International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Blockchain and Generative AI at Mastercard

Umesh Saini

Sayali Vhatkar

College of Management &Computer Application

MIT Art , Design & Technology University.

Executive Summary

Institution and use case. Mastercard Incorporated provides payment technology that links issuing and acquiring banks with merchants, businesses and public-sector organisations. The company recorded US$32.8 billion in net revenue in 2025, a 16% increase (Mastercard Inc., 2026a). This report examines a use case spanning Track A (Banking Operations) and Track C (Tokenisation): cross-border business-to-business (B2B) settlement between banks using tokenised deposits on Mastercard's permissioned Multi-Token Network (MTN). A Generative AI (GenAI) assistant is proposed to help compliance teams review alerts. India–UAE trade is used as the example corridor for a potential pilot.

Problem. International B2B payments may travel through several banks. Each institution can perform its own KYC and sanctions screening, apply charges, enter payment details and maintain a separate ledger. These steps can create delays, unclear total costs, payment corrections and reconciliation work. Here, these issues are treated as propositions to investigate—not established shortcomings of Mastercard, which operates a payment network rather than acting as a bank.

Solution. The report proposes a permissioned ledger shared by a consortium of regulated banks. Banks would use tokenised deposits, verify digital credentials before transfers, and use smart contracts to hold funds until required checks are satisfied. Any flagged transaction would remain on hold until a compliance officer reviews it. The ledger would record hashes, token movements and status updates only; personal and business information would remain off-chain, supporting the data-minimisation approach considered under the Digital Personal Data Protection Act, 2023. GenAI would explain alerts to analysts, not authorise payments.

Assessment. The idea appears suitable for a carefully staged pilot, although a central platform connected through APIs may achieve many of the same gains if participation remains low. Examples such as Ripple, JPMorgan Kinexys, TradeLens and we.trade suggest that adoption, governance and a sustainable commercial model can matter more than the underlying technology. Success would depend first on securing a committed group of regulated banks for one corridor and establishing governance arrangements reviewed by supervisors.

1. Institution Profile and Current Transaction Architecture

1.1 Institution profile

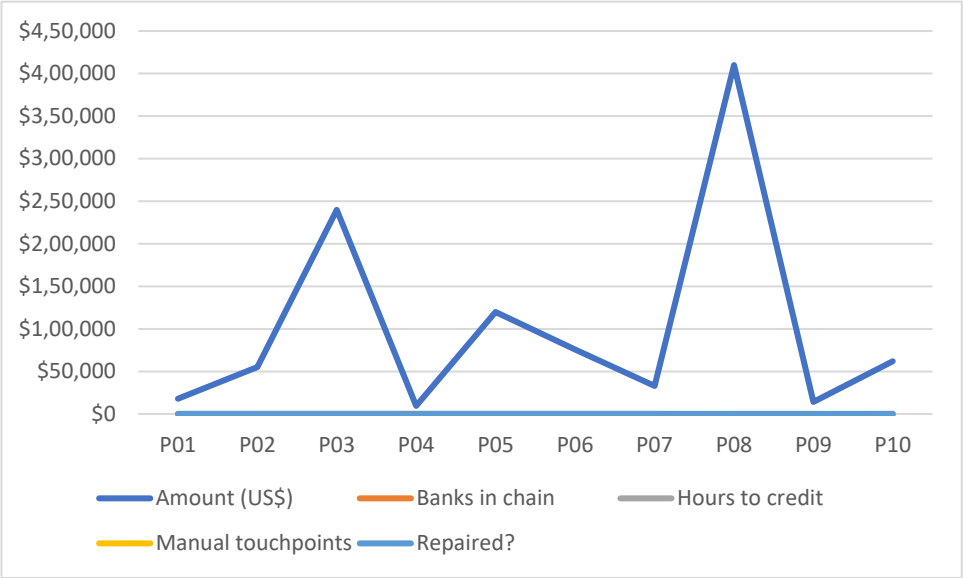
Institution profile - Mastercard Incorporated

Particular	Description
Institution	Mastercard Incorporated (NYSE: MA); headquartered in Purchase, New York
Type	Global payment-technology company and card network. Mastercard operates network switching, clearing and settlement; banks and other issuers provide the cards and accounts. Mastercard is not a bank and does not lend directly to cardholders.

Particular	Description
Products and services	Network processing and switching; cross-border money movement through Mastercard Move; fraud and risk analytics, data and cyber-intelligence services; and blockchain/digital-asset offerings such as Crypto Credential and the Multi-Token Network.
Customer segments	Issuing and acquiring banks, fintechs, merchants, corporates, governments and central banks
Scale (verified)	Net revenue of US$32,791 million in 2025 versus US$28,167 million in 2024 (+16%); revenue from the five largest customers was about US$6.9 billion, or 21% of the total (Mastercard Inc., 2026a, 2026b)
Operating footprint	Operates across more than 200 countries and territories (company-reported; to verify against the latest Form 10-K)
Principal regulators	Multiple. In India, Mastercard Asia/Pacific Pte. Ltd. operates its card network under authorisation by the Reserve Bank of India (RBI) under the Payment and Settlement Systems Act, 2007. As a listed US company it is also subject to SEC disclosure requirements.
Competitive context	Visa, American Express, UnionPay and domestic schemes such as NPCI's UPI and RuPay; SWIFT-based correspondent banking; fintech remitters; and stablecoin and tokenised-deposit networks such as JPMorgan's Kinexys
Project focus	Cross-border B2B settlement using tokenised deposits on MTN, supported by GenAI-assisted compliance review

Revenue has continued to grow, but the pattern behind that growth is especially relevant here. For the nine months ending 30 September 2025, Mastercard reported 15% growth in cross-border volume, compared with 9% growth in gross dollar volume and 10% growth in switched transactions, measured in local currency (Mastercard Inc., 2025). Cross-border payments are therefore an important source of both revenue and future growth, helping explain the company's interest in improving settlement.

Payment ID	Amount (US$)	Banks in chain	Hours to credit	Manual touchpoints	Repaired?
P01	$18,000	2	30	5	No
P02	$55,000	3	52	8	No
P03	$240,000	3	61	8	No
P04	$9,500	1	22	4	No
P05	$120,000	2	34	6	No
P06	$76,000	3	48	8	Yes
P07	$33,000	2	28	6	No
P08	$410,000	3	70	9	No
P09	$14,000	1	20	4	No
P10	$62,000	2	36	7	No



1.2 Digital channels and systems supporting the use case

- **Card and account-to-account network:** the core Mastercard switch authorises and clears transactions between issuers and acquirers worldwide.
- **Mastercard Move and cross-border services:** money-movement products that connect banks, fintechs and wallets for person-to-person and business payments. The Q4 2025 earnings presentation reports that Mastercard Move transaction growth exceeded 35% in 2025 (Mastercard Inc., 2026c; secondary summary, to verify).
- **Bank-side systems:** each participating bank runs its own core banking, payment hub and sanctions-screening systems, and connects to SWIFT or domestic rails (RTGS, NEFT, UPI) for the legs of a payment outside Mastercard's network.
- **Fraud and risk analytics:** Mastercard markets AI-based transaction scoring (its Decision Intelligence products) to issuers; exact capabilities should be confirmed from Mastercard's own documentation.
- **Digital-asset layer:** Crypto Credential (identity verification for blockchain transfers) and the Multi-Token Network, a private permissioned blockchain for settlement of tokenised deposits, regulated stablecoins and other tokenised assets.

1.3 Architecture classification (Unit I)

Mastercard's card network follows a centralised hub-and-spoke model. Mastercard operates the switch and maintains the network's clearing and settlement record, while issuing and acquiring banks keep their own account records. Cross-border bank transfers that take place outside this network are more fragmented: each bank maintains its own ledger, exchanges messages with other banks and reconciles records later. The current arrangement for this use case is therefore a combination of centralised and distributed systems.

The authoritative record depends on the payment stage. For a card purchase, the issuer maintains the cardholder's balance and Mastercard keeps the network clearing record. In a correspondent-banking transfer, no single record is shared by every institution: the sending bank, intermediary banks and receiving bank each maintain their own version. Nostro and vostro reconciliation helps them identify and resolve differences. A shared, tamper-evident record is one of the problems distributed ledger technology (DLT) is intended to address.

1.4 End-to-end transaction map

Figure 3 maps a typical cross-border B2B payment, starting with the company's instruction and ending with reconciliation. It highlights possible points of friction in correspondent banking generally. These are illustrative observations, not measured findings about Mastercard or any particular bank.

Verified and to-verify initiatives

Initiative	What the source says	Status / source quality
Crypto Credential	Announced in April 2023 as a verification layer used across all MTN interactions	Company announcement relayed by Crowdfund Insider (2023); confirm on Mastercard newsroom
Multi-Token Network (MTN)	Launched in 2023 as a private, permissioned network built around four pillars of trust (counterparties, assets, technology, consumer protection); reported to be built on Ethereum technology	Crowdfund Insider (2023); Blockworks (2023). Exact consensus design not publicly verified
Crypto Partner Program	Announced 11 March 2026 with 85+ partners; MTN positioned as a settlement layer for tokenised deposits and regulated stablecoins	Secondary sources (BlockEden.xyz, 2026); verify with Mastercard press release
Stablecoin settlement on MTN	A neobank stablecoin (SoFiUSD) reported to settle via MTN's interbank rails	Secondary source (BlockEden.xyz, 2026); to verify
AI fraud analytics	AI-based transaction scoring offered to issuers	Capability claimed in company materials; no figures used in this report
Indian regulatory history	RBI barred Mastercard Asia/Pacific from onboarding new domestic customers from 22 July 2021 for non-compliance with the 6 April 2018 data-storage circular, and lifted the restriction on 16 June 2022	Primary source: RBI (2022)

The sources reviewed for this report did not establish that Mastercard has run a blockchain pilot specifically on the India–UAE corridor. The corridor is therefore treated as a proposed example for the design, rather than an existing Mastercard deployment.

2. Business Problem and Current-State Analysis

2.1 Problem identification

Cross-border B2B transfers can be slow, and customers may not know the full cost at the outset. Several institutions may screen the payment separately, apply their own charges, re-enter details and reconcile records after processing. Settlement can also be affected by banking hours and cut-off times; a payment sent late on a Friday, for example, may not finish processing until the following working week. These are potential problems that must be checked against real transaction data, not assumed weaknesses at Mastercard. The question is whether Mastercard, as a network operator, could help banks offer a more predictable settlement process.

2.2 Current-state issues and root causes

Process step, issue, root cause and impact

Process step	Possible issue	Root cause	Likely business effect
KYC and sanctions at origin	Customer and counterparty verified again at each bank	No reusable, jointly trusted credential	Duplicated cost; slower onboarding
Payment message and FX	Fees and FX margin deducted at several hops	Several intermediaries and limited end-to-end price visibility	Unpredictable cost to the corporate
Correspondent processing	Re-screening and data re-keying	Each bank is liable for its own compliance	Delay; typographical and name-match errors
Credit to beneficiary	Funds credited only in bank hours	Legacy batch cut-offs; no 24x7 final settlement	Working capital locked for days
Reconciliation	Breaks between nostro/vostro records	Separate records without a common source of truth	Manual matching; operational risk
Exception handling	Repair queries by e-mail or message	Lack of shared status information and audit history	Staff effort; customer dissatisfaction

2.3 "Does this problem need a blockchain?" test

Blockchain suitability test

Criterion	Assessment for cross-border B2B settlement	Result
Multiple parties write to shared data	Originating bank, beneficiary bank, intermediaries, compliance providers and the network operator all create or update payment records	Yes
Limited mutual trust	Competing banks in different jurisdictions; no bank wants a rival to run the shared record	Yes
Need for a tamper-evident audit trail	Regulators in several countries need proof of who screened, approved and released what, and when	Yes
Costly intermediation or reconciliation	Multi-hop fees, repeated screening and nostro/vostro reconciliation add cost and time	Yes
Could one trusted central operator solve it?	Partly. Mastercard already runs a central switch trusted by many banks, so a central ledger with APIs is a credible alternative. The case for DLT rests on programmable 24x7 settlement in tokenised deposits and on interoperability between banks' own tokens	Partly
High throughput or anonymity needed?	No. B2B volumes are moderate and every participant must be identified	Favours permissioned DLT

The test suggests that DLT is most useful when several banks need to share a trusted record, automate settlement rules and see common compliance-status updates—especially where a single central platform would not meet those needs as well. If only two or three banks take part, a central ledger with APIs could provide much of the same functionality at lower cost. This trade-off is revisited in the feasibility assessment.

2.4 Data requirements and users

Data, source, user and decision supported

Data required	Likely source	User	Decision supported
Payment instruction (amount, currency, purpose)	Corporate via originating bank	Payment operations	Initiate and lock funds
Verified entity credential	Credential service, bank KYC	Compliance officer	Allow or block participation
Sanctions and watch-list screening result	Screening vendor	Compliance analyst	Clear, hold or escalate
Customer payment history	Originating bank	Fraud analyst	Judge whether the amount is unusual
FX rate and fee schedule	Rate provider, bank	Treasury	Price and approve conversion
Settlement and redemption status	Ledger, beneficiary bank	Operations, customer	Confirm completion; trigger refund on timeout

2.5 Problem statement

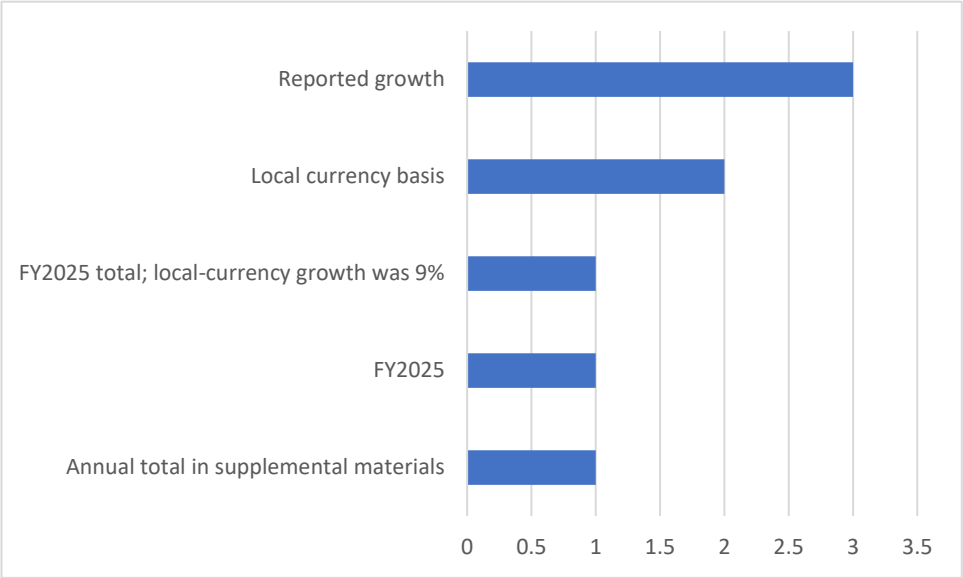
This study examines whether Mastercard and a group of regulated banks could use a permissioned ledger, tokenised deposits, verified credentials, smart-contract escrow and AI-assisted alert review to make cross-border B2B settlement faster. It also considers whether the approach could reduce manual work and payment repairs without weakening sanctions screening or data protection.

2.6 Baseline measures

Baseline measures (values come from the simulated sample in Appendix A, not from Mastercard)

Baseline measure	Calculation	Simulated baseline
Median settlement time	Median hours from payment instruction to credit in beneficiary account	35 hours (sample median)
Payment repair / exception rate	Payments needing manual repair or query / total payments x 100	10% (1 of 10 payments)
Manual touchpoints per payment	Count of manual entry, checking and approval steps	6.5 (sample mean)
Cost per payment	Operating cost of the payment unit / payments processed (excluding FX margin)	US$30 (assumption)

Metric	FY2025 value	Unit / basis
Gross dollar volume	10.6	US$ trillion
Gross dollar volume growth	9%	% YoY
Cross-border volume growth	15%	% YoY
Switched transactions growth	10%	% YoY
Net revenue growth	16%	% YoY
Payment network net revenue growth	12%	% YoY
Value-added services and solutions net revenue growth	26%	% YoY
FY2025 switched transactions	175464	million transactions



3. Blockchain Solution Design and Smart-Contract Logic

3.1 Choice of ledger type

Ledger options compared

Criterion	Public blockchain	Permissioned consortium	Central ledger + APIs
Who can join	Anyone	Vetted, regulated banks and approved fintechs	Customers of the operator
Identity / KYC	Pseudonymous	Known, credential-verified participants	Known to the operator
Privacy of payment data	Weak by default; all data visible	Channel-level privacy; sensitive data off-chain	Strong within one operator
Throughput and finality	Variable; probabilistic finality	High; fast deterministic finality	High
Neutral shared record	Yes	Yes	No; depends on one operator
Regulatory fit (RBI, data protection)	Poor for regulated bank settlement	Good	Good
Assessment	Rejected for bank settlement	Preferred option	Fallback if too few banks join

For this proposal, a consortium (permissioned) ledger is the strongest fit. Only approved institutions would participate, which supports clear identity checks, privacy controls, supervisory access and defined settlement finality. This is broadly consistent with published descriptions of MTN as a private permissioned network, rather than an open blockchain anyone can join.

3.2 Structure of the chain

- **Blocks and hash linking:** each block header holds the hash of the previous block, a timestamp and a Merkle root, so altering any past record breaks the chain and is detectable.
- **Merkle tree:** payment events (tokens locked, screening result recorded, tokens released, token redeemed) are hashed pairwise up to a single root. A bank can prove that one event is in a block without revealing the others.

- **Digital signatures and wallets:** every participant signs with a private key held in a hardware security module (HSM); others verify with the public key. Institutional wallets replace anonymous Bitcoin-style wallets, and key custody follows bank policy with multi-signature approval for large transfers.
- **On-chain versus off-chain:** on-chain data are payment-ID hashes, token amounts, status events, credential-validity flags and hashes of screening results. Customer personal data, invoices and contracts stay in each bank's secure storage and are referenced only by salted hash.
- **Timestamps:** block timestamps give a shared time for each event, which supports dispute resolution and regulatory reporting.

3.3 Consensus mechanism

Proof of Work, used by Bitcoin, is intended for an open network where participants may not know one another. It consumes substantial energy, and transaction finality is probabilistic, which makes it less suitable for settlement among identified, regulated banks. Proof of Stake can use less energy, but its open-validator model and reliance on token-based incentives are not an obvious fit for a bank-operated system handling deposits denominated in fiat currency.

For the proposed network, a Byzantine fault-tolerant (BFT) consensus protocol is recommended. Protocols such as PBFT or QBFT, which are available in some permissioned Ethereum-compatible systems, can confirm transactions quickly while tolerating a limited number of faulty or malicious validators. This is important because funds should only be released once the ledger has reached finality. Raft is simpler in some settings, but it is designed mainly to handle crashes rather than malicious behaviour. Mastercard has not publicly confirmed which consensus mechanism MTN uses; BFT is therefore a design recommendation for this project, not a statement about MTN's actual technology.

3.4 Smart-contract logic

The proposed contract places the sender's tokenised deposit in escrow and checks a set of predefined compliance conditions. If screening produces an alert, the funds remain locked until a human reviewer clears the case. The example is explanatory pseudo-code only; it is not ready for production deployment.

Oracles. The contract depends on two external feeds: the credential service (are both banks' credentials valid?) and the sanctions-screening result supplied by each bank's screening system. Oracle reliability is a primary risk (Task 4). Mitigations include signed oracle messages, multiple independent sources for critical inputs, and an explicit HELD state whenever an oracle is unavailable.

3.5 Tokenisation

Settlement asset options

Settlement asset	What it is	Fit for this design
Tokenised deposit	A digital form of a commercial-bank deposit. It remains a liability of the issuing bank and is intended to be redeemable at face value.	Preferred option. Keeps money inside the regulated banking system and preserves deposit-protection and AML controls
Regulated stablecoin	A token issued by a bank or non-bank and supported by reserve assets.	Acceptable where regulation allows; adds reserve and de-pegging risk
Wholesale CBDC (e-rupee)	Digital money issued by a central bank. The RBI has conducted wholesale and retail pilots.	Ideal settlement asset for interbank finality if the RBI permits cross-border use; policy-dependent
Volatile crypto-asset	Token whose price floats	Rejected: price risk is unacceptable for B2B settlement

In this design, banks would settle using tokenised deposits and manage the conversion between ordinary deposits and their tokenised equivalents. This avoids depending on a volatile crypto-asset. The Ripple case also illustrates why a settlement design should consider the price and regulatory risks that can arise when a fluctuating digital asset is used.

3.6 Solution architecture

Banks and corporate customers would use the service through their existing applications and supporting AI tools. Smart contracts would update the permissioned ledger, which would connect to banks' core systems and relevant payment rails, including SWIFT, Mastercard Move, RTGS, UPI and the e-rupee. The aim is to integrate with current infrastructure rather than ask banks to replace it. If regulators agree, supervisory teams could be given read-only access through an observer node.

3.7 Comparison of alternative approaches

A central ledger operated by Mastercard and connected through APIs would probably be faster and cheaper to build, particularly given the company's existing bank relationships. The trade-off is that participating banks would not jointly control the shared record, and transfers between different tokenised deposits could be harder to support. A public blockchain offers wider access but creates questions around privacy, identity and regulatory suitability. A consortium ledger takes more work to coordinate and govern, but better reflects the shared-control needs of regulated banks. A sensible path is to begin by digitising payment data and credentials, then move to a consortium network if enough banks commit. If they do not, the central-ledger option remains available.

4. Value, Feasibility, Regulation and Risk Evaluation

4.1 Benchmarking against syllabus case studies

Case benchmarks and lessons for the design

Case	What it shows	Lesson for this design
Ripple	Uses a network and the XRP digital asset for cross-border liquidity. Its adoption in the US was affected by prolonged legal uncertainty over the asset (litigation began in December 2020; later developments to verify)	Avoid dependence on a volatile token; settle in tokenised deposits or central bank money
JPMorgan Chase (Kinexys, formerly Onyx)	A large bank runs a permissioned network for tokenised deposits and institutional payments. Reports indicate MTN has been connected to JPMorgan's Kinexys Digital Payments (secondary source; to verify)	A strong anchor institution drives adoption; interoperability between competing permissioned networks may matter more than winning exclusivity
IBM-backed platforms (TradeLens, we.trade)	TradeLens, built by IBM and Maersk's GTD Solution, was discontinued: Maersk and IBM announced on 29 November 2022 that it had not reached the commercial viability needed, with shutdown planned by the end of Q1 2023. we.trade was reported to have shut in June 2022 after failing to secure further funding (GTR, 2022; Maersk and IBM, 2022)	The technology functioned, but adoption and commercial sustainability fell short. Secure committed members and a fee model before scaling

TradeLens offers a useful lesson for this proposal. Mastercard could start from a stronger position because it already has established relationships with banks and experience earning network fees. Even so, banks may be reluctant to rely on a settlement platform controlled by one commercial provider. Mastercard's five largest customers accounted for about

21% of revenue (Mastercard Inc., 2026b), which also suggests that major bank participants could have meaningful influence when governance terms are negotiated.

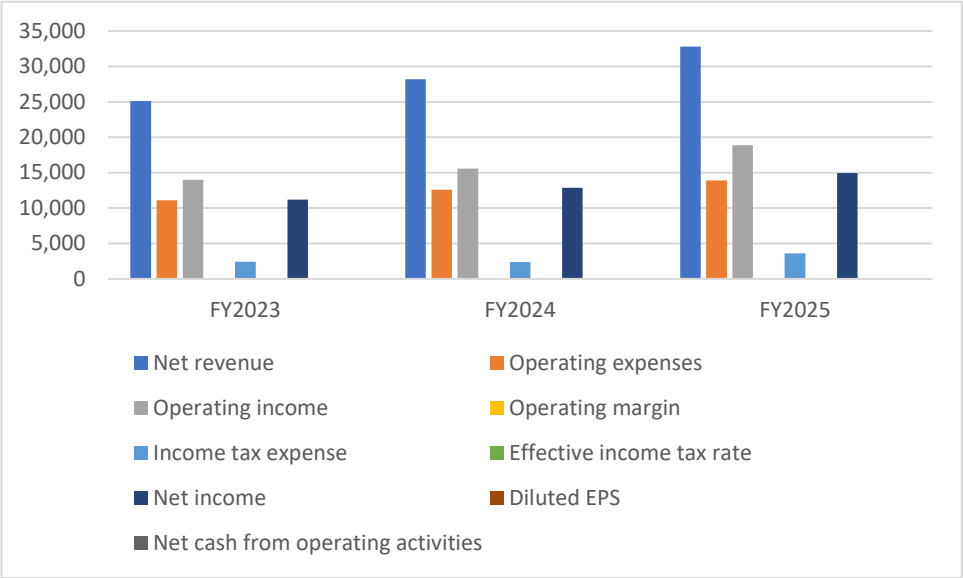
4.2 Expected value

Expected benefits (hypotheses to be tested in a pilot)

Area	Potential benefit to test
Speed	24x7 final settlement of tokenised deposits removes banking-hour delays; remaining delay is mainly human compliance review
Cost	Fewer intermediaries and less duplicate screening or data entry may lower per-payment cost
Transparency	Live shared status and a single audit trail replace e-mail repair queries
Fraud and compliance	Verified credentials and shared compliance state; ML scoring prioritises alerts for analysts
Working capital	Faster final settlement releases funds for exporters and importers
Customer experience	Predictable timing and visible payment status

Metric	FY2023	FY2024	FY2025
Net revenue	25,098	28,167	32,791
Operating expenses	11,090	12,585	13,894
Operating income	14,008	15,582	18,897
Operating margin	55.8%	55.3%	57.6%
Income tax expense	2,444	2,380	3,610
Effective income tax rate	17.9%	15.6%	19.4%
Net income	11,195	12,874	14,968
Diluted EPS	$11.83	$13.89	$16.52
Net cash from operating activities	0	0	

Chart data	
Fiscal Year	Net Revenue
2023	25098
2024	28167
2025	32791



4.3 Feasibility assessment

Feasibility factors and proposed actions

Factor	Assessment	Suggested action
Network adoption (business model)	Critical. Value rises with the number of banks, and no bank gains from an empty network	Start with one corridor and two to four committed anchor banks; agree fees up front
Governance	Who governs, who pays, how disputes and exits work are the main causes of consortium failure	Consortium charter with voting rules, fee model, liability and exit provisions before scale-up
Interoperability	Banks may issue their own tokens; other networks (e.g., Kinexys) exist	Use open standards and APIs; test cross-network transfers
Scalability and latency	B2B volumes are moderate; BFT networks can slow as validators grow	Limit validator set; test throughput in the sandbox
Key management	Loss or theft of an institutional key can freeze or divert funds	HSMs, multi-signature approvals, documented recovery
Legacy integration and skills	Core banking and screening systems vary by bank; skills are scarce	API gateway pattern; training; technology partner support

4.4 Regulatory and privacy position

RBI and payment-system rules. Mastercard's Indian operations are subject to the relevant authorisation under the Payment and Settlement Systems Act, 2007. A new settlement model would need to fit within applicable permissions and should be discussed with the Reserve Bank of India (RBI), potentially through a regulatory sandbox. The RBI's enforcement history highlights the importance of payment-data localisation: Mastercard was restricted from onboarding new domestic customers after non-compliance with the 6 April 2018 data-storage circular, and the restriction was lifted on 16 June 2022 after compliance was demonstrated (RBI, 2022). The proposed design should therefore ensure that Indian payment data remain stored in India and available for supervisory access.

Foreign exchange and AML. Cross-border payments made by Indian businesses must comply with the Foreign Exchange Management Act, 1999, including applicable purpose-code and authorised-dealer requirements, as well as the Prevention of Money Laundering Act, 2002 and RBI KYC directions. The receiving bank must also

follow the relevant UAE rules. Smart contracts can automate checks specified by the banks, but they do not remove the institutions' legal responsibilities.

Data protection and immutability. An immutable ledger can be difficult to reconcile with rights to correct or erase personal data under the Digital Personal Data Protection Act, 2023. The proposed safeguard is to keep personal information off-chain and record only salted hashes, token movements and status indicators. Source data would remain in bank-controlled systems, where changes or deletions can be managed. Destroying a relevant secret may also reduce the usefulness of a hash, but legal advice is needed to determine whether the specific hashes would still qualify as personal data.

Tokenised deposits and stablecoins. The legal treatment of tokenised deposits and the permissibility of regulated stablecoins for cross-border settlement depend on RBI policy and the rules of overseas regulators. This uncertainty is a major reason to begin with a controlled sandbox rather than a live, full-scale launch.

4.5 Risks, limitations and safeguards

Risk register (IDs match the heat map in Figure 7)

ID	Risk	Possible consequence	Safeguard
R1	Smart-contract bug	Wrong release or locked funds	Independent audit; formal verification of core logic; human approval for held payments
R2	Oracle failure or manipulation	Payment released on wrong screening or credential data	Signed feeds; multiple sources; default to HELD on failure
R3	Private-key compromise	Unauthorised transfers	HSMs; multi-signature; key rotation
R4	Consortium governance failure	Network stalls or members exit	Charter, voting rules, exit and liability terms
R5	GenAI hallucination	Fabricated or missed alert explanation	Ground outputs in supplied data; mandatory human review; log overrides
R6	AI bias in risk scoring	Some customer or country segments flagged unfairly	Test performance by segment; explainable scores; periodic audit
R7	Regulatory change or refusal	Pilot blocked or redesigned	Sandbox participation; early RBI dialogue; settle in regulated assets
R8	Public perception of crypto scandals	Loss of trust among corporates	Message that the network uses regulated bank money and no speculative token
R9	Token de-pegging or redemption failure	Loss to receiving bank	Prefer tokenised deposits; reserve and redemption rules

The risks that deserve the most attention are smart-contract defects (R1), compromised private keys (R3), regulatory rejection (R7) and weak consortium governance (R4). These issues cannot be solved by software alone. They need independent technical review, clear accountability and early agreement with regulators and participating banks.

4.6 Overall evaluation

The proposed model appears technically feasible and could offer business benefits, but the ledger itself is only one part of the challenge. The project would need enough regulated banks to join, supervisory comfort with tokenised-deposit settlement, and governance and fee arrangements that make participation worthwhile.

5. GenAI Demonstration, Future-State Design and KPIs

5.1 Future-state process

- **Step 1-2:** the corporate submits a payment; the ledger checks that both banks hold valid credentials, replacing repeated onboarding checks.
- **Step 3:** the originator's tokenised deposit is locked in escrow, so funds are committed and visible but not yet released.
- **Step 4:** rules and ML scoring screen the payment. When an alert is raised, the GenAI assistant explains it in plain language for the analyst.
- **Human check:** a compliance analyst approves or rejects alerts. Smart contracts never override a human decision.
- **Step 5-6:** on a CLEAR result or human approval, the contract releases tokens and the beneficiary bank redeems them into local deposits. If release does not occur by the timeout, funds return to the originator.
- **Step 7-8:** the customer sees live status, the audit trail is written to the ledger, and a dashboard tracks KPIs, overrides and model drift.

Compared with the existing process, the proposed service would give authorised participants a shared transaction record, reusable verified credentials, settlement outside normal banking hours and a clearer view of payment exceptions. Human officers would still make the compliance decisions.

5.2 GenAI prompt demonstration

Use case: explaining a sanctions/AML screening alert for a simulated cross-border payment. All data below are invented for a classroom exercise; no Mastercard, bank or customer data were used. **Tool used:** Claude (Anthropic), with the prompt run in this drafting session; the student should re-run it in the course-approved tool and attach screenshots.

Summary of the GenAI output

Factor	Observation	Effect on risk	Objective or judgement
Amount	USD 240,000 is 4 times the USD 60,000 average of prior payments	Raises	Objective
Beneficiary account age	Opened 45 days ago	Raises	Needs judgement (new suppliers are common)
Name similarity	86% match to a watch-list entry	Raises	Needs judgement (could be a false positive; identifiers required)
Originator history	Account held for 6 years; 4 prior payments to this beneficiary	Lowers (weakly)	Objective
Travel-rule data	All fields complete	Lowers	Objective
Beneficiary bank credential	Valid; expires in 20 days	Neutral (administrative)	Objective
Declared purpose	Advance payment for cotton yarn; cannot be verified from the data given	Neutral	Needs judgement

Output summary. The model linked the alert to three combined signals: the payment was four times the usual amount, the beneficiary account was relatively new, and the beneficiary name showed a close match with a watch-list entry. It correctly noted that none of these signals proves wrongdoing on its own. The analyst was advised to obtain the beneficiary's registration and ownership documents, the invoice or purchase order supporting the amount, identifying details for the watch-list entry, and evidence of the prior business relationship. In line with the prompt, the model did not recommend releasing or blocking the payment. It also stated that the screening

threshold and scoring rules were not provided and that four previous payments are too few to establish a strong pattern.

Critical review of the GenAI output

Criterion	Assessment
Accuracy	The arithmetic (240,000 / 60,000 = 4) and the factor classification were checked independently and are correct for the data supplied
Hallucination	No new facts were added in this run, because the prompt forbade it. The risk remains that a model could invent watch-list details or regulatory rules; every statement must be grounded in supplied data
Bias	The prompt instructed the model not to infer from names or countries. Without that instruction, models can reflect biases from training data, for example over-weighting particular jurisdictions. Bias testing by customer segment is required in production
Explainability	The narrative is a post-hoc explanation written by the model; it is not the real reasoning of the bank's scoring engine and cannot replace an audit trail of the rules that fired
Limitations	The model cannot query the actual watch list, cannot verify the beneficiary and cannot judge whether 86% should trigger an alert at this bank
Data confidentiality	Only invented data were used. Real alerts contain personal and commercial data and must only be processed in a bank-approved secure deployment

5.3 Human oversight and responsible use

- Use only simulated or anonymised data in public GenAI tools; production use requires an approved enterprise deployment with logging and access control.
- A qualified compliance analyst decides every held payment; the GenAI assistant and ML score only prioritise and explain.
- Smart-contract code drafted by GenAI must be audited independently and is never presented as deployment-ready.
- Log every override of an AI or contract finding and review override patterns monthly for bias and model drift.

5.4 Key performance indicators

KPIs, simulated baselines and illustrative pilot goals

KPI	How measured	Baseline (simulated)	Illustrative pilot goal
Median settlement time	Hours from instruction to beneficiary credit	35 h (sample median)	-60% (about 14 h); remaining time is mainly human review
Cost per payment	Payments-unit operating cost / payments processed	US$30 (assumed)	-30% (about US$21)
Payment repair / exception rate	Repaired payments / total payments	10% (sample)	-40% (about 6%)
Manual touchpoints per payment	Count of manual steps	6.5 (sample mean)	-40% (about 4)
Sanctions false positives reaching analysts	Alerts closed as false / alerts reviewed	90% (assumed)	-15% (about 76%)

These figures are illustrative targets, not guaranteed results. They represent possible gains from continuous settlement, reusable credentials and shared payment-status information. The baseline and targets should be recalculated once real data from the selected corridor are available. The proposed reduction in false positives is deliberately more cautious because screening quality also depends on watch-list data, which the network operator cannot fully control.

6.1 Prioritised recommendations

Recommendations linked to problems and expected benefits

Priority	Recommendation	Problem addressed	Expected benefit
1	Define one corridor (e.g., India-UAE) and measure baselines on real payment data	No verified baseline (Section 2.6)	Evidence base for every later decision
2	Form a bank consortium with a charter covering governance, fees, liability and exit before scaling	Governance and adoption risk (R4)	Avoids the TradeLens/we.trade failure pattern
3	Settle in tokenised deposits (and e-rupee if permitted); avoid volatile tokens	Settlement asset risk (R7, R9)	Regulatory fit; no price risk
4	Store only hashes and status events on-chain; keep personal data off-chain in India	Privacy and data-localisation (Section 4.4)	Compliance with DPDP Act and RBI storage rules
5	Deploy smart-contract escrow with human approval for held payments, after independent audit	Delay and reconciliation (Table 3); bug risk (R1)	Faster, consistent checks with human control
6	Deploy a bank-approved GenAI alert-explanation assistant with logging and bias testing	False positives and analyst effort	Less routine effort; better prioritisation

6.2 Phased implementation roadmap

Roadmap with owners, dependencies and success measures

Phase	Key activities	Owners	Dependencies	Success measure
Phase 1: Proof of concept (0-3 months)	Select corridor; measure baselines; build sandbox with test data; draft consortium principles; test GenAI prompts on simulated alerts	Network operator, anchor banks' payments, IT and compliance teams	Bank commitments; test environment; legal review	Baseline measured; test payments settle end to end in the sandbox
Phase 2: Corridor pilot (3-12 months)	Apply for regulatory sandbox; onboard partner banks; integrate with core banking and screening; run parallel with correspondent flow; train staff	Consortium banks, legal, compliance, IT	RBI sandbox approval; foreign regulator comfort; audited contracts	Pilot meets settlement-time and repair-rate goals with no compliance breach

Phase	Key activities	Owners	Dependencies	Success measure
Phase 3: Scale and govern (1-2 years)	Add corridors and currencies; formalise charter and fee model; connect to other networks; monitor models and contracts	Consortium board, senior management, data governance	Pilot success; sustainable fee model	Sustained KPI improvement at acceptable cost and risk

6.3 Change management and ecosystem actions

- **Consortium governance:** agree decision rights, fees, liability and exit terms in writing before the pilot; give regulators observer access.
- **Partner onboarding:** begin with a small group of banks that already trade on the corridor; offer a standard integration kit and sandbox support.
- **Skills:** blockchain and smart-contract literacy for operations, compliance and audit staff, plus training to challenge AI outputs rather than accept them.
- **Communication:** explain that the network supports analysts and officers rather than replacing them, and that it uses regulated bank money and no speculative token.
- **Pilot testing and feedback:** involve experienced compliance staff in designing contract rules; keep a structured channel for reporting wrong AI or contract outcomes.
- **Monitoring:** review KPIs, overrides, security incidents and participation each month, and report to the consortium board.

6.4 Conclusion

A permissioned ledger that combines tokenised deposits, credential checks, smart-contract escrow and AI-assisted alert review could make cross-border B2B payments faster and easier to track, while reducing some manual reconciliation work. A phased pilot would help test whether those benefits are real. However, the business case depends on how many banks take part. If participation stays low, a central ledger linked through APIs may deliver much of the same improvement at a lower cost.

The first requirement is a committed group of regulated banks prepared to use the service on one clearly defined corridor, with governance arrangements reviewed by supervisors. Without that commitment, even a well-designed platform may not attract enough transactions to remain commercially sustainable.

References

A.P. Moller - Maersk & IBM. (2022, November 29). Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform [Press statement, as reported by trade press].

BlockEden.xyz (Noda, D.). (2026, March 14). Mastercard's Multi-Token Network unites 85+ crypto partners as stablecoin settlement hits $1.26 trillion. https://blockeden.xyz/blog/2026/03/14/mastercard-multi-token-network-85-crypto-partners-1-26t-stablecoin-settlement/

Blockworks. (2023). Mastercard to continue crypto foray with beta launch of 'blockchain app store'. https://blockworks.com/news/mastercard-blockchain-app-store-beta

Crowdfund Insider. (2023). Mastercard unveils Multi Token Network (MTN) to scale, secure blockchain tech. https://www.crowdfundinsider.com/?p=209443

Dhameja, G., Singhal, B., & Panda, P. S. (2018). Beginning blockchain: A beginner's guide to building blockchain solutions. Apress.

Drescher, D. (2017). Blockchain basics: A non-technical introduction in 25 steps. Apress.

Euromoney Learning. (n.d.). What is blockchain? https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

Furlonger, D., & Uzureau, C. (2019). The real business of blockchain: How leaders can create value in a new digital age. Harvard Business Review Press.

Global Trade Review. (2022). Maersk and IBM pull the plug on TradeLens. https://www.gtreview.com/news/top-stories/maersk-and-ibm-pull-the-plug-on-tradelens/

Government of India. (2002). Prevention of Money Laundering Act, 2002; (1999) Foreign Exchange Management Act, 1999; (2007) Payment and Settlement Systems Act, 2007; (2023) Digital Personal Data Protection Act, 2023.

Mastercard Incorporated. (2025). Third quarter 2025 financial results (Form 8-K, Exhibit 99.1). U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1141391/000114139125000191/ma09302025-exx991xearnings.htm

Mastercard Incorporated. (2026a). Fourth quarter and full year 2025 financial results [Press release, 29 January 2026].

Mastercard Incorporated. (2026b). Annual report on Form 10-K for the fiscal year ended December 31, 2025. U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1141391/000114139126000013/ma-20251231.htm

Mastercard Incorporated. (2026c). 4Q25 earnings presentation. https://s25.q4cdn.com/479285134/files/doc_financials/2025/q4/4Q25-Mastercard-Earnings-Presentation.pdf

Reserve Bank of India. (2018, April 6). Storage of payment system data [Circular]. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

Reserve Bank of India. (2022, June 16). Reserve Bank of India lifts the business restrictions imposed on Mastercard Asia/Pacific Pte. Ltd. (Press Release 2022-2023/379). https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=53877

Securities and Exchange Board of India. (n.d.). Reports and statistics. https://www.sebi.gov.in/reports-and-statistics.html

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.

Appendix A: Simulated Baseline Dataset

The ten transactions in this appendix are fictional and are included only to demonstrate . They are not Mastercard or bank records, and the sample is too small to support statistical conclusions.

Simulated payment sample

Payment	Amount (US$)	Banks in chain	Hours to credit	Manual touchpoints	Repaired?
P01	18,000	2	30	5	No
P02	55,000	3	52	8	No
P03	240,000	3	61	8	No
P04	9,500	1	22	4	No
P05	120,000	2	34	6	No
P06	76,000	3	48	8	Yes
P07	33,000	2	28	6	No
P08	410,000	3	70	9	No
P09	14,000	1	20	4	No

Payment	Amount (US$)	Banks in chain	Hours to credit	Manual touchpoints	Repaired?
P10	62,000	2	36	7	No

Calculation: arranging settlement times in ascending order gives 20, 22, 28, 30, 34, 36, 48, 52, 61 and 70 hours. The median is (34 + 36) / 2, or 35 hours. The ten payments have 65 manual touchpoints in total, giving an average of 6.5. One payment required repair, equivalent to 10%. The US$30 cost estimate and 90% false-positive rate are assumptions rather than results from this sample.

Appendix B: GenAI Use Disclosure and Prompt Evidence

GenAI tools used

GenAI tool	Purpose	Section(s) of report
Claude (Anthropic)	Drafting assistance for report structure and text, chart and diagram generation code, and the alert-explanation demonstration; web search used to locate public sources	All sections; Task 5 (Sections 5.2-5.3)

contains the prompt used for the Task 5 demonstration. Before submission, the student should check each factual statement, repeat the demonstration using a tool approved by the course, replace items marked for verification with confirmed evidence, and ensure the final analysis reflects their own understanding and writing. No confidential or personal information was entered into a public AI tool.

Annexure: Self-Assessment Sheet

Field	Entry
Name	**Umesh Saini**
Roll No.	**ADT25COMM0148**
Institution chosen	**Mastercard Incorporated**
Use-case track	**Track A / C: cross-border payments with tokenised deposits**