Global Banking Practice

Blockchain and retail banking: Making the connection

June 2019

Blockchain and retail banking: Making the connection

Retail banks have made great strides in developing digital business models, introducing millions of people to mobile banking and becoming expert providers of data-based services. When it comes to blockchain, however, they have remained mostly on the sidelines.

Retail banking's hesitation on blockchain contrasts with efforts seen elsewhere. Governments, investment banks, and infrastructure providers are experimenting with the technology in the belief that a shared electronic ledger will help them cut costs and increase transparency. Investment banks, for example, envisage a world in which execution, post-trade, and settlement are instantaneous, eliminating numerous middle- and back-office processes. They are also focused on the potential for smart contracts to increase automation.

Large investments are being made in the blockchain arena. Across industries, venture-capital funding for blockchains reached $1 billion in 2017. Wholesale banks have launched hackathons, innovation labs, and collaborations with fintechs. New York-based software firm R3 works with more than 200 institutions to develop blockchain solutions on an open source platform.

Still, caution is understandable.[1] None of the financial industry's initiatives have been rolled out at scale, and tough regulatory requirements in banking create a high barrier to entry. The future regulation of blockchain itself remains uncertain. Some regulators, such as the UK's FCA, are still formulating policy. In the United States, the SEC has blocked attempts to launch blockchain-based ETFs.[2]

Despite those concerns, a few retail banks are dipping their toes in the blockchain pool. Santander, for example, worked with California-based Ripple in 2018 to launch the first blockchain-based money transfer service. Still, for the retail banking industry to move forward at scale, further proofs of value will likely be required. We have identified three pain points—remittances, know-your-customer/ID fraud, and risk scoring—that may represent the best places to start testing.

[1] Matt Higginson, Marie-Claude Nadeau, and Kausik Rajgopal, "Blockchain's Occam problem," McKinsey.com, January 2019.
[2] "Bitcoin ETFs Blocked By Lack Of Safeguards, SEC Chief Says," Bloomberg News, November 28, 2018.

How does it work?

Blockchain is a cryptographic distributed ledger containing a log of transactions stored on computers in a network. Each computer holds a copy of the ledger, so there can be no single point of failure. The system relies on a validation protocol (called a proof), which guarantees individual transactions based on existing records on the ledger. In this way, it is impossible to "sell the same thing twice." The ledger can also be programmed with "smart contracts," which are sets of conditions written as a program. These run until they validate a condition that automatically determines what happens next. In banking, smart contracts could, for example, be used to automate a payment if condition x or y is met. Blockchain technology offers capabilities in three areas:

— *Data handling:* Blockchains are distributed, trustless, and immutable (the record cannot be changed once it is written), which protects data and creates resistance to cyber-attacks. In addition, each transaction contains metadata, including a date and time stamp, creating certainty of execution. Data is also more available, transparent, and standardized than when contained in fragmented systems. It is shared via customer-agreed smart contracts (rather than third parties), enabling compliance with new regulations such as the EU's General Data Protection Regulation. These data-handling abilities offer opportunities for retail banks, including better risk scoring (for example by using personal data captured in smartphones). There are caveats, however: blockchains' processing speeds are faster than some current practices, but capacity is lower. There are also limitations on storage capacity, due to the high level of replication that makes the networks secure.

— *Disintermediation:* Distributed ledgers enable transactions to be verified without the need for a central authority, leading to cost savings and operational efficiency.

— *Establishing trust:* Distributed ledgers are "trustless"; they do not require intermediaries to underwrite transactions. That means they are implicitly reliable. All entries in the ledger may be accessible to members of the network at all times. This creates savings in retail banking processes that require duplication, such as onboarding.

The potential for retail banking

Early enthusiasm for blockchain technology among capital market infrastructure firms and wholesale banks has not been widely mirrored in the retail sector. Still, we believe there are three retail use cases that could eventually be deployed at scale, and which offer most in terms of blockchain's three key strengths—data handling, disintermediation, and trust. These are remittances, KYC/ID fraud prevention, and risk scoring.

Remittances

Cross-border payments total around $600 billion annually, and the market is set to maintain its recent growth of around 3 percent a year, driven by international trade. However, payments processing tends to be clunky, opaque, and highly mediated. As a result, costs are high. Fees are commonly 2 to 3 percent of transaction value and can be as much as 10 percent.

The emergence of numerous fintechs in payments (around one in four is focused on the segment) is increasing competition and leading to more efficiency in some parts of the value chain. In addition, incumbents are developing their own solutions. SWIFT, for example, is working with banks through its global payments innovation initiative to improve the cross-border payments experience. Still, blockchain may be able to generate value by fixing certain inefficiencies. If counterparties were to exchange crypto-assets (digital currencies that do not need a central regulating body) rather than fiat currencies, for example, payments could be made and settled in minutes via blockchains, rather than the current days. The distributed nature of blockchains would mean greater transparency and immutability (data recorded to blockchains cannot be altered). McKinsey estimates that blockchains applied to cross-border payments could save about $4 billion a year.

Some blockchain providers are already active in payments. Ripple connects banks and payments providers via RippleNet, allowing them to make payments with fiat currency or Ripple's own XRP crypto-asset. The network is based on a private, non-distributed ledger, which relies on a limited ecosystem of correspondent banks. Financial institutions are also making progress. J.P. Morgan, Royal Bank of Canada, and Australia & New Zealand Banking Group in late 2017 launched the Interbank Information Network (IIN), a cross-border payments service. "By leveraging blockchain technology, IIN will significantly reduce the number of participants currently needed to respond to compliance and other data-related inquiries that delay payments," J.P. Morgan said in a statement.[3]

Despite the growth of blockchain-based payments solutions, however, there remain significant barriers to adoption at scale. One issue is that blockchain networks are transparent to their members, meaning that there are limitations to anonymity in some scenarios. In response, several companies are experimenting with "tokenization," which disguises sensitive data by substituting it with a token that serves as a reference. However, this approach is still in the early stages of development. Another challenge is that real-time settlement is currently impossible due to lack of fungibility between crypto-assets and fiat currencies. There is inevitable friction in converting

[3] *J.P. Morgan Deploys Blockchain with New Correspondent Banking Network,* Business Wire, October 2017.

back and forth, particularly given recent volatility (the value of Bitcoin fell by 75 percent from December 2017 to November 2018). So-called stablecoins, the value of which are pegged to a real-world asset, are one solution, but they still require correspondent banks to make the eventual conversion.

Know-your-customer/ID fraud prevention

Know-your-customer protocols are critical tools in the battle against fraud, which is a significant and growing challenge. Banks lose $15 billion to $20 billion annually from identity fraud alone, according to Javelin research. Banks are also under intensifying regulatory pressure to protect customer data. The EU's General Data Protection Regulation, which went into effect in May 2018, strengthened the data rights of citizens and harmonized protection rules. Some European banks have invested as much as €30 million to ensure they are in compliance. A related issue is money laundering. A WealthInsight report estimates that global anti-money laundering (AML) spending alone exceeded $8 billion in 2017, up 36 percent from 2013. AML headcount increased as much as tenfold at major US banks over the past five years.

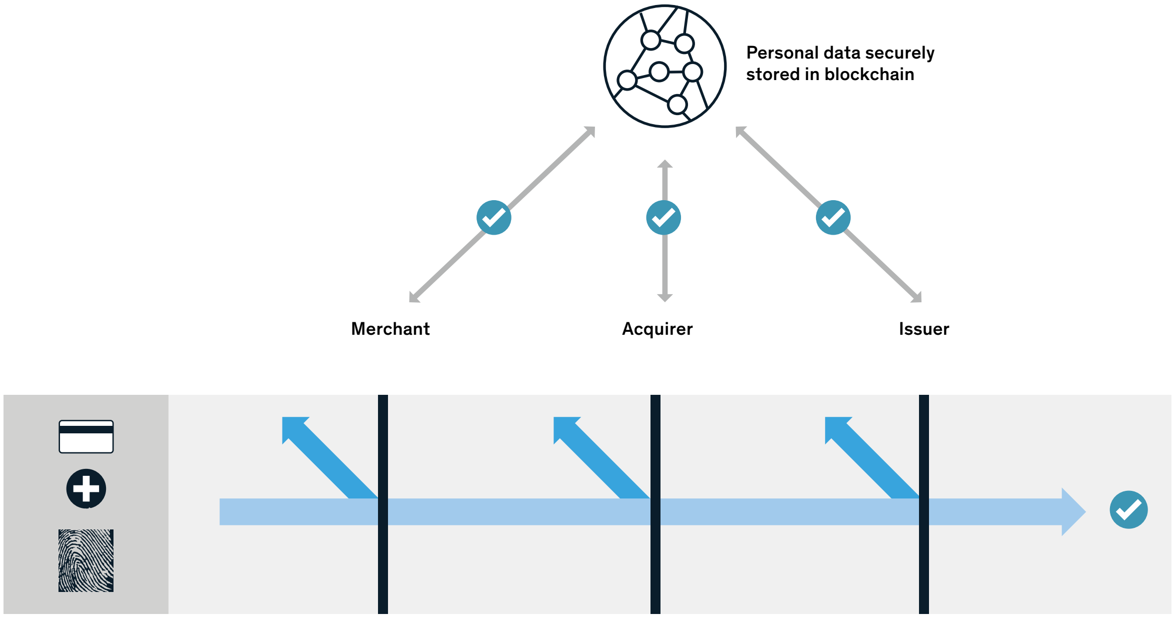
Retail banks have made significant efforts to combat fraud, protect data, and prevent money laundering, investing in automation and standardization, introducing real-time information sharing, and building predictive models. These initiatives have increased efficiency but have led to longer onboarding times and higher costs, reflecting the significant operating model changes and manual effort required.

Blockchain may be a potential solution. For onboarding or account opening, blockchain-based technology enables customers to use a digital fingerprint, which like an actual fingerprint can be used as a unique identifier. It can be stored on a distributed ledger and referenced by any bank in the network. The owner of the digital fingerprint can use it to submit new account applications and prove her identity universally.

The decentralized blockchain structure eliminates overlapping KYC and AML compliance checks (banks share authenticating information), lightens the information burden, and allows banks to disseminate data as it is updated (Exhibit 1).

Exhibit 1

A decentralized blockchain structure would eliminate overlapping compliance checks.



Source: McKinsey analysis

We estimate blockchain-based solutions for customer onboarding can create up to $1 billion of savings in operating costs for retail banks globally and reduce regulatory fines by $2 billion to $3 billion (Exhibit 2). In addition, we expect blockchain solutions to reduce annual losses from fraud by $7 billion to $9 billion.

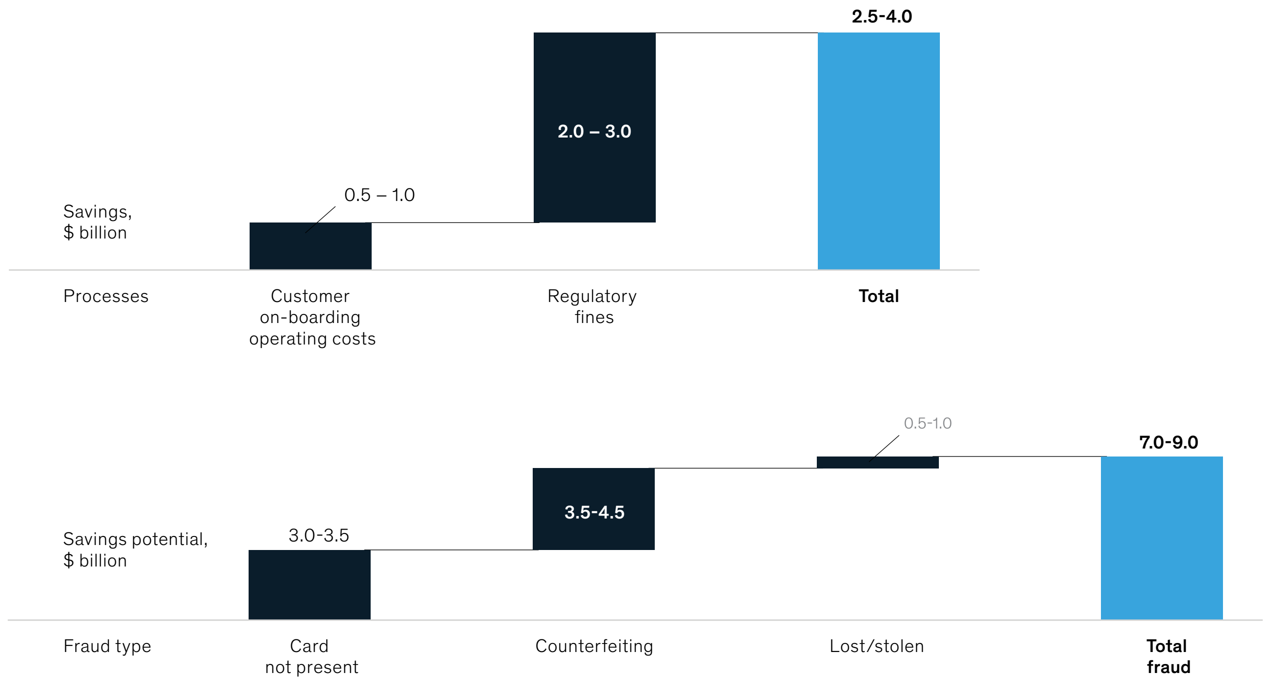
Blockchains are being tested and rolled out in ID fraud detection through, for example, the creation of digital identify networks. Bluzelle Networks, a blockchain-based data storage start-up, in 2017 worked with a consortium of three banks in Singapore—HSBC, OCBC, and Mitsubishi UFJ Financial Group—to test a platform for KYC. The project showed that a blockchain platform would improve efficiency, cut the risk of financial crime, and heighten responsiveness to performance and scheduling needs. It was predicted to reduce costs by 25 to 50 percent. SecureKey, a Canada-based fintech, developed a digital identity and authentication service that simplifies consumer access to online services, including digital banking. The service was developed through a collaboration with IBM and banks including National Bank of Canada, ScotiaBank, and TD. Elsewhere, Norbloc, a Swedish start-up that builds regulatory applications on blockchain platforms, is working with Belgium-based infrastructure provider Isabel Group to build a platform to simplify identity management. Mastercard has patented a system for identity and credential protection and verification via blockchain. Other start-ups working in the identify area include Cambridge Blockchain, Spring Labs (started by online lender Avant), and Blockstack, owned by Digital Asset Holdings.

Through individual management of private keys (a kind of digital signature used to approve transactions) blockchain technology also enables customers to control their personal data and share it without the help of an intermediary. Several operating systems and browsers provide key stores to protect private keys, and private vendors offer wallets or similar alternatives that are resistant to cyber-attacks.

Exhibit 2

Blockchain solutions for onboarding, regulatory compliance, and fraud could save banks significant amounts.

Global retail banks



Source: McKinsey Global Banking Pools; McKinsey Global Payments Map

Challenges in KYC and anti-fraud

Despite numerous experiments and proofs of concept, retail banks face challenges in implementing blockchain-based KYC and anti-fraud solutions. First, there are heavy capital costs associated with switching from individual to shared systems. In addition, banks must adapt to a significant evolution in culture, which is predicated on the need to share data. This is a relatively alien concept in an industry inured to the primacy of confidentiality, and raises questions over accountability: If Bank A completes the onboarding KYC of an individual and shares the data on a blockchain, is Bank B responsible for errors or fraud on its own account? In addition, is there sufficient incentive for Bank A to share its data? Data sharing has a cost because it risks undermining banks' ability to offer personalized services.

There are also practical challenges. Customers must agree to upload digital fingerprints and perform additional authentication steps during set up. Merchants are required to upgrade authentication systems at point of sale and adjust online checkout processes. Banks must create large networks to achieve benefits at scale, requiring data standardization and collaboration. Finally, there is the question of whether any bank would be willing to take the lead on creating a utility that offers no competitive advantage—the so-called *coopetition paradox.* (See "Blockchain's Occam problem," McKinsey.com.)

Risk assessment using customer data

Financial institutions are often required to make risk management decisions based on limited data, obtainable from a few brokerages and agencies. In some cases, the data does not even exist. The unbanked (estimated to be 40 percent of the world's population), the underbanked, and micro-SMEs may not have made enough non-cash financial transactions for assessing their credit-worthiness. As a result, banks tend to be conservative when making credit decisions.

Blockchain technology offers the potential for pooling large volumes of data that can be anonymized and protected by the ledger's encryption protocols. Data carried on a distributed ledger could be accessed without explicit at-the-time permission (customer consent can be granted via pre-programed smart contracts). Banks could theoretically view data that has been uploaded by any bank in the network. The result should be faster decisions, more efficient processes, and the potential for a more informed credit allocation process.

However, there are technical and cultural challenges. For example, there is need for significant processing power to run scoring models using data that is distributed across thousands or millions of sources. In addition, customers may choose to restrict access to protect their own privacy and security. Financial institutions are likely to need to work hard to bring them on board.

Fintechs have started to operate in this area. Spring Labs, for example, launched a decentralized network for credit assessment, raising about $15 million in an ICO in March 2018. Fintechs are also finding strong use cases in emerging markets, where liquidity can be short or access to financial resources challenging. One example is Turkish startup Colendi, which supports large merchants and retailers to enable installment purchases for individuals and micro SMEs at the point of sale. Overall, however, these are relatively small initiatives, suggesting there is some way to go before we see scaled up solutions.

The way ahead

Blockchain technology could bring value in core parts of the retail banking business model. However, retail banks have been slow to engage, and the technology faces challenges in terms of scaling, the volatility of crypto-assets, and trust. In addition, there is little evidence that incumbents have bought into the need to collaborate and share data. Despite that, we see three things that could help increase adoption:

— There needs to be a more seamless transition between fiat and digital assets, so that customers do not risk losses as they switch back and forth. One solution would be for central banks to issue a crypto fiat, which would support product manufacturing. It would also enable real-time peer-to-peer payments and potentially cross-border interbank clearing and settlement.

— Regulation is required so that participants have certainty around the status of crypto-assets, rules of engagement, and investor protection.

— Consumer identities should be created on the blockchain, enabling banks to offer real-time loan decisions based on authenticated ID. The government of Dubai is currently piloting such a project.

Finally, there needs to be a strategic watershed. Executives need to believe that the long-term benefits of blockchain are worth the cost. That requires taking a long-term view and working with the possibility that blockchain may lead to cannibalization of some revenue streams. The key to countering those concerns is to keep an eye on the prize, which is lower costs, less friction, and a safer retail banking system.

Matt Higginson is a partner in McKinsey's Boston office, **Atakan Hilal** is a partner in the Istanbul office, and **Erman Yugac** is an engagement manager in the London office.

The authors wish to thank Gökhan Sari and Sven Blumberg for their invaluable help and insight and Alp Ezgu and Kaan Basaran for their support in researching and writing this article.

June 2019

www.mckinsey.com/industries/
financial-services/our-insights

@McKBanking