BROADCOM®
SOFTWARE

A Guide to Digital Banking in the IoT Economy

HOW APIS ENABLE AN OMNICHANNEL, MOBILE-FIRST STRATEGY FOR NEXT-GENERATION BANKING EXPERIENCES

The digital revolution is here, driven by technologies like application programming interfaces (APIs) and the Internet of Things (IoT). It is changing communication, mobility and commerce, closing traditional establishments and paving the way for new digital entrants.

With mobile devices came an immediate and lasting change in consumer behavior and demands—for faster, more intuitive, more personalized, more secure and simply better services. As a result, much of what traditionally took place in a brick-and-mortar establishment moved online, then to mobile, and now to connected devices. Mobile-first, open APIs and IoT are not simply buzzwords but global trends that have profound implications for all industries.

The next era of banking

The banking industry is no exception. Bank locations are closing as many of the services consumers traditionally sought in person are now available online or via a mobile app. Those physical locations that do remain will change, and the range of banking services enabled by technology will continue to grow at a rapid pace.

81%

In a Forrester survey of global financial services decision makers, 81 percent plan to begin this year, or are already working on, a major transformation project.

5 OR 10 YEARS

Forrester predicts that banks without state-of-the-art digital banking platforms will find it hard to remain competitive in five or ten years' time.

The State of the Industry

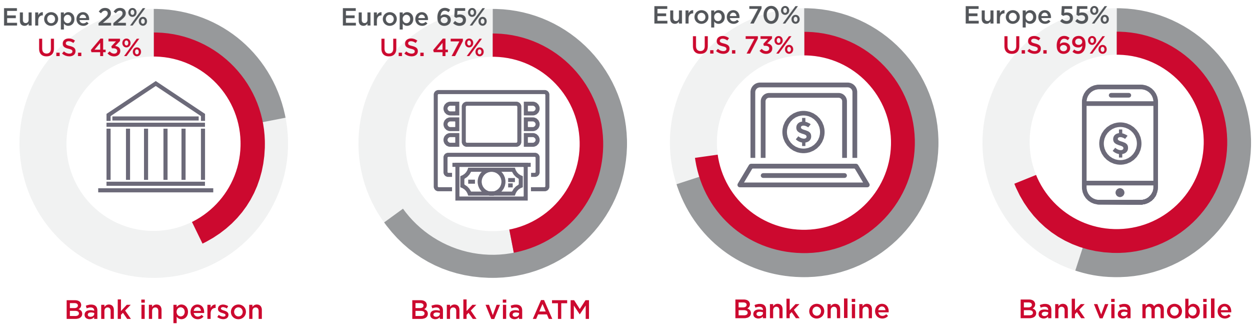
Banking is facing a growing digitalization. Branch use is in decline as consumers are seeking faster and more convenient methods, such as ATMs, online, or on-the-go via a smartphone, tablet or even a smartwatch.

The use of mobile devices for banking will increase as the range of services supported via mobile continues to expand—from text alerts, to balance checks, to deposits, and now to bill pay and transfers. Integration between traditional branches, ATMs, retailers and third-party services will only continue to increase the use of mobile as a dominant banking touchpoint.

As technology begins to change banking in physical locations and ATMs, it wouldn't be surprising to see a trend for consumers to move back to these touchpoints as well. In this new technology-driven era, consumers will increasingly take a multichannel approach to banking.

Banking Touchpoint Activity in U.S. and Europe

Percentage of online adults, at least once monthly



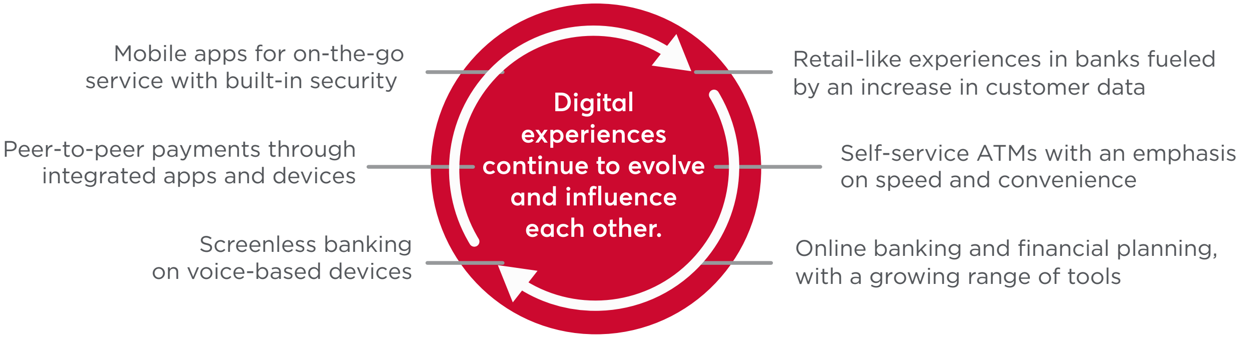
Banking Is Evolving

The industry is changing, as consumers use a combination of traditional channels and digital touchpoints to bank. For researching and buying financial products, investing, and resolving technical or service-related issues, traditional bank branches remain the preferred method for consumers.

Banks cannot abandon these established channels, but rather must invest to bring them into the digital age. In the U.S., 20 percent of online adults have visited branches and used online and mobile banking at least once in the past month.

A MULTI-CHANNEL APPROACH

Technology enables banks to improve the experience across all channels and will continue to drive next-generation digital experiences.


Mobile apps for on-the-go service with built-in security
Peer-to-peer payments through integrated apps and devices
Screenless banking on voice-based devices
Digital experiences continue to evolve and influence each other.
Retail-like experiences in banks fueled by an increase in customer data
Self-service ATMs with an emphasis on speed and convenience
Online banking and financial planning, with a growing range of tools

This trajectory isn't linear. As technology advances, it will drive changes across all channels—including the more traditional methods that could seemingly be made obsolete by digital touchpoints. Innovations in mobile and screenless banking, for example, will create new forms of in-person banking that will drive consumers back to these channels. What will enable this evolution?

APIs—the connective thread that is digitalizing, integrating and securing the next generation of banking in the age of IoT.

Smarter Banks

Rather than just moving banking to digital platforms, technology can enable new and improved services within branch locations. These experiences are built on the integration of powerful mobile apps, new connected technologies and existing branch systems. For example, beacon technology within the branch, integrated via APIs with the bank's mobile app, can provide users with real-time information about waits and availability of services for in-person banking.

KEY BENEFITS

Or, similar to the experience of mobile ordering in a coffee shop, users can check-in and join a digital queue from within the bank's mobile app to better schedule and receive in-person services. Via APIs, these services are securely integrated with the bank's internal systems to create a unified experience across branch and mobile app.

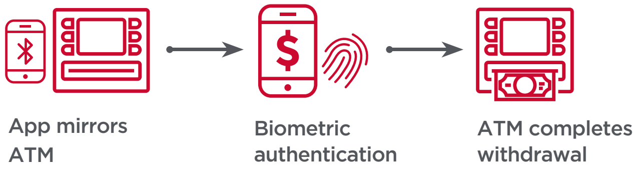
Finally, banks can invest in virtual assistants in branches for check-in and scheduling, or to answer frequently-asked questions. This both reduces wait time and enables banks to optimize internal resources. Virtual assistants (such as kiosks or voice-based devices) are integrated via APIs with internal systems to provide a range of services and information to users.

ATM 2.0

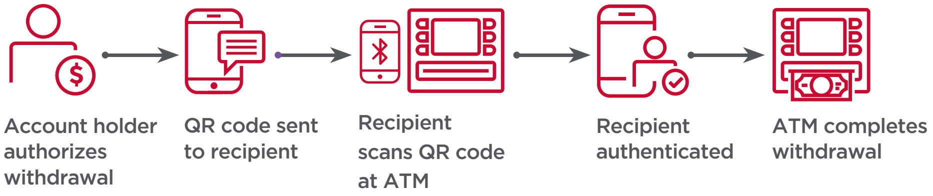
When ATMs were first introduced, the technology was state of the art. Since then, improvements have been gradual. We have yet to realize the full potential of these machines to combine new technologies with current capabilities.

Mobile technology offers this opportunity for next-generation ATM experiences. Via geolocation and APIs, mobile banking apps can recognize account holders at an ATM. When the account holder logs into the bank's mobile app at the ATM, the app mirrors the ATM screen and the account holder can then complete the transaction from his or her phone. Native mobile security features such as biometric authentication can be used to authorize the ATM transaction. This enables a faster transaction as account holders do not even need to take out their debit cards to complete the withdrawal. The transaction is also more secure as multiple factors, rather than just a PIN, are required to authenticate.

Let's say you want to allow a trusted person to make a one-time withdrawal from your account (for example, your teenaged daughter who does not yet have her own debit card). From within the bank's mobile app, the account holder can authorize an ATM withdrawal at a selected location. A QR code is then generated and shared with the recipient. The recipient scans the QR code from his or her mobile device at the ATM and is able to withdraw the designated amount of money from the sender's account, with the sender's approval and authorization.



App mirrors ATM → Biometric authentication → ATM completes withdrawal



Account holder authorizes withdrawal → QR code sent to recipient → Recipient scans QR code at ATM → Recipient authenticated → ATM completes withdrawal

Gone Mobile

APIs are changing banking in physical locations like branches and ATMs, and they are also bringing traditional services into the digital realm. Banking first moved online with the ability to view account balances, pay bills, make transfers and many more features offered over the Web. Gradually, banks built mobile apps to deliver these services on a smartphone. To enable speed, user experience and security, banks use APIs to govern the flow of data and protect internal resources while exposing functionality to mobile apps.

Mobile banking lay the foundation for a broad ecosystem of integrated services and functionality to develop alongside the bank's own investments. While much of digital banking now takes place through the bank's own app, a significant portion is driven by third-party apps and services such as peer-to-peer payment apps, budgeting apps and mobile wallets. These apps and services are enabled by APIs, which provide secure access to data and resources within the bank.

These mobile services are expanding to a wider range of connected devices such as smartwatches and smart home hubs. As banks recognize that mobile is an increasingly preferred channel for their customers, mobile-only banks are beginning to open. Amazon, for example, has recently discussed the possibility of offering checking accounts to its customers to more closely integrate with its retail experience.5 These trends are made possible by APIs which both enable these experiences and fuel innovation that results in further integration and digitalization in banking.

Screenless Banking

Interactions with banks have become faster and more intuitive as technology has, in some cases, removed the need to visit a physical location or even interact directly with the bank. As with all digital experiences, there is a continuing drive in banking to create more seamless experiences enabled by technology. The next evolution in mobile banking is to provide "screenless" interactions.

This concept of screenless banking began with contactless payments on smartphones and smartwatches to deliver faster and more secure retail transactions. These experiences represent a major shift away from traditional interactions with technology, which are typically done through tactile interfaces on smartphones and other touchscreen devices. The next trend in screenless user experiences is to enable voice as a new platform for interacting with technology.

In banking, integrations with connected, virtual assistant devices are driving voice as the next frontier for the mobile experience. Via APIs, banks allow services such as research, balance inquiries and even transfers to take place by voice on these connected device. But just like with mobile, ensuring the identity of the account holder in these transactions is paramount.

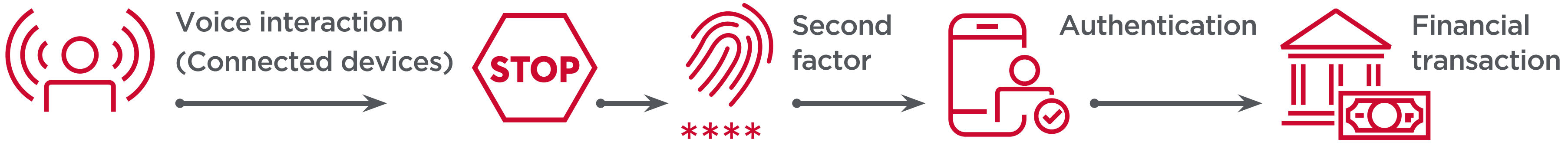
Authentication for Voice-Based Banking

Let's take a look at a real-world example of screenless banking, and the security that makes these user experiences feasible. In this scenario, the bank has enabled a voice-based, virtual assistant device to access a limited range of user account data and functionality.

The account holder asks the virtual assistant to open his banking app. If he wants to complete a high-risk transaction like a fund transfer, the bank can require that the device prompt for additional authentication to ensure the identity of the account holder. This can be accomplished in a number of ways. The user can log into his mobile banking app which will generate a one-time password he can share to authenticate.

Additionally, the virtual assistant can request that the user inputs a registered biometric, like a fingerprint or facial scan, into his mobile device. Or, if the account holder has previously registered his voice with his banking app, he can use voice recognition to authenticate on the connected device, creating a frictionless experience.

Now, these connected devices are able to act as an extension of the mobile banking experience, while the bank maintains security on the backend and user accounts are protected against fraudulent activity. Banks have the flexibility to set internal risk-based policies to create their own standards for which types of activity will require multi-factor or step-up authentication methods.


Voice interaction (Connected devices)

Second factor

Authentication

Financial transaction

An Industry Disrupted by Digital

ALL THESE ADVANCEMENTS ARE LEADING TO DIGITAL DISRUPTION IN THE BANKING INDUSTRY. NEW STANDARDS ARE FORMING THAT WILL CONTINUE TO DRIVE INNOVATION.

As banking has changed from an in-person, retail-like experience to online and now to mobile and connected devices, the industry is adopting new standards and creating regulations for data exchange and security.

The value of these connected banking experiences comes from their ability to take place on any app or device that the bank allows to access its data. Thus, innovation in the space continues to redefine banking and to provide new value to customers.

This is the concept of open banking: the use of open APIs to enable developers to build apps and technology integrations through secure access to the data and systems of traditional banks. Banks currently use internal APIs to build agile, customer-centric experiences on top of legacy systems. By creating open, external APIs, banks can enable third-party developers to create apps and services that expand the value the bank provides to its customers—such as through apps on smartphones, smartwatches and connected devices. Thus, banks spur additional integrations and services without having to invest internal resources.

This will enable a cycle of innovation that continues to change how banking is conducted. But open banking mandates that robust API management and security is in place.

New Experiences, New Challenges

By enabling new digital experiences on mobile apps, third party services, and connected devices, banks are opening themselves to risk by becoming further removed from the user's transaction. They therefore must ensure that they are able to authenticate the user and secure the transaction even though it takes place on a device that is outside the control of the bank.

Full Lifecycle in front of API management solutions address several key concerns:

INTEGRATION ECOSYSTEM

These new banking experiences are enabled by APIs, which provide the integration and scale to support a broader ecosystem of connected devices and interfaces. APIs allow banks to expose internal data and application functionality to approved apps and services, while monitoring and controlling the flow of data. As innovation continues in the banking industry, integration

will play a key role in enabling new digital experiences. Banks and service providers will create, deliver and consume significantly more APIs to support this digital innovation.

EASE OF AUTHENTICATION

Tools like session management and multifactor or risk-based authentication are used to protect consumers and banks in the digital arena. High-value transactions prompt for a step-up authentication method beyond the username and password to provide strengthened security. Additionally, if a user has been inactive for an extended period on a mobile or connected device, the session will expire and he or she will need to re-authenticate to complete a transaction. These risk-based authentication policies create a greater sense of trust for consumers as they adopt digital banking services.

STREAMLINED SECURITY

Finally, with the broad digital ecosystems created by APIs, banks must have a mindset of end-to-end security throughout not only their internal systems, apps and services, but also for new third- party integrations as well. By exposing customer data and account information to services like digital wallets or peer-to- peer payment apps, banks must ensure that data is protected, and that these services have access only to the limited data that the customer has consented to and that the bank has designated. This requires systems' security, app security and API security to protect all consumer and enterprise touchpoints from compromise.

Layer7 API Management provides the speed, scale and security to evolve your digital banking strategy for IoT.

TO LEARN MORE, PLEASE VISIT **THE LAYER7 PRODUCT PAGE**

SEE THESE KEY USE CASES IN ACTION NOW:

CONNECTED BANKING WITH SINGLE SIGN-ON

CONNECTED BANKING WITH BIOMETRIC AUTHENTICATION

BROADCOM®
SOFTWARE

For product information please visit our website at: broadcom.com

BC-XXXXEN August 2021