

Original Article

# Interoperability in Payment Card Systems: A Deep Dive into Issuers, Acquirers, and Network Operations

Naga Rishyendar Panguluri

Software Engineering, Discover Financial Services, USA.

Corresponding Author : [mommoh.joshua@mudiameuniversity.edu.ng](mailto:mommoh.joshua@mudiameuniversity.edu.ng)

Received: 19 November 2024

Revised: 25 December 2024

Accepted: 14 January 2025

Published: 30 January 2025

**Abstract** - Interoperability within payment card systems is an extremely vital element of the payment industry. It enables transactions among diverse systems, with issuers, acquirers, payment networks, and merchants all sharing a stake in the outcome. This paper appraises such interaction and indicates what technology supports cross-border and cross-platform processing of payments. We examine the roles and responsibilities of issuers who have charge over a cardholder account. In addition, the membership organizations provide the infrastructure behind transaction authorization and communication such as Visa or MasterCard and others. By exploring the technical standards, protocols, and regulatory guidelines that govern these interactions, this study shows the challenges and importance of achieving interoperability in the payment cycle. The paper then takes up such matters as the security scheme for contactless payments, prevention of fraud, and future trends like mobile wallets and contactless payment systems or systems for integrating blockchains into financial transactions, all of which require hints at a coherent, stable environment to flourish.

**Terminology Definition:** Issuers “are financial institutions, typically banks, that provide payment cards (such as credit, debit, or prepaid cards) to consumers.”. Acquirers “are banks or financial institutions that work with merchants to process payment card transactions.”

**Keywords** - Interoperability, payment card systems, issuers, acquirers, payment networks, transaction security.

## 1. Introduction

As one of the primary payment systems in the modern world, card-based transactions have turned out to be a major revolution. Nowadays, people and companies conduct rapid (fast) yet safe and efficient monetary exchanges. At its core is interoperability, or systems that set the ability of differing technologies and financial organizations to work seamlessly together to complete the transaction successfully. Regarding payment cards, interoperability refers to the smooth functioning of the ecosystem between issuers, acquirers and network operators.

The interoperability of Issuers and Acquirers through communication that transcends networks is a crucial factor in achieving this.

Issuers, usually banks or other financial organizations, give consumers payment cards that allow them to buy through their accounts. Acquirers, conversely, are like institutions as businesses that work with merchants to accept card payments. They, therefore, act as go-betweens between merchants and the card networks. Payment networks such as Visa, Mastercard and others ensure that Issuers work closely with Acquirers by processing transactions and guaranteeing their safety and approval status. The phenomenal rise of the digital ecosystem and the increase in global transitions in today's world make it more important

than ever for all these players to work together harmoniously. Consequently, the frameworks that link Issuers, Acquirers and Networks must operate in harmony, moving through the most complex types of transaction levels and checkpoints in order to ensure security, speed of transaction, regulatory compliance (regulatory requirements), stopping fraud and a host of other problems that regularly arise.

This paper examines the intricate links between issuers, acquirers and network operators, asking how interoperability is achieved. As well also dealing with the role of new technologies like mobile wallets, the blockchain-based payment method BitCoin and tapping credit cards (which come complete with encrypted NFC chips that enable smooth and faster checkout) that can complement the existing methods or even outpace existing and traditional methods of transactions. Understanding these dynamics is essential for those in the payment industry and consumers and businesses who depend on reliable, easy payment solutions in a rapidly changing financial landscape. While progress continues on payment card systems, complete interoperability among issuers, acquirers, and network operators is elusive because of inconsistent standards, divergent regulations, and unevenly adopted technologies from region to region. Most existing research ignores the operational, governance, and cross-border



challenges of adopting such systems, instead focusing on narrower technical priorities such as security. It also leaves much to explore in terms of how new technologies like blockchain, tokenization and artificial intelligence can help solve these challenges and the effect of interoperability gaps on SMEs and underserved markets. These gaps underline the necessity for comprehensive, multifaceted solutions to create inclusive and integrated payment ecosystems.

A robust interoperability environment in payment systems benefits all participants in the payment ecosystem. End users, including consumers, merchants, governments, and other types of enterprises, find it easier to make and accept payments. Providers to these end users, including banks, networks, processors and other service providers, gain revenue from payments in interoperable systems that they may not achieve with closed-loop (or non-interoperable) systems [1]. Digital financial services are often viewed as a key tool towards financial inclusion (Demirguc-Kunt et al., 2018). New technologies can significantly decrease transaction costs, reaching consumers who have been traditionally under-served (Goldfarb and Tucker, 2019) [2-3].

## 2. Who are Issuers, Acquirers, Network Operators

### 2.1. Issuers

*Issuers* are financial institutions, typically including banks and credit unions, that offer their cards (credit or debit) to consumers. They play an active role in handling and monitoring cardholders' personal financial networks.

*Their main tasks include:*

#### 2.1.1. Card Issuance

They offer consumers a payment card linked to their bank account or line of credit. This card lets consumers pay merchants, take cash from ATMs, and handle various other financial transactions.

#### 2.1.2. Account Management

By managing cardholders' accounts, issuers must ensure that the funds needed for the transaction are available. They handle billing together with interest charges (in the case of credit cards) and account statements.

#### 2.1.3. Transaction Authorization

When a cardholder initiates a payment, the issuer accepts the responsibility of agreeing in a broadcast message to let it go through or refusing it. The determination is based solely on the funds available in the account (for debit card transactions) or if there are enough open credit lines on his charge card (for credit card transactions).

### 2.2. Security Measures and Fraud Prevention

Issuers take steps such as encryption, PIN (personal identification number) implementation, and some systems to alert cardholders when abnormal transactions take place in order to protect the customer data on a card from unauthorized use or theft.

Payment networks coordinate the behaviour of banks, merchants, and consumers by setting certain prices and rules [4]. Bank payments are information services that provide the secure transfer of credits and debits between accounts, requiring verification, manipulation, and transfer of information [5]. Credit card issuers earn revenue from consumers and acquirers. As mentioned above, consumers may pay annual fees, finance charges if they revolve, and other fees, such as cash advance and over-the-limit fees. Issuers compete for cardholders on various dimensions, such as various fees, frequent usage awards, finance charges, and other characteristics [6]

### 2.3. Acquirers

*Acquirers* are partners with merchants and payment processors in the business of handling not only their payment transactions for payment cards but also those of the merchant.

Acquirers earn revenue from merchants by bilaterally setting merchant discount rates and paying interchange fees to issuers[6].

*Their main responsibilities:*

#### 2.3.1. Merchant Services

Existing merchants are allocated with necessary hardware and software systems for processing payment card business (e.g. point-of-sale terminals, system to facilitate payment through a Web, financial services or "store").

#### 2.3.2. Transaction Authorization

If a credit card is used, for example, the acquirer can send the transaction data to the relevant payment network showing a charge. Once this information is confirmed just before being forwarded by the business (merchant) owner at some concentration point to a bank which charges 1-3% as commission fees for transactions or, in some instances converting the foreign currency into its local money.

#### 2.3.3. Settlement and Funding

When a card-based customer completes a cash purchase, acquirers direct the settlement of funds from the issuer bank to the merchant that did business with them. They also ensure merchants receive payment for providing goods or services.

#### 2.3.4. Risk Management and Compliance

Part of the acquirer's work is to help merchants comply with set standards such as PCI-DSS (Payment Card Industry- Data Security Standards). These standards also set best practices to mitigate risks such as chargebacks and fraudulent activity.

### 2.4. Network operators

*Network operators*, often referred to as payment networks, are entities that facilitate communication between issuers and acquirers. Handling the flow of funds from the initiation (acquirer) to the final destination (issuer). Some of the largest network operators in the world include Visa, MasterCard, American Express, and Discover.

#### 2.4.1. Transaction Routing

When a cardholder makes a purchase, the payment network takes the transaction request and conveys it from an acquirer to the issuer for approval.

Having received authorization, the network carries this message back to an acquirer next so that they may complete transactions.

#### 2.4.2. Transaction Clearing and Settlement

Payment networks manage the clearing and settlement process, ascertaining that funds move from issuer to acquirer. Transaction information is also recorded here on the books.

#### 2.4.3. Security and Compliance

Networks enforce industry standards, encryption methods and other measures to protect client payment data in transit. They are also responsible for ensuring that each party involved in the Cardholder Data Environment (CDE), from the issuing bank to the cardholder service provider, complies with government regulations and industry requirements like (PCI-DSS).

#### 2.4.4. Brand and Acceptance

Payment networks provide the infrastructure and reputation needed for widespread acceptance of credit cards. Countless merchants worldwide recognize Visa, MasterCard, and others, getting it across to consumers that they can use their cards pretty much anywhere they choose.

#### 2.5. Interaction of the Three

Issuers give out the payment cards and grant permission for a transaction predicated on the cardholder's account. Acquirers work with merchants to accept cards and get transactions processed.

Network Operators provide infrastructure to route transactions and make sure that funds are shifted safely between people who owe them money, the issuer at one end of the route, and the acquirer on the other side.

Together, these three make for a smooth payment ecosystem, with easier acceptance of cards at a variety of locations across the world for simpler transactions on both ends without fear of risks associated with carrying hard cash.

### 3. Interoperability and its Relevance

Interoperability among payment systems as the foundation for enhancing cross-border payments requires technical, semantic and business system compatibility so that end users can seamlessly transact across systems [7].

Interoperation could be a tool to meet regulatory requirements, lower costs, expand access and choice in payment services (Negre and Cook, 2021), reduce risk and improve efficiency by promoting straight-through processing (Bech and Hancock, 2020), and spur adoption of innovative new products through network effects (Caskey and Sellon, 1994).[8-10]

Interoperability is the ability of different systems, platforms, or entities to exchange and use information with each other really well and without any compatibility problems. In the field of payment card systems, interoperability means that payments can go off smoothly between different issuers who issue credits to the cardholder, various acquirers and payment networks regardless of what type the card is, no matter what technologies or financial institutions are involved, cutting across boundaries.

All this simply lets users and merchants of credit cards handle things well between one another and with financial institutions, meaning that payments will be handled accurately across different devices or platforms and geographic locations.

#### 3.1. Why Is Interoperability Relevant?

In payment card systems, interoperability is key for a number of reasons, not least now that we are witnessing a rapidly rising global economy and increasingly sophisticated consumers demanding fast, secure financial transactions.

#### 3.2. Global Commerce

When businesses and consumers are dealing across borders, interoperability means that credit cards will work wherever consumers travel. A consumer in Japan visiting America can use his/her Visa card to buy groceries, and the transaction will be authorized, settled and cleared without a fuss. Without interoperability, these global transactions would be slow, inefficient and subject to all kinds of problems.

#### 3.3. Transparent User Experience

For consumers, interoperability creates an experience that is as transparent as possible when paying for goods and services. They don't have to concern themselves whether their card will work in a given shop, whether that merchant accepts the network for their payment or whether the value will be forthcoming. Such convenience promotes consumer confidence and increases the popularity level of digital payment methods.

With interoperability, a merchant can accept money from any number of consumers, even those using different payment methods from various providers. For enterprises, this extends their potential customer reach even further and creates new revenue streams by accepting more than one card, be it credit or debit, and whether or not payment systems like ApplePay will be supported. Therefore, with interoperability, the same compatibility issues are no longer an important criterion for determining whether or not a company should undertake business activities of any kind.

Significantly, different payment systems no longer need to be supported on the off chance that people may want to use them, credit cards are all now simply accepted without exception anywhere and everywhere since the advent of interoperability.

### **3.4. Ease of Receiving Money**

For merchants, interoperability makes accepting payments from any customer easier regardless of the system employed and/or network. This increases business opportunities and market share through merchants' ability to accept various credit or card payment cards and multiple wallets.

### **3.5. Security and Fraud Prevention**

Payment networks and institutions must define common protocols for data transmission, encryption and verification. In this way, fraud prevention becomes easier. Cross-system fraud prevention decreases both the probability and quantity of occurrences. Policies such as PCI-DSS (Payment Card Industry Data Security Standard) are essential for maintaining confidence in the payment ecosystem.

### **3.6. Innovation and Technological Advancement**

Encourages innovation as new technology and payment methods, such as mobile wallets and contactless payments, integrate smoothly into the existing payment ecosystem. If systems can readily be combined, innovations can be launched without disrupting existing systems, which will lead to even further progress within the financial industry.

### **3.7. Cost Efficiency**

Without interoperability, disparate systems must operate in isolation. This could cause unnecessary expenses for both Issuers and Acquirers alike. For example, one merchant may need to invest in a multitude of terminals or systems to cater for different types of cards and payment methods. Interoperability obviates the necessity for such duplicate investments at all levels, beneficial both to merchants and financial institutions.

### **3.8. Regulatory Compliance**

Given the increasing amount of regulation in the payment card industry with GDPR for data protection, the EU's Payment Services Directive PSD2, and Anti-money laundering (AML) regulations, interoperability means that all players across the ecosystem can comply with a common set of compliance standards. This takes the burden off of institutions trying to maintain consistency in regulatory practices and reporting, which is essential for the smooth functioning of the international payment system.

### **3.9. Consumer Confidence and Trust**

Consumers can be sure that their cards will function easily and without disjuncture across all channels and platforms, no matter which payment system underpins them. They will be more inclined to make free use of their credit facilities across channels and cutting across boundaries. Trust in the system's security, reliability, standardization and global acceptance is the foundation for adopting digital payment technology.

### **3.10. Security Technologies in Contactless Payments**

Contactless payments, though often preferred for their speed and convenience, present a unique risk to public safety. To overcome these, many of the advanced

technologies have been implemented to secure user data and prevent fraud. One such innovation is tokenization, the process of replacing sensitive payment data with a unique, random token during transactions. Thus, hackers cannot make unauthorized payments if they intercept the transaction data. Also, encryption protocols such as EMV (Europay, Mastercard, and Visa) standards protect data by encrypting it as it is transmitted so that only those with permission can decrypt it. When coupled with dynamic authentication measures (like one-time use cryptograms), this adds an additional layer of protection. Biometric authentication and device-specific credentials are another essential security feature in contactless payments. This means unique methods such as fingerprint scans, facial recognition, or secure PIN entry on smartphones must occur before a transaction is completed. However, Near-Field Communication (NFC), most frequently utilized in contactless payments, improves security even more by limiting its functionality only to small spaces, thereby limiting exposure to data interception. In addition, AI-driven real-time fraud detection systems analyze transaction behavior for irregularities, alerting suspected fraudulent activity in real-time. Together, these technologies ensure secure contactless payments while providing a seamless payment experience for users.

### **3.11. Interoperability from a Consumer Perspective**

Interoperability in payment card systems means that consumers can use their cards on different networks, at different merchants, and across different countries without the hassle of compatibility issues. This allows consumers to reach a wider set of services and pay for them across any relevant touchpoint, online or offline, without network concerns. That said, problems pertaining to security and fraud prevention, as well as the increased complexity that comes with having to manage various payment systems, may arise. With interoperability on the rise, consumers seek increased convenience and a high degree of trust that their repeated transactions over many networks are secure. At the end of the day, improved payment experiences and more options are the two pillars underpinning consumer satisfaction in an integrated payment environment.

### **3.12. Cross-border Transaction Challenges**

In the payment card system, cross-country transactions are challenging because of differences in the financial regulators of the country and the currency conversion for the transaction. Global payment networks like Visa, MasterCard, etc., have put much effort into creating interoperable systems. However, with no proper standardization in smaller or regional networks, there is massive inefficiency, exorbitant transaction fees, and time lag in processing the payment. Cross-border payments can also be less seamless than ideal, as the process of navigating different currencies, security procedures and consumer protections can be complicated. Nevertheless, better interoperability spurred by using common standards and new tech, such as blockchain, can simplify these processes, lower costs, and create a better overall experience for consumers and businesses involved in international trade.

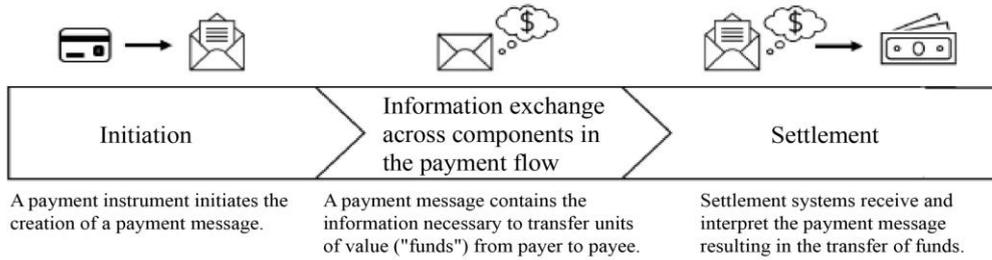


Fig. 1 A simplified view of elements of a payment system, source: <https://www.federalreserve.gov/econres/notes/feds-notes/fit-for-purpose-payment-system-interoperability-a-framework-20220714.html>

#### 4. Case Study

Literature references on interoperability in payment systems-

| Type                             | Summary   | Example |
|----------------------------------|---|---------|
| Scheme Interoperability          | When all participants of a system are bound by a scheme (common set of business rules) defining how transactions move |         |
| Network Interoperability         | When 2 payment schemes negotiate an exchange agreement (i.e. cross-border card payments)                              |         |
| Parallel System Interoperability | When the effect of interoperability is given to end customers of different schemes                                    |         |

Fig. 2 Types of Interoperability in Payments, source: [https://www.linkedin.com/posts/ali-ahmed2\\_payments-interoperability-settlement-activity-7258164645247492096-7YVX/](https://www.linkedin.com/posts/ali-ahmed2_payments-interoperability-settlement-activity-7258164645247492096-7YVX/)

According to the Africa Regional Integration Index (2019), the EAC, one of the most integrated RECs, has committed to deepening its digital economic integration (AUC et al. 2019). Business platforms exploit non-interoperable payment systems to lock in users and gain an unfair competitive advantage. Payment non-interoperability infringes on users' payment freedom, imposes additional

costs, and hinders the healthy development of the platform service supply chain. Therefore, some countries' governments have recently promoted payment interoperability [11,12]. B2C transactions on the web typically take several steps in which payment information and payment systems are used in order to complete them (Ruiz-Martínez et al. 2012),[13].

| Country/Region                    | Details  |
|-----------------------------------|--|
| Global                            | 76% of the global adult population had an account with a formal financial institution in 2021.<br>64% of adults globally made or received digital payments.<br>Digitalization has promoted financial inclusion, economic growth, and poverty reduction.  |
| Developing Countries              | 71% of adults had access to financial accounts in 2021, with only 57% making digital payments.<br>Barriers include informality, tax evasion, and lack of trust in financial institutions.<br>Limited internet and mobile access remain significant obstacles to financial inclusion.                               |
| Sub-Saharan Africa                | Mobile money has had a transformative impact, enabling widespread financial transactions (Jack et al., 2013; Suri, 2017).<br>Improved tax collection (Apeti and Edoh, 2023) and greater household financial stability.<br>Mobile money adoption has significantly bridged the gender divide (Suri and Jack, 2016). |
| South Asia                        | Financial inclusion has been slower due to limited digital infrastructure and high levels of informality.<br>Digital payments are emerging as tools to enhance economic empowerment, especially among underserved populations.   |
| Latin America                     | Digital payment adoption is improving but faces challenges with trust in financial institutions and cash-dominated economies.<br>Efforts to integrate mobile money solutions are growing but require better infrastructure and regulatory support.   |
| East Asia & Pacific               | The high penetration of mobile and digital technologies has accelerated financial inclusion.<br>Mobile money has improved consumption and stabilized remittance flows (Ky et al., 2018; Munyegera and Matsumoto, 2018).  |
| Middle East & North Africa (MENA) | Digital payment adoption lags due to cultural reliance on cash and insufficient mobile internet penetration.<br>Efforts to digitalize government payments and services are gradually improving inclusion.  |

## 5. Challenges & Considerations

While the interoperability of a payment card system has many advantages, such as hassle-free transactions and unparalleled customer experiences, it also poses potential security risks. The problems mostly stem from the necessity for diverse systems, institutions and technologies to communicate and trade-sensitive financial data. As these systems become increasingly interconnected, so does the risk of security breaches, fraud or the compromise of confidential information.

*Here are a few of the important security concerns in interoperability:*

### 5.1. Privacy and Data Protection

The crossing of different payment systems or their associated institutions increases the danger of revealing sensitive consumer information. Consumers' Economic data, including card numbers, national identification numbers and histories of transactions, become exposed as interoperability calls for data to be transmitted over different media. Data breaches by malicious actors can lead to identity thefts, financial fraud and substantial losses.

#### 5.1.1. Concerns

Data exchange across various systems could result in data leakage or unauthorized access to private and financial information.

#### 5.1.2. Mitigation

Strong encryption, secure data forwarding protocols, and adherence to data protection legislation (such as GDPR) will help offset some inherent risks.

### 5.2. Fraud and Tampering with Transactions

With many units involved in the trading process (issuers, acquirers and network operators), there are more potential spots at which fraud could happen. Cybercriminals can take advantage of any of these either by familiar procedures or systems. Credit card counterfeiters, scams, cyber heists, and bank account looting have become easier in linked systems where every link is less secure.

Mitigation: This ecosystem can reduce fraud risks through enhanced fraud detection mechanisms, Multi-Factor Authentication (MFA) and real-time transaction monitoring.

### 5.3. Inconsistency Laws and Regulation

The biggest challenge to interoperability is that not all parties in the payment ecosystem may be operating with one standard of security system infrastructure or abide by the same safety rules. Issuers and acquirers may often take a different approach to secure cardholder data. At the same time, within payment networks themselves, they can run their own variation of security protocols from one compliant

network member only able to communicate over public networks.

Because there are no uniform standards in place for all participants, any loophole found by someone might be exploited and potentially used as entry points by other parties connected to that same network. Therefore, it is important to create security standards to prevent the identification of such holes. Such standards can assist particular participants in the payment architecture in taking on certain burdens in common with others and thus provide common protection of all parts of transactions.

If different institutions use different security measures for payments, it provides possible points where hackers can break into the system.

Mitigation: Security policies such as the Payment Card Industry Data Security Standard (PCI-DSS) help all ecosystem members follow the same security requirements.

What is PCI-DSS? (payment card industry data security standard) is a set of security standards designed/purposed to ensure that the company or any firm acquires the standard of securing the environment using credit cards. It includes sections on data encryption, access control, monitoring, and vulnerability management to prevent breaches and fraud of cardholder data. If a company stores, processes or transmits payment card information, it must comply with PCI-DSS.

#### **5.4. Third-party Hazard**

The service providers, including payment processors, gateways and software vendors, play a crucial role in the payment card system. These third parties are often integrated into payment systems, and if they lack robust security measures, they could become entry points for cyberattacks. Attackers might choose these external vendors to find ways to integrate payment data, once achieved, and add it onto every transaction line that passes through and ends with fraudulent transactions.

In the event of a security breach at any third party, all parties involved stand to be affected. It would, therefore, cause major data breaches or financial losses, leading to mistrust in the entire ecosystem.

Mitigation: Rigorous management of risks in third parties, regularly conducting audits, and ensuring that vendors comply with the highest standards are important in preventing these hazards.

#### **5.5. Transparency and Lack of Agreement**

In almost any circumstance, an electronic repository from multiple sources often brings about such disagreements. Indeed, it may be that the flow of information between these parties does not offer complete transparency. If one party fails to identify a security breach or flaw, it could go undetected for some time and be used repeatedly as a backdoor into the system. Also, the involvement of multiple entities with various roles in the

payment ecosystem makes placing responsibility for a security incident difficult.

Deciding where a security breach has sprung up can take a long time, increasing the impact of any cyber attack. Mitigation: Clear accountability structures, regular monitoring, and effective response plans should all be implemented to minimize the magnitude and duration of security breaches.

#### **5.6. Transaction Authorization Risks**

An interoperable system's transaction authorization process involves interaction between a number of systems (issuer, acquirer and network). Should any of these systems have a security vulnerability, the entire transaction is open to compromise. For example, a flaw in the authorization process might permit unauthorized transactions to be approved or alternatively stop legitimate transactions from going through.

An authorization loophole can lead to unauthorized transactions, or it can stop legal payments from being made. This causes loss and frustration to the consumer.

Mitigation: Protection of the transaction approval process through strong authentication methods, EMV chip technology, tokenization and real-time approval checks.

What is EMV ? (Europay, Mastercard, and Visa), is an international standard for chip-based payment cards and mobile devices. Card with chip technology encrypts and stores card data, making it more secure than traditional magnetic-stripe cards. An EMV card creates a one-time transaction code for transactions, which means the data cannot be reused for fraudulent transactions. EMV is an abbreviation for Europay, MasterCard, and Visa, which is the technology that reduces the probability of card cloning. To improve security, it is frequently used for in-person, contactless, and online payments.

#### **5.7. Cross-Border Security Challenges**

Interoperability often involves cross-border transactions, where laws from different regulatory environments and standards of accreditation conflict. Different countries may have various rules applied to data protection, fraud prevention, or encryption, making it much more difficult and expensive for stakeholders across the border.

For example, the EU's General Data Protection Regulation (GDPR) has strict data-protection rules that do not necessarily match with actual practice in other international areas.

However, securing the entire payment ecosystem on a uniform basis might be difficult, given that cross-border transactions may involve varying compliance standards. Alternatively, global security standards and frameworks might emerge in the future, bringing all stakeholders involved in cross-border transactions under the same set of regulations.

One serious problem for payment card systems is security. Interoperability between systems across borders and between providers of financial services and merchants means more access points for cybercriminals, not fewer. Multifaceted security, then, becomes part of the essential solution. Japanese banks are now preparing to take this sort of approach because security-related concerns extend to consumer privacy, there is online financial transaction risk, and it must comply with the rules of securities markets.

To address these issues related to security, a more selective approach must be employed. With the merchant community, including legacy systems, encryption mechanisms can be added for their interconnection to ensure data is not intercepted during transmission; third-party providers are regulated both locally and by law. With effective security in place, interoperability will continue to move ahead without having an adverse effect on transactions.

## 6. Current Framework & Its Impact

Interoperability encompasses how one payment card can be harmonized for use on various payment card systems globally across issuing banks, acquiring banks, and payment networks. Localized market needs and regulatory environments can vary greatly. While many cross-border payment networks have implemented baseline interoperability standards within regions, this is far from solving the interoperability problem, where technologies, regulations and infrastructure capabilities can result in many fragmented systems. Particularly in emerging markets, this fragmentation leads to friction in cross-border transactions, higher costs, and more complex and less seamless user journeys. In addition, the absence of common protocols makes integrating smaller FIs and fintech players difficult, impeding competition and innovation.

Interoperability, or lack of it, is hugely significant. By reaching wider access to digital payments, they allow for reducing the cash dependence of the country and the economic behavior of people and thus promote greater financial inclusion with fully interoperable systems. Smooth cross-border business requires universal connectivity, and interoperability lowers transaction costs and simplifies business operations. This creates a payment experience for consumers that is smooth, safe, and easy to use. However, the existing interoperability gaps highlight the importance of global standards, increased collaboration between stakeholders, and emerging technology such as blockchain and artificial intelligence to create more streamlined and inclusive payment systems.

## 7. Future Scope

Given the evolution of technology and the changing nature of the global finance industry, interoperation payment cards future possibilities are enormous. The emergence of new technologies, changes in consumer behaviour and complex financial ecosystems will all determine what payment systems will look like in the future.

*The following are a few of the areas where payment card systems are expected to extend and develop in future:*

### 7.1. Crypto Economics

The widespread use of digital currencies, including cryptocurrencies like bitcoin and now government-created ones such as CBDCs (Central Bank Digital Currencies), has brought about both new opportunities and problems for payment card interoperability. To move these digital currencies into traditional payment systems, existing card networks must be compatible with blockchain-based settlement networks.

The future scope lies in payment card networks, which need to provide services for transactions using digital currency, so a user can, for example, pay in dollars or Pounds Sterling but also use Bitcoins. At present such an integration will mean creating new standards for Cross-platform transactions, added security measures and adhering to regulatory compliances. Extension of Mobile and Contactless payments with options of mobile wallets, wearables and contactless payments is changing how those who buy merchandise from consumers' perspective. The increasing desire for fast, secure, seamless payment experiences means that this new way of paying with mobile phones has to be assimilated into the traditional methods.

In future, payment card networks and financial institutions may include mobile payment technologies in their traditional card systems, allowing for the use of mobile wallets, smartphones and wearable devices. Users will be able to go anywhere in this world and use any device to do business with one single bank, including making transactions back and forth between regions without needing numerous cards anymore.

Because of this very reason, we expect that artificial intelligence (AI) and machine learning (ML) will play a key role in the security of interoperable payment systems. They can be used to spot sudden changes in transactions, understand the likelihood of fraud, and carry out and enhance real-time transaction authentication accordingly.

An example is the implementation of AI and ML technologies into the payment card system. AI applications can make detecting suspicious transaction activities easier and more efficient, giving consumers and businesses more power.

### 7.2. Blockchain and Distributed Ledger Technology (DLT)

Blockchain and distributed ledger technologies potentially represent an entirely new way for payment card systems to achieve interoperability. These decentralized, immutable and transparent ledgers provide a manner of secure, efficient accounting that is non-existent in traditional payment system logs across various platforms.

An example: In an authentication gateway at a payment network, the use of blockchain will provide efficient cross-

border transaction solutions with less delay than today's methods of sending an International Wire from one bank account to another. Mechanisms for payments on blockchain with protocols that have already been established and successful trials by networks such as Master card and PayPass to ensure low-cost payments around.

### **7.3. Enhanced Cross-Border Payments**

Cross-border payments are often slow and expensive and bogged down by paperwork. To make a fresh start, our industry has developed an advanced digital payment infrastructure.

Interoperability between the various international payment systems allows people to transfer funds to each other more easily. With all these advances in digital services at their fingertips, interoperability will play a pivotal role in the future.

Expect the appearance of greater collaboration among global payment networks, blockchain platforms and digital currencies. The goal will be to offer faster, cheaper, and transparent cross-border payments. For instance, this could lead to real-time settlement systems, eliminating the need for intermediaries and reducing transaction fees significantly.

### **7.4. Biometric Authentication and Identity Verification**

Biometric authentication can be expected to play a key role in meeting this need for secure, seamless payment methods to grow harmoniously with interoperable payment systems. Integrating biometrics (such as facial recognition, fingerprints and voice recognition) into payment systems will provide an added measure of security for users while giving them convenience.

Payment card systems will increasingly employ biometric authentication to confirm transactions and protect sensitive data. This prospect could mean that biometrics payment methods could be extended from device to device so that consumers of all types can enjoy faster, more secure payments while having a better overall user experience.

### **7.5. Regulatory Harmonization**

As the payment scene becomes more complex, regulatory agencies will need to establish common standards for interoperability.

The changing face of cross-border transactions, digital currencies and new forms of payment practices calls for consistent regulation, ensuring security, integrity, and consumer protection across different markets.

The next method likely to be developed for payment card interoperability is through close cooperation between international regulatory agencies, unified security mechanisms, and uniform compliance standards and data protection rules. It will all help towards smooth, secure cross-border payments that also meet compliance requirements as innovation often flourishes in the payment industry.

### **7.6. Internet of Things (IoT) and Smart Payments**

The payments are set to transform how consumers make payments in future. Smart devices, from smart speakers to automobiles, could have payment capabilities incorporated within them, enabling consumers to purchase anything just by saying the word.

With IoT ecosystems present, today's bulky transaction systems may vanish. On a device, consumers can make transactions so easy that our lives will never be the same. There should also be no need for money to be physically exchanged for payments to happen across time zones, which seems increasingly likely with these fast-developing Internet of Things payment systems.

Payment systems and financial institutions must work together to ensure these devices connect with payment systems in real-time in security. This may well lead us back toward cashless shops.

A comprehensive literature survey on blockchain interoperability is provided by Belchior et al. [14]. The authors broadly categorized blockchain interoperability solutions into the following three categories: Cryptocurrency-directed Approaches, Blockchain Engines, and Blockchain Connectors. The three broad categories are divided into subcategories. Authors in [15] categorized inter-blockchain communications into four distinct groups: sidechains, blockchain routers, smart contracts, and industrial solutions. Robinson [16] organized cross-chain solutions into three categories of value, namely, swap, cross-chain messaging, and state pinning techniques. Wang [17] discussed the current state of blockchain interoperability and broadly categorized blockchain interoperability solutions as chain-based, bridge-based, and app-based interoperability. Interoperability can be viewed, in Beck and De La Torre's (2007) terminology, as a market-enabling policy, possibly allowing the financial sector to expand its capacity [18]. If consumers can join more than one network simultaneously, interoperability does not necessarily promote entry (Bourreau and Kraemer, 2022). Second, the intensity of competition may not be the only relevant dimension for consumer welfare, which also depends on providers' incentives to invest in network quality and product innovation (Valletti and Cambini, 2005).<sup>1</sup> Finally, promoting competition does not necessarily lead to improved access to financial services. Croxson et al. (2022) argue that platforms by themselves are unlikely to promote financial inclusion without appropriate regulation.

## **8. Conclusion**

To conclude, people need an interoperable payment card system to ensure their transactions are smooth and safe and, most of all, distributed across different forms of facilities around the world. In the evolving global payment landscape, interoperability is important for allowing consumers, merchants, and financial institutions to transact easily while ensuring compliance with security standards. Equally, integrating emerging technologies such as mobile wallets, blockchain, and biometric authentication will create even more.

Transformational technologies with interoperability come with challenges in data security, fraud prevention, and adherence to regulations. Relying on standardized industry-wide protocols and robust security technology will have to be more necessary than ever as payment processors intensively intermingle. With the right technological advances, tactical collaborations, and regulatory frameworks in place, the future of payment card interoperability looks very shiny, the groundwork for still more inclusive, efficient and secure global financial transactions.

In conclusion, recommendations further to the research paper on the interoperability issue that must be considered are the need for global standards and common protocols within or between networks, issuers, and acquirers. It will also help to minimize fragmentation by providing the means to allow payment card systems to function seamlessly across countries and financial institutions. Uniquely accepted standards and interoperability standards will come from continued collaboration between industry stakeholders, payment networks, banks and fintechs, as well as regulators

at the global level. Embracing open APIs, on the other hand, can lead to better integration solutions being built around systems, which can lead to faster and more interoperable adoption of technologies in the enterprise!

Further, new technologies such as blockchain and artificial intelligence should be adopted to provide more efficient, secure payment systems. Blockchain can then solve the issue of making transaction validation streamlined, which results in delays and a higher possibility of fraud. At the same time, AI can keep track of records pertaining to transactions in pattern and alert about irregularities immediately. Moreover, promoting regulatory harmonization is key to defining a legal framework that promotes interoperability. Regulatory cooperation is important to ensure that governments support one another in mutually recognizing regulations, particularly in the area of data protection, to allow for seamless cross-border steerability. These strategies ensure the evolution of a more connected and efficient global payment card ecosystem.

## References

- [1] Carol Coye Benson, and Scott Loftesness, “Interoperability in Electronic Payments: Lessons and Opportunities,” CGAP Report Commissioned to Glenbrook, pp. 1-46, 2012. [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Asli Demircuc-Kunt et al., *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, World Bank, pp. 1-148, 2018. [[Google Scholar](#)] [[Publisher Link](#)]
- [3] Avi Goldfarb, and Catherine Tucker, “Digital Economics,” *Journal of Economic Literature*, vol. 57, no. 1, pp. 3-43, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Robert M. Hunt, “An Introduction to the Economics of Payment Card Networks,” *Review of Network Economics*, vol. 2, no. 2, pp. 80-96, 2003. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Tan Soo Fun et al., “A Lightweight and Private Mobile Payment Protocol by Using Mobile Network Operator,” *2008 International Conference on Computer and Communication Engineering*, Kuala Lumpur, Malaysia, pp. 162-166, 2008. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Sujit Chakravorti, “Theory of Credit Card Networks: A Survey of the Literature,” *Review of Network Economics*, vol. 2, no. 2, pp. 50-68, 2003. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Codruta Boar et al., “Interoperability between Payment Systems Across Borders,” *Bank for International Settlements*, no. 49, 2021. [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Alice Negre, and Will Cook, “Interoperability in Digital Financial Services: Emerging Guidance for Funders,” Technical Note, CGAP, pp. 1-22, 2021. [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Morten L. Bech, and Jenny Hancock, “Innovations in Payments,” *BIS Quarterly Review*, pp. 21-36, 2020. [[Google Scholar](#)] [[Publisher Link](#)]
- [10] John P. Caskey, and Gordon H. Sellon, “Is the Debit Card Revolution Finally Here?,” *Economic Review-Federal Reserve Bank of Kansas City*, pp. 79-95, 1994. [[Google Scholar](#)] [[Publisher Link](#)]
- [11] African Union, “Africa Regional Integration Index Report 2019,” United Nations Economic Commission for Africa, pp. 1-48, 2019. [[Google Scholar](#)] [[Publisher Link](#)]
- [12] Qingqi Long et al., “Effects of Payment Interoperability and Noninteroperability on Platform Competition,” *IEEE Transactions on Engineering Management*, vol. 71, pp. 13918-13935, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Antonio Ruiz-Martínez, Óscar Cánovas Reverte, and Antonio F. Gómez-Skarmeta, “Payment Frameworks for the Purchase of Electronic Products and Services,” *Computer Standards and Interfaces*, vol. 34, no. 1, pp. 80-92, 2012. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Rafael Belchior et al., “A Survey on Blockchain Interoperability: Past, Present, and Future Trends,” *ACM Computing Surveys*, vol. 54, no. 8, pp. 1-41, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Ilham A Qasse, Manar Abu Talib, and Qassim Nasir, “Inter Blockchain Communication: A Survey,” *Proceedings of the ArabWIC 6<sup>th</sup> Annual International Conference Research Track*, Rabat Morocco, pp. 1-6, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Peter Robinson, “Survey of Crosschain Communications Protocols,” *Computer Networks*, vol. 200, pp. 1-14, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Gang Wang, “SoK: Exploring Blockchains Interoperability,” *Cryptology ePrint Archive*, pp. 1-27, 2021. [[Google Scholar](#)] [[Publisher Link](#)]

- [18] Thorsten Beck, and Augusto De La Torre, "The Basic Analytics of Access to Financial Services," *Financial Markets, Institutions & Instruments*, vol. 16, no. 2, pp. 79-117, 2007. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Marc Bourreau, and Jan Kraemer, "Interoperability in Digital Markets," 2022. [[Google Scholar](#)]
- [20] Tommaso M. Valletti, and Carlo Cambini, "Investments and Network Competition," *RAND Journal of Economics*, vol. 36, no. 2, pp. 446-467, 2005. [[Google Scholar](#)] [[Publisher Link](#)]
- [21] Karen Croxson et al., *Platform-Based Business Models and Financial Inclusion*, pp. 1-30, 2022. [[Google Scholar](#)] [[Publisher Link](#)]
- [22] Gabriela Guibourg, "Interoperability and Network Externalities in Electronic Payments," Sveriges Riksbank Working Paper Series, no. 126, pp. 1-47, 2001. [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Udo Milkau, and Jürgen Bott, "Digitalisation in Payments: From Interoperability to Centralised Models?," *Journal of Payments Strategy & Systems*, vol. 9, no. 3, pp. 321-340, 2015. [[Google Scholar](#)] [[Publisher Link](#)]
- [24] Filip Covic, and Stefan Voß, "Interoperable Smart Card Data Management in Public Mass Transit," *Public Transport*, vol. 11, pp. 523-548, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Rosica Chejkova-Nikolov et al., "Interoperability of Bank Statements: A Case Study," *2015 38<sup>th</sup> International Convention on Information and Communication Technology, Electronics and Microelectronics*, Opatija, Croatia, pp. 1505-1510, 2015. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] Cosmas Muchinguri, "Investigating Failure to Implement Contactless Payments: A Case of Near Field Communication Payment Systems in South Africa," Master Thesis, University of Cape Town, pp. 1-101, 2016. [[Google Scholar](#)] [[Publisher Link](#)]
- [27] Qingqi Long et al., "Effects of Payment Interoperability and Noninteroperability on Platform Competition," *IEEE Transactions on Engineering Management*, vol. 71, pp. 13918-13935, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] Manfred Männle, "Interoperable Mobile Payment—A Requirements-Based Architecture," *Wirtschaftsinformatik 2003/Band 1*, pp. 95-101, 2003. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] Urs Gasser, and John G. Palfrey, "Case Study: Digital Identity Interoperability and Einnovation," *Berkman Center Research Publication*, pp. 1-49, 2007. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [30] Celene Ancalle, and Maria Gracia Garcia, "Impact of Interoperability Regulation on the Use of Digital Payments in Peru," Graduate Institute of International and Development Studies Working Paper, No. HEIDWP02-2024, 2024. [[Google Scholar](#)] [[Publisher Link](#)]
- [31] Rainer Schamberger, Gerald Madlmayr, and Thomas Grechenig, "Components for an Interoperable NFC Mobile Payment Ecosystem," *2013 5<sup>th</sup> International Workshop on Near Field Communication*, Zurich, Switzerland, pp. 1-5, 2013. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [32] Angela N. Lawson, and Jorge Herrada, "Fit-for-Purpose Payment System Interoperability: A Framework," *FEDS Notes*, 2022. [[Google Scholar](#)] [[Publisher Link](#)]
- [33] Gottfried Leibbrandt, "The Interoperability Revolution," *Journal of Payments Strategy & Systems*, vol. 2, no. 1, pp. 95-106, 2007. [[Google Scholar](#)] [[Publisher Link](#)]
- [34] Tavneet Suri et al., "Mobile Money," *VoxDevLit*, vol. 2, no. 2, pp. 1-33, 2023. [[Google Scholar](#)] [[Publisher Link](#)]
- [35] Ablam Estel Apeti, and Eyah Denise Edoh, "Tax Revenue and Mobile Money in Developing Countries," *Journal of Development Economics*, vol. 161, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [36] Ggombe Kasim Munyegera, and Tomoya Matsumoto, "ICT for Financial Access: Mobile Money and the Financial Behavior of Rural Households in Uganda," *Review of Development Economics*, vol. 22, no. 1, pp. 45-66, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [37] Serge Stéphane Ky, "Empowering Sub-Saharan Farmers: The Transformative Effect of Mobile Money in Agriculture," *SSRN*, pp. 1-30, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]