Payments System Research Briefing

Core Banking Systems and Options for Modernization

by: Julian Alcazar, Sam Baird, Emma Cronenweth, Fumiko Hayashi and Ken Isaacson

February 28, 2024

Each U.S. depository institution (DI)—including banks and credit unions—uses a back-end information technology system to process daily transactions and manage financial accounts. Many of these "core banking systems" are outdated and unable to fully accommodate modern services, such as open banking and instant payments. Modernizing these systems is a complex process, and DIs may consider a full replacement, a component-based replacement, or augmenting their existing system.

The core banking system of a depository institution (DI)—the back-end information technology system that processes daily banking transactions and updates financial accounts and records—is crucial to the products and services a DI offers its customers. Many DIs still use legacy core systems up to 40 years old that reside on mainframe hardware coded with outdated programming languages (McKinsey & Company 2022). To offer customers better payment services that take full advantage of modern payment methods—such as instant payments—these DIs will need to modernize their core systems.

Despite the importance of modernizing core systems, the systems themselves and the core banking services market are not well understood. Most DIs rely on core banking services providers for their core systems and ancillary services, so modernizing the systems requires close cooperation and coordination with these providers. In addition, ancillary financial services such as payments processing are often integrated with the legacy core systems, making the system architecture complex and difficult to change. This *Payments System Research Briefing* describes core systems and the options DIs have for modernizing them. Two forthcoming *Briefings* will examine the market structure surrounding core providers and explore the role of core providers in facilitating the adoption and broad use of instant payments.

Types of core banking services: Primary or ancillary, in-house or outsourced

Core banking systems provide DIs services that can be categorized broadly as primary or ancillary. Primary services are essential services that the core systems always provide, including account management, customer management, deposit and withdrawal processing, loan processing, and finance and accounting. Ancillary services are additional services the core provider may offer, including payment-related services, bank product interfaces, and customer support. Some DIs outsource all ancillary services to their core provider, while other DIs outsource ancillary services to other providers or perform some of them in-house. Table 1 describes these services in more detail.

Table 1: Core banking services

Service	Description
Primary	
Account management	Create and manage different types of accounts, such as checking, savings, loans, and credit card accounts
Customer management	Create and manage customer profiles, track customer activities, and manage customer relationships
Deposit (credit) and withdrawal (debit) processing	Post, process, and manage deposits (credits) to, and withdrawals (debits) from customer accounts
Loan processing	Issue, process, and manage various types of loans
Finance and accounting	Maintain general ledger, accounts payable, asset and liability management, and credit loss modeling
Ancillary	
Payments	Authorize and verify funds for outgoing payments (automated clearinghouse, wire, instant payments, cards), capture checks remotely, provide gateway services (or connections) to payment networks/operators, provide ATM management and processing, provide merchant services, and provide enterprise/business account/payment services
Bank product interfaces	Provide online/mobile banking apps and branch/teller system
Customer support	Provide technical support for call center and mobile/online chat
Fraud and risk management	Monitor transactions for suspicious activities and issue alerts for various types of bank fraud vulnerabilities
Compliance and audit	Manage compliance and risk-related functions such as anti-money laundering, countering financing of terrorism checks, and know-your-customer verification
Reporting and analytics	Generate various reports (for example, balance sheets, income statements, and customer transaction reports) and conduct data analyses to provide insights into customer behavior and market trends
Supporting third-party apps	Provide third-party access to customer data and integrate third-party apps (such as Venmo) to online/mobile banking apps

Based on their business needs, DIs employ different combinations of services offered by core providers and other service providers. Larger DIs with ample resources are more likely to use in-house core system processing and solutions, customizing features and functions to meet their specific needs. In contrast, most smaller DIs outsource to core service providers or other service providers, especially in three areas: IT, business processes, and product offerings (Capgemini 2013). DIs may outsource their IT by using a third party for services such as server management, infrastructure architecture, and network administration. They may outsource business processes by using a third party to manage an entire business process, such as accounting, finance, or customer support. And they may outsource product offerings by assigning product development and operations to a third-party provider. Although outsourcing limits DIs' control over some features and functions, it enables them to take advantage of the core (or other service) providers' broad solutions without the need for resource-intensive in-house development or operations.

Legacy core systems versus next generation

Core systems can be categorized as legacy or next generation (ICBA 2021; McKinsey & Company 2022). Legacy systems typically use a monolithic architecture where all components of the system are intertwined, potentially in a confusing way due to years of patches and customization. These systems often run on a single server or mainframe, with outdated technology stacks that require specialized skills to maintain. In contrast, next-generation systems use an open, modular architecture, where components are decoupled and can run independently on different servers or in the cloud. These systems use modern technologies such as microservices, application programming interfaces (APIs), and cloud computing.

Next-generation systems have many advantages over legacy systems (McKinsey & Company 2022). Their cloud-native infrastructure typically has lower operating and maintenance costs due to lower reliance on the hardware that may live on a DI's premises. Next-generation systems' plug-and-play features offer flexibility and scalability, increasing access to partnerships with various service providers and enabling a real-time customer experience. Furthermore, next-generation systems enable DIs to easily integrate datasets across the DIs' products and services, giving the DIs new tools and insights into customer behavior and market trends.

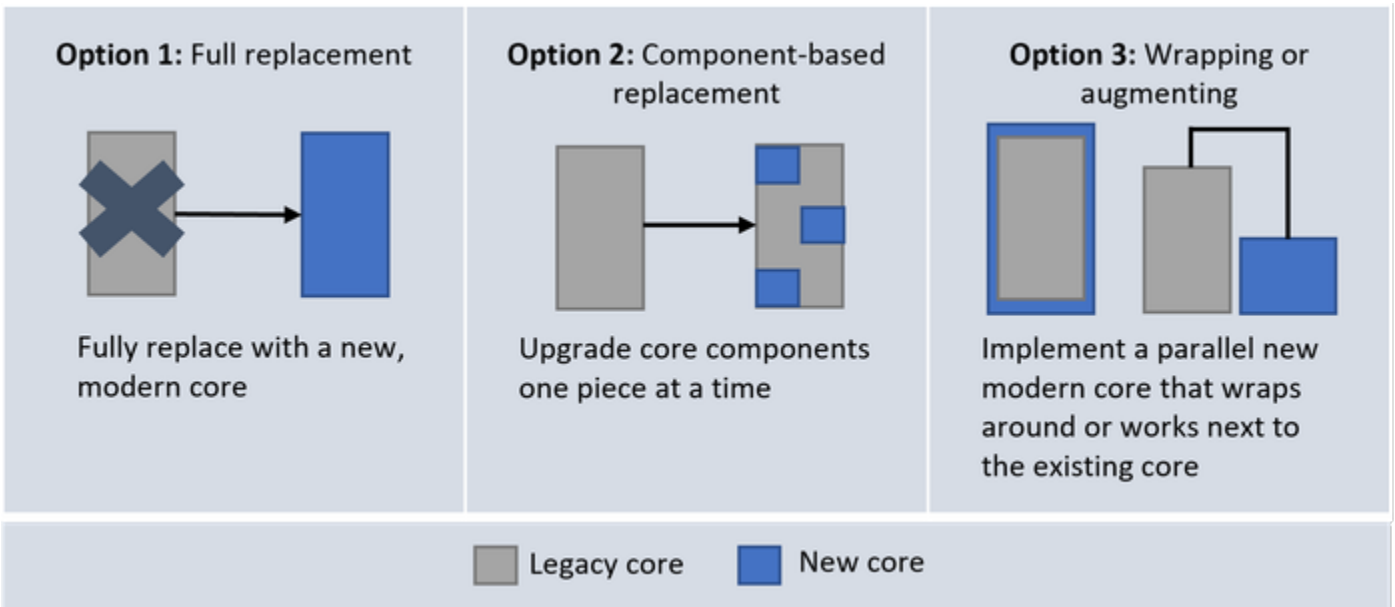
The flexibility and scalability of next-generation systems allow DIs to choose whether they pursue a "best-of-breed" strategy or use a fully integrated core system. The best-of-breed strategy enables a DI to pick and choose from vendor solutions that best meet their needs, which may shorten the time required to introduce a new product, such as an instant payment service. Although packaging primary and ancillary services in a next-generation system may not allow a DI to implement a customized feature easily, some DIs may prefer this system due to low internal and external maintenance costs, easy vendor management, and potentially more streamlined operations. Legacy systems may not allow a DI to pursue a best-of-breed strategy due to the technical limitations of integrating newer products into older code.

Despite the numerous advantages of next-generation systems, many DIs have concerns about these systems because they are usually offered by newer, less-proven core providers, such as Finastra, Q2, and Synapse. Lack of experience with next-generation systems and new core providers may increase many DIs' uncertainty about the systems' reliability, security, and ability to meet DIs' needs (ICBA 2021). Incumbent core providers—such as FIS, Fiserv, and Jack Henry and Associates—have long offered legacy core systems but more recently began offering next-generation systems as well. Although these core providers are known for their long track record of dependability, they have been criticized for their lack of services and responsiveness to smaller DIs (ABA 2023; Groenfeldt 2019). The lack of services and response from their core provider may inhibit an individual DI's ability to meet customers' needs and stay competitive.

Options for DIs to modernize their core systems

Meeting customer demands for modern services—such as open banking, instant payments, and more functional mobile banking—is a significant challenge for DIs with legacy core systems. However, modernizing these systems is a major endeavor involving extensive planning, expertise, coordination across technology and business domains within their organization, and cooperation with their core provider. The process requires significant time and financial investment, which varies based on approach. Figure 1 depicts the three options DIs have to modernize their core systems: (1) full replacement, (2) component-based replacement, and (3) wrapping or augmenting the existing system.

Figure 1: Three options for DIs to modernize their core system



Sources: Kumar, Salvaterra, and Kulkarni (2019) and authors' modifications.

A full replacement is the most risky and expensive option for modernizing a core system and is often the method of last resort when the legacy core system stops meeting business needs (Kumar, Salvaterra, and Kulkarni 2019). The replacement process can introduce many sources of risk, including the downtime of core systems, data migration, the reliability of the new system, and sufficiency of resources to support the transition. Full core conversions can take several years and cost millions (if not hundreds of millions) of dollars depending on the size and complexity of the DI, the scope of implementation, and the deployment approach (BAI 2016). Some industry experts liken this process to "open heart surgery" or "swapping jet engines while flying" (Deloitte 2017; Groenfeldt 2019).

Despite the risk and cost, some DIs have recently chosen to fully replace their core banking systems. Seattle Bank, a single branch bank with $650 million in assets, decided to fully replace its Fiserv core banking system with a modern, cloud-based core platform from Finastra (Groenfeldt 2019). The decision was driven by the bank's dissatisfaction with the inflexibility and fee structure of their previous legacy core provider. The new platform includes modern offerings such as enhanced bill pay, banking-as-a-service (BaaS), and open banking tools.[1] Notwithstanding this example, full replacements are rare, particularly among smaller DIs, as they require full commitment from the institution's leadership and careful coordination with the technology team.

Component-based replacement is less risky than full replacement, in part because DIs replace each component of a core system one at a time (BAI 2016). Disentangling functions of a core system may be difficult for many DIs due to the length of time the system has been in place and the number of layers added over time to keep the system functional. However, if a DI can separate components within their core system, component-based replacement may be a reasonable modernization strategy.

Some DIs have pursued this option. Zions, a regional bank operating in 11 states with $90 billion in assets, chose to upgrade the lending component of its core system before moving to the deposit component (Pape 2022). Zions' executive vice president detailed this strategy at the 2022 Digital Banking Conference, noting that the decision to start with the loan system was due to its lower customer engagement and visibility, minimizing potential negative outcomes from conversion issues. After extensively testing with thousands of simulations, Zions then upgraded the deposit component of its core system. Zions ran the old and new systems simultaneously and migrated branches one at a time to mitigate risk. The conversion helped simplify deposit products and streamline processes.

Instead of replacing a legacy core system, an existing legacy system can sometimes be "wrapped" or augmented with a next-generation parallel "shell" core. Also known as "building on top or the side," this option involves a next-generation core that plugs into the legacy core via API connections (Sarkar 2021). The next-generation parallel core allows DIs to expand their product offerings, connect to vendors, and remain flexible, while maintaining the integrity of the data and processes of the legacy core system. The next-generation parallel core can process transactions straight through to the legacy core. Because the legacy core and underlying data are maintained, this option is often less risky than replacing components. Although a parallel core solution may be less expensive than a full replacement, DIs may still face costs for integrating services and maintaining multiple core systems over time.

Several new core providers offer next-generation core platforms that wrap or build on top of an existing core, including Finastra, FintechOS, Finzly, Mambu, and SoFi (which acquired Technisys). Using these new core providers may enable DIs to implement instant payments relatively quickly, as some of these companies are the first to provide an API connection to the Federal Reserve's new instant payment service, FedNow (Fitzgerald 2023). These companies also provide an API connection to other payment infrastructures such as Real-Time Payments (RTP), automated clearinghouse (ACH), the Fedwire Funds Service, the Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT). Augmenting a core system with a payment platform that consolidates the processing of multiple payment methods helps DIs improve processing efficiency, reduce operating costs, and accelerate the time to introduce new services (Baumann and Fishman 2023).

An additional consideration for modernization: Transition to the cloud

No matter which of the three core modernization options DIs choose, they will also face a broader modernization challenge: transitioning to the cloud. Transitioning to the cloud implies that a DI moves existing processes from hardware or mainframes running in DI-managed physical locations to servers hosted by a core provider, vendor, or other third party. This transition can yield simplified hardware maintenance, faster and more flexible data access, faster updates, better scalability, and the ability to integrate with other microservices via APIs (Duepke and others 2019). Moreover, this transition can be pursued concurrently with all three core modernization approaches. For example, DIs may choose a full core system replacement with a cloud-based core provider or upgrade one component at a time to cloud services. DIs may also augment or wrap their legacy core system with services offered by a cloud-based next-generation core provider.

Although many DIs have already started transitioning to the cloud to some degree, they are slow to do so with their core systems. According to a report by Accenture, more than 90 percent of retail banks surveyed around the globe have used the cloud in some capacity, but their adoption for integral services, including core banking services, remains low (Abbott 2021). Influencing this low adoption rate are concerns about data security (and the associated regulatory risks) and outages of cloud service providers.[2] Insufficient transparency from cloud service providers in contract terms (such as data ownership, data

back-ups, and data security or privacy provisions) also makes it difficult for DIs to perform necessary due diligence, monitoring, and third-party risk management (U.S. Department of the Treasury 2023).[3]

Despite these concerns, some banks have transitioned to the cloud for their core systems. For example, Seattle Bank transitioned to Finastra's cloud-based banking platform in 2020, motivated in part by a plan to integrate with fintechs to provide BaaS solutions and embedded finance (Finastra 2019).[4] One of the benefits gained from transitioning to the cloud was the ability to deploy the Paycheck Protection Program soon after the CARES Act was signed during the pandemic (Seattle Bank 2020). In addition, Mascoma Bank, a DI with $2.6 billion of assets, transitioned to Thought Machine for its cloud-native core system (Fintech Futures 2022). This transition integrated previously siloed data and enabled Mascoma to easily implement new product offerings at a faster rate (Thought Machine 2022).

Summary

Core banking systems are the backbone of the products and services that DIs offer their customers. Core systems provide DIs primary services such as account and customer management, deposit and withdrawal processing, loan processing, and finance and accounting. Core systems also often provide ancillary services, such as payment processing and customer support.

While many DIs still use legacy core systems, some have begun modernizing their core systems to meet their customers' demand for modern services, including instant payments. Next-generation systems, which use modern architecture and technologies, have many advantages over legacy systems and help DIs offer their customers a better banking experience. However, modernizing legacy core systems can be complicated and requires coordination with both core service providers and any other service providers a DI might use.

To modernize legacy core systems, DIs have three options: a full replacement, a component-based replacement, or augmenting the legacy system. The time and financial investment required for modernization and the associated risks vary by option, but all three are a major undertaking. Ultimately, DIs that have already completed their core system modernization and realized the benefits have a competitive advantage in the banking and payments markets.

Endnotes

[1] BaaS describes a model in which DIs integrate their digital banking services seamlessly into the products of other nonbank businesses. Under this model, a DI allows a nonbank business to market the DI's products—such as mobile banking accounts, debit cards, loans, and payment services—under the nonbank business's name.

[2] In recent years, two incidents affected confidence in this way. In June 2021, an outage of a distributed denial-of-service (DDoS) protection service of Akamai Technologies, a U.S.-based cloud company, caused service disruptions at three of the four major Australian banks (Chanthadavong 2021). And in November and December 2023, about 60 U.S. credit unions experienced outages due to a ransomware attack against Trellance-owned Ongoing Operations, which provides business continuity services and cloud solutions (Birch 2023; Kapko 2023).

[3] Ownership of DIs' customer data is also often ambiguous in contract terms between a DI and its core provider. If the core provider owns the data, the DI will incur sizable cost when switching to another core provider (ICBA 2021).

[4] Embedded finance refers to financial solutions that are offered by consumer-facing businesses in conjunction with the purchase of goods and services. The purpose is to eliminate the need for consumers to leave the merchant's channel to make payments, borrow money, or procure insurance associated with the purchase. BaaS enables embedded finance as well as the provision of financial services by nonbanks (Lehman 2022).

Authors

Julian Alcazar

Senior Payments Specialist

Julian Alcazar is a Senior Payments Specialist for the Office of the Chief Payments Executive for Federal Reserve Financial Services. Julian received a B.A. in Sociology from California State University San Bernardino and Masters from the Georgetown University. His research focuses on emerging payments and their impact on consumers.

Sam Baird

Associate Payments Specialist

Sam Baird is an Associate Payments Specialist in the Payment Strategies Department at the Federal Reserve Bank of Kansas City. He joined the Federal Reserve Bank of Kansas City in January 2022 after receiving his BA in economics and political science with minors in mathematics and a certificate in public policy from the University of Nebraska-Lincoln in 2019. His research interests include emerging payment technologies, payment behavior of younger generations, consumer protection, and intermediaries in the banking system.

Fumiko Hayashi

Senior Policy Advisor

Fumiko Hayashi is a Senior Policy Advisor specializing in payments in the Economic Research Department at the Federal Reserve Bank of Kansas City. Since joining the Federal Reserve in 2001, Ms. Hayashi published studies on the ATM and debit card industry, regulatory developments around interchange fees and card network rules, consumer payment choice, various types of payment methods (including credit, debit, and prepaid cards, mobile and QR code-based payments, instant payments, and central bank digital currency), payment fraud and security, nonbanks and fintechs in the payment system. She is currently conducting research on undeserved consumers in payments, fraud and scams involving instant payments, role of intermediaries in the payment system modernization, among others.Prior to joining the Federal Reserve Bank of Kansas City, Ms. Hayashi conducted research examining consumer savings and long-tern care insurance, social security reform in Japan, and nursing home markets in the United States. She holds a B.A. and a M.A. in economics from Hitotsubashi University, and a Ph.D. in economics from the University of Minnesota.