Legal Independency of Virtual Banks, Their Preservation and Security

Zahra Asefkabiri[1*], Mostafa Elsan[2], Mehrab Darabpour[3]

1. PhD Student in Private Law, Faculty of Humanities, North Tehran Branch, Islamic Azad University, Tehran, Iran.

*Corresponding Author: Email: Asefkabiri.z@gmail.com

2. Associate Professor, Department of International Trade Law and Intellectual Property Law and Cyberspace, Faculty of Law, Shahid Beheshti University, Tehran, Iran.

Email: M_elsan@sbu.ac.ir

3. Professor, Department of International Trade Law and Intellectual Property Law and Cyberspace, Faculty of Law, Shahid Beheshti University, Tehran, Iran.

Email: info@drdarabpour.ir

S.D.I.L.
The SD Institute of Law Research & Study

Publisher:
Shahr-e- Danesh Research And Study Institute of Law

Article Type:
Original Research

DOI:
10.48300/jfel.2024.452421.1027

Received:
14 April 2024

Accepted:
13 August 2024

Published:
21 September 2024

ABSTRACT

In a rapid growing and developing world of technology, it is one of the very serious plans of banking industry to create opportunities for implementing virtual banking. Virtual Bank is a corporate entity which obtains full credentials of banking services from the banking regulatory system, and has an independent legal entity. The emergence of unexpected and unpredictable issues such as the compulsory keeping social distance among people as the result of such pandemics as Covid-19 and applying cost effective methods in space and time, have all pushed forward, more than ever, an urgent global movement toward establishing virtual banking, and on its turn, the industry has made it inevitable to establish virtual banking system on a nation-wide scale. Therefore, for the purpose

of utilizing the privileges of virtual banking, we need to recognize and manage the legal challenges which might be arisen in relation to the industry. This project firstly intends to make a comparative study of virtual banks so that recognition is made of the legal independent entity, its specifications, the requirements of creation and the application of virtual banking industry; then, in view of the fact that all data of these kinds of banks are interchanged in a virtual environment where they are more exposed to cyber-attacks hazards, we look for the kind of legal instruments which are reflected to be created for safekeeping and safeguarding such data.

Keywords: Virtual Bank- Neo Bank- Doctrine of Mitigation of Damages- Blockchain Technology- Regulatory Sandbox.

Funding: The author(s) received no financial support (funding, grants, and sponsorship) for the research, authorship, and/or publication of this article.

Author contributions:

Zahra Asef Kabiri: Conceptualization, Methodology, Software, Formal Analysis, Investigation, Resources, Writing - Original Draft, Writing - Review & Editing, Visualization.

Mostafa Elsan: Validation, Data Curation, Supervision, Project Administration.

Mehrab Darabpour: Validation, Data Curation, Supervision, Project Administration.

Competing interests:

The authors declare that they have no competing interests.

Citation:
Asef Kabiri, Zahra, Mostafa Elsan & Mehrab Darabpour. "Legal Independency of virtual banks, their preservation and security", Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

Extended Abstract

In recent years, one of the serious plans in the banking industry has been maximizing the application of technology and implementing the virtual banking. Global developments and the recent actions taken by countries, such as Hong Kong and Malaysia, in respect of virtual banking and its rapid spread in the world, indicate a fabulous reception of this kind of banking system in various countries. In respect of virtual banking development, Iran had a very good start and although long years have passed since the time the Regulations for virtual banking was approved, but no virtual banking was established and did not start its operation; it is so, while this kind of banking system may evolve the Iranian banking industry and may play a strategic role in getting the national economy out of the present situation.

United States of America is the pioneer in virtual banking system in the world. It is some years that virtual bank in this country has been set in operation and effective actions have been taken by far in this area; having account of ever-increasingly growth of digitally literate clients who are seeking simplicity, transparency and useful services, this system is expanding very quickly.

Thus, this kind of banking system has been providing its services to the clients in the world for years; however, such structure may confront too many legal challenges. One of the controversies is the exact definition of virtual banking. In fact, the question which should be responded is that whether a virtual bank is really a bank, or is it only a virtual branch of the traditional type of the banks? What are the characteristics of the traditional banks and virtual banks? Why a virtual bank is basically required to be existed, and what is the secret point of its success? Also, since virtual banks use digital storage of whatever data they have, they might pose as greater target for cyber-attacks. Therefore, security is one of the critical concerns to be considered in virtual banks; for this reason, some guidelines are provided in this research for enhancing their security.

Findings & Conclusion:

Virtual bank is a real bank too. This bank is a kind of corporation that obtains its full authorization of banking services from the regulatory or issuing authority concerned, however, without having any branch. This bank is not a virtual branch of another traditional bank. Despite virtual neobank which is the branch of a traditional bank, nonetheless, virtual bank might not be taken as synonymous as neobank, on this ground.

Neobank, however, renders its activities based upon the support of a

traditional bank; although, they might have an independent character and identity, but they are lacking an authorization of an independent banking system. Neobank, in interaction with another traditional bank, provides its online services, without having a physical branch. In fact, Neobanks practice as a digitally operating branch of traditional banks. Therefore, the value of a virtual bank must not ever be considered inferior and down-graded to a virtual branch.
Virtual banks really put much significance on their clients and inform them quickly of whatever happens in the course of banking operations and act on the data very intelligently.

Due to availability to huge amount of data, they are quite overwhelming on the client's life style and may provide them smart services and suggestions, while in the traditional banks, they are aware of minor information such as the costs of the clients only.

Also, among the reasons on a global movement toward virtual banking, mention could be made of the risks of the number of branches, the ability to provide unlimited financial services to the clients with due account of the virtual banking different environment, and the occurrence of unexpected events, such as the requirement of social distancing as the result of pandemics of covid-19. Nevertheless, the Regulations on Virtual Banks Establishment & Activities approved in 2011, no practical action has been taken for implementation of the said Regulations. These Regulations, in the same year of approval, provided a proper legal infrastructure for the establishment, administration, inspection and supervision on virtual banks; however, with a view and as compared to the rules and regulations of the advanced countries which approved specific instructions for the virtual banks during the recent years, such countries as Hong Kong and Malaysia, we would notice there are numerous defects and gaps in these Regulations. Thus, for the purpose of establishing a useful and efficient virtual bank, its Regulations must be updated accordingly.

Whereas, the matter of providing and safekeeping security of these banks are of significant importance, therefore, some guidelines should be designed for the purpose of providing security and safekeeping of virtual banks. The best solutions in this respect are those which impose some certain personal responsibilities over the shoulders of the clients of virtual banks and those solutions which utilize of block-chain technology. Also, Metaverse Space has such useful potentials that enables the banks to make renovated the relationships among the people

and cause to be revitalized the establishment of connections with the clients. Upon appearance of virtual bank into the metaverse space, we might be witnessing enhancement in transparency and preservation of data privacy, resulting in a glorious manifestation of this kind of banking system.

This Page Intentionally Left Blank

شخصیت استقلالی حقوقی و راهکارهای حفظ امنیت بانک‌های مجازی

زهرا عاصف کبیری[۱*]، مصطفی السان[۲]، مهراب داراب‌پور[۳]

۱. دانشجوی دکترای حقوق خصوصی، دانشکده علوم انسانی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.
*نویسنده مسئول: Email : Asefkabiri.z@gmail.com
۲. دانشیار، گروه حقوق تجارت بین‌الملل و حقوق مالکیت فکری و فضای مجازی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
Email : m_elsan@sbu.ac.ir
۳. استاد، گروه حقوق تجارت بین‌الملل و حقوق مالکیت فکری و فضای مجازی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
Email : info@drdarabpour.ir

پژوهشکدهٔ حقوق

نوع مقاله:
پژوهشی

DOI:
10.48300/jfel.2024.452421.1027

تاریخ دریافت:
۲۶ فروردین ۱۴۰۳

تاریخ پذیرش:
۲۳ مرداد ۱۴۰۳

تاریخ انتشار:
۳۱ شهریور ۱۴۰۳

چکیده:

با رشد و توسعه سریع فناوری، یکی از برنامه‌های جدی در صنعت بانکداری، ایجاد فرصت برای اجرایی نمودن بانکداری مجازی است. بانک مجازی شرکتی است که مجوز کامل خدمات بانکداری را از صادرکننده مجوز خود دریافت می‌کند و دارای شخصیت مستقل حقوقی است. بروز مسائل غیرقابل پیش‌بینی، مانند ضرورت فاصله‌گذاری اجتماعی ناشی از بیماری‌هایی مثل کرونا و صرفه‌جویی در زمان و مکان، ضرورت حرکت جهانی به سمت بانکداری مجازی را بیش‌ازپیش نمایان ساخته و تأسیس بانک‌های مجازی در کشور را اجتناب‌ناپذیر کرده است؛ ازاین‌رو، به‌منظور بهره‌مندی از مزایای بانکداری مجازی، باید از قبل چالش‌های حقوقی مرتبط با آن را شناسایی و مدیریت نمود. مطالعه در قوانین و مقررات موجود در کشورمان و سایر کشورها به شیوه کتابخانه‌ای و نگارش مطالب به‌صورت توصیفی - تحلیلی بوده است؛ لذا، این نوشتار بدواً درصدد بررسی تطبیقی بانک‌های مجازی است تا هویت مستقل حقوقی، مختصات و

ضرورت ایجاد و به‌کارگیری آن‌ها را شناسایی کند. آنگاه به این دلیل که تمامی داده‌های این‌گونه بانک‌ها در فضای مجازی بوده و در معرض خطر حملات سایبری بیشتری هستند، تمهیدات قانونی برای حفظ و تأمین امنیت آن‌ها اندیشیده است، تا با خطرات امنیت سایبری مقابله شود و از حریم خصوصی داده‌ها حفاظت گردد. همچنین، مدیریت ریسک در آن معمول شود و دولت‌ها نیز در تأسیس، مقررات گذاری و نظارت در عملکرد بانک‌های مجازی به نحو شایسته‌تری عمل نمایند.

کلیدواژه‌ها:
بانک مجازی - نئوبانک - قاعده مقابله با خسارات - فناوری بلاک چین - سند باکس نظارتی.

حامی مالی:
این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:
زهـرا عاصـف کبیـری: مفهوم‌سـازی، روش‌شناسـی، اسـتفاده از نرم‌افـزار، تحلیـل، تحقیـق و بررسـی، منابـع، نوشـتن ـ پیش‌نویـس اصلـی، نوشـتن – بررسـی و ویرایـش، تصویرسـازی.
مصطفی السان: اعتبار سنجی، نظارت بر داده‌ها، نظارت، مدیریت پروژه.
مهراب داراب‌پور: اعتبار سنجی، نظارت بر داده‌ها، نظارت، مدیریت پروژه.

تعارض منافع:
بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

استناددهی:

عاصف کبیری، زهرا، مصطفی السان و مهراب داراب‌پور. «شخصیت استقلالی حقوقی و راهکارهای حفظ امنیت بانک‌های مجازی». مجله پژوهش‌های حقوق مالی و اقتصادی ۱، ش. ۱ (۳۱ شهریور ۱۴۰۳): ۱۰۱-۱۳۸.

مقدمه

بانک‌ها در چرخه اقتصادی نقش اساسی دارند و عمدتاً تحت نظارت و کنترل دولت‌ها هستند. بدین جهت، تأسیس بانک در هر کشوری مستلزم رعایت تشریفات قانونی مفصلی است.[۱] بانک‌های فناوری محور هم، همچون نئوبانک‌ها و بانک‌های مجازی، از این امر مستثنا نیستند.

در سال‌های اخیر، یکی از برنامه‌های جدی در صنعت بانکداری به‌کارگیری حداکثری فناوری و موضوع پیاده‌سازی و عملیاتی نمودن بانکداری مجازی است. تحولات جهانی و اقدامات اخیر کشورهایی همچون هنگ‌کنگ و مالزی، در خصوص بانک مجازی و سرعت فراگیر آن در جهان، نشانگر اقبال این نوع بانکداری در کشورهای مختلف است. ایران در خصوص توسعه مقررات بانک مجازی شروع بسیار خوبی داشت و با آن‌که در سال ۱۳۹۰ «آیین‌نامه تأسیس و فعالیت بانک‌های مجازی» هم تصویب شد؛ ولی تاکنون هیچ بانک مجازی در ایران تأسیس نشده است.[۲] درصورتی‌که امروزه زمینه حقوقی و روانی جامعه در خصوص استفاده از بسترهای بانکداری مجازی، آماده‌ترین شرایط خود را دارا است. این نوع بانکداری می‌تواند صنعت بانکداری ایران را متحول ساخته و راهبردی برای برون‌رفت اقتصاد کشور از وضعیت کنونی باشد.[۳]

ایالات متحده آمریکا پیشگام بانک‌های مجازی در دنیا است. بانک مجازی در این کشور چندین سال است که راه‌اندازی شده و اقدامات مؤثری در این حوزه انجام شده است. با توجه به بخش رو به رشد مشتریان با سواد دیجیتالی که خواهان سادگی، شفافیت و خدمات مفید هستند، به‌سرعت در حال گسترش است.[۴]

انتظار می‌رود حدود ۱٫۸ میلیون بزرگ‌سال هنگ‌کنگی نیز تا سال ۲۰۲۵ در بانک مجازی حساب داشته باشند؛ ولی همچنان بسیاری از مردم این کشور، در خصوص اطلاعات شخصی خود به این نوع بانک‌ها اعتماد ندارند و یا به ثبات مالی این نوع بانکداری اعتقاد چندانی ندارند. بااین‌حال، باوجود اعتماد مردم به بانک‌های سنتی، مشتریانی که از این بانک‌ها ناامید شده‌اند، دو برابر بیشتر به بانک‌های مجازی

---

۱. مصطفی السان، حقوق بانکی (تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، ۱۳۹۳)، ۵-۷.

۲.«بانک مجازی فرصت تحول و نوزایی بانکداری»، راه پرداخت، تاریخ آخرین ویرایش ۱۳ تیر ۱۳۹۷، قابل دسترسی در: https://way2pay.ir/106759/.

۳. محمدجعفر نعناکار، «درآمدی حقوقی بر موجودیت نئوبانک‌ها»، آبان ۱۳۹۹، تاریخ دسترسی آذر ۱۴۰۰، قابل دسترسی در: https://way2pay.ir/206357/.

4. Virtual Banking - Overview of The Currrnt Landscape, Siapartners, last modified June 24, 2020, https://www.sia-partners.com/en/news-and-publications/from-our-experts/virtual-banking-overview-current-landscape.

Asef Kabiri, Zahra. "Legal Independency of Virtual Banks, their Preservation and Security", Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

مراجعه می‌کنند. بلومبرگ[5] تخمین زده است که بانک‌های مجازی تا سی درصد از درآمد بانک‌های سنتی در هنگ‌کنگ را به خود اختصاص خواهند داد.[6]

لذا این نوع بانک‌ها سال‌هاست که در جهان در حال ارائه خدمت‌رسانی به مشتریان هستند. بااین‌حال، چنین ساختاری می‌تواند با چالش‌های حقوقی فراوانی روبه‌رو باشد. یکی از این چالش‌ها، تعریف دقیق و هویت این نوع بانکداری است. در واقع سؤالی که باید به آن پاسخ داد این است که بانک مجازی واقعاً یک بانک است یا اینکه صرفاً یک شعبه مجازی برای بانک‌های سنتی است؟ مختصات بانک‌های سنتی و مجازی چیست و ضرورت وجود و رمز موفقیت بانک‌های مجازی در چیست؟

همچنین باید دانست که یکی از تعهدات بانک مجازی، تعهد به فراهم ساختن امنیت در این نوع بانکداری است و باید معتقد بود که تعهد بانک مجازی، به برقراری ایمنی، تعهد به‌وسیله است. افزون بر این، از آنجایی که بانک‌های مجازی هر چیزی که دارند به‌صورت مجازی ذخیره می‌کنند، در خطر تبدیل شدن به هدف بزرگ‌تری برای حملات سایبری هستند؛ که باید راهکارهایی برای تأمین امنیت و مدیریت ریسک در آن‌ها نیز ارائه داد.

لذا ساختار این نوشتار بدین شرح است: در قسمت اول، پس از تعریف دقیق و هویت این نوع بانک، به بیان مختصات و تمایز آن با بانک سنتی پرداخته می‌شود. همچنین، رمز موفقیت بانک‌های مجازی پیشرو و ضرورت بانکداری مجازی را بیان می‌کند. سپس در قسمت دوم، جهت حفظ و تأمین امنیت آن راهکارهایی را پیشنهاد می‌کند.

۱- هویت مستقل حقوقی و کامل بانک مجازی

امروزه به دلیل توسعه فناوری، دنیا با انواع جدیدی از بانک‌ها روبه‌رو شده است که ویژگی مشترک آن‌ها، فناوری محور بودنشان است. بزرگ‌ترین تفاوت آن‌ها با بانک‌های سنتی، متکی نبودنشان به مکان فیزیکی و امکان ارائه خدمات به‌صورت کاملاً آنلاین است.

برخی از بانک‌های فناوری محور، با پشتوانه یک بانک سنتی فعالیت می‌کنند. این بانک‌ها با وجود داشتن هویت مستقل، ولی مجوز بانکداری مستقل ندارند و در تعامل با یک بانک سنتی دیگر به ارائه خدمات آنلاین خود اقدام می‌کنند. همچنین، این بانک‌ها شعبه فیزیکی هم ندارند.[7] به این بانک‌ها

5. Bloomberg
6. Emily Lee, "Digital Financial Inclusion: Observations and Insights from Hong Kong's Virtual Banks", *Law and Contemporary Problems*, 84:95, 1, (2021), 95-96.
۷ . وحید شامخی و سعید باباخانی، «سناریوهای آینده بانک مجازی در ایران افق ۱۴۱۰»، شرکت تجارت الکترونیکی ارتباط

نئوبانک[۸] می‌گویند. در این بانک‌ها، ابتدا یک بانک سنتی وجود دارد که خواهان به‌دست آوردن چهره نئوبانکی برای خود است.[۹]

نمونه‌های موفقی از نئوبانک‌ها در ایران هم وجود دارد. ازجمله آن، بلوبانک است که همه‌ی عملیات بانکداری را به‌صورت کاملاً آنلاین انجام می‌دهد؛ ولی تمامی سپرده‌های مشتریان در این بانک، نزد بانک سامان نگهداری می‌شوند.[۱۰] در حقیقت، بر اساس مجوزی که بلوبانک دارد، به‌عنوان شعبه دیجیتال بانک سامان فعالیت می‌کند.[۱۱] بانک خاورمیانه نیز ارائه خدمات بانکداری دیجیتال خود را به‌صورت غیرحضوری و از طریق نئوبانکی با نام، بانکینو انجام می‌دهد.[۱۲]

دستورالعملی توسط بانک مرکزی در سال ۱۴۰۲،[۱۳] ابلاغ شد که در آن به چگونگی نحوه فعالیت نئوبانک‌ها پرداخت. مطابق آن، ارائه خدمات و انجام عملیات بانکی به‌صورت غیرحضوری تحت عناوینی مانند نئوبانک و شعبه مجازی، توسط مؤسسه اعتباری، صرفاً در قالب واحد دیجیتال ارائه خدمات بانکی و با شناسه اختصاصی مربوط به آن مجاز است و نباید این واحدها به‌گونه‌ای معرفی شوند که مخاطب آن‌هاها را به‌عنوان یک مؤسسه اعتباری مستقل قلمداد کند.

اما بانک مجازی[۱۴] یا VB هویت متفاوتی دارد. این نوع بانکداری به‌هیچ‌وجه، همانند بانکداری سایه[۱۵]– که شامل هرگونه فعالیت مشابه بانک‌ها است که یک شرکت یا مؤسسه مالی غیر بانکی (واسطه

فردا، ۱۳۹۹، تاریخ دسترسی خرداد ۱۴۰۱، قابل دسترسی در:
https://www.efarda.ir/VirtualBank_Future_Scenarios.pdf

8 . Neo Bank

۹. مهدی شامی زنجانی، «انتشار گفتگوها در میزگرد نئوبانک توسط عصر تراکنش»، خرداد ۱۴۰۰، تاریخ دسترسی ۱۲ تیر ۱۴۰۰، قابل دسترسی در:
http://shamizanjani.ir/

۱۰. مینا حاجی، «بلوبانک چیست و چگونه می‌توان در آن حساب باز کرد؟/ افتتاح حساب در ۷ دقیقه»، ۲۰ اسفند ۱۳۹۹، تاریخ دسترسی ۱ آذر ۱۴۰۰، قابل دسترسی در:
https://way2pay.ir/226957/

۱۱. غزل یگانگی، «نشست خبری بلوبانک با حضور مدیران و خبرنگاران برگزار شد/ ثبت بیش از ۲۲ میلیون تراکنش در بلوبانک»، ۲۶ مهر ۱۴۰۰، تاریخ دسترسی ۱۰ آذر ۱۴۰۰، قابل دسترسی در:
https://way2pay.ir/246148

۱۲. بانکینو چیست و چه خدماتی دارد؟»، عصر بانک، تاریخ آخرین ویرایش ۱۰ اردیبهشت ۱۴۰۱، قابل دسترسی در:
https://asrebank.ir/160818/.

۱۳. «ضوابط ناظر بر نحوه ایجاد، فعالیت و نظارت بر واحد دیجیتال ارائه خدمات بانکی توسط مؤسسات اعتباری»، مورخ ۱۴۰۲.

14. Virtual bank

15. Shadow Banking System

Asef Kabiri, Zahra. "Legal Independency of Virtual Banks, their Preservation and Security", Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

اعتباری) انجام می‌دهد- نیست.[۱۶] بانکداری مجازی به معنای حضور بانک‌ها در فضای مجازی با مفهوم کلی آن است. مطابق بند ۲ دستورالعمل بانک مجازی هنگ‌کنگ، «بانک مجازی به بانکی گفته می‌شود که خدمات بانکداری خرد را به‌جای شعب فیزیکی از طریق اینترنت یا سایر اشکال کانال‌های الکترونیکی ارائه می‌کند».

بانک مرکزی با تصویب آیین‌نامه تأسیس و فعالیت بانک‌های مجازی» مصوب ۱۳۹۰، از لحاظ قانونی بر امکان فعالیت بانک‌های مجازی، صحه گذاشت.[۱۷] در بند ۳ از ماده ۱ این آیین‌نامه، تعریف بانک مجازی این‌طور آمده است: «بانک مجازی، بانکی است بدون شعبه که عملیات و خدمات بانکی را صرفاً از طریق درگاه‌های الکترونیکی انجام می‌دهد». در ماده ۳۹ همان آیین‌نامه بیان شده است که «بانک مجازی مطلقاً مجاز به ایجاد شعبه، باجه و نظایر آن در داخل و خارج از کشور نیست». بنابراین، بانکداری می‌تواند تا به‌اندازه‌ای پیشرفت کند که بانکی را به حالت کاملاً مجازی و غیر فیزیکی در بیاورد.

اما با گذشت بیش از یک دهه از تاریخ این آیین‌نامه، هنوز بانک مجازی در ایران تأسیس نشده است.[۱۸] ولی نمونه‌های موفق این نوع بانکداری در دیگر کشورها وجود دارد؛ «وی‌بانک» چین،[۱۹] «زِدای‌بانک» هنگ‌کنگ،[۲۰] «اِن ۲۶» آلمان، کاکائوبانک کره‌جنوبی،[۲۱] از این قبیل هستند.

همچنین «First Internet Bank» یا First IB یک بانک مجازی در ایالت متحده آمریکا است که این بانک، تمام خدمات بانکی را به‌طور کاملاً آنلاین ارائه می‌دهد و هیچ شعبه فیزیکی ندارد. این بانک، در کنار بسیاری از خدمات بانکی سنتی، -از جمله افتتاح حساب‌جاری و پس‌انداز، کارت اعتباری و غیره- مجموعه‌ای از خدمات بانکداری شخصی، خدمات تجاری و وام‌ها را به مشتریان با هر نیاز بانکی که دارند ارائه می‌کند. بانک First IB مجوز انجام تجارت در تمام ۵۰ ایالت و قلمروهای ایالات‌متحده

---

۱۶. محمود باقری و محمد صادقی، «مسائل و تبعات حقوقی بانکداری سایه»، فصلنامه علمی دیدگاه‌های حقوق قضایی، ۲۶، ۹۶ (۱۴۰۰)، ۲-۳.

۱۷. مصطفی السان، حقوق تجارت الکترونیکی (تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، ۱۳۹۱)، ۷۵.

۱۸ . وحید شامخی و سعید باباخانی، پیشین، ۵۱.

19. Haosheng Chen et al., “Strengthen the security management of customer information in the virtual banks of Hong Kong through business continuity management to maintain its business sustainability”, *Sustainability* (Switzerland), 13(19), (2021),16. Article 10918. (accessed June 23, 2024)..

20. Djon Ly, “8 Virtual Banks in Hong Kong: How Do They Compare?”, 2024. At: https://statrys.com/blog/virtual-banks-hk . (accessed July 12, 2022).

21. Trung Viet Nguyen, “Virtual bank by FinTech firms – Global trending, challenges, solutions and experience of regulating virtual banks in Vietnam”, (Tilburg Law School – Master Thesis, *International Business Law* (LL.M.), June 24, 2020). 5&13

را داراست، در واقع، مجوز ایالتی ایندیانا این شرکت به آن اجازه می‌دهد تا مانند مجوز بانک ملی عمل کند.[۲۲]

بانکداری مجازی به‌عنوان یک ضرورت، سبب تغییرات اساسی در کیفیت خدمات شده است و می‌تواند محملی برای ورود به یک کسب‌وکار جدید در نظام بانکی تلقی شود. برای تبیین هر چه بهتر این موضوع، لازم است، اشاره‌ای به مختصات بانک‌های سنتی و بانک‌های مجازی شود، سپس علل موفقیت بانک‌های مجازی پیشرو و ضرورت وجودی آن بیان گردد.

۱-۱- مختصات بانک‌های سنتی

مختصات و ویژگی‌های اصلی بانک‌های سنتی را می‌توان در موارد زیر خلاصه کرد:

۱-۱-۱- خصیصه شعبه‌ای بودن بانک‌های سنتی

یکی از مهم‌ترین محل درآمدهای بانک‌های سنتی، شعبات آن‌ها است. شعبه بانک‌ها محرک دیداری در مورد کیفیت خدمات بانکی بودند و به‌عنوان اصلی‌ترین کانال ارتباطی بین مشتریان و بانک‌ها محسوب می‌شدند. پس عاملی تعیین‌کننده در جذب و نگهداری مشتریان بودند. همچنین، وجود شعب در بهترین موقعیت تجاری یک رکن برای جذب مشتری و رقابت با سایر بانک‌ها بود. بااین‌وجود، برای ایجاد هر شعبه به ساختمان، تجهیزات و نیروی انسانی نیاز است که بر بانک‌ها هزینه زیادی را تحمیل می‌کند.

۱-۱-۲- استفاده از فناوری جهت کاهش تردد مشتریان

بانک‌های سنتی با استفاده از فناوری، خدمات و تسهیلاتی را به شکل غیرحضوری ارائه می‌کنند که جهت تسهیل امور مشتریان و برای کمتر کردن تردد به شعب است.

۱-۱-۳ - ارائه خدمات با محدودیت‌های زمانی و مکانی

خدمات در این نوع بانک‌ها عموماً محدود و ارائه همین خدمات هم دارای محدودیت زمانی و مکانی است.

۱-۲- مختصات بانک‌های مجازی

22. Jennifer Schurman, “First Internet Bank”, May 2022.At: https://www.consumeraffairs.com/finance/first-internet-bank.html. (accessed July 12, 2022).

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

پس از بیان مختصر مختصات بانک‌های سنتی، باید ویژگی‌های اساسی بانک مجازی تشریح گردد که عبارت‌اند از:

۱-۲-۱- فقدان شعبه

کلیدی‌ترین ویژگی بانک‌های مجازی آن است که هیچ شعبه فیزیکی برای ارائه خدمات خود ندارند.[۲۳] ولی بانک مجازی صرفاً به معنای بانک بدون شعبه نیست؛ بلکه اساساً این نوع بانک به شعبه نیاز ندارد.[۲۴] در بند ۱۷ چارچوب مجوز برای بانک‌های دیجیتال یا مجازی کشور مالزی، مقرر شده که نخست، مطابق با بخش ۴۶ (۱) قانون شرکت‌ها ۲۰۱۶، برای بانک دیجیتال، ایجاد دفتر ثبت شده در مالزی الزامی است. این بانک باید اطمینان حاصل کند که دفتر ثبت شده آن به اندازه کافی با بانک مرکزی مالزی در طول فرآیند نظارت، ازجمله برای اهداف بررسی و تعامل با مدیریت ارشد و هیأت مدیره، ارتباط برقرار می‌کند. همچنین، این بانک مجاز به ایجاد دفاتر فیزیکی برای اهداف اداری است و اگر قصد تسهیل شکایات حضوری مشتریان را داشته باشد، دفتر ثبت شده و دفاتر فیزیکی نیز به‌عنوان مرکزی برای این منظور عمل خواهند کرد. دوم اینکه، یک بانک مجازی، مجاز به ایجاد شعبه یعنی یک محل ثابت تجاری برای تسهیل تراکنش‌های مشتریان نیست.[۲۵]

برخی از منتقدان بانک مجازی معتقدند که بانکداری، حوزه‌ای مرتبط با روانشناسی است و دسترسی به یک شعبه فیزیکی به افراد حس امنیت می‌بخشد. آنها نداشتن شعبه و ارائه خدمات به شکل صددرصد آنلاین را، منجر به از بین رفتن ارتباط بین بانک و مشتری می‌دانند. درست است که این نوع بانک‌ها دفتر مرکزی و دفاتر نمایندگی دارند، ولی اگر بانک مجازی در دنیای متاورس،[۲۶] وارد شود، دیگر این مسئله اصلاً مطرح نمی‌شود. بانکداری در متاورس، علاوه بر اینکه ممکن است فرصت‌های بسیاری را به ارمغان بیاورد و وضعیت بانک‌ها را به‌طور قابل توجهی بهبود بخشد؛ می‌تواند راه‌حل مؤثری برای رفع این مشکل باشد. در متاورس، بانک‌ها می‌توانند شعبه‌های مجازی خود را افتتاح کنند.[۲۷] مشتری

---

۲۳. وحید شامخی و سعید باباخانی، پیشین. ۹.

۲۴. رسول قربانی، «بالاخره گره کور بانک مجازی به دست بانک سپه باز خواهد شد؟»، ۱ شهریور ۱۳۹۱، تاریخ دسترسی ۱۵ مرداد ۱۴۰۱، قابل دسترسی در:

https://way2pay.ir/14533/

25. Bank Negara Malaysia (Central Bank of Malaysia), “Licensing Framework for Digital Banks”, Issued on: 31 December 2020.

26. Metaverse

۲۷ . بانک جی‌پی‌مورگان، سالن Onyx را در متاورس راه‌اندازی نموده است.

می‌تواند در قالب دیجیتالی خود (آواتار)[۲۸] از آن شعب بازدید کند و از خدماتی مانند، در میان گذاشتن برنامه‌های سرمایه‌گذاری خود با مشاور سرمایه‌گذاری آواتار یا شرکت در جلسه سرمایه‌گذار مجازی که توسط بانک سازماندهی شده است، استفاده کند؛ که این‌ها احساس اعتماد را افزایش می‌دهند و در نهایت به حفظ مشتری با بهبود نتیجه کمک می‌کنند؛ بنابراین، فضای متاورس دارای پتانسیلی است که می‌تواند بانک‌ها را قادر به بازسازی روابط افراد و احیای مجدد برقراری ارتباط با مشتریان در بانک‌های مجازی کند.[۲۹]

۱-۲-۲- یگانگی انجام امور به شکل تمام الکترونیکی

استفاده از فناوری در بانکداری مجازی به این صورت است که اساساً یک بانک بدون شعبه، تمام الکترونیکی و کاملاً غیرحضوری ایجاد می‌شود. در بانکداری مجازی، باید تمام مراحل از افتتاح حساب پایه تا واریز پول برای سپرده‌گذاری، دریافت و انتقال وجه و مبادله اسناد بین‌بانکی با تمام کشورهای جهان و غیره، از طریق ابزار الکترونیکی انجام شود؛ لذا بانکداری مجازی عرصه جدیدی در فضای مجازی است که می‌تواند موقعیت مناسبی را جهت ارائه خدمات بانکی به ارمغان آورد.[۳۰]

۱-۲-۳- ارائه خدمات بدون محدودیت‌های زمانی و مکانی

استفاده از سیستم‌های رایانه‌ای متمرکز، عدم محدودیت زمانی و مکانی جهت انجام عملیات بانکی، ازجمله ویژگی‌های بانک‌های مجازی است. این بانک‌ها، نقاط تماس با مشتری جهت ارائه خدمات متنوع را افزایش می‌دهند. در بانک‌های مجازی، گفتمان فروش با مشتری از طریق روش‌های تحلیل داده بهبود یافته و از ارائه خدمات به شکل ۷×۲۴ درآمد کسب می‌کند. به‌علاوه، ارائه خدمات برای مشتریان بانک شخصی‌سازی می‌شود. در مدیریت بانک و ارائه خدمات چابک شده و بر نیازها و خواسته‌های مشتری، به‌جای سهامداران بانک، تمرکز کرده و مشتری‌مداری را در اولویت خود قرار می‌دهد. همچنین، روش‌های جدید درآمدی ایجاد می‌کند، هزینه‌ها را کاهش داده و باعث افزایش

28. avatar

29. Swapan Sarkar, “Banking in Metaverse - Opportunities and Challenges”, *Management Accountant Journal*, 58, 1(2023), 63-65.

۳۰. رامین پورسعید و پیمان قنبری، «بررسی بانکداری مجازی در نظام حقوقی ایران»، دانش حقوق و مالیه، ۱(۱۳۹۶)، ۳۶-۳۶.

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

بهره‌وری می‌شوند.[۳۱]

۱-۳- دلایل موفقیت بانک‌های مجازی

دلایل بسیاری برای موفقیت بانک‌های مجازی وجود دارند. ازجمله این دلایل، آگاه کردن مشتری است. بانک‌های مجازی، مشتری را از هر آنچه اتفاق می‌افتد، آگاه می‌کنند در صورتی‌که بانک‌های سنتی فقط بدهکاری یا بستانکاری را مشخص می‌کنند و در خصوص چیستی، چگونگی، چرایی و مکان وقوع آن هیچ اطلاعاتی ارائه نمی‌دهند. همچنین، عملکرد هوشمند این بانک‌ها در رابطه با سبک زندگی مشتریان دلیل دیگری برای موفقیت آن‌ها است. این بانک‌ها هزینه‌های مشتری را به‌وسیله الگوریتم‌های نرم‌افزاری بررسی می‌کنند و در جست‌وجوی فرصت‌هایی هستند که به او کمک کنند تا کمتر هزینه کند یا بیش‌تر صرفه‌جویی کند.

بانک‌های مجازی در خصوص داده‌ها بسیار هوشمندانه عمل می‌کنند. به‌عنوان مثال، بانک مجازی مونزو با استفاده از API های گوگل‌مپ و سرویس‌ها، صورت‌حساب‌های مشتری را غنی‌تر می‌کند؛ بنابراین مشتری متوجه می‌شود که پرداخت‌هایی که داشته است در چه زمان و مکانی انجام شده است؛ در نتیجه، مشتری روزانه تعداد بیشتری از فعالیت‌های مالی خود را به بانک مونزو منتقل می‌کند. هنگامی‌که مشتریان، غنی‌سازی داده‌های تراکنش‌ها و سبک‌های زندگی خود را از بانک‌های جدید می‌بینند، شروع به استفاده بیشتر از آن‌ها می‌کنند؛ بنابراین، تمام تراکنش‌های سبک زندگی آن‌ها از طریق یک بانک هوشمند جدید انجام می‌شود. پس به این ترتیب، بانک‌های مجازی از سبک زندگی مالی مشتریان خودآگاه می‌شوند؛ درحالی‌که بانک‌های سنتی، فقط مخارج مشتریان را می‌دانند.[۳۲]

افزون‌براین، بانک‌های مجازی علاوه بر استفاده حداکثری از فناوری روز، شمول مالی را ارتقاء می‌دهند. این امر می‌تواند یکی‌دیگر از دلایل موفقیت این بانک‌ها بوده که شرح مختصری از آن در اینجا خالی از فایده نخواهد بود. شمول مالی،[۳۳] به این معنی است که افراد و مشاغل به محصولات و خدمات مالی مفید و مقرون‌به‌صرفه دسترسی دارند که نیازهای آن‌ها را برآورده می‌کند. این خدمات به روشی مسئولانه و پایدار ارائه می‌شوند. بانک‌های سنتی، از طریق شبکه‌های شعب گسترده خود، به

---

۳۱. وحید شامخی و سعید باباخانی، پیشین، ۱۱.

۳۲. کریس اسکینر، قطب‌نمای بانکداری دیجیتال: درس‌هایی از رهبران تحول دیجیتال، ترجمه و تحقیق مهدی شامی‌زنجانی، فراز نبیی و درسا پورحسن (تهران: راه پرداخت، ۱۳۹۹)، ۷۶-۸۵.

33. Financial inclusion

شمول مالی دست می‌یابند، درحالی‌که بانک‌های مجازی، با کم بودن هزینه‌های نهایی‌شان، به این مهم نائل می‌شوند. در واقع، بانک‌های مجازی، برخلاف بانک‌های سنتی، هزینه‌های عملیاتی کمتری دارند و مجبور نیستند برای شعبه‌های متعدد هزینه بپردازند؛ در نهایت این صرفه‌جویی در هزینه‌ها به نفع مشتریان نیز خواهد بود.[۳۴] پس خدمات مالی دیجیتال،[۳۵] به‌عنوان ابزاری برای فعال کردن شمول مالی و درنتیجه کمک به بهبود زندگی مردم هستند.[۳۶]

هنگامی که مرجع پولی هنگ‌کنگ،[۳۷] از متقاضیان بانک‌های مجازی دعوت به عمل آورد، دو هدف عمده داشت: هدف نخست، ترویج کاربرد فین‌تک و نوآوری در هنگ‌کنگ برای ارائه نوع جدیدی از تجربه مشتری بود و هدف دوم آن، ترویج شمول مالی بود. درحقیقت، هدف تجاری بانک‌های مجازی مشتریان خرده‌فروشی هستند که قبلاً برخی از آن‌ها به سیستم بانکی دسترسی نداشتند؛ ازاین‌روست که بانک‌های مجازی وضعیت شمول مالی را بهبود می‌بخشند و این امر می‌تواند عامل موفقیت آن‌ها بشود.[۳۸]

۱-۴- ضرورت وجود بانکداری مجازی

امروزه نمی‌توان امکاناتی را که فناوری در اختیار اشخاص قرار داده است، نادیده گرفت. ازجمله مزایای بانکداری مجازی می‌توان به راحتی، فراگیر بودن، سرعت تراکنش و مشتری‌مداری اشاره کرد. ازاین‌رو، اجرایی کردن بانکداری مجازی باید یک ضرورت قلمداد شود که ذیلاً دلایل آن بررسی می‌شود.

۱-۴-۱- مخاطرات وجود شعب

وجود شعب باعث از جریان افتادن بخشی از منابع بانکی است که این منابع می‌توانند به‌عنوان خدمات در اختیار مردم قرار گیرند؛ اما حبس این سرمایه‌ها در قالب ساختمان‌هایی که در اختیار بانک هستند، باعث کمبود منابع می‌شود. «بانک مونزو در خصوص نداشتن شعبه بیان کرده است که بدون شعبه نیز می‌توان خدمات مفید و سریع را به مشتریان ارائه داد. از افتتاح حساب در عرض چند دقیقه گرفته تا رفع

34. Donald Tse, “Cybersecurity and Technology Risk in Virtual Banking”, 4 January 2022. At: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-and-technology-risk-in-virtual-banking. (Accessed June 15, 2024).

35. Digital financial services (DFS)

36. Silvia Baur Yazbeck; Judith Frickenstein & David Medine, “Cyber Security In Financial Sector Development: Challenges and potential solutions for financial inclusion”, *CGAP*, (2019), 3.

37. Hong Kong Monetary Authority (HKMA)

38. Lee, op. cit., 100&102.

هر مشکل مالی مشتریان. در نتیجه، این بانک پولی که از راه‌اندازی نکردن شعب پس‌انداز می‌کند را در خدمات بهتر و جدیدتر که مردم می‌خواهند، سرمایه‌گذاری می‌کند».[۳۹] ازاین‌رو، نداشتن شعب، جلوگیری از حبس پول می‌کند. ازسوی‌دیگر،با توسعه دانش بیوانفورماتیک و تولید انواع حسگرهای زیستی، احراز هویت از راه‌دور ممکن شده و تنها کارکرد منحصربه‌فرد شعبه هم عملاً ازبین رفته است.

از بُعد هزینه‌ای نیز از آن‌جایی که این بانک فاقد شعبه فیزیکی است، به نیروی انسانی زیادی نیاز ندارد. همچنین، در عملیات‌های بانکی تعداد خطاها کمتر شده و یا حتی بدون خطا عمل می‌شود.[۴۰] پس نه‌تنها دلیلی برای داشتن شعب وجود ندارد، بلکه وجودش مخاطرات و ایراداتی هم به همراه دارد.

۱-۴-۲- توانایی ارائه خدمات نامحدود با توجه به سازکار متفاوت فضای مجازی

بانکداری مجازی را، نباید به شکل بانکداری الکترونیکی یا همان بانکداری مرسوم، ولی به شکل بانکداری بدون شعبه فیزیکی، محدود کرد که در این صورت بانکداری مجازی واقعی، محقق نمی‌شود. درحقیقت، در دنیای مجازی، سازکارها می‌توانند کاملاً متفاوت از آن چیزی باشند که در دنیای فعلی با ابعاد محدود وجود دارند. مفهومی مانند ارائه حساب مجازی از این قبیل است.[۴۱] پس باید از امتیاز این فضا به درستی استفاده کرد. بنابراین، خدمات بانک‌های مجازی نباید محدود به ارائه خدمات بانک‌های سنتی به‌صورت مجازی شود؛ زیرا این مسئله ارزش افزوده‌ای برای کاربران ایجاد نخواهد کرد. یک بانک مجازی باید بتواند ویژگی را در خود بپروراند که کاربران بانک‌های سنتی بخواهند به‌جای سیستم قبلی از خدمات بانک مجازی استفاده کنند که مورد اقبال کاربران است. اساساً کارکرد بانک‌های مجازی بالقوه، در ایران نیز باید از سیستم بانکی کنونی آن فراتر برود تا بتوانند به موفقیت دست یابند.

۱-۴-۳- بروز مسائل غیرقابل پیش‌بینی

ویروس کرونا و الزام مردم به حفظ فاصله اجتماعی، باعث افزایش رقابت بر سر سرویس‌های غیرحضوری شد و توجه به بانک مجازی را افزایش داد. این ویروس، راه را برای دیجیتالی‌تر کردن بازار هموار کرد.

---

39. Monzo Bank, “Why Monzo doesn’t have branches”, Accessed October 10, 2023. Available at: https://monzo.com.

۴۰ . وحید شامخی و سعید باباخانی، پیشین، ۱۱.

۴۱. باشگاه خبرنگاران جوان، «آیا «بانک الکترونیکی» همان «بانک مجازی» است؟»، تاریخ آخرین ویرایش ۱۱ خرداد ۱۳۹۳، قابل دسترسی در:
https://www.yjc.news/00KNYs.

هنگامی که بحران اقتصادی ناشی از همه‌گیری این ویروس افزایش یافت، بانکداری مجازی به عاملی در تسهیل معاملات تجاری تبدیل شد. اکوسیستم دیجیتال، بانک‌ها را به کارآفرینان، تأمین‌کنندگان، کارمندان و بازارهای جدید مرتبط کرد. دولت‌ها تلاش کردند تا کمک‌های فوری و مؤثر را به مردم ارائه کنند. به‌طور همزمان، بانکداری نوین امکان فاصله‌گذاری اجتماعی را فراهم و به تقویت مشارکت مالی در مکان‌های دورافتاده‌ای که مؤسسات مالی به‌طور فیزیکی حضور نداشتند، کمک کرد.[۴۲] البته باید بر اولویت دادن به اعتماد دیجیتال برای بانک‌ها، به ویژه در دوره پس از همه‌گیری، تأکید کرد؛ زیرا همه‌گیری تغییر به سمت بانکداری دیجیتال را تسریع کرد و بازگشتی از آن وجود ندارد.[۴۳] بنابراین، از زمان شروع این ویروس، کار از راه دور دیگر استثنا نیست، بلکه رویکرد پیش‌فرض برای انجام همه کارها است.[۴۴]

به‌علاوه، اتخاذ برخی اقدامات توسط بانک‌های مجازی، در جهت تداوم فرآیند کسب‌وکار خود در مواجه با چنین بلایای غیرمنتظره‌ای، بسیار پر اهمیت است. تحت‌تأثیر همه‌گیری کرونا، بسیاری از بانک‌ها در سراسر جهان به دلیل وقفه در تجارت خود شکست خورده‌اند. درحالی‌که «وی‌بانک»،[۴۵] با عملکردی مناسب توانست پایداری کسب‌وکار خود و امنیت اطلاعات مشتریان را تضمین کند. این بانک توانست با ترکیب ویژگی‌های تجاری خود و استفاده کامل از مزایای تجارت صرفاً آنلاین و مدیریت مداوم فناوری، از عملکرد بی‌وقفه خود اطمینان حاصل کند و به شرکت‌های کوچک و خرد و افراد حاضر در منطقه خدمت‌رسانی کند.[۴۶]

به‌هرحال، بروز مسائل غیرقابل‌پیش‌بینی، ضرورت حرکت جهانی به سمت بانکداری مجازی را بیش‌ازپیش نمایان ساخته و تأسیس بانک‌های مجازی در کشورمان را غیرقابل اجتناب نموده است.

۲- راهکارهای حفظ و تأمین امنیت بانک مجازی

بانک مجازی در وهله نخست یک بانک است؛ بنابراین تعهداتی دارد، یکی از این تعهدات، تأمین

42. LI FANG & Darwin G., Quintos, “Security Measures Applied on Digital Banking Towards Service Improvement Proposal”, *Journal of Business and Management Studies* (JBMS), 5(5) (2023), 47&52, accessed June 15, 2024.

43. Rendell, R. “Why Digital Trust Should Be a Top Priority For Banks”, 2022. At: https://www.paymentsjournal.com/why-digital-trust-should-be-a-toppriority-for-banks/. (accessed June 15, 2024).

44. GuardRails, “The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them”, 24 Jun 2023. At: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/. (Accessed June 17, 2024).

45. WeBank

46. Chen, op. cit., 5&16-17.

امنیت است. در این نوع بانکداری، تمامی امور اعم از نگهداری سوابق اطلاعات مشتریان، تراکنش‌ها، نقل‌وانتقال وجوه، از طریق تجهیزات الکترونیکی انجام می‌شود. به همین دلیل یکی از دغدغه‌های مردم برای استفاده از خدمات بانکداری مجازی هم، بحث امنیت است.

در نظرسنجی مشتریان بانکداری دیجیتال «پرایس‌واترهاوس‌کوپرز»[۴۷] که در سال ۲۰۱۹ از ۴۵۰۰ مشتری در سراسر هنگ‌کنگ، سنگاپور و مالزی گرفته شد، بیش از نیمی از پاسخ‌دهندگان هنگ‌کنگی، علاقه‌مند به استفاده از بانک مجازی بودند؛ بااین‌حال، سی‌وهشت‌درصد از آنان، پاسخ دادند که به بانک‌های مجازی درخصوص اطلاعات شخصی خود اعتماد ندارند و سی‌وسه‌درصد از مصاحبه‌شوندگان هم به ثبات مالی بانک‌های مجازی اعتقاد چندانی نداشتند.[۴۸]

بنابراین، توجه به مواردی نظیر استفاده از احراز هویت چند عاملی (MFA)،[۴۹] که دسترسی غیرمجاز را دشوار کند،[۵۰] تهیه نسخه پشتیبان به‌طور مداوم و مانند این‌ها ضروری است؛ لذا با توجه به این‌که عدم وجود ساختار فیزیکی در این نوع بانکداری، یک اصل بوده و تمامی خدمات بانکداری صرفاً از طریق پایگاه‌های الکترونیکی، به‌ویژه اینترنت انجام می‌شود، تبیین ساختار ایمنی مؤثر از طریق مبانی حقوقی و قانونی کاملاً ضروری است.[۵۱]

ازجمله ریسک‌های اصلی بانک‌های مجازی عبارت‌اند از:

– ریسک اطلاعات و امنیت سایبری:[۵۲] یک بانک کاملًا دیجیتالی، هدف مشخصی برای مجرمان سایبری است. بسیاری از رویدادهای تبلیغاتی پیرامون راه‌اندازی یک بانک مجازی جدید می‌تواند احتمال حمله سایبری را افزایش دهد. به‌عنوان مثال، یک بانک مجازی،[۵۳] در اولین روز راه‌اندازی خود با یک حمله انکار سرویس توزیع شده (DDoS)[۵۴] مواجه شد که منجر به تأخیر قابل توجهی در ارائه خدمت آن بانک گردید.

– ثبات فناوری و ریسک انعطاف‌پذیری:[۵۵] اتکای بانک‌های مجازی به فناوری، قرار گرفتن آن‌ها را

47. PricewaterhouseCoopers
48. Lee, op. cit., 95-96
49. Multi-factor authentication (MFA)
50. Patcha Bhujanga Rao, "A Study on Cyber Security Issues Affecting Online Banking And Transactions", Ijariie-ISSN (O)-2395-4396, 9 Issue-6 (2023), 1664.
۵۱. پورسعید و قنبری، پیشین. ۴۱.
52. Information and cybersecurity risk
53. Ping An One Connect
54. distributed denial of service (DDoS)
55. Technology stability and resilience risk

در معرض ریسک ناشی از سیستم‌های فناوری اطلاعات ناپایدار افزایش می‌دهد. به‌عنوان مثال، اگر یک کمپین تبلیغاتی، برای یک بانک مجازی که در مرحله اولیه راه‌اندازی است، بیش از تعداد مورد انتظار، مشتری جذب کند، باعث مشکلات ظرفیت سیستم می‌شود.

– ریسک رفتار شخصی: نوآوری در بطن بانک‌های مجازی است؛ لذا حضور مدیران متخصص امنیت سایبری بدیهی است. باید بین نوآوری و آگاهی سایبری هم تعادل ایجاد کرد. همهٔ اشخاص از مدیریت تا کارمندان و همچنین کاربران نیازمند آگاهی در خصوص فضای سایبری و خطرات آن هستند.

– ریسک نظارتی: بانک مجازی، به‌عنوان یک بانک دارای مجوز، باید از تمام مقررات قابل اجرا پیروی کند. فرآیندهای کسب‌وکار جدید و استفاده از فناوری‌های جدید، ممکن است باعث ایجاد شکاف‌های انطباق با مقررات موجودی که با تغییرات سریع فناوری به‌روز و سازگار نشدند، گردند؛ اما با رشد بانکداری مجازی، تدوین مقررات برای نوآوری مساعدتر می‌شود.[۵۶]

برای مقابله با ریسک‌های موجود در این نوع بانکداری، مطابق بند ۷ ماده ۱۷ آیین‌نامه بانک مجازی ایران، یکی از مواردی که طرح عملیاتی باید شامل آن باشد، مشخص کردن سامانه‌های مدیریت امنیت اطلاعات و برنامه‌های امنیتی است. این سامانه، مشتمل بر سخت‌افزارها، نرم‌افزارها و الگوهای مدیریتی است که نتیجه استفاده از آن‌ها پیشگیری از نفوذ، سوءاستفاده و کلاهبرداری است. پس بانک مجازی باید مجهز به سامانه مدیریت امنیت اطلاعات باشد.[۵۷] علاوه‌بر این، به موجب ماده ۴۴ آیین‌نامه یادشده، بانک مجازی مسئول ایمنی و سلامت خدمات و سامانه‌هایی که به مشتریان خود ارائه می‌دهد نیز هست.

مصلحت بانک مجازی ایجاب می‌کند که هیچ‌گاه امنیت کامل نظام ارتباطی پایگاه‌های الکترونیکی خود را تضمین نکند. بلکه با آگاه ساختن مشتری به مشکلات متعارف موجود، علاوه بر اجتناب از تدلیس قراردادی، زمینه معافیت از مسئولیت قراردادی را در مواردی که به حکم متعارف علمی از حدود اختیارات وی خارج است، فراهم سازد؛ که البته این امر نافی تعهد بانک به اطلاع‌رسانی در صورت اختلال یا تعرض به سیستم نیست. همچنین تأمین امنیت شبکه، رازداری کارکنان و مدرن بودن وسایل

56. Tse, *op. cit.*

۵۷. مصطفی السان، حقوق تجارت الکترونیکی، پیشین. ۸۳-۸۴

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

و شیوه‌های ارتباطی هم از دیگر تعهدات امنیتی این بانک‌ها است.[۵۸] همچنین رئیس بانک مرکزی چین نیز گفته است: «امنیت سایبری و حوادث مرتبط با فناوری به‌طور کامل قابل اجتناب نیستند. این به دلیل آسیب‌پذیری‌های ذاتی در سیستم‌ها، فناوری‌ها، فرآیندها و افراد و همچنین خطرات مداوم عوامل تهدید سایبری است».[۵۹]

در نتیجه، چون هیچ‌گاه برقراری امنیت در فضای مجازی به‌طور کامل امکان ندارد و هرگونه شرطی که انجام آن غیرمقدور باشد، حتی اگر در عقد گنجانده شود، مطابق با بند ۱ ماده ۲۳۲ قانون مدنی ایران، باطل خواهد بود؛ بنابراین، تعهد بانک مجازی، به برقراری ایمنی، در فضای ارتباط مالی اینترنتی، تعهد به وسیله است؛ یعنی، بانک مجازی باید نهایت تلاش خود را به‌کار گیرد و اقدام متعارف برای پیشگیری و کنترل امنیتی را انجام دهد؛ با وجود این ممکن است، نتیجه مدنظر محقق نگردد.[۶۰] به هرحال، برای حفظ و تأمین امنیت در بانکداری مجازی، ذیلاً راهکارهایی پیشنهاد می‌شود.

۲-۱- تحمیل برخی از مسئولیت‌های شخصی به مشتریان بانک مجازی

یکی از راه‌کارها برای اینکه در بانک مجازی تمام اینترنتی، امنیت افزایش یابد، بحث تحمیل مسئولیت شخصی کاربران است. در هر زمانی شخصی به اینترنت متصل می‌شود، باید تصمیماتی را برای امنیت سایبری خود اتخاذ کند. تهدیدات سایبری در حال ظهور، نیازمند تعامل با کل جامعه برای ایجاد محیط امن‌تر سایبری است که لازمه آن‌ها همکاری دولت و بخش خصوصی و مهم‌تر از همه آن‌ها، مردم یعنی کاربران از جمله مشتریان بانک مجازی است؛ لذا، دو موضوع مشارکت زیان‌دیده در وقوع زیان و یا بی‌تفاوتی وی پس از ورود یا افزایش آن نکات اساسی هستند که لازم است بررسی شوند.

۲-۱-۱- ضرورت قاعده مقابله با خسارت و تفاوت آن با مشارکت زیان‌دیده در وقوع زیان

یکی از اصول کلی حقوق این است که اگر کسی به دیگری ضرری وارد کند، ملزم است که زیان وارده را جبران کند؛ اما نکته‌ای که در این‌جا مدنظر است این است که اگر شخص زیان‌دیده در ایجاد یا مقابله با خسارت می‌توانسته بدون مشقت و با وجود امکانات کافی، از خسارت بکاهد یا مانع ایجاد آن یا مانع افزایش خسارت شود، مسئولیت به چه نحوی بر طرفین بار می‌شود.

نقض قرارداد توسط یکی از طرفین، معمولاً موجب ورود خسارات به طرفی که قرارداد را نقض ننموده،

---

۵۸. مصطفی السان، حقوق بانکداری اینترنتی (تهران: پژوهشکده پولی و بانکی، ۱۳۹۲)، ۱۲۰.

59. FANG, op. cit. 49.

۶۰. مصطفی السان، حقوق بانکداری اینترنتی، پیشین. ۱۷۵.

می‌گردد، در واقع هنگامی‌که شخصی به‌موجب قرارداد متعهد به انجام فعل یا ترک فعلی می‌شود، اگر از انجام تعهدات خویش خودداری کند، طرف دیگر می‌تواند علیه وی اقامه دعوی کرده و خساراتی را که بر اساس این نقض عهد به او وارد شده را دریافت دارد؛ یا اگر بر اساس فعل زیان‌بار دیگری، خسارتی به او وارد شود (غیر قراردادی) می‌تواند خسارات وارده را از فاعل فعل زیان‌بار دریافت کند. حال سؤال این است که هرگاه متعهد قراردادی، نقض تعهد کرد یا شخصی، فعل زیان‌باری بر اموال یا جسم دیگری وارد کند و زمینهٔ ورود خسارت و ضرر به متعهدله یا زیان‌دیده به وجود آید، آیا متعهدله قرارداد یا شخصی که در معرض ورود ضرر قرار دارد، هیچ وظیفه‌ای در خصوص جلوگیری یا کاهش آن خسارت ندارد؟

در غالب موارد، پس از نقض قرارداد، خواهان یعنی شخصی که از نقض قرارداد متضرر شده، می‌تواند از ورود خسارات و از هدر رفتن منابع اقتصادی جلوگیری نماید. در اینجاست که بحث قاعده مقابله با خسارت[۶۱] مطرح شده است. این تئوری به‌طور گسترده‌ای وارد قلمرو مسئولیت‌های قراردادی و قهری شده و در حقوق اکثر کشورها به آن اشاره شده است. در حقوق ایران، هرچند قاعده مقابله با خسارت در یک اصل قانونی به‌طور صریح نیامده است؛ اما مصادیقی در لابه‌لای قوانین موضوعه مانند بند ۳ ماده ۴ قانون مسئولیت مدنی مصوب ۱۳۳۹ می‌توان یافت.

پس «قاعده مقابله با خسارات بدین معناست که متضرر از نقض قرارداد یا نقض یک تعهد عمومی از باب مسئولیت مدنی باید از ضررهای ناشی از نقض اجتناب نماید یا تا حد امکان آنها را کاهش دهد؛ زیرا که این امر باعث جلوگیری از افزایش ضرر و زیان وارده به خود وی خواهد شد».[۶۲]

متضرر باید اقدامات لازم را جهت عدم وقوع خسارت و کاهش و عدم افزایش خسارت معمول دارد؛ اما این تکلیف برای وی یک تکلیف مثبت نیست و او را ملزم نمی‌کند که آن اقدامات را واقعاً انجام دهد؛ بلکه وی مخیر است به انجام یا عدم انجام آن، تنها اثری که این وظیفه دارد این است که ناقض قرارداد می‌تواند درصورتی‌که خواهان برای جبران خسارات ناشی از نقض قرارداد اقامه دعوی نموده و مطالبه خسارت کند به‌عنوان دفاع به قاعده مقابله با خسارات متوسل شود تا از خسارات مورد مطالبه بکاهد. لذا، خواهان در صورت عدم مقابله با خسارت، قادر به مطالبه خسارات احتمالی قابل اجتناب نیست.

حتی بحث جبران ضرر توسط شخص زیان‌دیده هم مطرح نیست. زیان‌دیده هیچ‌چیزی را جبران نمی‌کند، او نباید به خود (قاعده اقدام) و به دیگران (قاعده لا ضرر) ضرر وارد کند؛ همچنین، اگر او

61. Doctrine of mitigation of damages

۶۲. مهراب داراب‌پور و دیگران، چالش‌های حقوقی در معاملات بازرگانی بین‌المللی (تهران: خرسندی، ۱۳۹۶)، ۱۸۶-۱۸۷.

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

سبب ورود ضرر گردد (قاعده تسبیب)، شخصاً مسئول است. پس در صورت عدم مقابله با خسارات، علیه خود اقدام کرده و فقط شخص مکلف نمی‌تواند تمام خسارت را دریافت کند. ضمانت اجرای قاعده فقط محدود به عدم قابلیت جبران کل خسارت یا بخشی از آن است نه اینکه زیان‌دیده الزام واقعی به انجام دادن عملی داشته باشد.

در این قاعده، خواهان باید به‌طور متعارف عمل کرده باشد و اقدام وی تحت آن شرایط و در آن اوضاع و احوال، معقول باشد. حتی لازم نیست اقدام خواهان در جهت جلوگیری از خسارت به نتیجه برسد؛ بلکه ممکن است این اقدام نتیجه‌ای نداشته باشد و حتی موجب افزایش خسارت نیز گردد. در این فرض، این امر تأثیری بر میزان خسارتی که استحقاق مطالبه آن را دارد، نداشته و او حق مطالبه جبران تمام زیان‌های وارده بر خود را دارد، حتی زیان‌هایی که در اثر اقدام خود وی ایجاد شده است.

در مورد مبنای قاعده مقابله با خسارت، می‌توان به قاعده تسبیب اشاره نمود. همچنین، مبانی فقهی دیگری را مانند قاعده لا ضرر و قاعده اقدام نام برد؛ اما درواقع «قاعده مقابله با خسارت مثل قاعده اقدام یک قاعده عقلی است».[۶۳]

در کنار قاعده مقابله با خسارت، بحث مشارکت زیان‌دیده در وقوع زیان هم مطرح است. هرگاه زیان‌دیده در ورود ضرر ابتدایی به خود مشارکت داشته باشد، شخصاً مسئول زیان وارده است. در واقع ایجاد خسارت مرتبط با تقصیر هر دو طرف بوده است و بر اساس آن خسارت قابل مطالبه خواهان کاهش می‌یابد. تفاوت مهم این تأسیس با قاعده مقابله با خسارت در این است که قاعده مقابله با خسارت در خصوص شخص متضرر است؛ یعنی همین‌که ضرر واقع شد از آن لحظه به بعد برای زیان‌دیده وظیفه کاهش یا جلوگیری از افزایش خسارات ایجاد می‌شود؛ ولی در تقصیر مشترک، قبل از وقوع زیان، خود زیان‌دیده با زیان زننده باعث زیان می‌شوند.[۶۴]

باید توجه داشت که رعایت این قواعد، باعث جلوگیری از ورود ضرر و زیان و گسترش آن در بانک‌های مجازی هم خواهد شد.

۲-۱-۲- وظیفه مشتریان بانک مجازی در حفاظت از امنیت خود

اگر بانک مجازی کاملاً اینترنتی، به هر علتی چه قراردادی و چه خارج از قرارداد مقصر باشد و به

---

۶۳. مهراب داراب‌پور، مسئولیت‌های خارج از قرارداد (تهران: مجد، ۱۳۸۷)، ۹۱.

۶۴. نک: مهراب داراب‌پور و دیگران، اصول و مبانی حقوق تجارت بین‌الملل، کتاب ششم (تهران: انتشارات گنج دانش، ۱۳۹۷)، ۳۵-۶۹.

مشتریان (کاربران) بانک مجازی خسارتی وارد آید، طبیعتاً مسئول جبران خسارت است. در مقابل آیا در این فضای مجازی کاربران وظیفه‌ای در قبال محافظت از خود دارند؟

امروزه تقصیر شخص، دیگری را از رعایت احتیاط و مراقبت متعارف نسبت به مقصر معاف نمی‌سازد؛ بدین ترتیب، گاهی خواهان در قبال دیگران و گاهی در برابر خود متعهد به مراقبت است. کاربران در دنیای مجازی نیز باید اقدامات مقتضی را برای پیشگیری از ضرر و بعد از وقوع ضرر، برای کاهش خسارات و یا حداقل، برای عدم افزایش آن انجام دهند؛ زیرا امنیت آنلاین با کاربران آغاز می‌شود و باید آنان را برای محافظت از خود در برابر خطرات ناشی از اینترنت متقاعد کرد. افزایش حس مسئولیت شخصی کاربران برای مداخلات ایمنی آنلاین لازم است، اما کافی نیست؛ استراتژی مداخله به‌منظور افزایش رفتارهای ایمنی آنلاین باید با سطح آگاهی کاربران مطابقت داشته باشد و برای آن قانون‌نویسی شود و یک نهاد رسیدگی‌کننده فعال و سریع به وجود آید.

لذا وظیفه کاربران تغییر کرده است و مشتریان بانک‌های مجازی، هم قبل از وقوع ضرر و هم پس از آن وظایفی بر عهده دارند. البته در آغاز باید آموزش‌های لازم و امکانات کافی در اختیار آنان قرار بگیرد. همچنین، تصویب نوع و استاندارد رفتارهای ایمنی آنلاین ضروری است.

مطابق ماده ۴۵ آیین‌نامه بانک مجازی ایران، این بانک قبل از اعطای مجوز دسترسی به عملکردهای بانکداری الکترونیکی، باید برنامه‌های اطلاع‌رسانی و آموزشی مناسبی را در مورد محصولات و خدمات بانکداری الکترونیکی برای حصول اطمینان از اینکه، مشتری به‌درستی از آن‌ها اطلاع یافته است، تهیه نماید. برای این منظور، بانک مجازی می‌تواند، از طرق مختلف مانند بروشورهای تبلیغاتی استفاده نمایند.

بعد از این‌که بانک مجازی اقدامات لازم و کافی جهت آموزش مشتری را انجام داد، مشتریان این بانک، باید تمام نکات و توصیه‌های آموزشی و دستورالعمل‌های امنیتی صادره توسط بانک را کاملاً رعایت نمایند. مثل دانلود نرم‌افزارهای بانک مجازی از سایت‌های معتبر تعیین شده و منابع رسمی، مخفی نگه‌داشتن رمز عبور، استفاده از مدیریت رمز عبور و عدم استفاده از رایانه‌های عمومی برای دسترسی به اطلاعات حساب آنلاین، لذا، مشتری باید اقدامات پیشگیرانه را اعمال کند تا از بروز حادثه جلوگیری نماید. اگر این اقدامات را انجام ندهد؛ بر اساس منطق و مقررات عام مسئولیت مدنی و بحث مشارکت در ایجاد ضرر و یا بحث تعدد اسباب، با آنکه خود زیان‌دیده است، مسئول شناخته می‌شود. علت این امر عدم رعایت احتیاط کافی و عدم اقدام همانند یک انسان متعارف، است؛ ازاین‌رو زیان‌دیده آن

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

قسمت از خسارتی که به دست خود وی یا دیگری ایجاد شده است و یا می‌توانسته مانع از ایجاد آن شود را نمی‌تواند از زیان زننده بگیرد.

همچنین، در زمانی که ضرر حادث شد، وظیفه مشتری، برای مقابله با خسارت شروع می‌شود. اقدامات ممکن است منطبق با تهدید یا غیر منطبق با آن باشد. اگر این اقدامات منطبق باشند، معمولاً باعث کاهش خطرات حادث شده می‌شوند. به‌عنوان مثال، اگر برخی از اطلاعات محرمانه مالی مشتری در دسترس دیگران قرار گرفت یا از بین رفته باشد و یا رمز عبور او دیگر ایمن نباشد و سیستم وی کاملاً ویروسی شده و برخی از اطلاعات وی دیگر در دسترس نباشد؛ حتی در فرض مقصر بودن بانک مجازی مثلاً در عدم اقدام به بروزرسانی سیستم بانک مجازی، مشتری باید اقدامات متعارف را انجام دهد. مانند اطلاع به بانک مجازی از طرق پیش‌بینی شده، مانند ایمیل فوری عمل نماید تا از بروز ضرر بیش‌تر جلوگیری کند.

مطابق بند ۲۱ و ۲۲ دستورالعمل بانک مجازی هنگ‌کنگ، مشتریان باید از مسئولیت‌های خود برای حفظ امنیت در استفاده از خدمات بانکداری مجازی و مسئولیت احتمالی خود در صورت عدم انجام آن آگاه شوند. به‌ویژه، شرایط باید نشان دهد که چگونه هرگونه ضرر ناشی از نقض امنیت، خرابی سیستم یا خطای انسانی بین بانک و مشتریان تقسیم می‌شود. در این راستا، نظر مرجع پولی هنگ‌کنگ، این است که مشتری نباید در قبال هرگونه ضرر مستقیمی که در نتیجه تراکنش‌های غیرمجاز انجام شده و از طریق حساب خود متحمل می‌شود، مسئولیتی داشته باشد، مگر اینکه مشتری متقلبانه یا با سهل‌انگاری فاحش، مانند عدم محافظت صحیح از دستگاه‌ها یا کدهای مخفی خود برای دسترسی به خدمات بانکداری الکترونیکی، برعلیه خود اقدام کند.[۶۵]

در نتیجه از آنجایی که بحث اینترنت و فضای مجازی بسیار گسترده شده است و خسارات زیادی در این حوزه به کاربران اینترنت وارد می‌شود، بحث تحمیل مسئولیت شخصی به کاربر افزایش یافته است. اگر این‌گونه عمل شود امنیت فضای مجازی بهتر تأمین خواهد شد. به‌علاوه، از آنجایی که دنیا به‌سرعت به سمت بانکداری مجازی در حرکت است، باید برای حفظ امنیت امور مالی مشتریان این بانک‌ها نیز به این قاعده عقلی استناد نمود؛ بنابراین، حتی اگر بانک مجازی مقصر باشد، می‌تواند به‌عنوان دفاع به‌قاعده مقابله با خسارات متوسل شود و از خسارات مورد مطالبه بکاهد. کاربر، عامل کلیدی در امنیت فضای مجازی است و اغلب حفره‌های امنیتی که برای متخلفان در این فضا ایجاد می‌شود، نیز به‌وسیله

65. Hong Kong Monetary Authority, “Guide to Authorization, Chapter 9, Authorization of Virtual Banks”, Issue Date, 23 Mar 2022.

خود کاربر ایجاد می‌شود. پس با ایجاد مقابله خودکار آمد و رفتارهای محافظه‌کارانه به‌سادگی می‌توان از تهدیدات آنلاین جلوگیری کرد.

۲-۲ مدیریت ریسک امنیت

مدیریت ریسک امنیت سایبری و فناوری، یک چالش بزرگ برای بانک‌های مجازی است. اگرچه حملات سایبری و عدم انعطاف‌پذیری سیستم می‌تواند هم برای بانک‌های سنتی و هم برای بانک‌های مجازی، مضر باشد؛ اما مسلماً تأثیر بیشتری بر بانک‌های دومی دارد. بانک‌های مجازی باید یک رویکرد مدیریت ریسکِ مناسب با هدف خود، اتخاذ کنند که راحتی پلتفرم‌های دیجیتال و برنامه‌های تلفن همراه را با حفاظت از داده‌ها، کنترل‌های امنیت سایبری و زیرساخت فناوری اطلاعات انعطاف‌پذیر، متعادل سازند. با ارتقای اعتماد از طریق استفاده از آخرین فناوری برای دفاع سایبری، می‌توانند تجربیات بانکی نوآورانه و قابل اعتماد را برای همه مشتریان خود فراهم کنند.

در بانک مجازی باید مسئولیت‌ها واضح باشد و تعامل منظمی با رهبران کسب‌وکار ایجاد شود. همچنین باید نظارت دقیق اصلاحی بر مقررات وجود داشته باشد تا شکاف‌های شناسایی شده را برطرف کند. علاوه بر این‌ها برای کاهش ریسک در بانک مجازی ذیلاً چندین مؤلفه ارائه می‌شود:

۲-۲-۱- داشتن اصول راهنما و ارزیابی منظم ریسک

محرمانه بودن اطلاعات مشتری، حفاظت از سپرده‌های مشتریان و مبارزه با پول‌شویی در بانک مجازی نباید هرگز به خطر بیفتند؛ ازاین‌رو، این موارد مشمول کنترل الزامی هستند. همچنین، رمزگذاری داده‌ها، پیکربندی ایمن و یک ساختار سیستم بسیار انعطاف‌پذیر، باید در این بانک‌ها وجود داشته باشد.[۶۶] اگر بانک‌های مجازی نتوانند داده‌ها را رمزگذاری کنند، ممکن است نتوانند اعتماد مشتریان را جلب کنند و مشتریان تمایلی به استفاده از بانک‌های مجازی نداشته باشند.[۶۷] بنابراین، برای کاهش ریسک، به اصول راهنمای واضحی، نیاز است.

همچنین، با توجه به محیط کسب‌وکار پویاتر بانک‌های مجازی، بررسی تشخیص انواع شکست‌های کنترلی باید به شکل منظم‌تری نسبت به بانک‌های معمولی انجام شود؛ پس در بانک مجازی به ارزیابی منظم ریسک و آزمایش کنترلی مستمر نیاز است.

66. Tse, op. cit.
67. Nguyen, op. cit., 28

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

۲-۲-۲ - به‌کارگیری سَندباکس نظارتی

«سَندباکس نظارتی»،[۶۸] چارچوبی است که توسط یک تنظیم‌کننده راه‌انـدازی شده است که به استارت‌آپ‌های فین‌تک و دیگر نوآوران اجازه می‌دهد تا آزمایش‌هایی را در یک محیط کنترل‌شده تحت نظارت یک تنظیم‌کننده انجام دهند.

در هنگ‌کنگ، بانک‌هایی که از سازمان پولی این کشور مجوز گرفته باشند، می‌توانند برای ورود، حضور و تحت نظارت بودن در سندباکس این سازمان درخواست بدهند. مزیت اصلی این امر این است که این بانک‌ها می‌توانند در طول دوره آزمایشی، با رعایت برخی از معیارها، بدون نیاز به پیروی کامل از الزامات نظارتی متداول این سازمان، طرح‌هایی را به‌صورت آزمایشی اجرا کنند که شامل خدمات بانکداری واقعی است. به‌عبارت دیگر، بانک‌هایی که می‌خواهند در سندباکس سازمان پولی هنگ‌کنگ فعالیت کنند، می‌توانند پیش از راه‌اندازی رسمی طرح‌های فین‌تک خود، آن‌ها را به شکل واقعی بررسی کنند. این بررسی‌ها به آن‌ها امکانی را می‌دهد که آسان‌تر و در محیطی کنترل شده در مورد خدماتشان داده‌های واقعی و بازخورد کاربران را جمع‌آوری کنند تا اگر لازم باشد، اصلاحات مناسبی در آن‌ها اعمال نمایند. بعد از اتمام دوره سندباکس، بانک‌ها می‌توانند خدماتشان را به‌طور رسمی و در مقیاسی گسترده‌تر عرضه کنند، به‌شرط آن‌که بتوانند از سایر الزامات نظارتی که خارج از بستر سندباکس شامل حالشان می‌شود، پیروی کنند.[۶۹]

وقتی خدمات به‌صورت موفقیت‌آمیز از سندباکس خارج شوند، به این معنی است که نهادهای نظارتی، مدل تجاری و ریسک‌های آن را مورد بررسی قرار داده‌اند. پس در این محیط، امنیت خدمات و مدیریت ریسک نیز سنجیده شده است. در بانک مجازی، مدیران ریسک، باید برای مدیریت یک پروفایل ریسک متفاوت، با تمرکز بیشتر بر فناوری، آماده باشند. یکی از راهکارها برای مدیریت بهتر ریسک، به‌کارگیری همین سندباکس نظارتی است که خدمات جدید با قرار گرفتن در یک محیط کنترل‌شده، آزمایش می‌شوند تا اطمینان حاصل شود که عوامل خطر آنان کشف و مدیریت می‌شوند.[۷۰]

۲-۲-۳ مدیریت تداوم کسب‌وکار

---

68. Regulatory Sandboxes

۶۹. بیکر و مکنزی، راهنمای بین‌المللی سندباکس‌های رگولاتوری فین‌تک، ترجمه راه پرداخت، (تهران: انتشارات راه پرداخت، ۱۳۹۸)، ۷-۹.

70 Tse, op. cit.

اگرچه بانک‌های مجازی چندین سال است که فعالیت می‌کنند، بسیاری از خطرات به‌طور کامل پیشگیری و کنترل نشده‌اند که ممکن است برای پایداری کسب‌وکار آنها مضر باشد. هنگامی که مرکز داده‌های بانک مجازی، ریسک امنیت اطلاعات را دارد، مانند حفره‌های امنیتی یا نفوذ غیرمجاز که منجر به کندتر شدن کارکرد آن یا قطع شدن سیستم‌های اطلاعاتی می‌شود. این امر باعث زیان‌های اقتصادی هنگفت و زیان اعتباری به آن بانک می‌گردد؛ بنابراین، بانک‌های مجازی باید مدیریت امنیتی و پیشگیری را به‌موقع انجام دهند. به‌خصوص در صورت بروز خطرات امنیت اطلاعات، این بانک‌ها باید از عملکرد عادی سیستم اطلاعاتی اطمینان حاصل کنند و یا بتوانند پس از وقفه به موقع بازیابی شوند تا از ضرر به اموال مشتریان و اثرات اجتماعی ناشی از آن حملات، بکاهند.

از مدیریت تداوم کسب‌وکار،[۷۱] به‌عنوان یکی از مؤثرترین برنامه‌ها در مواجهه با بحران، حوادث و بلایای طبیعی، به‌ویژه در مورد برنامه‌های سازمان برای ادامه عملیات یا از سرگیری عملیات استفاده می‌شود.

در هنگ‌کنگ، فرآیندهای مدیریت تداوم کسب‌وکار، فرآیندهای مدیریت یکپارچه برای شرکت‌ها هستند. این فرآیندها شرکت‌ها را قادر می‌سازند بحران‌های بالقوه و تأثیرات مرتبط را به رسمیت بشناسند و استراتژی‌ها، برنامه‌ها و ترتیبات پاسخ به ریسک و بازیابی تداوم تجارت را تدوین کنند. هدف اصلی این نوع مدیریت، بهبود قابلیت‌های پیشگیری از ریسک شرکت برای مقابله مؤثر با وقفه‌های غیرمنتظره تجاری و کاهش عوارض جانبی است. اصول اساسی آن، اطمینان از این است که عملیات اصلی تجارت مؤسسات، می‌توانند همیشه به حرکت خود ادامه دهند. علاوه‌بر این، BCM سناریوهای کسب‌وکار را از پیش برنامه‌ریزی کرده است تا در صورت شکست فرآیندهای کلیدی آن، برای بانک‌های مجازی آماده باشند. به‌طور خلاصه، پیاده‌سازی BCM می‌تواند امنیت اطلاعات مشتریان را در بانک‌های مجازی هنگ‌کنگ تقویت کند تا پایداری کسب‌وکار خود را حفظ کند. پس برای مواجهه با ریسک‌های جدید، باید روش‌های مدیریت ریسک مدرن به‌کار گرفته شود.[۷۲]

در بند ۱۴ تا ۱۷ دستورالعمل بانک مجازی هنگ‌کنگ، ریسک فناوری و مدیریت ریسک، بیان شده و تأکید شده است که: ریسک‌های مربوط به فناوری به‌ویژه امنیت اطلاعات، انعطاف‌پذیری سیستم و مدیریت تداوم کسب‌وکار، برای یک بانک مجازی اهمیت حیاتی دارد. نقض امنیت و دست‌کاری

71. Business Continuity Management (BCM)
72. Chen, op. cit., 2-7.

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

غیرمجاز در سیستم‌های بانک می‌تواند منجر به زیان مالی و همچنین از دست رفتن اعتبار بانک شود. اصل کلی این است که کنترل‌های مربوط به امنیت و فناوری موجود باید مناسب با هدف باشند. در این رابطه، متقاضی تأسیس بانک مجازی، ملزم به استخدام یک کارشناس واجد شرایط و مستقل خواهد بود. متقاضی، باید انواع ریسک‌هایی که در معرض آن قرار دارد را بشناسد و سیستم‌های مناسبی را برای شناسایی، اندازه‌گیری، نظارت و کنترل این ریسک‌ها ایجاد کند.[۷۳] این دستورالعمل، متقاضیان را ملزم می‌کند که یک گزارش ارزیابی مستقل و متخصصانه از سیستم‌های فناوری اطلاعات خود را دریافت کنند و آن را به مرجع پولی هنگ‌کنگ ارائه کنند. بررسی منظم سیستم‌ها و امنیت آن نیز باید توسط متقاضی با در نظر گرفتن هرگونه تغییر در فناوری انجام شود.[۷۴]

به‌طورکلی، محیط نظارتی بانکی، با هدف تعیین و حفظ استانداردهای قانونی و نظارتی منسجم برای اهداف پیشگیری و کاهش ریسک است. درنتیجه، استانداردهای نظارتی به‌طور اجتناب‌ناپذیری به ریسک‌ها گره خورده‌اند. به همین دلیل، چارچوب نظارتی مبتنی بر ریسک مرجع پولی هنگ‌کنگ، هشت نوع ریسک اساسی یعنی اعتبار، نرخ بهره، بازار، نقدینگی، عملیات و شهرت را به همراه ریسک‌های قانونی و استراتژیک تجویز می‌کند.[۷۵]

مقررات فوق در مورد الزامات خاص مدیریت ریسک فناوری اطلاعات توضیحی ارائه نمی‌دهد، بلکه فقط ایجاب می‌کند که باید «مناسب برای هدف» باشد. قضاوت در مورد ریسک‌های اصلی بانک‌های مجازی و اقدامات مدیریتی آن‌ها بر اساس تفاوت مشتریان اصلی که به آن‌ها خدمت می‌کنند، است. البته عملیات تجاری بانک‌های مجازی در هنگ‌کنگ، باید از آیین‌نامه عملکرد بانکی صادر شده توسط انجمن بانک‌های هنگ‌کنگ [۷۶] پیروی کنند. از نظر کسب، استفاده و ذخیره‌سازی داده‌های مشتری، آن‌ها باید با فرمان داده‌های شخصی (حریم خصوصی)[۷۷] مطابقت داشته باشند. جنبه حفاظت از داده‌ها، (PDPO)، تصریح می‌کند که کاربران داده‌ها ملزم به انجام کلیه اقدامات عملی برای محافظت از داده‌های شخصی در برابر دسترسی، پردازش، حذف، از دست دادن یا استفاده غیرمجاز یا تصادفی هستند. درنتیجه، بانک‌های مجازی باید مشخصات قراردادی یا روش‌های دیگر (مانند BCM) را اتخاذ

73. Hong Kong Monetary Authority, op. cit.
74. Gabriela Kennedy, "Asia Pacific new ", Elsevier, COMPUTER LAW & SECURITY REVIEW, 34 (2018), 424, accessed June 23, 2024.
75. Lee, op. cit., 104
76. Hong Kong Association of Banks (HKAB)
77. Personal Data (Privacy) Ordinance (PDPO)

کنند تا اطمینان حاصل شود که پردازش داده‌ها الزامات امنیت داده‌ها را برآورده می‌کند و پایداری کسب‌وکار خود را حفظ می‌کند.[۷۸]

۲-۲-۴- بیمه کردن

راهکار دیگر، جهت حفظ امنیت بانک‌های مجازی، بیمه کردن موجودی حساب است. در ایالت متحده آمریکا تا ۲۵۰۰۰۰ دلار از موجودی حساب در اکثر بانک‌های توسط شرکت بیمه سپرده فدرال (FDIC) محافظت و بیمه می‌شوند.[۷۹] در این کشور، همه بانک‌ها، از جمله بانک‌های مجازی، اعلام می‌کنند که آیا در این شرکت بیمه شده‌اند و به چه‌میزان. پس برای کاهش خطرات، بسیاری از بانک‌های مجازی تحت طرح حمایت از سپرده‌ها در محل خود، بیمه شده‌اند. در اتحادیه اروپا نیز، بانک‌های مجازی تابع استانداردهای مشابه بانک‌های سنتی هستند و سپرده‌ها تحت دستورالعمل طرح تضمین سپرده،[۸۰] محافظت می‌شوند. در هنگ‌کنگ، هر بانک دارای مجوز، ازجمله بانک‌های مجازی، باید بخشی از طرح حفاظت از سپرده [۸۱] باشد، مگر اینکه هیئت‌مدیره به آن‌ها معافیت بدهد. هیئت حفاظت از سپرده هنگ‌کنگ،[۸۲] که یک نهاد حقوقی مستقل است، مسئول نظارت بر طرح حفاظت از سپرده است.[۸۳]

۲-۲-۵- استفاده از فناوری بلاکچین

به‌طور عمده، داده‌های ذخیره شده و مدیریت شده متمرکز، به بانک‌های مجازی کمک می‌کند تا مقررات مربوط به بانکداری یا حفاظت از حریم خصوصی داده‌ها را راحت‌تر رعایت کنند. بانک‌های مجازی در بهره‌برداری از فناوری و روند جدید مزیت دارند. استفاده از فناوری بلاکچین، تأثیر قابل توجهی بر مدل‌های کسب‌وکار بانکی خواهد داشت.[۸۴] فرآیند رمزنگاری شبکه‌های بلاکچین با استفاده از سیستمی پیچیده صورت می‌گیرد که باعث تأمین امنیت شبکه می‌شود. بلاکچین یک دفترکل توزیع شده، غیرمتمرکز و غیرقابل‌تغییر است که امکان ثبت تراکنش‌ها را در یک شبکه فراهم می‌کند. در

78. Chen, op. cit., 7.
79. Jason Fragoso, “Online Banking Security: How To Keep Your Accounts Safe”, February 21, 2024, At: https://www.aura.com/learn/online-banking-security . (accessed June 15, 2024).
80. The Deposit Guarantee Scheme Directive.
81. Deposit Protection Scheme (DPS)
82. The Hong Kong Deposit Protection Board
83. Statrys, “Are Virtual Bank Accounts Safe? Tips on Safety Best Practices”, 2023-08-17, At: https://statrys.com/blog/are-virtual-bank-accounts-safe. (Accessed June 15, 2024).
84. Nguyen, op. cit.,12-13.

سال‌های اخیر، بلاکچین به‌عنوان فناوری قابل استفاده در بخش‌های مختلف ظاهر شده است.[۸۵]

در بلاکچین اعتماد به سیستم، ایجاد می‌شود. با استفاده از کدباز[۸۶] بسیاری از عرضه‌کنندگان بلاکچین، به کاربران شبکه خود جهت به‌روزرسانی و بهبود کد مبنایی بلاکچین، متکی هستند؛ به‌این‌ترتیب تا زمانی که هر کاربر به کد مبنایی بلاکچین اعتماد کند، سیستم، قابل اعتماد باقی می‌ماند، مگر این‌که کسی دارای بیش از ۵۱ درصد از کل توان محاسباتی در شبکه باشد. برای کنترل یک شبکه، یک هکر باید اکثریت قدرت استخراج را داشته باشد که به‌عنوان قانون «حمله ۵۱٪»[۸۷] شناخته می‌شود. علاوه‌بر هزینه و سختی کار این حمله، اشخاصی که سعی دارند به شبکه حمله کنند، نه تنها باید ۵۱ درصد از شبکه را کنترل کنند، بلکه باید بلاکچین تغییر یافته را نیز در زمان بسیار دقیقی معرفی کنند؛ بنابراین، امکان به نتیجه رسیدن‌شان بسیار کم است،[۸۸] اما محال نیست؛ لذا، می‌توان ویژگی تغییرناپذیری را به‌عنوان «بسیار دشوار برای تغییر»، توصیف کرد که در مقابل «دائماً غیرقابل تغییر» قرار می‌گیرد.[۸۹]

با این‌حال، حقوقدانان کشور هنگ‌کنگ بر این باورند که بهره‌مندی بانک‌های مجازی از فناوری دفترکل توزیع شده به‌عنوان بخشی از زیرساخت فناوری اطلاعات، باعث کاهش خطرات حملات سایبری می‌شود. چراکه با استفاده از یک سیستم غیرمتمرکز، سازمان‌دهی یک حمله برای مهاجمان سایبری دشوارتر خواهد شد.[۹۰] همچنین در سال ۲۰۱۷، مرجع پولی هنگ‌کنگ، چندین قرارداد همکاری با چین و سایر کشورها امضا کرده است تا به‌طور مشترک یک زیرساخت فرامرزی مبتنی بر فناوری دفترکل توزیع شده، برای دیجیتالی کردن و مبادله اسناد تجاری بین این دو، برای به حداقل رساندن تقلب و افزایش بهره‌وری ایجاد کنند.[۹۱]

85. Roshan Khadka, “The Impact of Blockchain Technology in Banking: How can blockchain revolutionize the banking industry?”, Centria University of Applied Sciences, October 2020. Accessed 2 February 2022.

86. Open Source

87. 51% Attack Rule

88. Jake Frankenfield, “51% Attack”. June 2022.

۸۹. پریسا قربانی زیردهی و غزاله دخیلی، «بلاکچین و رمز ارز»، مجله حقوق بانکی، ۱۴-۱۵(۱۳۹۷-۱۳۹۸)، ۱۰۷.

90. Dominic Wai and Joshua Chu- from Onc Lawyers, “Hong Kong: Virtual banking and data privacy”, Accessed April 27, 2022.

91. Chen, op. cit.,.7.

نتیجه‌گیری

بانک مجازی بانکی فراگیر است که تمام خدمات بانکی را به‌طور کاملاً آنلاین به مشتریان خود ارائه می‌دهد و فاقد شعبه فیزیکی است. برخلاف نئوبانک که صرفاً شعبه مجازی یک بانک سنتی است؛ بنابراین، نباید هیچ‌گاه ارزش یک بانک مجازی را به شعبه مجازی تنزل مقام داد. بانک مجازی در کنار به‌کارگیری حداکثری فناوری، از یک‌سو، نوع جدیدی از تجربه را برای مشتریان رقم می‌زند و از سوی دیگر، وضعیت شمول مالی را بهبود می‌بخشد.

ادغام بانکداری و فناوری، ریسک‌های جدیدی را برای بانک‌های مجازی به ارمغان آورده است. عملکرد این بانک‌ها موجب نگرانی‌های متعددی در مورد حفاظت از حریم خصوصی داده‌ها و امنیت سایبری شده است؛ بنابراین، تأمین امنیت در این بانک‌ها حائز اهمیت فراوان است که باید برای این مهم به دنبال راهکارهایی بود. در کشورهای مختلف، اقدامات زیادی برای تنظیم، نظارت و ایجاد بانک‌های مجازی انجام شده و روش‌های مختلفی در این رابطه اعمال می‌شود. برخی کشورها مقررات خاصی را برای بانک‌های مجازی وضع کردند و قوانینی هم در خصوص حفاظت از داده‌های شخصی و امنیت سایبری تصویب نمودند.

به‌علاوه، اعمال سَندباکس نظارتی و بهره‌مندی از فناوری بلاکچین، در کنار مدیریت تداوم کسب‌وکار، نیز می‌تواند خطرات این فضا را کاهش دهد. همچنین، با ورود بانک مجازی به دنیای متاورس، شفافیت افزایش یافته و از داده‌ها حفاظت می‌شود؛ زیرا خدمات در متاورس بر روی بلاکچین اجرا می‌شوند که این بالاترین درجه شفافیت و حفظ حریم خصوصی داده‌ها را به دنبال دارد. در کنار این اقدامات، تحمیل برخی از مسئولیت‌های شخصی به مشتریان بانک مجازی، ازجمله مقابله با خسارات، راهکاری مبتنی بر عقل و قانون بوده که مانع ایجاد حفره‌های امنیتی شده و امنیت فضای سایبری را تأمین می‌کند.

کشور ایران در سال ۱۳۹۰ آیین‌نامه تأسیس و فعالیت بانک‌های مجازی را تصویب نمود که در همان سال تصویب، زیرساخت حقوقی مناسبی را برای تأسیس، اداره، بازرسی و نظارت بانک مجازی فراهم آورد؛ ولی اکنون ـ با بررسی سایر مقررات کشورهای پیشرو که در سال‌های اخیر، دستورالعمل‌های اختصاصی خود را برای بانک‌های مجازی تصویب کردند همچون، هنگ‌کنگ و مالزی ـ می‌توان متوجه نقص و خلأهای بی‌شماری در آن شد؛ ازاین‌رو، برای تأسیس بانک مجازی کارآمد باید مقررات آن به‌روزرسانی شود.

Asef Kabiri, Zahra. “Legal Independency of Virtual Banks, their Preservation and Security”, Journal of Financial and Economic Law Research. V. 1, No. 1 (September 21, 2024): 101-138.

البته، برای مقابله علیه تهدیدات امنیتی، همکاری عمومی ضرورت دارد. کاربران، آژانس‌های نظارتی، متخصصان امنیت سایبری و مؤسسات مالی باید با هم همکاری داشته باشند. قوانین سخت‌گیرانه پایبندی به الزامات امنیتی را تضمین کرده و محیط تراکنش‌هایی آنلاین را تقویت می‌کند. برای فناوری‌ها و فرآیندهای امنیتی نیز ضروری است که دائماً در حال نوآوری باشند تا با استراتژی‌های در حال تغییر مورد استفاده مجرمان سایبری مقابله شود.

درست است که بانک مجازی در ایران تأسیس نشده است؛ ولی با توجه به وجود چنین نهادهایی در دیگر کشورها، می‌توان احتمال تشکیل چنین بانک‌هایی را در ایران داد؛ لذا، غفلت از این نوع بانکداری می‌تواند کشور را از منافع آن محروم سازد. برای تأسیس این نوع بانک، در کنار اقدامات فنی، باید مقررات شایسته‌ای نیز بر مبنای پیشنهادات این تحقیق وضع و تصویب نمود.

فهرست منابع

الف) منابع فارسی

کتب

- اسکینر، کریس. قطب‌نمای بانکداری دیجیتال: درس‌هایی از رهبران تحول دیجیتال. ترجمه و تحقیق مهدی شامی‌زنجانی، فراز نبیی و درسا پورحسن. تهران: راه پرداخت، ۱۳۹۹.
- السان، مصطفی. حقوق بانکداری اینترنتی، ویرایش دوم. تهران: پژوهشکده پولی و بانکی، ۱۳۹۲.
- السان، مصطفی. حقوق بانکی، ویراست دوم با اضافات. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، ۱۳۹۳.
- السان، مصطفی. حقوق تجارت الکترونیکی. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، ۱۳۹۱.
- داراب‌پور، مهراب. قاعده مقابله با خسارت. تهران: کتابخانه گنج دانش، ۱۳۷۷.
- داراب‌پور، مهراب. مسئولیت‌های خارج از قرارداد. تهران: مجد، ۱۳۸۷.
- داراب‌پور، مهراب، محسن عبداللهی، رضا اسلامی، باقر شاملو و محمدحسین رمضانی‌قوام‌آبادی. اصول و مبانی حقوق تجارت بین‌الملل: کتاب ششم- مسئولیت‌ها، تعارض‌قوانین، حل‌وفصل اختلافات تجاری بین‌المللی حقوق بشر، محیط زیست، توسعه پایدار و جرائم تجاری بین‌المللی. تهران: انتشارات گنج دانش، ۱۳۹۷.
- داراب‌پور، مهراب، مصطفی السان، علی‌اکبر ادیب، محمد علیخانی، مریم غنی‌زاده، مرجان فاضلی و محمد داراب‌پور. چالش‌های حقوقی در معاملات بازرگانی بین‌المللی. تهران: خرسندی، ۱۳۹۶.

گزارش‌ها و مقالات چاپی و الکترونیکی

- بیکر و مکنزی. راهنمای بین‌المللی سندباکس‌های رگولاتوری فین‌تک. ترجمه راه پرداخت. تهران: انتشارات راه پرداخت، ۱۳۹۸.

مقاله چاپی

- قربانی زیردهی، پریسا و غزاله دخیلی. «بلاکچین و رمز ارز». مجله حقوق بانکی، ۱۴-۱۵(۱۳۹۷-۱۳۹۸)، ۹۳-۱۷۰.

مقالات برخط و الکترونیکی

- باقری، محمود و محمد صادقی. «مسائل و تبعات حقوقی بانکداری سایه». فصلنامه علمی دیدگاه‌های حقوق قضایی، دوره ۲۶، ۹۶ (۱۴۰۰): ۱ تا ۲۲. تاریخ دسترسی ۱۵ مرداد ۱۴۰۳، نشانی صفحه اینترنتی:

https://jlviews.ujsas.ac.ir/article_703690_2f12cbd09acabdec0c8bb8cf7485069a.pdf.

- پورسعید، رامین و پیمان قنبری. «بررسی بانکداری مجازی در نظام حقوقی ایران». دانش حقوق و مالیه، ۱ (۱۳۹۶): ۳۱ -۴۷. تاریخ دسترسی ۱۱ مرداد ۱۴۰۱، نشانی صفحه اینترنتی:

https://malieh.dmk.ir/article-1-30-fa.pdf.

- شامخی، وحید و سعید باباخانی. «سناریوهای آینده بانک مجازی در ایران افق ۱۴۱۰». شرکت تجارت الکترونیکی ارتباط فردا، ۱۳۹۹. تاریخ دسترسی خرداد ۱۴۰۱، قابل دسترسی در:

https://www.efarda.ir/VirtualBank_Future_Scenarios.pdf

مطالب برخط

– قربانی، رسول. «بالاخره گره کور بانک مجازی به دست بانک سپه باز خواهد شد؟». ۱ شهریور ۱۳۹۱. تاریخ دسترسی ۱۵ مرداد ۱۴۰۱. قابل دسترسی در:

https://way2pay.ir/14533/

– یگانگی، غزل. «نشست خبری بلوبانک با حضور مدیران و خبرنگاران برگزار شد/ ثبت بیش از ۲۲ میلیون تراکنش در بلوبانک». ۲۶ مهر ۱۴۰۰. تاریخ دسترسی ۱۰ آذر ۱۴۰۰. قابل دسترسی در:

https://way2pay.ir/246148/

– محمدجعفر نعناکار، «درآمدی حقوقی بر موجودیت نئوبانک‌ها». آذر ۱۴۰۰. تاریخ دسترسی ۷ آبان ۱۳۹۹. قابل دسترسی در:

https://way2pay.ir/206357/

– شامی زنجانی، مهدی. «انتشار گفتگوها در میزگرد نئوبانک توسط عصر تراکنش». خرداد ۱۴۰۰. تاریخ دسترسی ۱۲ تیر ۱۴۰۰. قابل دسترسی در:

http://shamizanjani.ir/

– حاجی، مینا. «بلوبانک چیست و چگونه می‌توان در آن حساب باز کرد؟/ افتتاح حساب در ۷ دقیقه». ۲۰ اسفند ۱۳۹۹. تاریخ دسترسی ۱ آذر ۱۴۰۰. قابل دسترسی در:

https://way2pay.ir/226957/

وب‌سایت‌های اینترنتی

– باشگاه خبرنگاران جوان. «آیا "بانک الکترونیکی" همان "بانک مجازی" است؟». تاریخ آخرین ویرایش ۱۱ خرداد ۱۳۹۳. قابل دسترسی در:

https://www.yjc.news/00KNYs.

– راه پرداخت. «بانک مجازی فرصت تحول و نوزایی بانکداری». تاریخ آخرین ویرایش ۱۳ تیر سال ۱۳۹۷، قابل دسترسی در:

https://way2pay.ir/106759/.

– عصر بانک. «بانکینو چیست و چه خدماتی دارد؟». تاریخ آخرین ویرایش ۱۰ اردیبهشت ۱۴۰۱. قابل دسترسی در:

https://asrebank.ir/160818/.

مقررات

– «آیین‌نامه تأسیس و فعالیت بانک‌های مجازی». مورخ ۱۳۹۰/۲/۲۷. مصوب شورای پول و اعتبار.

– «ضوابط ناظر بر نحوه ایجاد، فعالیت و نظارت بر واحد دیجیتال ارائه خدمات بانکی توسط مؤسسات اعتباری». تاریخ ابلاغ ۱۴۰۲/۹/۱۳. مصوب کمیسیون مقررات و نظارت مؤسسات اعتباری بانک مرکزی.

ب) منابع خارجی
مقالات و مقررات

- Baur-Yazbeck, Silvia ; Frickenstein, Judith & Medine, David, “Cyber Security in Financial Sector Development: Challenges and potential solutions for financial inclusion”, CGAP, (2019). 1-15. Accessed June 2024.

- Bhujanga Rao, Patcha, “A Study on Cybrr Security Issues Affecting Online Banking And Transactions”. Ijariie-ISSN(O)-2395-4396, Vol-9 Issue-6 (2023).1654-1665.

- Chen, Haosheng; Tse, Daniel; Si, Pengfei; Gao, Gefei; Yin, Chang, “Strengthen the security management of customer information in the virtual banks of Hong Kong through business continuity management to maintain its business sustainability”. Sustainability (Switzerland), 13(19), (2021), 1-24. Article 10918. https://doi.org/10.3390/su131910918.

- FANG, LI & Quintos, Darwin G. “Security Measures Applied on Digital Banking Towards Service Improvement Proposal”. *Journal of Business and Management Studies* (JBMS), 5(5) (2023), 47-77. accessed June 23, 2024. DOI: 10.32996/jbms.2023.5.5.5.

- Hong Kong Monetary Authority. “Guide to Authorization, Chapter 9, Authorization of Virtual Banks”, Issue Date, 23 Mar 2022. Available at: https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/guide-authorization/Chapter-9.pdf

- Kennedy, Gabriela, “Asia Pacific new”. Elsevier, Computer Law & Security Review, 34 (2018). 423-432. accessed June 23, 2024.

- Khadka, Roshan, “The Impact of Blockchain Technology in Banking”, Centria University of Applied Sciences, October 2020. Accessed February 2, 2022.
https://www.theseus.fi/bitstream/handle/10024/346030/Roshan_Khadka.pdf?sequence=2%26isAllowed=y.

- Lee, Emily, “Digital Financial Inclusion: Observations and Insights from Hong Kong’s Virtual Banks”, Law and Contemporary Problems, Vol. 84:95, 1 (2021). 95-113. accessed June 23, 2024. https://law.nus.edu.sg/ewbclb/wp-content/uploads/sites/6/2022/12/Digital-Financial-Inclusion-Observations-and-Insights-from-Hong-Kongs-Virtual-Banks-as-Compared-to-Singapores-Digit.pdf

- Bank Negara Malaysia (Central Bank of Malaysia). “Licensing Framework for Digital Banks”. Issued on: 31 December 2020. Available at: https://www.bnm.gov.my/documents/20124/938039/20201231_Licensing+Framework+for+Digital+Banks.pdf

-Sarkar, Swapan. “Banking in Metaverse - Opportunities and Challenges”. Management Accountant Journal, 58, 1(2023), 63-67. Accessed Murch 20, 2023. DOI: 10.33516/maj.v58i1.63-67p.

مطالب برخط و وب‌سایت‌های اینترنتی

- Djon Ly. “8 Virtual Banks in Hong Kong: How Do They Compare?”. 2024-05-16. At: https://statrys.com/blog/virtual-banks-hk . accessed July 12, 2022

- Dominic Wai. and Joshua Chu- from ONC Lawyers, “Hong Kong: Virtual banking and data privacy”, (n d), https://www.dataguidance.com/opinion/hong-kong-virtual-banking-and-data-privacy. (Accessed April 27, 2022).

- Fragoso, Jason, “Online Banking Security: How To Keep Your Accounts Safe”, February 21, 2024, At: https://www.aura.com/learn/online-banking-security . (accessed June 15, 2024).

- GuardRails. “The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them”. 24 Jun 2023. At: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/. (Accessed June 17, 2024).

- https://www.consumeraffairs.com/finance/first-internet-bank.html. (accessed July 12, 2022).

- https://www.investopedia.com/terms/1/51-attack.asp. (accessed September 14, 2022).

- Jake Frankenfield. “51% Attack”. June 2022.

- Jennifer Schurman, “First Internet Bank”. May 2022.

- Monzo Bank. “Why Monzo doesn›t have branches”. Accessed October 10, 2023. Available at: https://monzo.com.

- Nguyen, Trung Viet, “Virtual bank by FinTech firms – Global trending, challenges, solutions and experience of regulating virtual banks in Vietnam”, Master Thesis, Tilburg Law School, 2020.

- Rendell, R. “Why Digital Trust Should Be a Top Priority For Banks”, 2022. At: https://www.paymentsjournal.com/why-digital-trust-should-be-a-toppriority-for-banks/ . (accessed June 15, 2024).

- Siapartners, “Virtual BaNnking - Overeview of The Current Landscape”, last modified June 24, 2020, https://www.sia-partners.com/en/news-and-publications/from-our-experts/virtual-banking-overview-current-landscape.

- Statrys. “Are Virtual Bank Accounts Safe? Tips on Safety Best Practices”. 2023-08-17, At: https://statrys.com/blog/are-virtual-bank-accounts-safe . (Accessed June 15, 2024)

- Tse, Donald. “Cybersecurity and Technology Risk in Virtual Banking”. 4 January 2022. At: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-and-technology-risk-in-virtual-banking . (Accessed June 15, 2024).