The Evolving Payments Landscape

Technological Innovation in Payment Systems

Established financial institutions and their technology partners are contributing significantly to financial technology innovation in the payments market. This article provides a holistic overview of the technological innovations and challenges in the evolving payments landscape.

The payments market hosts a wealth of different participants, including banks, government agencies, corporations, and private households, each with a specific set of risk drivers and efficiency needs. But in a strict sense, each payment could be defined as a transfer of funds that fulfills an obligation of the payer vis-à-vis the payee.

A multitude of payment service providers operate a diverse set of payment systems that facilitate these transfers of funds according to formal arrangements and standardized rules. This diversity stems from the diverging needs and technological challenges in the different market segments. As a result, new dynamics and innovative solutions are being observed in the evolving payments landscape, including:

• disruptive online payment services in the retail segment of the market (such as Alipay, Venmo/PayPal, Skrill, Dwolla, 2Checkout, and TransferWise);
• new regulations like Europe’s revised Payment Services Directive (PSD2) and sandbox approaches that provide a relaxed regulatory environment to test new services;
• new payment systems with improved user experience and faster availability of funds, including the Australian New Payments Platform and the United Kingdom’s Faster Payments Service; and
• new cyber-resilient payment systems for real-time settlement of payments between financial institutions, such as the TARGET Instant Payments Settlement (TIPS).

Two key dimensions allow for a neat segmentation of the payments landscape into distinct clusters, each comprising payments with similar characteristics and processing needs:

• types of participants in the payment, typically grouped in two categories—financial institutions and nonfinancial institutions¹ (government agencies, corporations, or private households); and
geographic scope of the payment defined by the location of the payer and payee.

Wholesale payments are transfers of often high-value funds between financial institutions. Guaranteeing an orderly and timely settlement of wholesale payments is crucial for the wellbeing of financial markets. Wholesale payment systems, therefore, must ensure high maturity in information security, operational reliability, and cyber-resilience.

Retail payments are defined as payments between nonfinancial institutions. Their average value tends to be several orders of magnitude smaller than wholesale payments. By contrast, their share in the total number of payments is significantly higher. Operators of these systems are primarily focused on improving the user experience, the timeliness of processing, integration with other platforms, and ensuring adequate scaling.

A distinction is often made between domestic and cross-border payments. Domestic payments are transactions between payers and payees in the same jurisdiction, whereas the geographic scope of cross-border payments covers multiple countries. As payment systems in the Euro zone are increasingly integrated with or replaced by single systems, payments within this zone could be considered domestic payments.

DOMESTIC WHOLESALE PAYMENT INNOVATION

Safety requirements and efficiency standards formulated by international standard organizations like the Committee on Payments and Market Infrastructures (CPMI) are directly reflected in the technological blueprints of the next generation of wholesale payment systems. Additionally, operators of these future systems focus on broadening access, extending functionality, improving integration, and conducting end-to-end risk management.

Cyber-Resilience: Strengthening the Ability to Respond to Emerging Threats

The interconnectedness of information systems in wholesale payment processing have significantly deepened, while the sophistication of cyberattacks has increased. Increasing data breaches have resulted in additional incident detection and response capability investments.

Preventive controls are complemented by behavioral analysis techniques such as network intrusion detection and security information and event-management solutions, as well as intelligence-based penetration testing like CBEST.2

Supervising authorities put forward highly ambitious incident recovery objectives, both in terms of recovery point and recovery time. Current cyber-resilience requirements stipulate that critical operations should resume within two hours of an incident.3 Blueprints for next-generation wholesale payment systems elaborate on security by design that could deliver near-zero downtime for known resilience issues like viruses, hardware issues, or environmental failures.4

Wholesale payment systems operate on multiple sites and technology-diverse contingency platforms are in place. Research demonstrates that technology diversity can assist in rapid recovery in case a cyberattack renders the core system inoperative.

Broadened Access to Wholesale Payment Systems

Several operators have considered extending access beyond traditional financial institutions. As these access restrictions are still common, licensed nonbank payment services can only access wholesale systems through their main competitors—banks. Nonbank payment services like systems supporting small online payments typically have to connect to backbone infrastructure in the payments landscape—for example, to wire customer funds to bank accounts of payees.
The Bank of England will keep pace with the changing structure of the financial industry, which includes the unbundling of financial service provisions driven by nonbank payment service providers. By extending access to the wholesale payment systems, operators can help level the playing field between different types of payment service providers. While this might increase competition and innovation in the payments market, significant technology governance implications for the operators regarding third-party risk management and end-point security strategies might occur.

Promoting Interoperability between Payment Processing Systems

Multiple standards currently exist for structuring a payment message—for example, a fund transfer order containing all financial information related to a specific payment that is sent to a payment system. Global momentum has been observed for adopting the single open methodology prescribed in ISO 20022, a multipart international standard for electronic data interchange between financial institutions (www.iso20022.org).

Adopting ISO 20022-based messaging standards unlocks strategic benefits. A business case assessment commissioned by the Federal Reserve Bank highlighted that standardized message formats could promote automation and drive down costs. The Bank of England seeks to promote ISO 20022-based interoperability with retail payment systems, which will enable users to reroute payments to a retail system in case of an outage. Finally, a common set of data dictionary elements could be leveraged, allowing for improved regulatory reporting and monitoring.

Multiple operators of wholesale systems have already indicated that they will be adopting ISO 20022-based messaging standards, including the European Central Bank (ECB), the Federal Reserve, and EBA Clearing.

Enhancing User Functionality in a Changing Payment Environment

Emerging user demands for wholesale payments primarily deal with users’ desire to optimize processing efficiency and interact with the system. Users increasingly demand immediate payment processing at any given time, but significant technical barriers exist. The next generation of wholesale systems will need to run end-of-day batches while the service remains in operation. Additionally, system architecture should allow for the introduction of parallel hardware to conduct major maintenance and upgrading activities while the service remains available. Being technically capable of operating close to 24 hours a day is a requirement for the next-generation wholesale systems of the Bank of England. With the TIPS system, ECB will offer a service that supports the immediate processing of interbank transactions on a 24/7/365 basis.

The next generation of wholesale systems will also provide external-facing APIs to their users. These APIs allow integration with users’ systems, as well as exploit the available payment data in the system. Examples of payment data analyses are managing financial risk (especially liquidity management) and transaction and account limits. Furthermore, APIs could also enable wholesale payment track-and-trace functionalities that are being developed by the industry, with the most notable initiative being the bank-owned cooperative SWIFT’s Global Payment Innovation (GPI) tracker (www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi/features).

End-to-End Risk Management in Payment Processing

Wholesale payment systems do not operate in a vacuum—they are highly interconnected with the systems of their users and other third parties. Banks demand even tighter interweaving to improve payment processing efficiency and establish adequate monitoring capabilities, but because
they themselves are part of vastly broad ecosystems, the number of endpoints in the network dramatically increase. Cyber-events such as the 2016 compromise of the Bank of Bangladesh’s information systems demonstrated that a compromise might crystallize at any organization or step in the payment processing chain and then impact the entire ecosystem. Risk assessments increasingly cover risks related to connected third-party infrastructure.

Operators participate in cyber-intelligence acquisition and sharing initiatives to scan their systems for known attack vectors (for example, FS-ISAC; www.fsisac.com). Additionally, SWIFT has established an extensive program that aims to improve the cybersecurity posture of participants in the wholesale payment industry (www.swift.com/myswift/customer-security-programme-esp/programme-description). The program prescribes compliance with a minimal set of generally accepted cybersecurity measures, as well as tools for real-time monitoring that could prevent fraudulent or out-of-policy payment instructions.

DOMESTIC RETAIL PAYMENT INNOVATION

In contrast to wholesale payment systems, the focus on retail payment innovation has been primarily placed on improving the end-user experience.

Changing User Requirements: The Anywhere-Anytime-Anyhow Paradigm

The recent expansion of digital services has resulted in important changes in consumer habits and expectations. In line with the expectations for these digital services, consumers demand timely availability of funds to the payee and significant flexibility.

Retail payment innovation emphasizes faster processing, but different solution designs exist. Initiatives based on bank transfers are implemented around the world, such as the New Payments Platform in Australia, Faster Payments Service in the UK, Swish in Sweden, and FAST in Singapore. Additionally, time-efficient payment solutions are provided by payment card schemes such as Visa Direct, e-money providers such as PayPal, and cryptocurrencies such as Bitcoin.

The vast majority of these initiatives aim for always-on systems that provide near-real-time (typically less than 10 seconds) availability of funds to the beneficiary or a rejection of the payment. The Euro Retail Payments Board has endorsed the general design for a pan-European instant payment scheme called SCT Inst (www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer). Multiple SCT Inst-compliant systems are currently being developed, such as EBA Clearing and Stet. The technical challenges for real-time processing of retail payments include the need for systems with high availability and resiliency. To guarantee maximal reachability, the European ACH Association has developed an interoperability framework for SCT Inst-compliant systems. Furthermore, the stringent time restrictions put further pressure on risk-mitigating activities, including analyzing payment instructions for the detection of fraud and money laundering.

In addition, physical items are increasingly being turned into smart objects that are able to interact with other objects in their environment (the Internet of Things, or IoT). Automatic payment for services by these smart objects is an often-recited interaction pattern, such as cars automatically paying an insurance premium in a pay-as-you-go model or in pay-per-use leasing models.

Different architectural approaches are currently being reviewed for smart object payment solutions. Internet of Value proposals comprise a blockchain with virtual currency. Alternatively, incumbent card schemes propose the exchange of tokenized payment card data (www.mastercard.us/content/mccom-admin/faq-category-admin/tokenization.html).

Research indicates that the existing encryption key management protocols and access management designs might not be suitable. The implementation of an Internet of Value would require a drastic improvement of the scalability of blockchain technology. Technological constructs that allow for periodic recoding of balances are proposed by ETH Zurich’s Duplex Micropayment, Bitcoin’s Lightning Network, and Ethereum’s Raiden micropayments.
Opening the Retail Payment Industry

Recently, more and more diverse participants are entering the retail payment market. Digital innovators supported by new technologies and a revision of the regulatory framework reinforce the retail payment service offer. The strengthening of the demand side is being driven by the acquisition of hard-to-reach consumers.

To improve innovation, transparency, and competition in the payment industry, the European Commission revised its regulatory framework with PSD2. At the core of PSD2 is the requirement for banks to provide licensed services with secure access to individual bank accounts. The European Banking Authority has drafted regulatory technical standards that specify the information security requirements related to strong customer authentication and standardization of APIs.9 Payment initiation services like SOFORT, iDeal, and Trustly—which establish software bridges between e-commerce websites and online banking platforms—are examples of participants that benefit from the revised regulatory framework.

The widespread adoption of the Internet and advances in information technology have enabled the rise of peer-to-peer payments. Mobile wallets contain tokenized versions of credit cards and allow for payments through the use of near-field-communication (NFC) chips and QR codes. Cryptocurrencies like Bitcoin are linked to a blockchain-based peer-to-peer payment system. The main technological challenge for users these payment systems is to securely store the private keys to their coins, whereas the operators of these systems are looking for scalable transaction-validation algorithms.

Mobile network operators offer alternative payment systems based on carrier billing systems like Boku or deposits with the carrier, as is the case for M-Pesa in Africa. Mobile carrier–backed payment systems like M-Pesa have significantly improved financial inclusion in developing countries. The need for mobile networks with extensive coverage is crucial in this context and an important technical challenge for the operators of these systems.

Digital Platforms as a Driver of Competitive Advantage

In most jurisdictions, banks are expected to contribute to the development of new retail systems. Additionally, substantial investments are needed to integrate the bank’s internal system with new payment systems. Because of these significant costs, many initiatives are looking into flexible and open system designs that allow innovative services to directly interface with modernized systems.

The providers of these innovative services benefit from open API development that extends beyond the minimum requirements to comply with PSD2 or the Open Banking Standard (https://theodi.org/project/open-banking-setting-a-standard-and-enabling-innovation). Additional API functionality would allow banks to further facilitate and monetize access to banking data. The Australian New Payments Platform, for example, envisions services like submitting payments in bulk or providing invoice information with payments.

Guaranteeing information security and significant API standardization across different banks are important technological challenges. The providers of innovative services, on the other hand, will have to provide mechanisms for the strong authentication of bank account holders, as well as tools to set up secure communication mechanisms with the banks. As there are no regulatory technical specifications for additional API functionality, a lack of standardization might make it difficult for providers of innovative services to connect with a broad set of banks.

Nonbank service providers that recently entered the retail payment market are following a similar strategy. For example, Alipay and WePay have distilled typical usage scenarios for their services and have started to develop an extensive partner network. Currently, the usage scenarios are strongly focused on online-to-offline models, which combine online customer acquisition
with physical delivery of services and products. Examples of these scenarios are paying for utility bills, online shopping, topping off mobile phone credit, and buying train tickets.

Proxy Services for Simpler Payment Addressing

Traditionally, retail payment systems rely on payers knowing a piece of the payees’ personal financial information, such as account numbers. This has been identified as a major contributor to friction in retail systems, especially in the context of real-time or instant payments.

Payment-addressing proxy services operate a centralized database that registers the relationship among a user of a payment service, their account details, and one or more unique proxy identifiers. Payers can refer to these unique proxy identifiers to address a payment to a payee. Typical examples of unique proxy identifiers are email addresses, social media identifiers, and mobile phone numbers.

Payment-addressing services are rapidly being adopted, such as PromptPay in Thailand, clearXchange in the US, and the New Payments Platform in Australia. The Mobile Proxy Forum aims to develop a pan-European standardized proxy lookup service, which would provide an interoperability framework to allow pan-European payment systems to access the service.

Big Data Opportunities

Payment-related data contains a lot of information on the interests, activities, and behavioral patterns of customers. Multiple applications for operators of payment services can be envisioned.

First, advanced statistical analysis of payment data will enable more effective risk and compliance assessments. Contemporary big data solutions enable banks and other payment service providers to aggregate payment data originating from different types of transactions (for example, payments with credit cards, debit cards, checks, and wire transfers) into a centralized platform, which results in a more complete overview of customers’ transactions. The resulting data warehouses will enable advanced statistical analysis techniques to better incorporate behavioral, temporal, and spatial techniques in the detection of fraud and money laundering.

Secondly, payment-related data can be used to continuously improve the user experience, which can deliver a competitive advantage in an environment with increasingly demanding end users. Payment service providers can create a single account and transaction overview across multiple channels of usage, which results in better insight and personal finance management applications for the end user. Additionally, the aggregated data can be used for alternative algorithm-based credit scoring. The regulatory framework established in PSD2 explicitly acknowledges this type of account information service providers.

Finally, payment service providers can try to monetize the data. Conducting advanced market analyses on payment data can provide valuable insights into the market segments and assist platform partners in driving their reward programs and identifying cross-selling opportunities.

The major challenges for the storage and third-party use of payment-related data remain the information security and privacy requirements stipulated by the regulating authorities.

CROSS-BORDER PAYMENT INNOVATION

Cross-border payments are increasingly expected to have the same characteristics as domestic payments. Payers and payees demand that these payments are cost-effective, timely, predictable, and traceable. A prime driver for the current uncertainty regarding the timing and cost of international transactions is the omnipresence of correspondent banking. Correspondent banking is the practice of using one or more intermediaries between banks in different countries. This is typically needed if the payer’s bank has limited access to the foreign financial market in which the payee is located. Currency conversion is often required.
Because of the high complexity of cross-border payments, currency conversion risks, and diverging regulation in multiple jurisdictions, technological innovation is comparatively limited.

**Efficiency Gains through Disintermediation**

Increasingly, cross-border payment systems proposed by digital innovators are based on business models that center on the disintermediation of financial institutions. Cryptocurrencies might allow for cross-border payments without any middleman, but a spectrum of varying levels of disintermediation is being observed.

Peer-to-peer payment systems for cross-border transactions allow for bypassing banks and their correspondents, and thereby avoid commission charges of these intermediaries. Algorithms match cross-border payments with payments going in the opposite direction and reroute the flow of funds. The inherent challenge of these systems is the assumption that an equal amount of payments in both directions can be found. TransferWise, Midpoint, CurrencyFair, and WeSwap offer this type of cross-border payment system.

Disintermediation efforts in cross-border payments do not only come from fintech (an abbreviation for financial technologies) challengers. Banks are also looking into different technology-based opportunities for settling cross-border transactions. R3, a consortium of banks and technology companies, analyzed the usability of Ripple’s digital asset XRP and distributed-ledger technology (DLT) to settle cross-border payments between banks instantly without the need for a relationship between these banks. In addition, the International Payments Framework Association has developed a standard to enable financial institutions to directly link with domestic payment systems in other jurisdictions.

**Enhancing Transparency, Predictability, and Traceability**

At the same time, banks are revising their information systems and business processes to improve the existing correspondent banking model. SWIFT takes the lead in this evolution with its GPI initiative. GPI centers on a set of multilateral service agreements between participating GPI banks, which specifies business rules related to timeliness, transparency of costs, and the transmission of rich payment data in correspondent banking.

An end-to-end tracking solution will allow GPI banks to check the status of cross-border payments from the moment the payment is ordered until it is confirmed. In addition to providing transparency in the routing of funds between correspondent banks, the tracking solution will provide an overview of the bank fees and foreign exchange rates. The technical challenges for the participating GPI banks include the adoption of the unique transaction reference (UETR), used for tracking payment routing in their systems, as well as API infrastructure for interaction with the tracker. Additionally, GPI banks might consider the provision of software bridges to allow their corporate customers to check the status of their payments.

Sharing rich payment data in the correspondent banking chain further improves correspondent banking efficiency. Currently, corporate clients are often asked to provide additional payment information for compliance checks. Furthermore, reconciliation of payments and invoices often requires manual intervention, which could be avoided when rich payment data is conveyed together with the payments. A solution is designed around a cloud-based information layer that could be queried with the UETR of a payment.

While peer-to-peer platforms allow for full transparency and reasonable predictability on the timing of fund availability with the payee, the security guarantees are not considered to be at the same standard of the improved correspondent banking model. Therefore, it is expected that these
peer-to-peer platforms will primarily be used for lower-end retail payments and not for important corporate payments.

CONCLUSION

Diverse payment system innovations are being developed by a multitude of operators. Domestic wholesale payment innovations are primarily driven by a desire to increase predictability and security, whereas domestic retail payments demand improved user experience and cost efficiency. Innovations for cross-border payments aim to improve the efficiency, transparency, and traceability of payments.

Regulations and requirements might have a strong impact on the technological evolution of the payments market. Wholesale payment systems typically face stringent security requirements and regulatory uncertainty regarding new technologies. Globally active retail payment services must deal with the challenges of operating in multiple jurisdictions with deviating legislation. On the other hand, new regulatory frameworks (like PSD2) are opening up the retail payment market for new entrants.

Agile fintech startups do not appear to drive innovation in each payment segment. While these entrants take the lead in innovating retail payments by improving the user experience, wholesale payment systems are revised under incumbents with extensive experience in dealing with security requirements and regulations.

Finally, although it has been identified as a key technology for future financial infrastructure by the World Economic Forum, blockchain is not being adopted in the technological blueprints for the next generation of wholesale payment systems. Both the ECB and the Bank of England announced that they are considering the possibility of DLT interfacing.

REFERENCES

ABOUT THE AUTHOR

Filip Caron is a faculty member at the Decision Sciences and Information Management Department at KU Leuven and is associated with the Leuven Institute for Research on Information Systems. His research interests include information governance and financial technology. Caron received a PhD in management information systems from KU Leuven. He has authored more than 30 academic publications, and teaches graduate courses in business analysis and process management. Contact him at filip.caron@kuleuven.be.

Senior Software Engineer

Innovative Software Engineering, LLC (“ISE”) is seeking a qualified individual to fill the role of Senior Software Engineer in our Coralville, IA office. Position is responsible for creating information systems by designing, developing and installing software solutions. Essential duties include software system design and architecture incorporating technologies such as C++, JAVA, C# and .NET. Develop software solutions by studying information needs, conferring with users, studying systems flow, data usage, work processes, investigating problem areas and following the software development lifecycle. Determine operational feasibility by evaluating analysis, problem definition, requirements, solution development and proposed solutions. Document and demonstrate solutions by developing documentation, flowcharts, layouts, diagrams, charts, code comments and clean code. Prepare and install solution by determining and designing system specifications, standards and programming. Improve operations by conducting systems analysis and recommending changes in policies and procedures. Guide the development and design tasks of team members and provide comprehensive code review feedback. Interface with customers on describing design, architecture and detailed technical analysis and manage customer relationships by facilitating dialogue, formulating and driving business development and managing expectations and deliverables.

B.S. in Computer Science, Computer Engineering or Electrical Engineering required. Five years of post-graduate, progressive experience in Software Engineering or Software Development required. Must possess demonstrated understanding of programming concepts, practices and procedures and object-oriented concepts, as well as demonstrated ability with C, C++, C#, JAVA, communications systems, web services architecture and/or system level requirements capture. Demonstrated ability to leverage design patterns as a developer also required.

To apply email resume to Humanresources@iseinc.biz