WCRG Global Research WORLD COMET RESEARCH GROUP

International Journal of Modern Innovations and Emerging Trends
Vol. 5, No. 1, 2022
Doi: 10.67228/30715628/IJMIET-2022PI1P8N
PP. 01-18

Original Article

Next-Generation Payment Technologies in Digital Commerce

Dr. Priya Natarajan

Associate Professor, University of Madras, India.

Received: 05-02-2022 Revised: 05-26-2022 Accepted: 06-01-2022 Published: 06-03-2022

ABSTRACT

Digital commerce payments have evolved from simple card-not-present transactions to complex ecosystems including mobile wallets, instant payments, tokenization, embedded finance, and programmable money. At the same time, new threats such as account takeover, synthetic identities, SIM swap fraud, token theft, and API abuse have increased. Next-generation payment technologies—such as biometric authentication, EMV tokenization, contactless and QR payments, real-time payment rails, blockchain settlement, central bank digital currencies (CBDCs), and pay-by-bank/A2A systems—aim to improve security, interoperability, user experience, and compliance. These systems replace static credentials with dynamic tokens and cryptograms, reducing fraud risk and improving authorization. Phishing-resistant authentication methods like biometrics and passkeys are also gaining adoption. Modern payment rails like real-time payments and open banking enable faster transactions and lower fees but require stronger fraud detection. Blockchain networks and stablecoins may enable faster cross-border settlement, while CBDCs could provide sovereign digital money with programmable features, though design, regulation, and privacy remain challenges. Overall, the most practical approach is layered modernization: combining tokenization and strong authentication, intelligent transaction routing across multiple rails, and AI-based fraud detection with privacy-preserving technologies. Future adoption of blockchain and CBDCs will depend on interoperability, regulation, and secure key management.

KEYWORDS

Digital commerce, payment security, tokenization, real-time payments, open banking, pay-by-bank, CBDC, blockchain settlement, biometric authentication, fraud detection.

WCRG Global Research
ISSN: 3071-5628
PP: 01-18.

1. INTRODUCTION

1.1. Background

Over the last 10 years, digital commerce has been on the rise owing to mass adoption of smartphones, application-based marketplaces, subscription and recurring payments, and the fact that small business owners can sell to customers around the world with the help of platforms. In such a setting, payments are not an off-the-record operation, but it dictates revenue acquisition at the moment of checkout and has a major impact on customer trust, conversion, and retention. Meanwhile, payment flows are one of the possible areas of attack by attackers due to its concentration of valuable resources: identity signals, credentials, and authorization of large-volume transactions. Traditional card payment systems were developed based on centralized mediation on trust, card networks and card issuers dictate authorization, card related disputes are settled via chargeback and then settled with delays that facilitate investigation and reconciliation. The new balance in digital commerce is growing to require instant-on confirmation, one seamless experience over gadgets and devices, and little or no friction on authentication rather than heightened approval rates, reduced loss to fraud and control over payment expenses, including interchange and alteration expenses. The emergence of real-time account-to-account transfers and open banking designs increases the impact of these pressures, but also causes fees to be lower, reversibility reduced, and the fraud prevention timeline shifted further back in the transaction lifecycle. Simultaneously, regulators all over the world are putting more pressure on consumer protection, operational resilience, data privacy and safe authentication and demand that the payment stakeholders exhibit enhanced security and increased transparency. Collectively, these forces drive the transition to next-generation payment technologies reliant on the ability to combine modern identity mechanisms, cryptographic credential protection, diversified payment rails, and real-time risk analytics to satisfy the conflicting needs of speed, safety, compliance, and commercial performance.

1.2. Evolution of Payment Technology

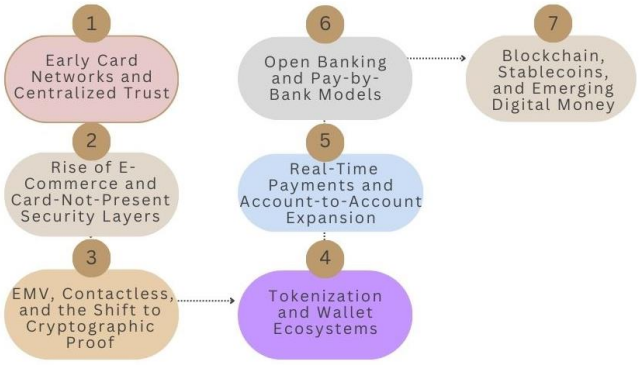

Fig 1 - Evolution of Payment Technology

1.2.1. Early Card Networks and Centralized Trust

The payment technology started with the scaling that was centralized by card networks and distributed the trust among issuers, acquirers, and merchants. Limited data (card details, basic transaction attributes) was used to make the decision of authorization, and the risk was handled via

ISSN: 3071-5628
PP: 01-18.

network rules as well as post-processing of transactions like chargebacks. This model was efficient in real life business and later customized to accommodate payments online, however it was designed with delayed settlements, manual exceptions management and fixed fraud control.

1.2.2. Rise of E-Commerce and Card-Not-Present Security Layers

With the growth of online shopping, fraud has changed to the card-not-present (CNP) type, which makes it vulnerable to the use of PAN/CVV credentials only. Layers of security came in as a way of compensating such as CVV checks and later the 3-D Secure (3DS) to identify cardholders and redirect cardholder liability, as per defined circumstances. As time went on, 3DS developed into risk-based and frictionless authentication, which represented the necessity to trade-off on checkout drop-off and prevent identity-driven fraud at the same time.

1.2.3. EMV, Contactless, and the Shift to Cryptographic Proof

In the physical trade, the use of EMV chip minimized counterfeit fraud whereby magnetic stripe information was substituted with cryptographic transaction validation. This formed the basis of safer face-to-face interactions, which would later facilitate NFC contactless payment, where distance, tokenization, and device integrity controls made it possible to complete transactions more quickly with fewer friction than traditional swipe payments.

1.2.4. Tokenization and Wallet Ecosystems

With the increased the digitalness and mobile-first character of payments, the concept of tokenization as a fundamental control increased to minimize the exposure of credentials. Controlled tokens and dynamic cryptograms substituted reusable card numbers by network tokenization and wallet tokenization (as in mobile wallets by device tokens). This enhanced security features of breaching data as well as contributed to operational advantages like automatic credit update, reduced declines due to expired cards, and enhanced lifecycle management of recurrent billing.

1.2.5. Real-Time Payments and Account-to-Account Expansion

To enhance the liquidity and shorten the settlement delays, many of the regions launched real-time payment rails that allowed the instant transfer and 24/7 availability. As much as these rails may reduce the expenses and time of merchants to confirm a transaction, it lowers the time frame in which you can recover the fraud hence more focus is being placed on preventive features such as payee confirmation, transaction signing, and real-time identification of anomalies. This transformation is indicative of a larger shift towards more of a risk resolution approach of disputes to the prevention-first execution controls.

1.2.6. Open Banking and Pay-by-Bank Models

Open banking increased the payment innovation by opening bank capabilities through API-based customer consent frameworks. Pay-by-Bank models make use of these APIs to make direct payments to accounts, potentially with benefits against the use of cards, and a larger amount of data

ISSN: 3071-5628
PP: 01-18.

to make risk decisions. Non-uniform standards, divergent authentication experiences, and discontinuous APIs are, however, critical issues to achieve uniform adoption at scale.

1.2.7. Blockchain, Stablecoins, and Emerging Digital Money

The most recent phase of development studies the concept of blockchain-supported settlement, stablecoins, and central bank digital currencies (CBDCs) as the new values transfer methods and programmable money. Such systems offer expedited cross-border settlement and novel ways of business, although the provision of such systems requires regulatory certainty, compliance functionality, consumer protection, and the usability of custody, and interoperability with existing financial infrastructure. Consequently, the short-term improvement can be seen in terms of hybrid deployments whereby users bill out using more user-friendly interfaces but back-end settlement is optimized on more modern rails.

1.3. Problem Statement

Even with significant digital payment transformation, gaps that are still present amidst digital transformation impede security, efficiency, and scalability of contemporary business. On the security front, identity and user deception, or phishing, credential stuffing, account takeover and mule-account laundering, have become focused on system vulnerabilities to passwords, recovery processes, and socially engineered approvals. Meanwhile, the state of interoperability remains limited by disjointed payment rails, localized schemes, and inconsistent authentication requirements and proprietary wallet ecosystems, to increase the complexity of integration and introduce uneven user experiences across markets. Latidity and reliability bring a new conflict: to secure conversion merchants require quick and reliable authorizations, but increased fraud prevention measures cause friction, and speedy payment rails shorten time to apprehend and prevent fraud before money is permanently transferred away. Prices are getting even harder as dealers working across borders face not only interchange and processing charges but also operational costs including manual verifications, customer care, refunds and dispute/chargeback processes that can eat up margins in spite of the headline costs of processing appearing competitive. Lastly, privacy and compliance form a challenging balancing act, on one end, more data and cross-channel indicators are known to detect fraud effectively and, on the other end, regulators and consumer demands are growing more aggressive and mandatory in the form of data minimization, limited purpose, transparency, and tougher governance. All these factors drive the necessity of a single assessment model to compare next-generation payment technologies across quantifiable trade-offs, and help stakeholders to progress towards the layered modernization of a process, to enhance security and performance without reducing usability, compliance, or even operational sustainability.

2. LITERATURE SURVEY

2.1. Digital Payment Security Foundations

The previous literature is always seen to pose e-commerce fraud as an issue of identity, authentication, and trust rather than a flaw in the payment rails. Since attackers frequently achieve success by masquerading as legitimate users (via account takeover, stolen credentials or synthetic

ISSN: 3071-5628
PP: 01-18.

identities), the literature advocates strategies of defense-in-depth by integrating several weak signals into more effective decisions. Such common layers are device fingerprinting to identify abnormal hardware/software setup, behavioral analytics to gauge whether the interaction behavior of the user is within historic norms, and transaction risk scoring that integrates context (location, velocity, purchase history, merchant category, prior disputes) to derive a probability of fraud. EMV and 3-D Secure (3DS) work is often tested at the cost of security and conversion: enhanced security reduced fraud and transferred the risk, but additional friction could also result in cart abandonment. Consequently, authentication conditions that address challenges only when a risk state is observed (adaptive authentication) and continuous authentication post-authentication are frequently advised as risk factors are not prevented by authentication alone (e.g. account reconfiguration, address redirection, or high-risk shipping).

2.2. Tokenization and Credential Security

The concept of tokenization is also frequently characterized as one of the fundamental tools of mitigating credit card credential theft since it restricts the exposure of primary account numbers (PANs), and undermines the usefulness of stolen merchant databases. The literature separates gadgets between merchant/processor token, and network token, and commonly highlights the benefits of network tokenization: tokens may be domain-constrained (reducing reuse in case of theft), they may be cryptographically tied to a device or a merchant and it can enhance the performance of an authorization via tokens being fresher and updated over time (e.g. reissue of a card). Nevertheless, studies, also point out that tokenization is not a control in isolation the security of the token vault, encryption-at-rest, and strong key management practices define whether the system becomes risk-reducing meaningfully. Hardware-secured security (e.g. HSM or trusted execution environment) to store the keys, strong isolation of privileges to access the keys, stop-and-roll key rotation, and cryptographic operations that should be audited are emphasized in the best-practice discussion. The greater implication is that tokenization minimizes the attack surface and the blast radius only in the case it is used with strict cryptographic governance and operational measures that it does not make keys, mappings, and signing operations the new single point of failure.

2.3. Real-Time Payments and Fraud Dynamics

Significant changes in fraud economics exist when it comes to real-time or instant payments, since the money is settled rapidly and is not easily reversible, making the time frame in which fraudulent payments go detected and recovered significantly smaller. Studies thus say the attacker strategies have switched to non-standard card-not-present theft to scams and social engineering, particularly the authorized push payment (APP) attacks whereby the victims are led into causing legitimate transfers. In such a setting, the red flag about fraud will not be to ask whether the payer is a real person, but whether the payer is being defrauded, which is more difficult to ascertain using exclusively transactional data. Research also records the development of mule networks that clean money at very high velocity through accounts layer making it hard to trace money that has been laundered by the events. Thus, best controls focus on preventive and in-flow controls: confirmation-of-payee (name/identifier matching) to prevent misplacement, sign-transactions or strong step-up

ISSN: 3071-5628
PP: 01-18.

authentication at high-risk transfer, and real-time detection of anomalies based on behavioral and network indicators (e.g., new payee pattern, unusual-time transfer, device anomalies, sudden-payee pattern and large-transfers). Several debates also emphasize on ecosystem-level coordination such as shared intelligence, quick reporting, and shared dispute management since instant payments require a type of response that is equally expeditious as the fraud.

2.4. Open Banking and Pay-by-Bank

A great deal of literature on open banking revolves around interoperability and governance of security because the model relies on APIs between banks, fintechs and merchants where access is provided via consent. There is a common motif of consent management: making sure that the consent is explicit, time-bound, revocable and adequately scoped (least privilege), and can be explained in a way that is clear to the end users, who might not be knowledgeable about what the access to their data will be used for. Studies point out that participants have a diverse security posture, hence API security (strong authentication, mutual TLS, OAuth flows, rate limiting, fraud monitoring, and standardized audit logs) emerges as the core of the systemic resilience. Arguably due to its emphasis on lower prices than card payment to merchants, pay-by-bank is addressed as an efficiency and a campaign problem. Literature identifies areas of difficulty, including different experiences between customers who have gone through banks, discrepancy in understanding strong customer authentication (SCA), and disparity in disputes/refund experiences when compared to card chargebacks. Consequently, best-practice proposals invoke standards harmonization (identity, SCA suggests), robustly-liability regimes, and risk-based SCA: allowing technical security to shine well commercially when the flow of payment causes confusion (or suffers unexpected drop-off).

2.5. Blockchain, Stablecoins, and CBDCs

Payments using blockchain are often marketed as supporting near-real-time settlement, programmable transfer, and enhanced cross-border efficiency, although the literature also highlights implementation obstacles that are both practical and not necessarily technical. Such issues as regulatory compliance (KYC/AML requirements), responsibilities of governance and operations in decentralized systems, volatility (particularly in non-stable assets), and custody risk are where most of the users and institutions are still struggling to cover their responsibilities. The volatility of stablecoins is lower in comparison with conventional cryptocurrencies, but studies continue to refer to reserve transparency, issuer risk, depegging events, and jurisdictional oversight as significant factors of trust. CBDC studies are more architectural, assessing design options of account-based versus token-based models, privacy and traceability trade-off, offline payment facility, and survivability under network failure. The other significant theme is integration: how CBDCs will coexist with commercial banks, card networks and instant payment rails without affecting the deposit bases and disrupting the payment ecosystem. In general, the literature indicates that distributed ledger technology has the potential to enhance settlement and interoperability but it requires full-scale implementation through the understanding of governance, consumer protections, operations security, and effective integration with current financial infrastructure.

ISSN: 3071-5628
PP: 01-18.

2.6. AI/ML in Fraud Detection

Detection research on fraud detection is desirably employing machine learning as a critical part in dealing with scale, complexity, and the speed at which attack patterns are changing. Some of these common methods are, supervised classification models using labeled fraud outcomes, anomaly detectors which identify variations in behavior, and graph based approaches that identify collusive patterns like mule rings or coordinated account takeovers. Other variables stressed in the literature include feature richness that consists of device signals, behavioral biometrics, merchant context, bank relationships and time, since fraud is not often suggested by a single variable. Simultaneously, research points to operational and ethical risks: drift in the models due to modification of consumer behavior and attack strategies; adversarial manipulation due to fraudsters investigating systems to discover decision limits; and biases that can unfairly affect particular groups of users in case training data is based on historical inequalities. Explainability is a longstanding and insistent demand in controlled settings and drives research towards interpretable models, post-hoc explanation systems and governance systems that capture decisions and allow appeals. The overarching conclusion is that AI/ML has been tasked with tasks most effectively when it operates under human in-the-loop, in conjunction with much better monitoring, retraining requests, and with a well-defined accountability control, and the models should be viewed as dynamic socio-technical systems instead of as fixed prediction-generation machines.

3. METHODOLOGY

3.1. System Model of Digital Commerce Payments

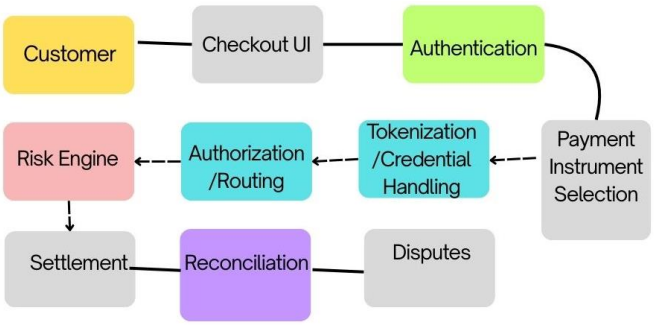

Fig 2 - System Model of Digital Commerce Payments

3.1.1. Customer

The payment flow is initiated by the customer, i.e. the creation of a purchase intent, provision of cart information, shipping and (where necessary) identity indicators like email/phone. Security wise, the stage is where the first trust is provided based on the account status in terms of login, past activity, device, and integrity of a session.

3.1.2. Checkout UI

The orchestration layer is the checkout interface which receives the inputs, offers payment options and directs the user through the process. A properly built checkout ensures minimum friction and still helps in security suasion (e.g. step-up verification) and transparency (total cost, fees,

ISSN: 3071-5628
PP: 01-18.

delivery). It is also critical in minimizing the end user error and social-engineering vulnerability by providing clear payee/merchant validation and consistent messages.

3.1.3. Authentication

Authentication grants user permissions to transact depending on the services, including an introductory level of basic authentication login sessions and power-defense authentication (SCA, often referred to as OTP, biometrics, or 3DS challenge flows). In modern systems, there is a trend towards risk-based authentication, with step-up checks only being enforced when perceived risk increases, and the conversion rates moderated against the rate of fraud prevention.

3.1.4. Payment Instrument Selection

In this case, the customer selects the funding source, which can be either cards, wallets, UPI/pay-by-bank, BNPL, and other options. This option can be used to settle not only chargebacks and user experience, but also the fraud and dispute model (chargebacks vs. push-payment disputes), and the compliance needs (e.g., SCA rules, consent flows, or provisioning wallet tokens).

3.1.5. Tokenization/Credential Handling

Sensitive credentials (such as bank account identifiers or card PANs) must be minimally exposed by tokenizing and safely handling them once a method is chosen. This measure is generally associated with substituting unencrypted credentials with tokens (network tokens or vault tokens), transmitting data encrypted, and the protection of keys in physically backed modules which minimizes the hazard of credential theft and replay.

3.1.6. Authorization/Routing

This system then places an authorization request via a payment gateway/processor and directs it to the required network or even bank (acquirer → scheme → issuer, or bank rails to pay-by-bank). Routing logic can be optimized by approval, cost and reliability and leverage smart retries, multi-acquirer methodologies and fallback options without violating compliance and evading suspicious traffic behavior.

3.1.7. Risk Engine

The risk engine gets the transaction to assess in real time with the aid of signals such as device fingerprinting, velocity checks, geolocation, past purchase behavior, behavioral biometrics and known fraud intelligence. It renders a decision (approve, decline, challenge, or review), and can initiate step-up authentication (or further verification), which forms the primary adaptive control layer against identity fraud as well as account takeover.

3.1.8. Settlement

This is the process of batching, clearing files, interchange/fees, and posting of movements done between accounts of the participants, the accuracy of this operation is crucial as any errors in it create downstream consolidation and dispute labors.

ISSN: 3071-5628
PP: 01-18.

3.1.9. Reconciliation

Reconciliation compares internal order books with payment processor files, bank statements and settlement files to verify what has been remitted, what fees have been imposed and what is pending to be paid. Reconciliation processes should be very strong to identify mismatches (partial captures, duplicate charges, failed refunds) and are required to enable financial reporting, visibility of cash flows, and audit readiness.

3.1.10. Disputes

The disputes handle after transaction disputes like chargeback, refunds, non-delivery claims, and unauthorized transaction claims. Evidence management (logs, delivery proof, authentication results, risk decisions), clear workflow and scheme/bank adherence timelines are needed in this step because the results of any dispute have a direct impact on fraud losses, reputation of the merchant and further performance of the authorization process.

3.2. Evaluation Framework and Metrics

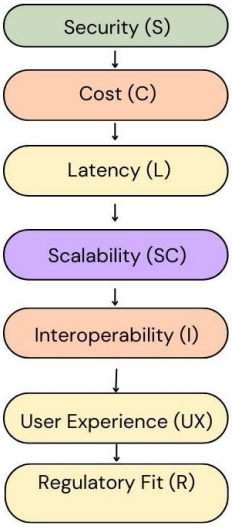

Fig 3 - Evaluation Framework and Metrics

3.2.1. Security (S)

Security is an assessment of the vulnerability of a payment technology to those common attack patterns of credential theft, account takeover by phishing, man-in-the-middle (MITM) cross-site scripting, and replaying attacks. A high score in security indicates the presence of several controls, such as high-quality authentication, cryptographic (signing, encryption, secure key storage), tokenization, and real-time fraud detection and also the capacity to limit the amount of damage in the event of compromise. It also ponders the extent to which malicious individuals are likely to compromise defenses via social engineering or manipulating devices/sessions.

3.2.2. Cost (C)

Cost measures all the economic effects of implementing and using the technology and not only the cost of processing transactions. It comprises infrastructure costs (integration, monitoring,

ISSN: 3071-5628
PP: 01-18.

compliance tooling, customer support), operational overheads (disputes, manual reviews), as well as the risk costs (losses due to fraud, chargebacks, reimbursement liabilities). A technology can seem to be cheap per transaction but still receive a low score in case it works to enhance downstream fraud, refunds, or support load.

3.2.3. Latency (L)

Latency is defined as the time taken between the point in which a customer places a payment and the point at which the merchant receives an approved response or a rejection. This involves checkout rendering latency, authentications (e.g., OTP/3DS challenges), network routing, issuer responsiveness and risk-engine decisioning. Reduced latency usually enhances conversion and decreases abandonment, but an excessively sensitive approach to latency reduction may undermine security when eliminating the required verification.

3.2.4. Scalability (SC)

Scalability measures the ability of the technology to support more transactions and peaks of transactions without slowing down or diminishing performance (festive sales, flash deals, salary days, etc.). These comprise throughput capacity (TPS), concurrency behavior, failover behavior, rate limiting, and partial outage resilience. High scalability means high-quality architecture - horizontal scaling, redundant routing, queueing / backpressure management and stress predictable performance.

3.2.5. Interoperability (I)

Interoperability measures the ease with which the technology diplomatizes between banks, payment networks, devices and platforms as well as geographic markets. When the technology is based on common standards, has uniform APIs/SDKs and is compatible across multiple ecosystems, not requiring bank-by-bank adoptions, technologies achieve greater scores. Bad interoperability can be visible in the form of disjointed user experiences, cross-issuer, or cross-region authentication, or support.

3.2.6. User Experience (UX)

User experience determines friction and its effect on conversion, trust and repeat use. It takes into account the step count, prompts clearness, the ease of authentication, error rates, and the reliability of the flow of payment between the channels (web/app/store). High UX score depicts secure by design flows: step-up when necessary only on risk-related reasons, entrance of limited details in swift approvals, and clear communication which lowers drop-off and misunderstanding.

3.2.7. Regulatory Fit (R)

Regulatory fit will also assess the compliance with the technology with rules including KYC/AML rules, consumer protection regulations, privacy of data, high customer authentication rules, and auditability. It also addresses readiness to report, timelines of dispute, record retention and controls anticipated by the regulators and networks. By scoring high it means that the technology is

ISSN: 3071-5628
PP: 01-18.

deployable with clearly understood governance, documentation and legal certainty across jurisdictions.

3.3. Threat Modeling Approach

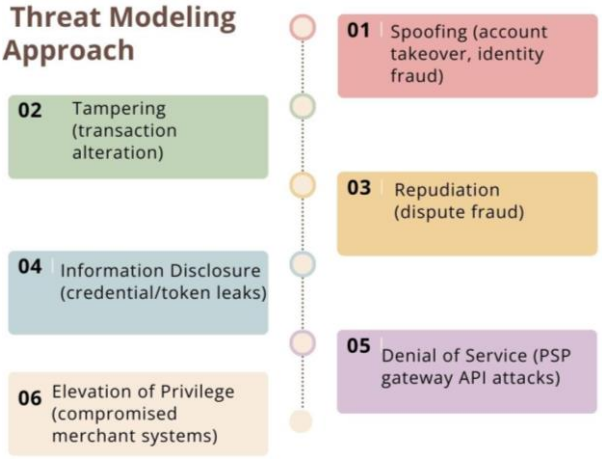

Fig 4 - Threat Modeling Approach

3.3.1. Spoofing (account takeover, identity fraud)

Their threat is related to the validity of the system determining the identity of the customer (or the merchant) actually. In online transactions, this is represented as account takeover with stolen passwords/OTPs, SIM-swap, session hijacking or fake identity that is weak at onboarding checks. Mitigations often have strong authentication (MFA/SCA), device and session binding, behavioral anomaly detection, and controls of account recovery flows- since reset of passwords and delivery of OTP is a common area of weakness.

3.3.2. Tampering (transaction alteration)

Tampering is defined as the submission of unauthorized alterations to transaction details (amount, beneficiary/payee, shipping address and order contents) in transit or in compromised application components. These can be man-in-the-middle attacks on API requests, checkout parameter manipulation, malware modifying payee information in a banking flow, and so forth. Well-secured features are end-to-end integrity (TLS and request signing), computing totals/binding totals on the server, idempotency (in particular), API gateways that are secure, and signing transactions as a commit of payment to the final amount/payee.

3.3.3. Repudiation (dispute fraud)

Repudiation threats are threats in which a party denies executing a transaction, which amounts to chargebacks, refund abuse, or friendly fraud. Even in the case where there is a real customer, it can be tricky to demonstrate authorization due to ambiguous flows, poor evidence trails or inconsistent authentication. Mitigations are based on non-repudiation cues, auditing: robust authentication records (e.g. 3DS results), device / session telemetry, time-stamped order and delivery

ISSN: 3071-5628
PP: 01-18.

records, unchangeable event records, and understandable communications to customers that would lead to better outcomes in dispute resolution.

3.3.4. Information Disclosure (credential/token leaks)

Information disclosure includes information about sensitive data (card numbers, bank credentials, tokens, session identifiers or cryptographic keys). The leaks may occur by insecure storage, misconfigured cloud sources, insecure API, Third Party scripts, or malware on the merchant side (e.g. formjacking). The controls cover tokenization to minimize raw credential presence, in-transit and at-rest encryption, stringent key management (HSM/hardware-backed storage), least-privilege access, best practices in the supply-chain (of the software), and monitoring of data exfiltration symptoms.

3.3.5. Denial of Service (PSP gateway API attacks)

Denial-of-service attacks will attack to cripple or even shut down payment processing by flooding with traffic spikes or malicious requests through gateways or authentication endpoints, or bank APIs. The implication on the business is direct: checkouts, lost income and bad faith, during high season. Rate limiting, bot detection, WAF / CDN protections, autoscaling, circuit breakers/timeouts, regional redundancy, graceful degradation schemes (i.e. alternative routing, retries in queues) can all be mitigated to ensure legitimate traffic is handled.

3.3.6. Elevation of Privilege (compromised merchant systems)

Privilege escalation is an attack mechanism where attackers acquire greater access privileges to merchant or payment systems to be able to perform operations such as reversing payout bank accounts, modifying risk settings, finding access to token vaults, or sending fake refunds. This is usually as a result of hacked admin accounts, poor CI/CD pipelines, lax IAM policies, or non-patched server vulnerabilities. Mitigations are based on providing strong identity and access control (MFA, least privilege, privileged access management), segmentation of sensitive systems, secure configuration baselines, periodic patching, tamper-evident logging and tight restrictions against high risk activities including modifying payout and using refunds.

3.4. Comparative Technology Set

This paper provides a comparison of a sample of contemporary payment and authentication technologies which cut across card networks, account-to-account rails and new digital money systems. While front-end identity controls such as biometric authentication and passkeys are considered more resistant to passwords and OTPs, and leave devices bound to credentials, phishing-resistant authentication, and tend to enhance both security and user user experience. EMV, network tokenization are the next stage in the development of the mature card ecosystem, with chip-based standards and tokenized credentials lowering counterfeit and credential theft and affecting the authorization rates, the liability consequences, and the complexity of operational processes. NFC contactless and QR payments are explored at the point of interaction with different assumptions of trust; NFC is usually based on secure elements and the use of proximity as it can happen, whereas

ISSN: 3071-5628
PP: 01-18.

QR movements can differ greatly in terms of security based on whether these are static or dynamic payments and how the intent to pay is authenticated. At the account-to-account interface, real-time payment rails (RTP/instant transfers) are evaluated based on the advantage of speed as well as availability coupled with an increased impact of fraud given the rapid, often irreversible settlement as the risk control accents focus towards confirmation-of-payee and real-time risk controls. Pay-by-bank through open banking is represented as a safer option prone to cost-reduction and card reliance reduction, whilst creating variability between consents flows, SCA experiences and API security maturity among banks. Blockchain settlement and stablecoins are discussed in terms of near-instant cross-border and programmable settlement and fewer intermediaries but realize governance and custody, compliance and depegging/issuer risks that determine adoption. And lastly, CBDCs (retail and wholesale models) are added to get state-backed design of digital money comparing architectural decisions in privacy, offline asset, mediator functions, and integration with current payment systems. Collectively, these technologies present a fair ground to address trade-offs in terms of security, cost, latency, scalability, interoperability, user experience and regulatory fit.

3.5. Experimental/Analytical Procedure

Since this paper is a survey-plus-framework article instead of an implementation study, its results are generated via an effective analytical pipeline that transforms evidence about standards, academic literature, and industry practice into similarly balanced results. The initial step is to create structured comparison tables comparing each of the technologies in the comparative set to the proposed metrics (Security, Cost, Latency, Scalability, Interoperability, User Experience, Regulatory Fit). These tables also adopt a common set of definitions and scoring rubrics in order that strengths and limitation become visible simultaneously and they clearly point out assumptions (e.g., market maturity, a typical deployment model, required reliance on bank/issuer capabilities). Second, we conduct a lifecycle mapping where we place each of the technologies on a shared digital commerce payment lifecycle, such as authentication and credential handling through authorization, settlement, reconciliation and disputes, to observe where the technologies add primary value and where they lead to new dependencies and gaps. With this step, it becomes clear whether or not a technology can mitigate risk at the user authentication point, at credentials storage, or at transaction execution, or primarily, in back office settlement and reporting. Third, we map threat-control in the form of the STRIDE categories to follow how the various technologies address (or do not address) the spoofing vulnerability, tampering, repudiation, information disclosure, denial of service and elevation of privilege. Such mapping associates the threats to tangible controls, including device binding, transaction signing, tokenization, securing key storage, confirmation-of-payee, rate limiting, and management of privileged access. Lastly we will cover a demonstration of the adoption scoring which will demonstrate how the stakeholders can use the framework to adopt to varying priorities. We show an example of a weighted scorecard where weights of examples represent popular opinion (e.g., merchants object more to cost and conversion, regulators object more to security and compliance, banks object more to risk containment and interoperability). Using the same procedure on technologies, the process shows how the conclusions change depending on the interested party objectives and the logic of evaluation remains clear and reproducible.

ISSN: 3071-5628
PP: 01-18.

4. RESULT AND DISCUSSION

4.1. Comparative Analysis

Table 1: Comparative Analysis

Technology	Security	Cost to Merchant	Latency	Dispute Handling	Interoperability	Key Risks
Tokenization (Network)	High	Medium	Low	Strong (card rails)	High	Token vault / key mgmt
Passkeys/Biometrics	High	Low	Very Low	N/A	Medium-High	Device loss, recovery
Real-Time Payments	Medium-High	Low	Very Low	Limited reversals	Medium	APP fraud, mule accounts
Pay-by-Bank	Medium	Low	Low	Varies by scheme	Medium	API fragmentation
QR Payments	Medium	Low	Low	Varies	Medium	Code spoofing, phishing
Stablecoins	Medium	Low-Medium	Low	Limited	Medium	Compliance, custody
CBDC	Potentially High	Unknown	Low	Policy-defined	TBD	Privacy, rollout

The comparative analysis makes the point of trade off of security, economics and operational practicability between payment and authentication technologies over the transaction lifecycle. Host-based Network tokenization has a strong security rating since it minimises exposure of raw card credentials and utilises well-developed card-rail controls, whereas most networks have low latency and robust dispute resolution due to the presence of well-developed chargeback procedures; the primary drawback is that the risk is concentrated in token vaults, cryptographic keys, and lifecycle management software. Passkeys and biometrics are also high-security and have minimal latency with lowmerchant cost due to the increased identity layer security; password and phishing risk reduction, but interoperability may also vary among platforms and browsers, and the main operation issue, account recovery, occurs when a user switches systems or loses devices. Real-time payments are extremely low latency with extremely low costs, with the reduced reversibility shifted towards scamming like authorized push payment (APP) fraud and mule networks and the security becomes highly reliant on confirmation-of-payee, transaction signing, and real-time suspicious transactions, rather than post-hoc recovery efforts. Merchants find pay-by-bank more appealing because its fees are lower, and it is normally very quick to authorize, but fragmentation must be avoided since it may lead to an inconsistent user experience, and may further increase integration costs. QR payments are still cheap and can be widely implemented, although security and the results of dispute resolution can be uneven: weaker ones allow code spoofing, redirection, and phishing, whereas more secure frameworks are based on dynamic QR codes and verified presentation of the payee. A fundamental issue with stablecoins is that they may allow easy transfer of funds and efficient cross-border settlement, yet underlying they have endemic key risks in compliance, custody and governance, and limited consumer protection in the event of a dispute compared to cards. Lastly, CBDCs should be

ISSN: 3071-5628
PP: 01-18.

high security and low latency in nature but the costs to merchants and the multi-country adoption are unpredictable as they will rely on the national rollout decisions; privacy expectations, offline capability, and integration with current rails will be the primary determinants of interoperability and adoption. In general, the older infrastructures are preferred in terms of managing the disputes whereas the newer rails are more efficient in speed and cost with higher preventive measures and governance to control the fraud and operational risks.

4.2. Transaction Lifecycle Mapping

Table 2: Transaction Lifecycle Mapping

Lifecycle Stage	Legacy Weakness	Next-Gen Enhancement
Login/Identity	Password reuse	Passkeys, biometrics, risk-based auth
Checkout	PAN exposure	Network tokenization, dynamic cryptograms
Authorization	Static rules	ML risk scoring, adaptive routing
Settlement	Batch delay	RTP rails, programmable settlement
Post-Transaction	High disputes	Better authentication signals, confirmation steps

Transaction lifecycle mapping explains the way next-generation payment technologies deal with certain vulnerabilities that are present in the current digital commerce processes. The systemic vulnerability in the traditional reliance on passwords at the point of login and identity includes those of credential stuffing, cross site reuse, phishing (including weak recovery), and identity reuse. Next-gen controls include passkeys, biometrics, and risk-based authentication to minimize such exposures with credentials that are device-bound, phishing-resistant and step-up checks that vary in number and intensity based on context signals of high risk (new device, abnormal behavior, unusual location). Legacy systems can also leak sensitive card information (PAN and CVV) during checkout through various different parts, which is a broader blast radius of merchant-side attacks on compromise and attack by a third party script. Network tokenization and dynamic cryptograms can be used to make this attack surface area smaller, overwriting reusable credentials with tokens and cryptograph values used each transaction, allowing received data to be less valuable, and more difficult to reuse. At the authorization phase, older methods of fraud prevention are often based on fixed rules and crude thresholds that are not adept at keeping up with changing patterns of attacks and result into either high false identification or lost fraud. Innovations of the next generation add machine-learning risk scoring and adaptive routing and combine richer signals (device, behavior, merchant context, historical outcomes) to make decisions on when to approve, challenge, or decline and intelligently choose processing paths that maximize the approval rate, at the same time managing risk. uint Settlement, in the card flow may include downstream viscoelasticity, batch clearing, and late availability of funds, which reduce adaptability and delays solution of downstream problems. Programmable settlement and real-time payment rails make it easier to move funds more quickly and condition automation (where possible), enhancing visibility of cash-flows and making operational workflows more responsive, but must be more strongly front-end controlled by their lower reversibility. Lastly, during the post-transaction stage, the magnitude of the disputes in the legacy environments are usually steep due to the prevalence of friendly fraud, confusion, weak

ISSN: 3071-5628
PP: 01-18.

authorization evidence. Better authentication indicators (e.g. certified 3DS results, binding devices), more explicit confirmation procedures (confirmation-of-payee, explicit, transaction sums), and more secure event recording enhance non-repudiation and reduce controversy by making customer intent more verifiable and the integrity of transactions more verifiable and defendable.

4.3. Discussion of Key Findings

4.3.1. Security vs. Friction Trade-Off

It is logical to acknowledge that this NSA system has vast potential for automation and thus supports a growing population of customers, so long as such automation does not impair security.<|human|>4.3.1 Security vs. Friction Trade-Off: Friction and Security: The fact is that it is only natural to admit that this NSA system represents enormous automation opportunities and, consequently, serves an ever-increasing customer base, provided it does not negatively affect security. Authentication methods that are resistant to phishing, such as passkeys and biometrics, may lead to a material decrease in account takeover and account fraud through credentials, although this requires system availability: device compatibility, platform support, and support for an effective account recovery workflow. When recovery is not strong, the locked out devices of the user can cause them support burden and churn. Meanwhile, excessive verification (OTPs, frequent re-challenges, strict declines, etc.) may also increase friction at the checkout and reduce conversion rates. Due to this, risk-based step-up authentication, using more intense challenges when the transaction situation appears suspicious, is becoming more popular in the literature and in practice, theory matching security with customer experience.

4.3.2. Rail Diversification and Smart Routing

Applying several payment rails, including cards, real-time transfer, and pay-by-bank, is a major trend in the business to be resilient and economically efficient. The smart routing feature can help merchants to choose an optimal route at the transaction level depending on the cost, the anticipated success in the authorizations, the latency and risk indicators (e.g., issuer behavior and past performance). The method helps to be less reliant on a single network and it can enhance acceptance in the times of outages or network-specific problems by the issuer. Nonetheless, diversification is associated with complexity: fragmented standards, inconsistent bank APIs, and inconsistent authentication needs arise, raising integration costs and maintenance, i.e. routing intelligence should be accompanied by robust observability and governance.

4.3.3. Instant Payments Shift Fraud Left

Real-time payment rails alter the fraud control threshold since money flow is speedy and reversal is minimal, leaving minimal chance of recovery after the event has occurred. This moves the fraud management left which means that frauding has to be prohibited at a young age before the execution, and disputes or chargeback later are no longer needed. Confirmation-of-payee, transaction signing, behavioral analytics, device binding, velocity limits, and real-time anomaly detection are some of the control techniques that are now very important to halt fraud and mule-based laundering. In reality, RTP security practices effectively integrate both of these aspects together: technical

ISSN: 3071-5628
PP: 01-18.

restrictions with explicitly deployable controls: the presence of clear payees screens and scam alerts since most of RTP-based fraud is socially engineered, not necessarily technical in nature.

4.3.4. Blockchain and CBDC Practicality

The advantages of blockchain settlement, stablecoins, and CBDCs are considerable, particularly regarding payments between countries, a quicker settlement, or programmability, yet the need to be practical in terms of safeguards will determine the system adoption in mainstream trade. Real-world viability (often dominated by consumer protection (refunds/disputes), compliance tooling (screening, monitoring, reporting), and usability of custody (key management, recovery, and fraud recourse)) can be far deciding than raw transaction speed. Due to these limitations, hybrid models can be considered the most viable options in the near future: the customers follow the traditional checkout procedures (cards or bank payments) and the blockchain elements perform their functions on behalf of settlement, treasury, or cross-border optimization. This strategy is the most capturing of efficiency improvements, and it does not require both parties to take on the entire burden of implementing on-chain custody and regulatory risk.

5. CONCLUSION

Newer payment technologies are quickly transforming the digital trade by taking security and performance enhancements off the shelf toward identity, authentication and cryptography defense, and are extending the range of rails that can be used beyond the card networks. Phishing-resistant authentication, and by extension stronger identity indicators, decrease the use of weak secrets such as passwords and OTPs significantly enhancing fraudulent losses and user experience, given the inclusion of reliable device support and recovery mechanisms. Simultaneously, network tokenization is also meaningful because it will reduce card data credit exposure by replacing reusable credential data with controlled tokens and dynamic cryptographic values, as well as enhance resilience against compromises of merchant side and minimize changes to credential lifecycle overhead. At the rails layer, pay-by-bank and real-time payment models can achieve reduced processing costs and quicker liquidity, although these must only be sustained by behavioral controls that are appropriate in low-reversibility environments such as confirmation-of-payee, transaction signature, behavioral analytics, velocity limits and real-time anomaly detection and prevention of scams prior to execution. These trends also enhance the strategic significance of multi-rail orchestration: smart routing between cards, real-time transfers, and bank APIs can enhance acceptance, minimize costs, and enhance resiliency to outages but it demands meticulous integration design, observability, and conventions to prevent the complexity caused by fragmentation. Far beyond that, blockchain settlement, stablecoins, and CBDCs show potential transformation in cross-border business and use case programmable money, although mainstream adoption hinges less on raw transaction speed and more on trust and usability: established regulatory clarity, cross-border standards, consumer protection, and safe custody and recovery practices that can be used by people who are not experts in the field. Combined, these facts indicate a layered modernization approach to digital commerce actors: harden identity and minimize credentialing, focus on multi-rail routing and real-time risk controls, and consider blockchain or CBDC-based settlement of transactions in which governance, compliance, and user protection needs

ISSN: 3071-5628
PP: 01-18.

may be achieved. Integrating privacy-conscience analytics, auditable decisioning and robust operational governance: It is imperative to embed privacy conscience analytics, auditable decisioning and robust operational governance throughout the payment lifecycle to make the faster, cheaper payments sustainable at scale.

REFERENCES

[1] Hayashi, F., Markiewicz, K., & Minhas, S. (2018). *The Initial Effects of EMV Migration on Chargebacks in the United States.* Federal Reserve Bank of Kansas City Working Paper.
[2] U.S. Payments Forum. (2017). *Understanding the U.S. EMV Liability Shifts.* White paper.
[3] Froud, D. (2016). *The global implications of US EMV adoption. Computer Fraud & Security.*
[4] Broadcom (CA Technologies). (c. 2014). *3-D Secure Authentication Using Advanced Models.* Technical paper/guide.
[5] Worldpay. (n.d.). *Navigating frictionless 3D Secure for enterprise merchants.* Industry article.
[6] Fiserv (Carat). (c. 2022). *Network Tokens Whitepaper.* White paper (PDF).
[7] Ogundele, O., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012). *Fraud Reduction on EMV Payment Cards by the Implementation of Stringent Security Features.* (paper as hosted on ResearchGate).