates require continuous oversight of how AI systems manage personal data.

4 AI Accountability by Design

Regulatory frameworks must enforce fairness, transparency, and explainability in AI-led fraud detection and transaction monitoring.

5 Stablecoin Simplification

Regulation should focus on orchestration - simplifying blockchain complexity while enforcing AML and CTF safeguards.

6 Global Standard Unification

Fragmented regulatory landscapes must converge to reduce compliance friction and close exploitable gaps in cross-border payments.

7 Quantum-Ready Standards

Policymakers must embed crypto-agility into national cybersecurity agendas to prepare for the impact of quantum decryption.

SISA

THANK YOU!

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING