Open Banking: An Analysis of Technological and Policy Issues

by Nir Kshetri[53]

Abstract

Open banking has been a trend that is gaining a broader acceptance among financial institutions and consumers. Digital technologies such as application programming interfaces (APIs), cloud computing, artificial intelligence and machine learning and blockchain have helped financial institutions develop new open banking capabilities to be responsive to the needs of individuals and businesses. Understanding the technological and policy factors underlying open banking is critical for the further growth of this new market. This article analyzes the roles of these technologies and tools in facilitating the growth of open banking. Also discussed are lessons learned and policy implications.

Introduction

Open banking has gained increasing acceptance among financial institutions and consumers. *According to the market research* company Research and Markets, the size of the global open banking market was US$ 7 billion in 2018, which is expected to reach US$ 43 billion by 2026 (Research and Markets, 2022). One estimate suggested that as of early 2021, up to 87% of countries offered *open banking* in some form (Sieber, 2021). The rapid growth of this phenomenon is driven fundamentally by digital *technologies and tools*

---

53. The University of North Carolina at Greensboro, USA.

such as application programming interfaces (APIs), *cloud* computing, artificial intelligence (AI) and machine learning (ML), and blockchain. Emphasizing the importance of many of these technologies in open banking, Swiss technology company Temenos, which *specializes in enterprise software for financial services, put the issue this way:* "[Open banking participants] require a resilient, secure and scalable technology platform that is cloud-native, API-first, built on microservices and enabled by AI" (p. 3).

The availability and responsible use of these technologies are key to the success of open banking. Adequate public policies will obviously play a major role in ensuring such conditions and facilitating the growth of the open banking industry and market. For instance, it is crucial to understand unintended consequences and potential biases in AI algorithms when they are used in open banking. Socially sensitive data such as gender, ethnicity, family status and other demographic data may lead to unintended consequences when the providers of financial services utilize such data to develop strategic pricing models. Analytics and algorithmic pricing could change the pricing and access to credit for very marginalized groups (deloitte.com, 2018). The success of open banking scheme hinges critically upon the measures taken to enhance the customer experience, protect information privacy and strengthen cybersecurity (deloitte.com, 2018).

This article gives an overview of key technologies and tools that are facilitating or likely to facilitate the growth of open banking. It also focuses on lessons learned and discusses policy implications.

Key enabling technologies

This section focuses on key digital technologies that are being utilized or have the potential for use in the future to facilitate the growth of the open banking industry and market.

Application programming interface

In *open banking*, financial institutions interact with each other at the customer's direction on an a la carte basis (Voas et al., 2022). *Open banking* customers may include individuals, trusts, estates, private businesses, public

sector entities, investors and even other banking entities (Laplante and Kshetri, 2021). Such interactions are facilitated by APIs. An API is a set of programming codes and protocols that works as an intermediary to allow two applications to talk to each other. API banking specifically *involves a set of protocols to make a bank's services available to other* third-party providers *via APIs* (Rao, 2020). It provides a real time solution for processing transactions in a secure manner (ICICI 2022). For instance, third-party providers need a lot of personal information to develop a customer-oriented application. API can extract the required information from external servers. For example, if a third-party provider needs information about a customer's transaction history, it can submit a request to an API Banking. The requested information is retrieved from the bank database and sent it back to the third-party provider. This process is referred to as API Call (PayCEC, *2022).*

An encouraging trend is that financial institutions have introduced APIs for diverse client types, platforms and operating systems to fulfill various *open banking* needs, which is likely to facilitate the growth of *open banking.* As early as in 2020, India's ICICI Bank's API Banking portal had 250 APIs that allowed businesses, fintech companies, and e-commerce start-ups to connect with the bank (Corneille, 2020). Likewise, Singaporean multinational banking and financial services corporation DBS's developer portal offers over 200 APIs. The APIs have facilitated payment and loan innovation with firms such as ride-hailing and food delivery company Grab, online property search company PropertyGuru and multinational fast food chain McDonald's (Open Future World, 2022).

Cloud computing

Open banking requires financial institutions to perform real time processing of a large amount of data from diverse sources. These institutions' on-premises legacy systems often lack the capabilities to meet the needs of open banking, which entail dealing petabytes of data in real time in order to authenticate various transactions initiated through APIs. It is not possible to aggregate and analyze these data on existing on-premises systems that lack the required agility (Finextra 2020).

In order to handle the open banking ecosystem's requirements, banks thus need to have a platform that is resilient and scalable. Cloud computing is an ideal means to deal with such challenges. The scalability of cloud offering makes it possible to collect, store, analyze and distribute data easily. Financial institutions can access *cloud services on demand* and pay only for what they consume (Finextra 2020). Cloud computing solutions can thus help banks *reduce the expense and overhead* costs associated with handling huge data volumes since they are not required to run hardware on premises. Such solutions also offer the flexibility required in handling data volume fluctuation (Beatty, 2020). In addition, cloud computing can also be used to organize big data and a test environment for developers to innovate securely (Beatty, 2020).

Cloud computing also provides a safe and secure environment for sensitive data and reduces cybersecurity and other risks (Beatty, 2020). Infrastructure as a service (IaaS) providers such as AWS offer cybersecurity services that are more advanced than what any organization can achieve by themselves (Finextra 2020).

Artificial intelligence and machine learning

AI involves simulation of human intelligence by machines to perform tasks that seemed to be possible only with human thinking and logic before. ML is a type of AI that helps increase accuracy of software applications in predicting outcomes without explicit programming. AI and ML help banks to analyze huge volume of data effectively. Euro Banking Association has identified three strategic areas in financial services that are likely to be impact by AI and ML: processes, products and services, and markets (EBA, 2020). In a use case discussed in Voas et al. (2022), members of a household struggle to manage multiple recurring payments such as mortgage, credit cards, car insurance, home insurance, life insurance, healthcare, property and income taxes, and utilities. In such situations, *AI can learn by* observing the transactions to provide additional insights that can help optimize cashflow, and minimize late payments, and thus improve the credit rating for members of the household (Voas et al., 2022).

Blockchain

In open banking transactions, financial institutions can ask potential customers about their willingness to give financial services providers access to their data. A potential problem is that if individuals and businesses say they are willing to do so in order to get access to financial services, they need to give access to all of their financial and personal data (Ben-Ari et al., nd). Surveys have found that consumers are reluctant to share their bank details with third parties. A key point that needs to be emphasized here is that financial transactional and personal data are more sensitive compared to other forms of information. For instance, a survey conducted by De Nederlandsche Bank (DNB) found that only 25% of Dutch consumers shared their payment data in 2020 in order to get access to new services. Most of the consumers had shared data only with their existing banks. Consumers had more confidence in the bank of that had their main payment account, compared to other parties. The survey found that consumers are not likely to provide their data to new player entering into the payment market in the future (Finextra 2021).

The above challenge can be potentially addressed with blockchain-based self-sovereign identity, which gives consumers control over their information they use to prove who they are. This means that consumers choose what information to share, with whom, and when. Financial institutions and other parties they transact with gain access to consumer data when the data subjects grant it to them. The data can only be used for its intended purpose (Grant, 2022).

Financial institutions can also benefit from blockchain-based self-sovereign identity since valuable resources are not wasted in building trust with consumers. In such a model, the burden of responsibility for data privacy and security is with consumers rather than the financial institutions (Grant, 2022). It is also important to note that due to privacy regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act and other factors, financial institutions and other companies have adopted personal data minimization policies (Kshetri, 2021a). Such policies can help protect themselves from liabilities arising from a negligent act related to data handling. Blockchain adoption is compatible with such policies since financial institutions do not store customer data in a blockchain model.

In blockchain-based solutions, personal data can be seen only with the subject's permission and such data cannot be stored by a third party. Moreover, the proof of identity is stored in a cryptographic format. This means that blockchain-based systems can be designed to provide a high level of privacy protection. Indeed, secure storage and transmission of digitally signed documents have the potential to be most popular blockchain applications. Due to blockchain's "super audit trail", such applications have been built and tested in diverse areas such as supply chain and trade financing, logistics and shipping, and insurance in order to validate the identity of individuals as well as digital and physical assets (Mainelli, 2017; Kshetri, 2021b).

In order to illustrate the above point, we can consider the Canadian identity and authentication provider SecureKey and its network Verified.Me. SecureKey received investments from Canada's big banks including CIBC, BMO, Desjardins, TD, and Scotiabank (Galang, 2017). The Verified.Me service is available on both cellular devices and desktop, which helps users verify their identity to access services provided by financial institutions. It is built on IBM Blockchain Platform, which uses the Linux Foundation's Hyperledger. Users can prove that they are who they say they are faster and with a high level of privacy protection (Comben, 2019). The company uses a blockchain-based "triple blind" privacy protocol to connect individuals to partnering online services using an existing credential. The "triple blind" mechanism means that consumers can use their bank credentials to log in and access their cellular phone services. The bank cannot see the data's destination and the recipient cannot see the bank used or bank account information. SecureKey, as a middleman, is also "blind" and cannot see information about the user of the services (Ho, 2017).

An additional benefit of blockchain is that it can improve reliability of financial and other reporting, and compliance with various laws and regulations (deloitte.com, 2020). By maintaining immutable records of the process and history of transactions, this technology can make regulatory reporting and compliance simpler, more automated and more efficient (Fintech Times, 2021).

Lessons and policy implications

Open banking's potential to address the challenges facing the financial sector has not yet been fully realized. Especially, privacy and security issues have been of concern among large proportions of lenders and consumers, which have hindered the adoption of open banking (Laplante and Kshetri, 2021; Rose, 2021). The potential of AI and other technologies to improve the security and efficiency the financial system has not been fully realized (EBA, 2020).

Partnerships and collaborations at various levels are needed to facilitate the adoption of the above technologies and their responsible use. For instance, currently AI is mainly being used to enhance operations and improve products and services (EBA, 2020). Several organizational factors such as availability and accessibility of data, resources and concerns about cybersecurity and societal challenges related to bias, transparency, and liability are among major barriers that hinder the adoption of AI (EBA, 2020). It is important for financial institutions to work collaboratively to address these issues. For instance, AI can be used to identify threats facing the banking industry. Financial institutions should make full use of the data that are made available and accessible through open banking. In order to extract valuable insights from data, efforts also need to be directed toward increasing the quality of the data (EBA, 2020).

National governments can also play a key role in facilitating the development of digital infrastructures to enrich the *open banking* ecosystem. In some countries, the governments have already taken initiatives and actions on this front. In India, for instance, the digital infrastructure known as the India Stack has been a key part of the *open banking* ecosystem. The *India Stack* consists of a set of open *APIs* along with a universal digital ID system Aadhaar, which makes it possible for the government and private companies to develop and deploy cashless and paperless products (SignDesk nd). The Aadhaar identification system consists of a 12-digit unique identity card launched by the government in 2010 enables biometric checks to verify the identity of individuals and digitally authenticate them for a variety of services. As of July 2022, there were 1.33 billion users registered for the Aadhaar (https://www.biometricupdate.com/202207/uidai-ceo-lauds-successes-of-aadhaar -biometric-id-at-india-digital-week-2022). Financial institutions can also conduct electronic know-your-customer (eKYC) of customers using the

Aadhaar system, which reduces their costs of verifying the identity of customers. Various APIs are available to facilitate *open banking*. For instance, Aadhaar holders can use online electronic signature service eSign to digitally sign a document. Likewise, the Ministry of Electronics and Information Technology has provided digital locker facility for documents known as DigiLocker (Fintechnews Singapore, 2021).

The India Stack also includes an interoperable payments system known as the Unified Payment Interface (UPI) (Carriere-Swallow et al., 2021). A key goal of the India Stack is to create a unified software platform for stakeholders such as government agencies, businesses, startups and developers. The UPI allows consumers to access bank accounts from registered apps such as mobile wallets in order to make transactions to any bank. As of early 2021, the UPI accounted for about 30% of retail transactions (Fintechnews Singapore, 2021).

Public private partnerships can also be used to enrich open banking ecosystem. For instance, as discussed above, AI is a key technology facilitating the development of AI. However, AI is at a nascent stage of development. The use of AI in open banking can lead to many policy and ethical dilemmas. Regulators and financial institutions can team up to develop standardized AI specifications for various areas related to open banking such as information exchange, infrastructure, governance, and security. It is important for such specifications to cover AI algorithms and models for validating and verifying mandatory regulatory compliance, audits, market risks analysis, anomalies, and outliers (Kannan, nd).

Finally, national governments and international developmental organizations can also collaborate to make digital technologies, and infrastructures available to various open banking participants, which can help accelerate the diffusion and adoption of *open banking*. The Association of Southeast Asian Nations (ASEAN) Financial Innovation Network (AFIN), which was formed by the Monetary Authority of Singapore (MAS), the International Finance Corporation (IFC) and the ASEAN Bankers Association has introduced API Exchange (APIX) (Monetary Authority of Singapore, nd). A key goal of the APIX is to support financial innovation and inclusion in the ASEAN economies by providing a global, open-architecture platform. In addition, the MAS has introduced an API guidance and collaboration platform,

which has encouraged financial institutions to open up their data and services (Open Future World 2022). Third party providers can integrate and test solutions with each other via a cloud-based architecture (Voas et al., 2022).

Concluding comments

A number of digital technologies are driving open banking, which has the potential to promote financial inclusion and provide better access to a wide range of financial products and services to individuals and organizations. For instance, *open banking* makes it possible for borrowers to obtain better terms and pricing. Among the technologies and tools discussed above, while blockchain is not currently being used widely in open banking, this technology holds tremendous potential to address privacy concerns of consumers, which has been a key barrier to the expanded use of this new financial product.

Measures at the firm, industry, national, and international levels are needed to further accelerate the diffusion of *open banking*. For instance, at the firm level, financial institutions need to develop tools, policies and procedures regarding cloud data management and a responsible use of AI. Close collaboration among financial institutions can help achieve various goals of open banking. In addition to inter-firm collaborations at the industry level, public-private partnerships are needed to address privacy, security and other challenges such as those related to AI ethics and model bias.

References

Beatty, A. (2020). How the cloud is the path to open banking, 7th December, https://www.fin-techfutures.com/2020/12/how-the-cloud-is-the-path-to-open-banking/

Ben-Ari, A., Green, M., Butcher, I., and O'Neill, P. (nd). Securing open banking with blockchain and Intel® SGX technology, White Paper, https://www.intel.co.uk/content/dam/www/central-libraries/us/en/documents/final-pdf-applied-blockchain-and-intel-sgx-12.pdf

Carriere-Swallow, Y., Haksar, V., and Patnam, M. (2021). India's Approach to Open Banking: Some Implications for Financial Inclusion, February 26, https://www.imf.org/en/Publica-tions/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Fi-nancial-Inclusion-50049

Comben, Ch. (2019). Why Canadian banks are choosing the SecureKey blockchain system May 9, https://coinrivet.com/canadian-banks-choosing-securekey-blockchain-system/

Corneille, E. (2020). 4 top Indian private banks' APIs enabling innovations in open banking October 07, https://ibsintelligence.com/ibsi-news/4-top-indian-private-banks-apis-enabling-innovations-in-open-banking/

deloitte.com (2018). Open banking What does it mean for analytics and AI? September 2018, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-analytics-ai-060918.pdf

deloitte.com (2020) Blockchain and internal control: The COSO perspective: New risks and the need for new controls, July https://www2.deloitte.com/us/en/pages/audit/articles/blockchain-and-internal-control-coso-perspective-risk.html

EBA (2020). Artificial Intelligence in the era of Open Banking, August, pp. 36–37. Euro Banking Association, https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/management-summary-artificial-intelligence-in-the-era-of-open-banking/

Finextra (2020). How the cloud adds value to open banking business models and strategy, 13 November, https://www.finextra.com/newsarticle/36927/how-the-cloud-adds-value-to-open-banking-business-models-and-strategy

Finextra (2021) Open banking will only succeed if consumers are 'onboard' 09 March 2021 https://www.finextra.com/blogposting/19992/open-banking-will-only-succeed-if-consumers-are-onboard

Fintech Times (2021). Hardbacon: 5 Fintech Trends That Will Reshape the Financial Services Landscape, The Fintech Times, https://thefintechtimes.com/hardbacon-5-fintech-trends-that-will-reshape-the-financial-services-landscape/

Fintechnews Singapore (2021), India's Open Banking Landscape Thrives on the Back of Digital Public Infrastructure, March 15, https://fintechnews.sg/49565/india/indias-open-banking-landscape-thrives-on-the-back-of-digital-public-infrastructure/

Galang, J. (2017). With IBM partnership, SecureKey enters next phase of developing secure digital identity network. Betakit, Retrieved from (http://betakit.com/with-ibm-partnership-securekey-enters-next-phase-of-developing-secure-digital-identity-network/).

Grant, J. (2022). The role of blockchain in the Open Banking era, January 24, https://fintech-weekly.com/magazine/articles/the-role-of-blockchain-in-the-open-banking-era

Ho, S. (2017). Canada's SecureKey receives U.S. grant to build digital identity network. The Globe and Mail, http://www.theglobeandmail.com/technology/canadas-securekey-wins-us-grant-to-help-build-digital-identity-network/article34022647/ .

Hope, K. (2022). Open Banking and the Rise of Bankingas-a-Service https://www.temenos.com/wp-content/uploads/2022/06/Open-Banking-and-the-Rise-of-Banking-as-a-Service-V4.pdf

ICICI (2022). What is API Banking? https://www.icicibank.com/business-banking/cash-management-services/api-banking

Kannan, V. (nd). Open intelligence – AI in banking and financial services https://www.tcs.com/what-we-do/industries/banking/white-paper/ethical-ai-solutions-strategies-banking-financial-institutions

Kshetri, N. (2021a). Cybersecurity Management: An Organizational and Strategic Approach, The University of Toronto Press: Toronto

Kshetri, N. (2021b). Blockchain and Supply Chain Management. Elsevier: Amsterdam, Netherlands, Oxford, the U.K. and, New York, USA

Laplante, P., and Kshetri, N. (2021).Open Banking: Definition and Description, IEEE Computer, 54(10): 122-128

Mainelli, M. (2017). Blockchain Will Help Us Prove Our Identities in a Digital World. Harvard Business Review, Retrieved from (https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world).

Monetary Authority of Singapore. (nd). API Exchange (APIX), https://www.mas.gov.sg/development/fintech/api-exchange

Open Future World (2022). Open Finance Global Progress Ebook: Singapore Special Editorial Focus, May 16, https://openfuture.world/open-finance-global-progress-ebook-singapore-special-editorial-focus/

PayCEC. (2022). The history, overview, and future of Open Banking In The UK, 15 Aug, https://www.paycec.com/news/the-history-overview-and-future-of-open-banking-in-the-uk

Rao, H. (2020). What is API Banking and How it is Enabling? JULY 30, https://razorpay.com/learn/business-banking/what-is-api-banking/

Research and Markets (2022). Insights on the Open Banking Global Market to 2031 - by Financial Services, Distribution Channel and Region, October 28, https://www.globenewswire.com/en/news-release/2022/10/28/2543585/28124/en/Insights-on-the-Open-Banking-Global-Market-to-2031-by-Financial-Services-Distribution-Channel-and-Region.html

Rose, K. (2021). 41% of lenders taking 'wait and see' approach to Open Banking, March 31, 2021, https://bestadvice.co.uk/41-of-lenders-taking-wait-and-see-approach-to-open-banking/

Sieber, S. (2021). "Open Banking: What Does It Mean For The US?" March 3, https://www.forbes.com/sites/scarlettsieber/2021/03/03/open-banking-what-does-it-mean-for-the-us/?sh=180aa28db52a

SignDesk (nd) How India Stack Transforms India into a Cashless Economy?, https://signdesk.com/in/aadhaar/india-stack-transforms-india-cashless-economy

Voas, J., Laplante, P, Kassab, M., Lu, S., Ostrovsky, R., Kshetri, N. (2022). Cybersecurity Considerations for Open Banking Technology and Emerging Standards, January 3, The National Institute of Standards and Technology, https://csrc.nist.gov/publications/detail/nistir/8389/draft