International Law Review, Volume 41, Issue 74, Summer 2024/ pp. 35-64

Financial Messaging and International Law: SWIFT, Sanctions, and Alternative Networks
(Original Research)

Marzieh Ghobadi *
Hamid Ghanbari **

(DOI) : 10.22066/cilamag.2024.2015816.2476
Date Recived: 14 Nov.2023 Date Accepted: 2 Jul.2024

Abstract
The imposition of financial messaging sanctions against select states in recent years has proven to be a markedly effective measure within the realm of international affairs. In this context, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) has been particularly targeted by sanctioning entities- such as political blocs and sovereign governments- as a potent instrument to exert coercive pressure on recalcitrant states. This development has, in turn, prompted certain affected states to seek out alternative financial networks and technological solutions to circumvent the SWIFT system. Concurrently, the advent of recent advancements in financial and blockchain-based technologies has given rise to the notion of establishing faster, more cost-effective, and more transparent monetary transaction mechanisms as potential replacements for the existing SWIFT infrastructure. This confluence of developments has raised a series of issues in public international law that warrant rigorous examination. Employing a descriptive-analytical method, this article seeks to elucidate the multifaceted legal challenges surrounding the sanctioning of the SWIFT system in the realm of international law. While introducing the significance of SWIFT and exploring the relevant domestic laws in Iran, it critically examines the legitimacy, or lack thereof, of the international sanctions imposed on the SWIFT network. Furthermore, it evaluates the responses of various states to the SWIFT-related sanctions and some of the alternative solutions proposed by governments. Findings suggest that the imposition of sanctions on the SWIFT network has had profound implications on the global financial landscape. One key consequence has been the acceleration of efforts by sanctioned states to

* Corresponding Author, Assistant Professor, Department of Law, Islamic Azad University, Shahrood Branch, Semnan, Iran; marzieh.ghobadi@yahoo.com

** International Law Researcher, Central Bank of Islamic Republic of Iran, Tehran, Iran; hamid.ghanbari1982@gmail.com

develop and implement alternative financial messaging systems, such as Russia's SPFS (System for Transfer of Financial Messages) and China's CIPS (Cross-Border Interbank Payment System).

Keywords
SWIFT, Financial Messaging, Restrictive Measure, Block Chain, Confidentiality

پیام‌رسانی مالی و حقوق بین‌الملل: سوئیفت، تحریم‌ها و شبکه‌های جایگزین (پژوهشی)

مرضیه قبادی *
حمید قنبری **

(DOI) : 10.22066/cilamag.2024.2015816.2476
تاریخ دریافت: ۱۴۰۲/۰۸/۲۴ تاریخ پذیرش: ۱۴۰۳/۰۴/۱۲

چکیده
تحریم شبکه‌های پیام‌رسانی مالی، یکی از مهم‌ترین و مؤثرترین قسمت‌های تحریم‌های مالی و اقتصادی است که در سال‌های اخیر علیه کشورهای متعددی وضع و اجرا شده است. در این میان سوئیفت[1] به‌عنوان مهم‌ترین سکوی پیام‌رسانی مالی بین‌المللی به‌طور خاص مورد توجه واضعان تحریم‌های بین‌المللی بوده است. تلاش‌های بسیار گروه‌های سیاسی (نظیر کنشگران تحریم‌ها، گروه‌های طرفدار حقوق بشر و حتی حامیان فلسطین) و دولت‌های گوناگون برای استفاده از سوئیفت در جهت اعمال فشار بر دولت‌ها، برخی دولت‌ها را بر آن داشته است تا شبکه‌ها و راهکارهای جایگزین را برای سوئیفت فراهم کنند. هم‌زمان، پیشرفت‌های نوین در فناوری‌های مالی و *بلاکچین* باعث شده است که ایدهٔ تأسیس سازکارهای سریع‌تر، ارزان‌تر و شفاف‌تر از سوئیفت مطرح شود. مجموعهٔ این تحولات، مسائلی را در حقوق بین‌الملل طرح کرد که مستلزم بررسی است. در این راستا مقالهٔ حاضر به بیان چالش‌های حقوقی تحریم سوئیفت در حوزهٔ حقوق بین‌الملل

* نویسنده مسئول، استادیار گروه حقوق، دانشگاه آزاد اسلامی، واحد شاهرود، شاهرود، ایران marzieh.ghobadi@yahoo.com
** پژوهشگر حقوق بین‌الملل، مشاور بانک مرکزی جمهوری اسلامی ایران hamid.ghanbari1982@gmail.com

1. SWIFT (Society of Worldwide Interbank Financial Telecommunication)

می‌پردازد و ضمن معرفی جایگاه و اهمیت سوئیفت و مسائل مرتبط با حقوق داخلی ایران، مشروعیت تحریم‌های بین‌المللی مرتبط با سوئیفت را بررسی می‌کند. در ادامه واکنش‌های کشورهای مختلف به تحریم سوئیفت و برخی راهکارهای جایگزین کشورها ارزیابی شده است. یافته‌های مقاله نشان می‌دهد که تحریم‌های اعمال‌شده بر شبکهٔ سوئیفت، تأثیرات عمیقی بر چشم‌انداز مالی جهانی داشته است. یکی از پیامدهای کلیدی این تحریم‌ها، تسریع تلاش‌های کشورهای تحریم‌شده برای توسعه و اجرای سیستم‌های پیام‌رسانی مالی جایگزین مانند SPFS (سیستم انتقال پیام‌های مالی) روسیه و CIPS (سیستم پرداخت بین‌بانکی فرامرزی) چین بوده است.

واژگان کلیدی

سوئیفت، پیام‌رسانی مالی، اقدامات محدودکننده، بلاکچین، محرمانگی

مقدمه

با گسترش تجارت بین‌الملل و رشد و توسعهٔ روزافزون تجارت بین‌الملل، پرداخت‌های بین‌المللی نیز اهمیتی دوچندان پیدا می‌کنند. فرایند انجام پرداخت بین‌المللی مستلزم سه عنصر مهم است: ۱ـ روابط بانکی بین‌المللی (وجود بانک پرداخت‌کننده و بانک دریافت‌کننده)، ۲ـ سیستم تسویهٔ بین‌المللی و ۳ـ پیام‌رسانی مالی بین‌المللی.[۲] در صورتی که هر یک از این عناصر وجود نداشته باشند، انجام پرداخت بین‌المللی میسر نخواهد بود. با توجه به اینکه پیام‌رسانی مالی بین‌الملل موضوع بسیار مهمی است، از چند دههٔ پیش، سوئیفت یا جامعهٔ جهانی ارتباطات مالی بین بانکی تأسیس شد. سوئیفت که ابتدا در ۱۹۷۳ کار خود را با عضویت ۲۳۹ بانک در ۱۵ کشور آغاز کرد، اکنون حدود ۲۵۰۰ سهام‌دار دارد و در حال حاضر بیش از ۱۱۰۰۰ بانک و مؤسسهٔ مالی در سراسر دنیا به آن متصل هستند.[۳] روزانه نزدیک به ۴۰ میلیون پیام مالی از طریق سوئیفت مخابره می‌شود و روند استفاده از سوئیفت در سال‌های اخیر همواره رو به رشد بوده است.[۴] اهمیت سوئیفت در نظام مالی بین‌المللی باعث شده است که در سال‌های اخیر تلاش‌های متعددی از جانب دولت‌ها و برخی گروه‌های سیاسی[۵] به عمل آید تا از یک سو دسترسی اشخاص و سازمان‌هایی را که قصد اعمال فشار به آن‌ها را دارند به این شبکه منع یا محدود نموده و از سوی دیگر، از داده‌ها و اطلاعات

2. Colin Bamford, *Principles of International Financial Law*, (London: Oxford University Press, 2019).

3. Liana Wong, *International Financial Messaging Systems*. Congressional Research Service, 2021.

4. Marco Cipriani, Linda S. Goldberg, and Gabriele La Spada, "Financial Sanctions, SWIFT, and the Architecture of the International Payment System," *Journal of Economic Perspectives*, 37, 22 (2019).

۵. به‌عنوان مثال، برخی فعالان سیاسی حامی فلسطین خواستار قطع دسترسی رژیم صهیونیستی به سوئیفت شده‌اند. همچنین مخالفان دولت بلاروس خواستار قطع دسترسی بلاروس به سوئیفت شده‌اند و موارد مشابه دیگری نیز در رسانه‌ها بیان شده است. Wong, *International Financial Messaging Systems, 7*

سوئیفت برای ردیابی و محدودیت برخی معاملات و تراکنش‌های مالی استفاده کنند. اگرچه سوئیفت در بسیاری موارد در مقابل این اعمال فشارها مقاومت کرده است، در برخی موارد نیز نتوانسته در مقابل فشارها مقاومت کند و ناچار به قطع ارتباط برخی بانک‌ها و مؤسسات مالی شده است.

در نتیجهٔ این اعمال فشارها و محدودیت‌ها و همچنین با توجه به برخی تهدیدها و ریسک‌های عملیاتی که در سال‌های اخیر مطرح شده است، برخی کشورها در صدد برآمده‌اند که راهکارها و مکانیزم‌هایی به‌عنوان جایگزین سوئیفت طراحی و اجرا کنند. ایجاد و گسترش فناوری‌های نوین مبتنی بر رمزارز[۶] و *بلاکچین*[۷] باعث شده است که از جهت فنی نیز چنین ایده‌هایی نسبت به گذشته، عملیاتی‌تر به نظر برسند و لذا در حال حاضر، چندین مکانیزم جایگزین برای سوئیفت در حال شکل‌گیری است که هر یک نقاط ضعف و قوت خود را دارند.

با توجه به اینکه مکانیزم‌های پیام‌رسانی مالی در خلأ عمل نمی‌کنند و در بستر حقوقی جاری می‌شوند، لازم است فعالیت آن‌ها در پرتو قواعد و مقررات جاری حقوقی بررسی و تحلیل شود. در این راستا مقاله ابعاد حقوقی مکانیزم‌های پیام‌رسانی مالی بین‌المللی را بررسی می‌کند. بنابراین در بخش اول این مقاله به منظور آشنایی بیشتر با موضوع، پیشینهٔ شکل‌گیری سوئیفت به‌عنوان مهم‌ترین مکانیزم بین‌المللی پیام‌رسانی مالی و مشکلات و چالش‌های آن بررسی خواهد شد. در بخش دوم، استفاده از سوئیفت در راستای اجرای تحریم‌ها و آثار و محدودیت‌های آن در حقوق بین‌الملل، و در بخش سوم، راهکارهای جایگزین سوئیفت و مزایا و چالش‌های آن‌ها در نظام بانکی معاصر بررسی و تلاش خواهد شد ارزیابی واقع‌بینانه‌ای از قابلیت پیاده‌سازی راهکارهای گوناگون ارائه‌شده با تأکید بر ریسک‌های حقوقی هر کدام به عمل آید. در بخش چهارم، مکانیزم‌های پیام‌رسانی مالی جایگزین سوئیفت بررسی شده است.

---

۶. رمزارز یا ارز دیجیتال (Cryptocurrency) نوعی دارایی دیجیتال است که برای تبادل، از رمزنگاری استفاده و به‌صورت غیرمتمرکز بر روی شبکه‌های بلاکچین عمل می‌کند. این ارزها توسط هیچ نهاد مرکزی کنترل نمی‌شوند و تراکنش‌ها توسط شبکه‌ای از رایانه‌ها تأیید می‌شوند که امنیت و شفافیت بالایی دارند. ویژگی‌های مهم رمزارزها شامل غیرمتمرکزبودن، امنیت بالا، حفظ ناشناس‌بودن کاربران، غیرقابل‌تغییربودن تراکنش‌ها و شفافیت در سیستم معاملات است. نمونه‌های معروف رمزارزها شامل بیت‌کوین، اتریوم، ریپل و لایت‌کوین هستند که کاربردهای مختلفی ازجمله تبادل مالی، قراردادهای هوشمند و تراکنش‌های سریع و ارزان را فراهم می‌کنند.

۷. *بلاکچین* یک فناوری توزیع‌شده و غیرمتمرکز است که برای ثبت و ذخیره‌سازی تراکنش‌ها و اطلاعات به‌صورت امن و شفاف استفاده می‌شود. این فناوری از زنجیره‌ای از بلوک‌ها تشکیل شده که هر بلوک شامل مجموعه‌ای از تراکنش‌ها و یک کد هش منحصربه‌فرد است که بلوک قبلی را به بلوک بعدی متصل می‌کند. ویژگی‌های کلیدی *بلاکچین* شامل غیرقابل تغییربودن داده‌ها، شفافیت در ثبت تراکنش‌ها، امنیت بالا به دلیل استفاده از رمزنگاری و عدم نیاز به واسطهٔ مرکزی برای تأیید تراکنش‌ها است. *بلاکچین* در زمینه‌های مختلفی ازجمله ارزهای دیجیتال، قراردادهای هوشمند، مدیریت زنجیرهٔ تأمین و رأی‌گیری الکترونیکی کاربرد دارد.

۱. پیشینه، وضعیت حقوقی و کارکرد سوئیفت

به منظور درک بهتر جایگاه سوئیفت در نظام مالی بین‌المللی لازم است ابتدا وضعیت پیام‌رسانی مالی پیش از تأسیس سوئیفت و چالش‌های آن بررسی شود. سپس وضعیت حقوقی سوئیفت از حیث ترکیب سهام‌داری، سرمایه و ابعاد نظارتی بررسی و در نهایت، کارکردهای سوئیفت و استانداردهای حاکم بر آن معرفی شود.

۱-۱. پیام‌رسانی مالی پیش از سوئیفت

در نیمهٔ قرن بیستم، پیش از آنکه سوئیفت برای تبادل اطلاعات مالی استفاده شود، ارتباطات بانک‌ها از طریق تلکس بود. تلکس وسیلهٔ ارتباطی بود که ابتدا از خطوط تلگراف و بعدها از خطوط تلفن برای انتقال پیام استفاده می‌کرد و می‌توان آن را نوعی چاپگر تلفنی نامید. تلکس ابتدا در دههٔ ۱۹۳۰ در بازارهای مالی به کار گرفته و جایگزین تلگراف شد. تلکس به‌سرعت جای تلگراف را گرفت و در ۱۹۵۷ حدود ۳۰۰۰۰ کاربر در سطح جهان داشت و این رقم در اواخر دههٔ ۱۹۷۰ به بیش از یک میلیون رسید. با این حال، استفاده از تلکس، هم هزینهٔ نسبتاً بالا و هم ریسک‌های عملیاتی قابل‌توجهی داشت. منظور از ریسک‌های عملیاتی این بود که بانک‌ها و مؤسسات مالی در پیام‌هایی که ارسال می‌کردند از فرمت واحد و استانداردی استفاده نمی‌کردند و همین امر موجب شده بود که برای ارسال پیام مالی و تأیید آن نیاز به ارسال چندین تلکس و تأییدیه وجود داشته باشد تا طرفین مطمئن شوند که پیام خود را به‌درستی منتقل و پیام طرف مقابل را به‌درستی دریافت کرده‌اند. در برخی منابع به این نکته اشاره شده است که برای ارسال پیام مالی بین‌المللی معمولاً نیاز به ارسال بیش از ۱۰ تلکس وجود داشت.[۸]

در اوایل دههٔ ۱۹۷۰ تلاش‌هایی به عمل آمد که جایگزینی برای تلکس یافت شود که هزینه‌ها و مشکلات فوق را نداشته باشد. یکی از مهم‌ترین اقدامات در این راستا، ابتکار *سیتی بانک* امریکا در ۱۹۷۳ بود. در این سال یکی از شرکت‌های فناوری وابسته به این بانک به نام *شرکت فناوری تراکنش*،[۹] مکانیزمی را برای پیام‌رسانی مالی طراحی کرد و نام آن را *مارتی* گذاشت که مخفف «ورودی‌های تلگرافی قابل خواندن با ماشین»[۱۰] بود. *سیتی بانک* این مکانیزم را بعد از معرفی در ۱۹۷۳ در نیمهٔ ۱۹۷۴ به‌صورت موردی و آزمایشی با یکی از شعب خارجی خود امتحان کرد و سپس از همهٔ بانک‌هایی که با آن‌ها رابطه داشت درخواست کرد که به آن محلق شوند. بانک‌های اروپایی از این مکانیزم استقبال نکردند چرا که با ایجاد مکانیزم توسط یک بانک و الحاق همهٔ

8. Susan V. Scott and Markos Zachariadis, "Origins and Development of SWIFT, 1973–2009," *Business History* 54, 3 (2012) 462–82.

9. Transaction Technology Inc.

10. MARTI (Machine Readable Telegraphic Input)

بانک‌های دیگر به آن مخالف بودند و به‌درستی فکر می‌کردند چنین روشی برای ایجاد مکانیزم پیام‌رسانی مالی منجر به انحصار و سوءاستفاده خواهد شد.[۱۱]

۱-۲. تأسیس سوئیفت

در ۱۹۷۳ تلاش دیگری نیز برای ایجاد مکانیزم پیام‌رسانی مالی انجام شد که این بار به دلیل مشارکت و پشتیبانی بانک‌های مختلف از کشورهای گوناگون، با پذیرش و استقبال بانک‌های سراسر جهان روبه‌رو شد. این تلاش، ایجاد سوئیفت یا جامعهٔ جهانی پیام‌رسانی مالی بین بانکی[۱۲] بود. سوئیفت با مشارکت ۲۳۹ بانک از ۱۵ کشور و به‌عنوان مؤسسهٔ مالی غیرانتفاعی تشکیل شد. هدف از تأسیس سوئیفت این‌گونه عنوان شد که قرار است مکانیزمی باشد برای پردازش داده‌ها و پیام‌رسانی مالی بین بانک‌ها در سطح جهان بر اساس استانداردهایی که توسط شرکت‌های خصوصی و برای اهداف جامعهٔ بین‌المللی بانکی تهیه می‌شوند. مرکز اصلی سوئیفت در بلژیک قرار دارد و به‌صورت شرکت تعاونی است که مالکیت آن در اختیار اعضای آن قرار دارد. در ابتدا فقط بانک‌ها امکان عضویت در سوئیفت را داشتند اما در حال حاضر شرکت‌ها و اشخاص فعال در معاملات بین‌المللی و مؤسسات مدیریت سرمایه‌گذاری (شرکت‌های تأمین سرمایه) نیز امکان عضویت در سوئیفت را دارند.

۱-۳. سرمایه و ترکیب سهام‌داری سوئیفت

سرمایهٔ اولیهٔ تأسیس سوئیفت از طریق مشارکت مالی بانک‌های عضو آن تأمین شد. این بانک‌ها در ابتدا برای ایجاد شبکهٔ امن و استاندارد برای تبادل اطلاعات مالی بین‌المللی به هم پیوستند و هزینه‌های اولیهٔ تأسیس و توسعهٔ زیرساخت‌های فنی سوئیفت را تأمین کردند. به‌تدریج از محل سود حاصل از فعالیت‌های سوئیفت، وام‌های دریافتی بازپرداخت شدند. سوئیفت سود خود را صرف توسعه و نگهداری سیستم‌ها می‌کند و بخشی از آن نیز صرف پرداخت تخفیف در هزینه‌های اعضای استفاده‌کننده از آن می‌شود. در حال حاضر، ترکیب سهام‌داری سوئیفت، هر سه سال یک بار به‌روز می‌شود و میزان سهم اعضا در سوئیفت متناسب با میزان استفادهٔ هر یک از اعضا از خدمات آن است. سهام‌داران سوئیفت، هیئت‌مدیرهٔ آن را انتخاب می‌کنند که متشکل از ۲۵ عضو است و مسئولیت ادارهٔ سوئیفت و نظارت بر عملکرد مدیران و کارکنان آن را بر عهده دارند.

اعضای مستقیم سوئیفت بانک‌ها، مؤسسات مالی و اعتباری، شرکت‌های سرمایه‌گذاری،

11. Susan V. Scott, and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community*. Taylor & Francis, 2014.

12. *SWIFT (The Society for Worldwide Interbank Financial Telecommunication).*

صرافی‌ها، شرکت‌های بیمه و سایر نهادها و مؤسساتی هستند که به انحاء مختلف در حوزهٔ بازارهای مالی و پولی فعالیت می‌کنند. این دسته از کاربران می‌توانند به‌طور مستقیم و بدون واسطه از خدمات سوئیفت برای انتقال اطلاعات و دستورالعمل‌های مالی و همچنین انتقال ارز بین بانکی استفاده کنند. سهام‌داران سوئیفت به گروه‌های مختلفی تقسیم می‌شوند که عبارت‌اند از: ۱ـ گروه کاربری محدود، ۲ـ گروه ملی، ۳ـ گروه‌های کاربر ملی و ۴ـ گروه‌های مشاوره و کاری. در اساسنامهٔ سوئیفت، تعریف گروه‌های فوق و حقوق، تکالیف و محدودیت‌های آن‌ها بیان شده است. بدین ترتیب، اگرچه به‌طور کلی سوئیفت شرکت تعاونی یا به عبارت دقیق‌تر، تعاونی با مسئولیت محدود است، قواعدی خاص نظیر تقسیم‌بندی سهام‌داران به گروه‌های خاص در آن اعمال می‌شود که در اساسنامه قید شده است.[۱۳]

۱-۴. نظارت بر سوئیفت

علاوه بر وظایف نظارتی هیئت‌مدیرهٔ سوئیفت، بانک مرکزی بلژیک و بانک‌های مرکزی کشورهای عضو گروه ۱۰[۱۴] نیز بر سوئیفت نظارت می‌کنند. این امر بر اساس توافقی است که در ۱۹۹۸ در گروه ۱۰ انجام و مقرر شد که بانک‌های مرکزی آن گروه بر سوئیفت نظارت داشته باشند.[۱۵] نظارت بانک‌های مرکزی بر سوئیفت به دلیل اهمیتی است که این نهاد از منظر ریسک سیستمی دارد، چرا که نظام پرداخت‌های بین‌المللی تا حدود زیادی به عملکرد صحیح و قابل اطمینان سوئیفت وابسته است و در صورتی که سوئیفت نتواند این نقش را به‌خوبی انجام دهد، امکان دارد مخاطرات گسترده‌ای در نظام مالی بین‌المللی به وجود آید. لازم به ذکر است که در ۲۰۱۲ نهادی تحت عنوان مجمع نظارت بر سوئیفت[۱۶] شکل گرفت که متشکل از ۱۵ بانک مرکزی است و هدف آن به اشتراک‌گذاشتن اطلاعات نظارتی سوئیفت است.[۱۷] علاوه بر این، نهادهایی که از اجتماع کاربران یا سهام‌داران[۱۸] سوئیفت تشکیل می‌شوند نیز ضمن همکاری و مساعدت به سوئیفت، در برخی موارد، نقش نظارتی را نیز ایفا می‌کنند. گروه‌های عضو ملی و گروه کاربر ملی در این زمینه قابل

۱۳. ایوب منصوری رضی، *رژیم حقوقی حاکم بر سوئیفت* (تهران: انتشارات شهر دانش، ۱۳۹۸)، ۳۴-۳۷.

۱۴. گروه ۱۰ یا G10 (Group of Ten) شامل ده کشور صنعتی بزرگ جهان (بلژیک، کانادا، فرانسه، آلمان، ایتالیا، ژاپن، هلند، سوئد، سوئیس، بریتانیا و ایالات متحدهٔ امریکا) است که در ۱۹۶۲ برای همکاری در مسائل مربوط به صندوق بین‌المللی پول (IMF) و تنظیمات پولی و مالی بین‌المللی تشکیل شد. این گروه نقش مهمی در امور پول و مالی بین‌المللی و همکاری‌های اقتصادی ایفا و در نشست‌ها و مذاکرات جهانی در مورد سیاست‌های اقتصادی و مالی شرکت می‌کند. این گروه به‌ویژه در مدیریت بحران‌های مالی و ایجاد ثبات در نظام مالی بین‌المللی فعال است.

۱۵. همان، ۵۸.

16. SWIFT oversight forum

17. Wong, *International Financial Messaging Systems*, 11.

۱۸. نظیر کمیته‌های مشورتی اجرایی و کمیته‌های منطقه‌ای سوئیفت.

ذکر هستند. این گروه‌ها نقش‌های مختلفی را نظیر مشاوره به هیئت‌مدیرهٔ سوئیفت و اظهارنظر و عندالاقتضا اعتراض نسبت به جذب کاربر جدید سوئیفت ایفا می‌کنند.

۱-۵. کارکرد سوئیفت و استانداردهای حاکم بر آن

در رابطه با نقش و کارکرد سوئیفت باید به این نکته توجه داشت که سوئیفت بانک نیست که برای مشتریان خود حساب افتتاح و نگهداری کند. علاوه بر این، سوئیفت سیستم تسویهٔ پرداخت‌ها نیست و خدمات تسویه ارائه نمی‌کند، بلکه فقط مکانیزم تبادل اطلاعات مالی است که دو کارکرد اساسی دارد: ۱ـ شبکه‌ای را برای انتقال اطلاعات مالی فراهم می‌کند که از امنیت و قابلیت اتکای قابل‌توجهی برخوردار است؛ ۲ـ متن پیام‌های استاندارد را تعریف و در اختیار اعضا قرار می‌دهد که با استفاده از آن می‌توانند با کمترین هزینه و با بیشترین اطمینان دریافت‌ها، پرداخت‌ها و معاملات میان خود و مشتریانشان را انجام داده و پیام‌های لازم را مخابره کنند. بنابراین، سوئیفت نقش بانک‌های کارگزار را از میان نمی‌برد و این نقش کماکان به قوت خود باقی است.

در اینجا این پرسش قابل طرح است که نقش بانک‌های کارگزار چیست؟ بانک تسویهٔ بین‌المللی[۱۹] روابط کارگزاری بانکی را این‌گونه تعریف کرده است: «روابط کارگزاری بانکی عبارت است از توافقی که بر اساس آن یک بانک که بانک کارگزار خوانده می‌شود، سپرده‌های بانک‌های دیگر را می‌پذیرد و پرداخت‌های آن‌ها را انجام داده و سایر خدمات را به آن‌ها ارائه می‌کند».[۲۰] به عبارت دیگر، خدمات کارگزاری به خدماتی گفته می‌شود که بانک برای انجام پرداخت‌ها به بانک دیگر ارائه می‌کند. می‌توان گفت در زمانی که مشتری بانک قصد انجام پرداختی به مشتری بانک دیگری را داشته باشد، اگر دو بانک مزبور نزد یکدیگر حساب داشته باشند، پرداخت‌ها از طریق حساب‌های فی ما بین آن دو بانک انجام می‌شود. اما اگر دو بانک مذکور نزد یکدیگر حساب نداشته باشند، نیاز به استفاده از خدمات بانک واسط وجود دارد که به آن بانک کارگزار گفته می‌شود. برای انجام پرداخت‌های بین‌المللی معمولاً نیاز به انجام یک یا چند بانک کارگزار وجود دارد چرا که این طور نیست که همهٔ بانک‌هایی که مبدأ و مقصد پرداخت در آن‌هاست، نزد یکدیگر حساب داشته باشند.

۱۹. بانک تسویهٔ بین‌المللی (Bank for International Settlements - BIS) یک سازمان بین‌المللی است که در۱۹۳۰ با هدف اصلی ترویج همکاری‌های پولی و مالی بین بانک‌های مرکزی جهان تأسیس شد. این بانک به‌عنوان «بانک بانک‌های مرکزی» عمل می‌کند و تسهیلاتی برای تسویهٔ حساب‌های بین‌المللی، ارائهٔ مشاوره‌های تخصصی به بانک‌های مرکزی، و انجام تحقیقات اقتصادی و مالی فراهم می‌کند. بانک تسویهٔ بین‌المللی همچنین نقش مهمی در تقویت ثبات مالی جهانی و تدوین استانداردها و سیاست‌های مربوط به نظارت و مقررات مالی ایفا می‌کند. مقر اصلی این بانک در بازل سوئیس است.

20. OPERATIONS, BANKING. "Bank for International Settlements—BIS." *Correspondent Banking* (2019). Available at: https://www.bis.org/cpmi/publ/d147.pdf., Last accessed on July 5, 2024.

شبکهٔ پیام‌رسانی سوئیفت از سه مرکز داده استفاده می‌کند که در ایالات متحدهٔ امریکا، هلند و سوئیس مستقر هستند و انتقال اطلاعات سوئیفت نیز از طریق فیبرهای نوری انجام می‌شود.[۲۱] انتقال اطلاعات سوئیفت با سرعت بسیار بالایی انجام می‌شود که تقریباً می‌توان آن را با انتقال آنی برابر دانست و در صورتی که در هر یک از مراکز دادهٔ اشاره‌شده ترافیک بالایی وجود داشته باشد یا به هر دلیل دیگری آن مرکز از کار بیفتد، دو مرکز دیگر می‌توانند کلیهٔ داده‌ها را پردازش و منتقل کنند.

سوئیفت برای پیام‌رسانی مالی از استانداردهایی استفاده می‌کند که به‌طور مداوم در حال به‌روزرسانی هستند. به‌عنوان مثال، از استاندارد ISO 9362 که در ۱۹۹۴ معرفی شد برای تعیین فرمت شناسهٔ تجاری،[۲۲] از استاندارد ISO 10383 که در ۲۰۰۳ معرفی شد برای شناسایی معاملات و تبادلات، و از استاندارد ISO 13616 که آن هم در ۲۰۰۳ معرفی شد برای شناسایی بین‌المللی حساب‌های بانکی[۲۳] استفاده می‌شود که بر اساس آن شمارهٔ حساب‌های بانکی به‌طور متحدالشکلی در دنیا تعریف می‌شوند و قابلیت شناسایی خواهند داشت. در نهایت، استاندارد مهم ISO 20022 وجود دارد که مربوط به پیام‌های مالی الکترونیکی بین مؤسسات اعتباری است و شامل پیام‌های راجع به پرداخت‌ها و دریافت‌ها، بدهکارکردن و بستانکارکردن، معاملات اوراق بهادار و معاملات تجاری می‌شود. البته سوئیفت در رابطه با استانداردهای مزبور فقط استفاده‌کننده نیست و در تدوین این استانداردها نیز نقش مهمی دارد و سازمان بین‌المللی استانداردسازی[۲۴] (ISO) سوئیفت را به‌عنوان مقام ثبت‌کننده[۲۵] معرفی کرده است؛ بدین معنا که سوئیفت در تعریف و به‌روزرسانی قواعد مربوط به استانداردهای یادشده خصوصاً استاندارد ISO 20022 نقش دارد. مقام ثبت‌کننده نهادی است که مسئولیت مدیریت و نگهداری استانداردهای خاص را بر عهده دارد و وظایفی را شامل ثبت و تخصیص کدها، اطمینان از رعایت استانداردها و ارائهٔ راهنمایی به کاربران آن استاندارد انجام می‌دهد. سوئیفت به‌عنوان مقام ثبت‌کننده برای استاندارد ISO 9362 که کدهای شناسایی بانک‌ها (BIC) را تعیین می‌کند، معرفی شده است. این نقش سوئیفت شامل تخصیص و مدیریت کدهای BIC است که در تراکنش‌های مالی بین‌المللی برای شناسایی بانک‌ها استفاده می‌شوند و به بهبود شفافیت و کارایی در سیستم مالی جهانی کمک می‌کند.

21. Cipriani et al., *Financial Sanctions, SWIFT, and the Architecture of the International Payment System*, 15.
22. BIC (Business Identifier Code)
23. IBAN (International Bank Account Number)
24. International Standardization Organization
25. Registration Authority

۲. عملکرد سوئیفت و چالش‌های آن

۲-۱. تحلیل آماری میزان استفاده از سوئیفت

نگاهی به گزارش‌های سالانهٔ سوئیفت نشان‌دهندهٔ این است که در طی سالیان متمادی، رشد قابل توجه و مداومی در حجم و گسترهٔ فعالیت‌های آن وجود داشته است. به‌عنوان مثال در ۲۰۰۹ روزانه از طریق سوئیفت ۱۴٫۹ میلیون پیام مبادله شده است. این عدد در ۲۰۲۲ به ۴۴٫۸ میلیون پیام رسیده است. همچنین در ۲۰۰۹ کل پیام‌هایی که سالانه در سوئیفت مخابره می‌شد، ۳٫۸ میلیارد پیام بود. این عدد در ۲۰۲۲ به ۱۱٫۲ میلیارد پیام رسیده است.[۲۶] از جهت سطح گستردگی بیش از ۱۱۵۰۰ مؤسسه و نهاد مالی به سوئیفت دسترسی دارند. این مؤسسات در بیش از ۲۰۰ کشور و سرزمین قرار دارند.[۲۷] سوئیفت بیش از ۴ میلیارد حساب را پوشش می‌دهد. رشد سوئیفت در ۲۰۲۲ نسبت به ۲۰۲۱ برابر ۶٫۲ درصد بوده است. از جهت سرعت، ۴۸ درصد پیام‌هایی که از طریق سوئیفت ارسال می‌شوند، ظرف مدت ۵ دقیقه به ذی‌نفع نهایی می‌رسند و تقریباً تمامی پیام‌ها را ظرف مدت ۲۴ ساعت به مقصد می‌رساند.[۲۸] از حیث نوع ارزی که موضوع پیام‌های مالی است، همان‌طور که انتظار می‌رود، بیشترین حجم به دلار امریکا اختصاص دارد که سهمی حدود ۴۰ درصد را از آن خود کرده است. سپس یورو با سهم حدود ۳۵ درصد قرار دارد و بعد از آن سایر ارزها ازجمله یوآن چین قرار دارند.[۲۹]

ملاحظهٔ آمارها و روندهای فوق نشان می‌دهد که علی‌رغم مکانیزم‌های جایگزینی که در سال‌های اخیر به‌عنوان جایگزین سوئیفت ظهور کرده‌اند، همچنان سوئیفت به‌عنوان مهم‌ترین شبکهٔ پیام‌رسانی مالی، اهمیتی ویژه در نظام مالی بین‌المللی دارد. با این حال، این بدان معنا نیست که سوئیفت با چالش‌ها و مشکلات خاص خود روبه‌رو نیست. در ادامه به برخی از این چالش‌ها اشاره می‌شود.

۲-۲. معایب و مزایای سوئیفت

یکی از معایب و مشکلات سوئیفت، عدم انتقال بدون واسطهٔ اطلاعات است. همان‌طور که پیش از این اشاره شد، سوئیفت صرفاً شبکهٔ پیام‌رسانی مالی است و نقش مکانیزم تسویه و بانکداری کارگزاری را بر عهده ندارد؛ لذا در مواردی که از سوئیفت استفاده می‌شود، همچنان نیاز به استفاده از شبکهٔ کارگزاری بانکی به قوت خود باقی است. در نتیجه در مواردی که دو بانک به‌طور مستقیم

26. SWIFT Annual Review (2022) 4.

۲۷. منظور از سرزمین، مناطقی است که از منظر حقوق بین‌الملل نمی‌توان آن‌ها را کشور تلقی کرد اما جزء حاکمیت کشورهای دیگر هم نیستند.

28. Ibid.

29. Wong, *International Financial Messaging Systems*, 4.

با یکدیگر رابطه نداشته باشند، انتقال منابع از طریق یک یا چند بانک کارگزار انجام می‌شود. این امر بدین معناست که برای یک انتقال وجه، نیاز به ارسال چندین پیام وجود دارد. اگرچه انتقال پیام در هر مرحله توسط سوئیفت به‌سرعت انجام می‌شود، مشکل در اینجاست که گاه برای انتقال وجه از مبدأ به مقصد نهایی لازم است چندین انتقال انجام شده و به تعبیر دیگر، فاصله میان مبدأ و مقصد نهایی در چند گام پیموده شود و برای هر گام، یک پیام مالی باید ارسال شود. این امر در عین اینکه هزینه‌های انتقال را افزایش می‌دهد، موجب ایجاد پیچیدگی‌های حقوقی و مقرراتی نیز می‌شود. نخست اینکه از شفافیت نقل و انتقال‌های بانکی کاسته می‌شود، چرا که بانک دریافت‌کنندهٔ پیام مالی، صرفاً اطلاعات محدود و مشخص را در مورد بانک فرستنده، متقاضی اولیه و ذی‌نفع نهایی دریافت می‌کند و اطلاعات کامل زنجیرهٔ پرداخت در اختیار وی قرار نمی‌گیرد و این امر، بررسی مطابقت یا عدم مطابقت پرداخت با قوانین و مقررات جاری را دشوار می‌کند. ثانیاً هر بانک در هر مرحله از پرداخت، موظف به بررسی قانونی‌بودن آن مرحله از پرداخت است که در نهایت منجر می‌شود برای نهایی‌شدن پرداخت، چندین بار بررسی صورت گیرد و این امر به نوبهٔ خود باعث طولانی‌شدن و پیچیدگی جریان پرداخت می‌شود. سوئیفت برای کمک به حل این مشکل، در ۲۰۱۷ خدمتی را تحت عنوان «ابتکار پرداخت‌های جهانی سوئیفت»[۳۰] معرفی کرد. این خدمت، یک سامانهٔ اضافی به سوئیفت است که کاربران را قادر می‌سازد کل زنجیرهٔ پرداخت را از ابتدا تا انتها مشاهده کنند. هدف از ارائهٔ این خدمت این بود که شفافیت، سرعت و قابلیت اتکای سوئیفت را افزایش دهد. این خدمت با استقبال قابل‌توجهی مواجه شد، تا جایی که در ۲۰۱۹ بیش از ۵۰ درصد پیام‌ها با استفاده از این خدمت ارسال می‌شدند و در سال‌های بعد این رقم به بالای ۷۵ درصد رسید.[۳۱]

در سال‌های اخیر، برخی از بانک‌ها و مؤسسات مالی استفاده‌کننده از سوئیفت با حملات سایبری مواجه شده‌اند که منجر به انتقال متقلبانهٔ منابع از حساب‌های آن‌ها شده است. این امر باعث شده است که نگرانی‌هایی برای سایر بانک‌ها و مؤسسات مالی در سراسر دنیا به وجود آید که امکان دارد آن‌ها نیز در آینده در معرض حملات مشابهی قرار گیرند. به‌عنوان مثال، در ۲۰۱۶ تعدادی هکر که به نظر می‌رسد از کره شمالی بوده‌اند، به اطلاعات و رمزهای عبور کارکنان بانک مرکزی بنگلادش دسترسی پیدا کردند. آن‌ها از این اطلاعات برای صدور دستور پرداخت‌هایی به بانک *فدرال رزرو* نیویورک و سایر بانک‌ها استفاده کردند و در صدد برآمدند که حدود ۱ میلیارد دلار از دارایی‌های بانک مرکزی بنگلادش را منتقل کنند. حدود ۸۱ میلیون دلار از این مبلغ به چهار حساب در یک بانک فیلیپینی و حدود ۲۰ میلیون دلار هم به حساب یک سازمان غیردولتی نزد

30. SWIFT Global Payments Innovation

31. Retrieved from: https://www.swift.com/our-solutions/swift-gpi, Last accessed on July 5, 2024.

بانکی در سریلانکا منتقل شد. یکی از کارکنان بانک سریلانکایی متوجه شد که مبلغ ۲۰ میلیون دلار برای یک سازمان غیردولتی کوچک، نامتعارف و مشکوک است و لذا با بانک‌هایی که در زنجیرهٔ پرداخت بودند ازجمله بانک مرکزی بنگلادش تماس گرفت تا تأیید آن‌ها را اخذ کند. در این مقطع بانک مرکزی بنگلادش متوجه موضوع شد و دستور موقت مبنی بر عدم انجام این انتقال را دریافت کرد. در رابطه با ۸۱ میلیون دلاری که به فیلیپین منتقل شده بود، حدود یک‌پنجم آن به حساب‌های بانک مرکزی بنگلادش بازگردانده شد اما مابقی همچنان تحت پیگیری قرار دارد.[۳۲] در این مورد مقامات بانک مرکزی بنگلادش مدعی هستند که سیستم‌های امنیتی سوئیفت ضعف داشته است و اتصال سوئیفت به سامانهٔ پرداخت‌های ناخالص آنی بانک مرکزی بنگلادش که سه ماه قبل از آن انجام شده بود، باعث بروز این ریسک شده است. سوئیفت این ادعا را رد می‌کند و مدعی است که قصور از ناحیهٔ بانک مرکزی بنگلادش بوده است و زیرساخت‌های آن از امنیت کامل برخوردار نبوده‌اند و سوئیفت حاضر است کمک‌های لازم را به بانک مرکزی بنگلادش ارائه دهد تا زیرساخت‌های خود را از جهت امنیتی ارتقاء دهد. این موضوع مشابه با اختلافاتی است که گاه بین بانک‌ها و مشتریان در رابطه با عدم استفادهٔ صحیح از اطلاعات کارت‌های آن‌ها بروز می‌کند و در مقررات پرداخت‌های الکترونیکی به آن اشاره شده و مسئولیت‌هایی برای بانک در رابطه با امنیت سیستم، آموزش به مشتریان و ارائهٔ هشدارهای لازم به آن‌ها در نظر گرفته می‌شود.[۳۳]

مواردی از این دست بسیار است و *بنیاد کارنگی برای صلح بین‌المللی*، پایگاه داده‌ای را در خصوص تهدیدات علیه پیام‌رسانی مالی بین‌المللی فراهم کرده است که این حملات را از ۲۰۰۷ تا آوریل ۲۰۲۲ نشان می‌دهد و حاوی بیش از ۲۰۰ حملهٔ سایبری است که شامل حملات به سوئیفت نیز می‌شود. در این پایگاه داده موارد قابل‌توجهی نظیر حملهٔ ۳۹۰ میلیون دلاری به بانک مرکزی مالزی و تلاش برای انتقال وجوه آن از طریق سوئیفت ذکر شده است که باعث ایجاد نگرانی‌هایی نسبت به امکان توفیق هکرها در این زمینه می‌شود. در نتیجهٔ این نگرانی‌ها این پرسش به ذهن خطور می‌کند که آیا امکان ایجاد مکانیزم‌های جایگزینی برای سوئیفت وجود ندارد که چنین دغدغه‌هایی در مورد آن وجود نداشته باشد؟ برخی به این پرسش پاسخ مثبت می‌دهند و پیام‌رسانی مالی مبتنی بر *بلاکچین* را به‌عنوان راهکار معرفی می‌کنند که در ادامهٔ مقاله به آن اشاره خواهد شد. اما پیش از آن لازم است رابطهٔ سوئیفت و نظام تحریم‌های مالی و اقتصادی بین‌المللی به اختصار بررسی شود.

32. Wong, *International Financial Messaging Systems*, 6.

۳۳. فهیمه فیروزبخت، *حقوق انتقال الکترونیکی وجوه* (تهران: انتشارات مجد، ۱۳۹۸)، ۱۰۹-۱۱۱.

۳. سوئیفت و تحریم‌های بین‌المللی

با توجه به آنچه تا کنون در مورد سوئیفت و نقش و اهمیت آن گفته شد، عجیب نیست که سوئیفت از سوی واضعان تحریم‌های بین‌المللی مورد توجه قرار گرفته و از آن برای اجرای تحریم‌ها یا رصد اجرای آن‌ها استفاده کنند. در ادامه به سابقهٔ تاریخی همکاری سوئیفت با تحریم‌های امریکا و اسناد بین‌المللی راجع به آن و نیز نقش سوئیفت در اجرای تحریم‌های ایران و تلاش‌هایی که در جهت گسترش نقش تحریمی آن به عمل آمده است پرداخته خواهد شد.

۳-۱. مذاکرات ایالات متحدهٔ امریکا و اتحادیهٔ اروپا در مورد سوئیفت

ایالات متحدهٔ امریکا پس از حملات یازدهم سپتامبر ۲۰۰۱ برنامه‌ای را تحت عنوان «برنامهٔ ردیابی تأمین مالی تروریسم»[۳۴] طراحی کرد. هدف از این برنامه که تحت نظر وزارت خزانه‌داری ایالات متحده اجرا می‌شد این بود که اطلاعات مربوط به عملیات مالی تروریست‌ها تجزیه و تحلیل شود تا بدین وسیله بتوان مانع از فعالیت‌های آنان شد. برای اجرای این برنامه، نیاز به آن وجود داشت که به اطلاعات موجود در مراکز پیام‌رسانی مبادلات مالی که مهم‌ترین و جامع‌ترین آن‌ها سوئیفت است، دسترسی حاصل شود و پس از اخذ اطلاعات از آن مراکز، تجزیه و تحلیل‌های لازم در مورد آن‌ها صورت گیرد. بر این اساس، ایالات متحده، اقدام به درخواست اطلاعات مالی از سوئیفت کرد و سوئیفت نیز اطلاعات مربوطه را در اختیار آن قرار می‌داد. این تبادل اطلاعات تا مدت‌ها بر اساس قوانین و مقررات ایالات متحدهٔ امریکا و بدون آنکه بر اساس قوانین و مقررات اتحادیهٔ اروپا برای آن مجوزی وجود داشته باشد، انجام می‌شد و در نهایت با افشای این همکاری، اعتراضات وسیعی نسبت به آن ابراز شد. از این رو مقامات امریکایی بر آن شدند تا مبانی قانونی و رسمی لازم برای گسترش این همکاری را فراهم آورند و بدین منظور، پیشنهاد انعقاد موافقت‌نامه‌ای با اتحادیهٔ اروپا تحت عنوان موافقت‌نامهٔ سوئیفت را دادند که بعدها به موافقت‌نامهٔ سوئیفت یک[۳۵] مشهور شد. با این حال، روند تصویب موافقت‌نامهٔ سوئیفت یک با پنهان‌کاری‌ها و ایرادات فراوان همراه بود و همین امر باعث شد پارلمان اروپا با آن مخالفت و آن را ملغی کند. پس از انقضای موافقت‌نامهٔ سوئیفت یک، مذاکرات برای انعقاد موافقت‌نامهٔ دیگری تحت عنوان موافقت‌نامهٔ سوئیفت دو[۳۶] آغاز شد که در نهایت در ۱۳ ژوئیهٔ ۲۰۱۰ به تصویب رسید.[۳۷] روند انعقاد این دو معاهده به اختصار به شرح زیر بوده است.

---

34. Terrorist Finance Tracking Program. For more information, see https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp, Last accessed on July 5, 2024.

35. SWIFT I Agreement

36. SWIFT II Agreement

۳۷. حمید قنبری، «کشف رمز غیرقانونی: سوئیفت چگونه با امریکا همکاری می‌کند؟»، *تجارت فردا* ۶۰ (۱۳۹۲).

در ۲۷ ژوئیهٔ ۲۰۰۹ شورای اتحادیهٔ اروپا به رئیس آن شورا اجازه داد با همکاری کمیسیون اروپا مذاکرات مربوط به انعقاد موافقت‌نامهٔ سوئیفت را آغاز کند. موضوع این مذاکرات، «موافقت‌نامه‌ای در خصوص فرآیندهای پیام‌رسانی راجع به داده‌های مالی از اتحادیهٔ اروپا به ایالات متحدهٔ امریکا در راستای برنامهٔ ردیابی تأمین مالی تروریسم» بود. مذاکرات مزبور بر اساس معاهدهٔ اتحادیهٔ اروپا به گونه‌ای انجام شد تا در ۳۰ نوامبر ۲۰۰۹ موافقت‌نامهٔ سوئیفت یک منعقد شد. این تاریخ، درست یک روز قبل از لازم‌الاجراشدن معاهدهٔ لیسبون یا معاهدهٔ کارکرد اتحادیهٔ اروپا[۳۸] بود که ناسخ معاهدهٔ اتحادیهٔ اروپا بود و ترتیبات انعقاد موافقت‌نامه‌ها در اتحادیهٔ اروپا را تغییر می‌داد. بر اساس معاهدهٔ اخیر، انعقاد موافقت‌نامه‌ها در اتحادیهٔ اروپا نیازمند آن بود که رضایت شورا و پارلمان اروپا هر دو وجود داشته باشد. مشخص بود که تعجیل در انعقاد موافقت‌نامه صرفاً به این دلیل بوده است که نیازی به رضایت پارلمان اروپا به این موافقت‌نامه وجود نداشته باشد. همین تعجیل موجب برانگیختن حساسیت پارلمان شد و پارلمان اروپا، از شورا به دلیل تصویب این موافقت‌نامه بدون توجه کافی به حساسیت مسئلهٔ حفاظت از داده‌ها انتقاد کرد و نهایتاً در ۱۱ فوریهٔ ۲۰۱۱ با رأی ۳۷۸ به ۹۶ و با ۳۱ رأی ممتنع، موافقت‌نامهٔ مزبور را مردود اعلام کرد.[۳۹]

موافقت‌نامهٔ سوئیفت یک، از یک مقدمه و ۱۵ ماده تشکیل شده است. این موافقت‌نامه به قطعنامهٔ ۱۳۷۳ شورای امنیت در رابطه با مبارزه با تأمین مالی تروریسم و نیز به «کنوانسیون اروپایی حقوق بشر و آزادی‌های اساسی» و «منشور حقوق بنیادین اتحادیهٔ اروپا» نیز در رابطه با حق حریم خصوصی اشاره دارد. چارچوب اجرایی درخواست اطلاعات در این موافقت‌نامه به این صورت پیش‌بینی شده بود که خزانه‌داری امریکا ابتدا می‌بایست بر اساس ماده ۸ موافقت‌نامهٔ معاضدت قضایی بین ایالات متحدهٔ امریکا و اتحادیهٔ اروپا (که در ۲۵ ژوئن ۲۰۰۳ منعقد شده بود) تقاضای دریافت اطلاعات را به‌طور رسمی به مقامات صالح دولت عضو اتحادیهٔ اروپا که ارائه‌دهندهٔ خدمات مالی در آن مستقر است ارسال کند. مقام صالح مزبور باید بررسی کند که آیا درخواست واصله از سوی دولت امریکا با موافقت‌نامهٔ سوئیفت یک و همچنین با موافقت‌نامهٔ معاضدت قضایی مطابقت دارد یا خیر. اگر به این نتیجه رسید که اجرای درخواست در چارچوب موافقت‌نامه‌های یادشده می‌گنجد، اطلاعات را از ارائه‌دهندهٔ خدمات مالی (یا خدمات پیام‌رسانی مالی) دریافت و آن را به خزانه‌داری امریکا ارسال می‌کند. در موافقت‌نامهٔ سوئیفت یک برای حفاظت از داده‌ها و حقوق اساسی کسانی که اطلاعات به آن‌ها مربوط می‌شد نیز تضمین‌هایی وجود داشت. نخست اینکه تأمین مالی تروریسم و اهداف و انواع جمع‌آوری و پردازش اطلاعات، به‌دقت در موافقت‌نامهٔ تعریف شده بود. دوم اینکه مقرر شده بود درخواست اطلاعات باید مبتنی بر اطلاعات و شواهدی باشند

38. The Treaty on Functioning of the European Union, 1957.

۳۹. همان.

که ظن وجود رابطه‌ای با تروریسم یا تأمین مالی آن را ایجاد کنند. سوم اینکه اطلاعات باید به نحو ایمن نگهداری شوند و از دسترسی غیرمجاز به آن جلوگیری شود و در نهایت اینکه مقررات مشخص و دقیقی در مورد امحای اطلاعات پس از استفاده از آن‌ها در موافقت‌نامه درج شده بود. با این حال منتقدان موافقت‌نامه معتقد بودند که این تضمین‌ها برای رعایت حقوق شهروندان کافی نیستند و لازم است به نحو مؤثرتری از حقوق آنان حمایت شود. آنان همچنین معتقد بودند چارچوب‌های موافقت‌نامهٔ سوئیفت یک اجازه می‌دهند که حجم بسیار وسیع و گسترده‌ای از اطلاعات که بعضاً هیچ ارتباطی به ایالات متحدهٔ امریکا ندارند، به خزانه‌داری و مقامات امنیتی آن کشور منتقل شوند.[۴۰]

پارلمان اروپا پس از آنکه موافقت‌نامهٔ سوئیفت یک را رد کرد، در ۵ مه ۲۰۱۰ قطعنامه‌ای را تصویب کرد[۴۱] که در آن نگرانی‌ها و دیدگاه‌های خود در خصوص این مسئله را بیان می‌کرد. شش روز بعد، شورای اتحادیهٔ اروپا به کمیسیون اروپا اجازه داد مذاکرات مربوط به انعقاد موافقت‌نامهٔ سوئیفت دو را با امریکا آغاز کند. مذاکرات در نیمهٔ ژوئن ۲۰۱۰ به پایان رسید و موافقت‌نامهٔ سوئیفت دو در ۲۲ ژوئن ۲۰۱۰ به تصویب شورای اتحادیه رسید و در ۸ ژوئیهٔ ۲۰۱۰ نیز پارلمان اروپا آن را تصویب کرد. موافقت‌نامهٔ سوئیفت دو از یک مقدمه و ۲۳ ماده تشکیل شده و در مقدمهٔ آن به اهمیت حقوق بشر و حفاظت از داده‌ها و اطلاعات اشاره، و به این نکته نیز تصریح شده است که اقدامات امنیتی که برای مبارزه با تروریسم و برقراری امنیت انجام می‌شوند باید متناسب با مخاطراتی باشند که قصد جلوگیری از آن‌ها وجود دارد. در موافقت‌نامهٔ سوئیفت دو به خزانه‌داری امریکا اجازه داده شده است که درخواست خود را مستقیماً به ارائه‌کنندهٔ اطلاعات ارسال کند و تنها کافی است که یک رونوشت آن درخواست به پلیس اروپا[۴۲] (Europol) فرستاده شود. پلیس اروپا پس از دریافت درخواست، آن را بررسی می‌کند تا مطمئن شود درخواست مزبور، قانونی و در چارچوب موافقت‌نامهٔ سوئیفت دو است و اگر به این نتیجه رسید که مغایرتی وجود ندارد، مراتب را

---

۴۰. همان.

41. *European Parliament resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorize the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing*, available at: https://www.europarl.europa.eu/doceo/document/TA-7-2010-0143_EN.html, Last accessed on July 5, 2024.

۴۲. *یوروپل* (Europol) یا ادارهٔ پلیس اروپا، سازمانی است که وظیفهٔ همکاری و هماهنگی بین نیروهای پلیس کشورهای عضو اتحادیهٔ اروپا را بر عهده دارد. این سازمان در ۱۹۹۹ تأسیس شد و مقر آن در لاهه هلند قرار دارد. *یوروپل* در زمینه‌هایی مانند مبارزه با تروریسم، جرایم سازمان‌یافته، قاچاق مواد مخدر، قاچاق انسان، جرایم سایبری و دیگر فعالیت‌های غیرقانونی بین‌المللی فعالیت می‌کند. این سازمان به جمع‌آوری و تبادل اطلاعات بین نیروهای پلیس کشورهای عضو، تحلیل داده‌ها و پشتیبانی عملیاتی می‌پردازد تا امنیت داخلی اتحادیهٔ اروپا را تقویت کند. *یوروپل* به‌عنوان مرکز هماهنگی، تسهیل‌کنندهٔ همکاری‌های بین‌المللی در راستای مقابله با جرایم پیچیده و فراملی است.

به ارائه‌کنندهٔ اطلاعات (سوئیفت) اطلاع می‌دهد و بدین ترتیب، ارائه‌کنندهٔ اطلاعات، آن را مستقیماً به خزانه‌داری امریکا ارسال می‌کند. بنابراین در اینجا اولاً معاهدهٔ معاضدت قضایی بین دولت امریکا و اتحادیهٔ اروپا مورد توجه قرار نگرفته است و ثانیاً خزانه‌داری امریکا می‌تواند مستقیماً از مؤسسات و نهادهای اروپایی درخواست اطلاعات کند. بر اساس ماده ۱۳ موافقت‌نامهٔ سوئیفت دو، یک رکن نظارتی در نظر گرفته شده است که در موافقت‌نامهٔ سوئیفت یک وجود نداشت. این رکن موظف است هر شش ماه در رابطه با نحوهٔ اجرای موافقت‌نامه گزارش بدهد و از سه عضو از کمیسیون اروپا، دو متخصص در زمینهٔ حمایت از داده‌ها و یک متخصص با سابقهٔ قضایی تشکیل می‌شود.[۴۳]

با توجه به مطالب فوق ملاحظه می‌شود که روند همکاری سوئیفت از فرایند غیررسمی آغاز شده و سپس برای حصول اطمینان از جامعیت و رسمی‌بودن آن به‌صورت همکاری قانونی و بر اساس موافقت‌نامه‌های بین‌المللی حرکت کرده است. اتحادیهٔ اروپا تلاش کرده است تا در این راستا بین دو دغدغهٔ مبارزه با تروریسم و تأمین مالی آن از یک سو و حفظ امنیت داده‌ها و حریم خصوصی از سوی دیگر توازن برقرار کند. با این حال، همواره این‌گونه نبوده است که دریافت اطلاعات از سوئیفت از طریق مذاکره با اتحادیهٔ اروپا انجام شود، بلکه در برخی مواقع ایالات متحدهٔ امریکا به‌طور مستقیم به سوئیفت مراجعه کرده است که در ادامه به آن اشاره می‌شود.

۳-۲. اقدامات ایالات متحده در راستای دریافت اطلاعات از سوئیفت

خوان زاراته از معماران تحریم‌های مالی ایالات متحدهٔ امریکا، تلاش‌های این کشور را برای دریافت اطلاعات از سوئیفت و جلب همکاری آن، این‌گونه روایت می‌کند. «در اواخر دههٔ ۱۹۸۰ وزارت دادگستری از سوئیفت خواست که سیستم انتقال پیام خود را تغییر دهد. مقامات امریکایی تحت رهبری *باب مولر* که در آن زمان معاون دادستان کل بود، قصد داشتند سیستم پیام‌رسانی سوئیفت را دگرگون کرده و از پشت پردهٔ مبادلات مالی آگاه شوند تا از این طریق، مبدأ پول‌های ارسالی و گیرندهٔ آن‌ها را شناسایی کنند. آن‌ها در این باره پیشرفت کمی داشتند چرا که مقامات امریکایی هیچ‌گونه مجوز قانونی برای اعمال این تغییرات نداشتند. این حقیقتی بود که مقامات سوئیفت و وکلایشان به آن اشراف داشتند».[۴۴] مدتی بعد *کِنِت دَم*، معاون دپارتمان وزارت خزانه‌داری امریکا از مدیرعامل سوئیفت برای بازدید از وزارت خزانه‌داری امریکا دعوت کرد. در آن جلسه به مدیرعامل سوئیفت گفته شد که خزانه‌داری امریکا خواهان دسترسی به اطلاعات سوئیفت است. او در پاسخ سعی کرد ماهیت کلی سوئیفت، حساسیت‌ها و محدودیت‌های موجود و لزوم پایبندی سوئیفت به

۴۳. همان.

۴۴. خوان زاراته، *جنگ خزانه‌داری امریکا*، ترجمهٔ ادارهٔ مطالعات و نوآوری بانک انصار (تهران: انتشارات دانشگاه جامع امام حسین، ۱۳۹۸)،۳۷-۳۸.

محدودیت‌های قانونی را تشریح کند. نمایندهٔ خزانه‌داری امریکا در مقابل، امکان طرح دعوای حقوقی علیه سوئیفت را مطرح نمود و در عین حال به او اطمینان داد که برای حفظ اطلاعات محرمانه و حصول هر گونه توافقی اقدامات لازم انجام خواهد شد. مدتی بعد سوئیفت موافقت خود را برای همکاری با خزانه‌داری امریکا اعلام کرد.[۴۵] از اکتبر ۲۰۰۱ خزانه‌داری امریکا ماهانه یک درخواست به سوئیفت ارائه می‌کرد که حاوی چندین تقاضا برای دریافت اطلاعات بود.[۴۶] *زاراته* در ادامه توضیح می‌دهد که مدتی بعد ایالات متحدهٔ امریکا این روند دریافت اطلاعات به‌صورت موردی را ناکافی دانست و درخواست دریافت اطلاعات به‌صورت سیستمی را برای مدت موقت مطرح کرد. این درخواست به‌سختی و با ارائهٔ شواهد و مدارکی حاکی از استفادهٔ تروریست‌ها از شبکهٔ پرداخت بانکی پذیرفته شد و *فدرال رزرو* امریکا و به‌طور خاص، رئیس وقت آن، *آلن گرینسپن*، نقش مهمی در قانع‌کردن بانک‌های مرکزی کشورهای گروه ۱۰ به‌عنوان ناظران سوئیفت به تشویق و اقناع سوئیفت به همکاری در این زمینه داشت.

در مجموع، ایالات متحدهٔ امریکا از دو طریق مذاکرات و جلسات غیررسمی و نیز انعقاد موافقت‌نامه‌های رسمی در صدد آن برآمد تا از اطلاعات سوئیفت برای اجرای تحریم‌ها و ردیابی شبکه‌ها و سازمان‌های تروریستی و دیگر سازمان‌ها و نهادهایی که هدف اقدامات محدودکنندهٔ آن کشور بودند استفاده کند. اما اینها صرفاً شامل یک جنبه از رابطهٔ سوئیفت با تحریم‌ها و اقدامات محدودکنندهٔ بین‌المللی می‌شود که می‌توان آن را بُعد یا جنبهٔ اطلاعاتی سوئیفت نامید، بدین معنا که از سوئیفت اطلاعات و داده‌هایی دریافت می‌شود تا با تحلیل آن‌ها با تروریسم و تأمین مالی آن مقابله شود. جنبهٔ دیگر رابطهٔ سوئیفت با تحریم‌ها، محروم‌کردن کشورهای هدف تحریم‌ها از استفاده از سوئیفت و به عبارت دیگر، منع دسترسی به سوئیفت است که در ادامه بررسی می‌شود.

۳-۳. سوئیفت و تحریم‌های ایران

تحریم را در ادبیات حقوق بین‌الملل اقتصادی به وضع محدودیت‌های اقتصادی برای رسیدن به اهداف سیاسی تعریف کرده‌اند.[۴۷] از این منظر می‌توان اعمال فشار به سوئیفت برای قطع دسترسی بانک‌ها و مؤسسات مالی کشورهای هدف تحریم را از مصادیق بارز تحریم‌های اقتصادی محسوب کرد. کنگرهٔ ایالات متحدهٔ امریکا در ۲۰۱۲ قانون تحریم‌ها، پاسخگوکردن و حقوق بشر در ایران[۴۸] را تصویب کرد. در این قانون از سوئیفت خواسته شده بود که ارائهٔ خدمات به بانک‌های تحریم‌شدهٔ

۴۵. همان، ۳۹-۴۰.

۴۶. همان، ۴۲.

47. Andreas F. Lowenfeld, *International Economic Law*, 2nd ed. (Oxford University Press, 2008) 891-925.

48. *Iran Sanctions, Accountability, and Human Rights Act*, 2012.

ایرانی را قطع کند و اگر این امر توسط سوئیفت انجام نمی‌شد، امکان تحریم خود سوئیفت وجود داشت. سوئیفت در ۱۷ اکتبر ۲۰۱۲ اعلام کرد که با چراغ سبزی که از مقامات اتحادیهٔ اروپا دریافت کرده است، ارائهٔ خدمت به برخی بانک‌های ایرانی را قطع کرده است و آنچه قانون فوق‌الذکر در پی تحقق آن بود، عملاً اجرایی شده است. اقدام سوئیفت بر اساس تحریم اتحادیهٔ اروپا در ۱۵ مارس ۲۰۱۲ علیه بانک‌های ایرانی بود که پیام‌رسانی مالی به برخی بانک‌های ایرانی را مشمول تحریم قرار می‌داد. در اوت ۲۰۱۲ کنگره با تصویب قانون کاهش تهدید ایران و وضعیت حقوق بشر در سوریه[۴۹] به دولت امریکا اجازه داد که هر پیام‌رسان مالی را که به ایران ارائهٔ خدمت کند، مشمول تحریم قرار دهد. این دو تحریم (تحریم اتحادیهٔ اروپا و تحریم ایالات متحدهٔ امریکا) تا زمانی که برنامهٔ جامع اقدام مشترک (برجام) میان ایران و کشورهای گروه ۵+۱ مورد توافق قرار گرفت به قوت خود باقی بودند. بعد از آن، تحریم یادشده رفع شد.

با اجرای برجام، تحریم‌های مزبور رفع شدند. البته در متن برجام، قید شده بود که تحریم سوئیفت در روز انتقال (هشت سال بعد از توافق) رفع خواهند شد اما این امر بدین معنا نبود که اتصال بانک‌ها به سوئیفت نیز بعد از ۸ سال انجام‌شدنی بود. تحریم سوئیفت در مقررهٔ شمارهٔ ۴۱۳/۲۰۱۰ اتحادیهٔ اروپا ذکر شده بود. در متن این تحریم قید شده بود که ارائهٔ خدمات پیام‌رسانی مالی به اشخاصی که در فهرست‌های ۸ و ۹ تحریم یادشده قرار دارند، ممنوع است. بنابراین اگر شخصی در فهرست‌های مزبور قرار نداشت، بی‌هیچ مانعی می‌توانست از خدمات سوئیفت استفاده کند، کما اینکه برخی از بانک‌های ایرانی که مشمول تحریم‌های اتحادیهٔ اروپا قرار نگرفته بودند در دوران قبل از برجام نیز از خدمات سوئیفت استفاده می‌کردند. بر اساس آنچه در برجام و پیوست‌های ضمیمهٔ ۲ آن قید شده بود، اکثر بانک‌ها و مؤسسات مالی ایرانی در روز اجرا از فهرست تحریم‌های اتحادیهٔ اروپا خارج شدند. بنابراین تحریم سوئیفت در خصوص آن‌ها از تاریخ اجرای برجام رفع می‌شد. اما با توجه به اینکه در متن برجام، بانک‌ها، شرکت‌ها و مؤسسات مالی معدودی وجود داشتند که تحریم‌های آن‌ها تا روز اجرا به قوت خود باقی خواهد بود، امکان لغو کامل این تحریم وجود نداشت و اتحادیهٔ اروپا ناگزیر بود که اصل این تحریم را تا روز اجرا به قوت خود نگه دارد.[۵۰]

پس از انتخاب *دونالد ترامپ* به‌عنوان رئیس‌جمهور ایالات متحدهٔ امریکا، وی اعلام کرد که همان‌طور که در کارزارهای انتخابات ریاست جمهوری مکرراً از برجام انتقاد می‌کرد، از این توافق خارج خواهد شد. وی در نهایت این تهدید خود را در ماه مه ۲۰۱۸ عملیاتی و خروج ایالات متحدهٔ امریکا از برجام را اعلام کرد. البته این خروج به‌صورت فوری اعمال نشد و به شرکت‌ها و بانک‌های طرف معامله و قرارداد با ایران، مدت ۶ ماه فرصت داده شد که به تجارت و همکاری با ایران خاتمه

49. *Iran Threat Reduction and Syria Human Rights Act*, 2012.

۵۰. حمید قنبری، «عیارسنجی ۳ باور ضد برجام»، *دنیای اقتصاد* ۳۵۸۷(۱۳۹۴/۷/۱).

دهند. سوئیفت در نوامبر ۲۰۱۲ اعلام کرد که دسترسی بانک‌های ایرانی به خدمات خود را قطع می‌کند. البته تصریح نکرد که این اقدام را در راستای اجرای تحریم‌های ایالات متحدهٔ امریکا انجام می‌دهد بلکه آن را اقدامی در راستای منافع عمومی نظام مالی بین‌المللی اعلام کرد.[۵۱] به نظر می‌رسد سوئیفت به‌عنوان شخص حقوقی غیرامریکایی از این امر اکراه داشت که تصریح کند بر اساس تحریم‌های امریکا دسترسی بانک‌های ایرانی به خدمات خود را قطع کرده است، خصوصاً که در آن زمان خروج امریکا از برجام، مورد تأیید و پشتیبانی اتحادیهٔ اروپا نبود و کشورهای اروپایی اعلام کرده بودند که به‌رغم خروج امریکا از برجام به آن پایبند خواهند ماند. اما وقایع و زمان‌بندی اتصال و قطع اتصال سوئیفت به‌روشنی بیانگر آن است که اقدام سوئیفت در راستای اجرای تحریم‌های ایالات متحدهٔ امریکا بود. جدول زیر، تصویر روشن‌تری از وضعیت تحریم‌های امریکا در رابطه با قطع خدمات سوئیفت به ایران ارائه می‌کند.[۵۲]

تاریخ	اقدام
۲۰۱۲/۲/۱۳	گزارش بانکی کمیتهٔ سنا قید می‌کند که اگر سوئیفت اجازهٔ استفاده از خدمات خود به بانک‌های تحریم‌شدهٔ ایرانی را بدهد، باید بتوان آن را مشمول تحریم قرار داد.
۲۰۱۲/۲/۱۷	سوئیفت اعلام کرد که آن دسته از بانک‌های ایرانی را که در فهرست تحریم‌های اتحادیهٔ اروپا قرار دارند از دسترسی به خدمات خود محروم کرده است.
۲۰۱۲/۳/۱۵	اتحادیهٔ اروپا تحریم‌های جدیدی را علیه ایران وضع می‌کند. سوئیفت در راستای اجرای این تحریم‌ها، دسترسی برخی بانک‌های دیگر ایرانی به خدمات خود را قطع می‌کند.
۲۰۱۲/۸/۱۰	پیشنهاد تحریم پیام‌رسان‌های مالی در صورت ارائهٔ خدمات به بانک‌های تحریم‌شدهٔ ایرانی در کنگرهٔ امریکا مصوب می‌شود.
۲۰۱۶/۱/۱۶	بر اساس برجام، تحریم‌های هسته‌ای علیه ایران برداشته می‌شوند.
۲۰۱۶/۲/۱۷	بانک‌های ایرانی به سوئیفت متصل می‌شوند.
۲۰۱۸/۵/۸	*ترامپ* از برجام خارج می‌شود و مقرر می‌دارد که تجارت با ایران باید در بازه‌های زمانی ۶ یا ۹ ماهه (حسب مورد) خاتمه یابد.
۲۰۱۸/۱۱/۲	*منوچین* وزیر خزانه‌داری امریکا اخطار می‌دهد که اگر سوئیفت ارتباط بانک‌های ایرانی را قطع نکند، مشمول تحریم امریکا قرار خواهد گرفت.
۲۰۱۸/۱۱/۸	سوئیفت ارائهٔ خدمت به بانک‌های ایرانی را که مشمول بازگشت تحریم‌های امریکا قرار گرفته‌اند، قطع می‌کند.

51. Retrieved from: https://www.swift.com/about-us/legal/compliance-0/swift-and-sanctions, Last accessed on July 5, 2024.

52. Wong, *International Financial Messaging Systems*, 14.

۳-۴. تلاش‌های بین‌المللی برای گسترش نقش تحریمی سوئیفت

اقدامات برای اعمال فشار به سوئیفت جهت قطع خدمات خود به بانک‌ها و مؤسسات مالی با اهداف سیاسی، محدود به آنچه در بالا گفته شد، نبوده، بلکه شامل برخی موارد مهم دیگر نیز هست که در ادامه به برخی از آن‌ها اشاره می‌شود.

در ۲۰۱۷ در یک گزارش کارشناسی کمیتهٔ تخصصی شورای امنیت سازمان ملل متحد که بر اساس قطعنامهٔ شمارهٔ ۲۳۴۵ سال ۲۰۱۷ سازمان ملل متحد تشکیل شده بود و مقرر بود در خصوص اجرای تحریم‌های آن شورا علیه کره شمالی و خصوصاً قطعنامهٔ شمارهٔ ۱۸۴۷ (۲۰۰۹) گزارش دهد، این نکته قید شد که شرکت‌ها و سازمان‌های متعددی در کره شمالی از خدمات بانک‌های بین‌المللی و سوئیفت برای دورزدن تحریم‌ها استفاده می‌کنند.[۵۳] این امر منجر به این شد که مقامات دولت بلژیک اعلام کنند به سوئیفت ابلاغ خواهد شد که دیگر حق اجازهٔ استفاده از خدمات به بانک‌های کره شمالی را ندارد و نتیجه این شد که دسترسی هفت بانک کره شمالی به سوئیفت که تا آن زمان برقرار بود، قطع شود. البته از میان این هفت بانک، سه بانک در فهرست تحریم‌های شورای امنیت قرار داشتند اما چهار بانک دیگر مشمول تحریم نبودند و سوئیفت اعلام کرد که به دلیل کاستی‌ها و ایرادات این بانک‌ها، دسترسی به خدمات آن‌ها را قطع می‌کند. برخی بر این باورند که این اقدام در نتیجهٔ فشارهای دیپلماتیک بر سوئیفت و دولت بلژیک انجام شده است.[۵۴]

نمونهٔ دیگر استفاده از سوئیفت برای اعمال فشار سیاسی به دولت‌ها، روسیه است. پس از حملهٔ روسیه به اوکراین، ابتدا دولت اوکراین در ۲۲ فوریهٔ ۲۰۲۲ پیشنهاد قطع ارتباط بانک‌های روسیه با سوئیفت را مطرح کرد. روز بعد، وزیر دارایی فرانسه همین پیشنهاد را تکرار کرد. صدر اعظم آلمان نیز مطالب مشابهی را بیان کرد و خواستار قطع خدمات سوئیفت به بانک‌های روسیه شدد. در نهایت، در اول مارس ۲۰۲۲ اتحادیهٔ اروپا و انگلستان توافق کردند که سوئیفت خدمت‌رسانی به ۷ بانک بزرگ روسیه را قطع کند و در ۳۱ مه همان سال، یک بانک دیگر نیز به این تعداد اضافه شد.[۵۵]

علاوه بر تلاش‌های دولت‌ها و سازمان‌های بین‌المللی برای استفاده از سوئیفت به‌عنوان اهرم فشار، گاه احزاب و گروه‌های سیاسی نیز برای اعمال فشار بر دولت‌های هدف به سوئیفت متوسل می‌شوند. به‌عنوان مثال در ۲۰۰۴ برخی گروه‌های طرفدار حقوق بشر خواستار قطع ارتباط سوئیفت با بانک‌های برمه در واکنش به اقدامات حکومت نظامی آن کشور شدند. سوئیفت این خواسته را

53. United Nations. "Report by the Panel of Experts Established Pursuant to Resolution 1874 (2009)". *Report of the Panel of Experts established pursuant to resolution 1874 (2009)* (2019).

54. Wong, *International Financial Messaging Systems*, 14.

55. Retrieved from: https://en.wikipedia.org/wiki/SWIFT_ban_against_Russian_banks, Last accessed on July 5, 2024.

اجابت نکرد و به بی‌طرفی خود در موضوعات سیاسی اشاره نمود. در ۲۰۱۴ گروه‌های طرفدار فلسطین خواستار قطع ارتباط سوئیفت با بانک‌های رژیم اشغالگر شدند. سوئیفت این پیشنهاد را به دلیل مشابهی نپذیرفت. در ۲۰۲۱ گروه‌های مخالف حکومت بلاروس به دلایل مشابهی خواستار قطع خدمات سوئیفت به بانک‌های آن کشور شدند اما سوئیفت این درخواست را نیز رد کرد.[۵۶]

با توجه به مطالب فوق ملاحظه می‌شود که سوئیفت از سه کانال مختلف که عبارت‌اند از دولت‌ها، سازمان‌های بین‌المللی و گروه‌های سیاسی که در بالا به آن‌ها اشاره شد، تحت فشار قرار دارد که با ملاحظات سیاسی، دسترسی برخی بانک‌ها و مؤسسات مالی به خدمات خود را محدود یا قطع کند. اگرچه سوئیفت تا کنون در مقابل خواسته‌های گروه‌ها و احزاب سیاسی مقاومت کرده است، در مقابل دولت‌ها و سازمان‌های بین‌المللی تاب مقاومت نداشته و حتی در مواردی که ایالات متحدهٔ امریکا از جهت قانونی صلاحیت اعمال فشار به سوئیفت را نداشته است، سوئیفت تحریم های امریکا را تحت لوای منافع نظام مالی بین‌المللی، ایرادات و کاستی‌های بانک‌های هدف تحریم و نظایر آن اجرا کرده و به تصمیمات آن گردن نهاده است. این امر در کنار همکاری کامل سوئیفت با نهادهای ناظر بر اجرای تحریم‌ها در امر ارائه و تجزیه و تحلیل اطلاعات تراکنش‌های مالی، نشانگر ریسک‌های بالقوهٔ سوئیفت خصوصاً برای کشورها تحت تحریم است و لذا ضرورت توجه به مکانیزم‌های جایگزین پیام‌رسانی مالی را روشن می‌سازد که در بخش پایانی این مقاله به برخی از آن‌ها اشاره می‌شود.

۴. مکانیزم‌های پیام‌رسانی مالی، جایگزین احتمالی سوئیفت

با توجه به مخاطرات و چالش‌های پیام‌رسانی مالی از طریق سوئیفت، برخی کشورها در صدد برآمده‌اند که جایگزین‌هایی را برای سوئیفت طراحی و عملیاتی کنند. در این راستا به برخی از این مکانیزم‌های جایگزین و قابلیت‌ها و ملاحظات مربوط به هر کدام اشاره می‌شود.

۴-۱. سامانهٔ پیام‌رسانی الکترونیک مالی (سپام)

سامانهٔ پیام‌رسانی الکترونیکی مالی (سپام) سامانه‌ای است که بانک مرکزی جمهوری اسلامی ایران به منظور الکترونیکی‌کردن مراودات بانکی و ایجاد زیرساخت یکپارچهٔ خدمت‌رسانی راه‌اندازی کرده است. با راه‌اندازی این سامانه، تمامی سیستم‌های بانکی تحت پروتکل‌های استاندارد مبادلات مالی به یکدیگر متصل شده و ارتباطات، مکاتبات و مراودات میان بانک‌ها و بانک مرکزی به‌صورت کاملاً الکترونیکی انجام می‌شود. سپام نه‌تنها برای تمام مراودات مالی عمدهٔ بانک‌ها از قبیل اعتبارات اسنادی ارزی و ریالی، ضمانت‌نامه‌های ارزی و ریالی، حوالجات ارزی، مکاتبات، استعلام‌ها

56. Wong, *International Financial Messaging Systems*, 14.

و مذاکرات قابل استفاده است بلکه امکان اتصال به بانک‌های خارجی و نیز واحدهای بانکی تحریم‌شدهٔ ایرانی در خارج از کشور را نیز دارد به گونه‌ای که بدون به‌کارگیری امکانات مؤسسهٔ سوئیفت و نگرانی‌های مربوط به آن، با زبانی مشترک و آشنا، تعاملات مالی با آخرین فناوری‌های موجود صورت گیرد و در عین حال، از ارسال پیام‌های مالی داخلی به خارج از کشور نیز پرهیز شود.[۵۷] البته بانک‌های کشورهای خارجی مقررات تحریم‌ها را رعایت می‌کنند اما اگر برخی از بانک‌های خارجی به هر دلیل تصمیم به برقراری رابطه با بانک‌های ایرانی در شرایط تحریم بگیرند، امکان اتصال آن‌ها به سپام وجود خواهد داشت و از این جهت مانع عملیاتی و فنی وجود ندارد.

پروژهٔ سپام در۱۳۹۰ در بانک مرکزی شروع شد و ابتدا امکان‌سنجی و بررسی نیازمندی‌های مربوطه، و سپس برگزاری مناقصه و انعقاد قرارداد با شرکت برنده انجام و دوره‌های آموزشی مربوطه برگزار شد و نرم‌افزارهای لازم در بانک مرکزی نصب و مورد آزمون قرار گرفت و در تیر ۱۳۹۱ افتتاح شد. تمامی بانک‌های ایران از طریق شبکهٔ ملی بین بانکی (مبین) به سرور عملیاتی سپام متصل شده و از آن بهره‌برداری می‌کنند. سپام هم پیام‌رسانی ارزی را پشتیبانی می‌کند و هم پیام‌رسانی ریالی را. سپام ریالی پیرو تصویب دستورالعمل اعتبار اسنادی داخلی – ریالی در جلسهٔ ۱۳۹۱/۹/۷ شورای پول و اعتبار و ابلاغ آن طی بخشنامهٔ شمارهٔ ۲۴۴۷۰۰/۹۱ در ۱۳۹۱/۹/۱۵ به بانک‌های کشور برقرار شد. برای برقرارسازی سپام ریالی، شیوه‌نامهٔ مربوط به این کار توسط بانک مرکزی تهیه و پیام‌های فارسی اعتبار اسنادی بر اساس استانداردهای جهانی سوئیفت تدوین شد. این شیوه‌نامه در بهمن ۱۳۹۱ برای تمامی بانک‌ها ارسال شد و پرتال سپام ریالی از دی ماه ۱۳۹۳ به بهره‌برداری کامل رسید.[۵۸]

در رابطه با ارزیابی سپام می‌توان گفت با توجه به اینکه سپام به‌طور کامل توسط بانک مرکزی ایران طراحی شده است، برای انتقال پیام‌های بین بانکی از قابلیت اطمینان قابل‌توجهی برخوردار است و این قابلیت که شعب ایرانی بانک‌های خارجی و حتی بانک‌های خارجی نیز قابلیت اتصال به آن را دارند، جزء مزایای مهم آن محسوب می‌شود. با این حال، در رابطه با قابلیت جایگزینی کامل آن به جای سوئیفت باید به چند نکته توجه داشت: نخست اینکه سپام برای بسیاری از بانک‌های خارجی شناخته‌شده نیست و از آنجا که کشورهای خارجی در طراحی و عملیاتی‌سازی آن مشارکتی نداشته‌اند ممکن است تردیدهایی نسبت به امنیت و قابلیت اتکای آن داشته باشند که رفع آن‌ها گاه ساده نیست. همان‌طور که در ابتدای این مقاله و در بحث از پیشینهٔ سوئیفت اشاره شد، بانک‌های کشورهای دیگر معمولاً به سیستم‌های پیام‌رسانی مالی که توسط یک کشور

۵۷. سیدمحمود احمدی و مهدی خندان سویری، (تهران: نظام‌های پرداخت و بانکداری الکترونیک در ایران، انتشارات پژوهشکدهٔ پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، ۱۳۹۴)، ۲۰۴.

۵۸. همان، ۲۰۸.

دیگر و بدون مشارکت بین‌المللی طراحی شده باشد روی خوش نشان نمی‌دهند. نکتهٔ دوم این است که بانک‌های خارجی نیاز به سیستم پیام‌رسانی مالی دارند که تمامی نیازهای آن‌ها را پوشش دهد. نظر به اینکه سپام علی‌رغم قابلیت‌های فنی خود، توسط اکثریت بانک‌های خارجی پذیرفته نشده است، اگر برخی از بانک‌ها آن را بپذیرند، ناچارند در کنار آن یک سیستم دیگر را برای پیام‌رسانی مالی بپذیرند که این امر برای آن‌ها ایجاد هزینهٔ مضاعف خواهد کرد و ممکن است فعالیت هم‌زمان دو پیام‌رسان مالی برای آن‌ها ریسک‌های عملیاتی نیز داشته باشد؛ لذا استقبال از این سامانه در بانک‌های خارجی محدود خواهد بود. معذلک باید توجه داشت که سپام با استفاده از فناوری و استانداردهای روز دنیا و امکان اتصال به SWIFT Net می‌تواند نسبت به تبادل پیام‌های مالی با تمام اعضای سوئیفت با رعایت تمامی شرایط و قوانین اقدام کند.

۴-۲. مکانیزم‌های پیام‌رسانی مالی چین و روسیه

چین و روسیه مکانیزم‌هایی را برای پیام‌رسانی مالی طراحی و عملیاتی نموده‌اند که در ادامه به برخی ویژگی‌های آن‌ها اشاره می‌شود. لازم به ذکر است در مورد اینکه ایران در شرایط تحریم‌ها از این مکانیزم‌ها استفاده می‌کند یا خیر، اطلاعات قابل دسترسی وجود ندارد که بتوان در خصوص آن اظهارنظر کرد.

نظام پرداخت‌های فرامرزی چین[۵۹] یک نظام پرداخت طراحی و عملیاتی‌شده توسط دولت چین است که کارکرد اصلی آن تسهیل پرداخت‌های مربوط به پول ملی چین، یوآن است. این مکانیزم در ۸ اکتبر ۲۰۱۵ راه‌اندازی شد و هدف آن حمایت از تجارت بین‌المللی و تسهیل پرداخت‌های فرامرزی، تأمین مالی و سرمایه‌گذاری در راستای بین‌المللی‌کردن یوآن چین عنوان شد.[۶۰]

این سیستم توسط شرکت خدمات پرداخت بین‌المللی چین راهبری می‌شود که خود تحت مالکیت بانک مرکزی چین[۶۱] قرار دارد. مؤسسات مالی که از خدمات این شرکت بهره می‌برند به دو دسته قابل تقسیم هستند: مؤسسات مالی که به‌طور مستقیم به این سیستم متصل هستند و مؤسساتی که به‌طور غیرمستقیم و از طریق مؤسسات دستهٔ نخست به این سامانه متصل می‌شوند. مؤسسات دستهٔ نخست، دارای حساب مشخص نزد سیستم هستند و می‌توانند بدون واسطه از طریق این سامانه پیام ارسال و دریافت کنند. هنگامی که این سیستم در اکتبر ۲۰۱۵ راه‌اندازی شد، ۱۹ مؤسسه به‌طور مستقیم و ۱۷۶ مؤسسه به‌طور غیرمستقیم به آن دسترسی داشتند.[۶۲] بر

59. Cross Border Interbank Payment System (CIPS)

60. China International Payment Service Corp. About the System. Retrieved from: https://www.cips.com.cn/cipsen/7052/7057/index.html, Last accessed on July 5, 2024.

61. Peoples Bank of China (PBOC)

62. Ibid.

اساس گزارش سالانهٔ بانک مرکزی چین در پایان ۲۰۲۲، روزانه به‌طور متوسط ۱۶۳۰۰ تراکنش از طریق این سامانه انجام می‌شود و تا کنون مبلغ ۲۲٫۸۵ تریلیون یوآن از این طریق منتقل شده است.[۶۳] در حال حاضر این سیستم، پیام‌های مالی بانک‌ها و مؤسسات مالی در بیش از ۱۰۰ کشور جهان را منتقل می‌کند. ترکیب کشورهای مختلفی که در این سیستم حضور دارند و سهم هر کدام از آن‌ها نیز جالب است. چین بیشترین سهم را دارد؛ بعد از آن، دیگر کشورهای آسیایی، سپس کشورهای اروپایی و در نهایت امریکا قرار دارند.[۶۴] همچنین همکاری‌هایی میان مکانیزم پیام‌رسانی مالی چین و سوئیفت در سال‌های اخیر خصوصاً در زمینه‌های تحقیقاتی راجع به پول‌های دیجیتال شکل گرفته است.

در خصوص مکانیزم پیام‌رسانی مالی چین باید به چند نکته توجه داشت: نخست اینکه با توجه به تقسیم کاربران از این مکانیزم به دو دستهٔ مستقیم و غیرمستقیم، استفاده از آن، نیاز بانک‌ها و مؤسسات اعتباری به سوئیفت را از بین نمی‌برد. توضیح اینکه کاربران مستقیم می‌توانند تمامی پیام‌های مالی خود را از طریق این مکانیزم مخابره کنند اما کاربران غیرمستقیم نیاز به این خواهند داشت که برخی از پیام‌های خود را از طریق سوئیفت مخابره کنند. بنابراین، وابستگی به سوئیفت همچنان باقی خواهد بود.[۶۵] دوم اینکه بانک‌هایی که پیام‌های مالی خود را از طریق سامانهٔ طراحی شده توسط چین مخابره می‌کنند موظف‌اند که مقررات بانکی و مالی چین، خصوصاً مقررات کنترل سرمایهٔ آن را که بعضاً سخت و جدی هم هستند رعایت کنند. این امر می‌تواند در استفاده از این مکانیزم، مانع یا محدودیت ایجاد کند.[۶۶] در نهایت، سومین موضوع این است که جذابیت مکانیزم یادشده عمدتاً برای بانک‌هایی است که مبادلات بالایی با یوآن چین یا بانک‌های چینی دارند. با این حال، به دلیل سیاست‌های خاص اقتصادی چین و دستکاری ارزش یوآن توسط مقامات چین به منظور به‌دست‌آوردن مزیت رقابتی صادراتی، یوآن چین هنوز نتوانسته است سهم قابل‌توجهی در تبادلات مالی بین‌المللی به دست آورد. از این رو سامانهٔ یادشده نیز رشد و توسعهٔ مورد انتظار را نداشته است.

کشور روسیه نیز در ۲۰۱۴ در پاسخ به تحریم‌های ایالات متحدهٔ امریکا و اتحادیهٔ اروپا طراحی مکانیزمی را تحت عنوان نظام انتقال پیام‌های مالی[۶۷] آغاز کرد. این مکانیزم در ۲۰۱۷ عملیاتی شد و گفته می‌شود که بیش از ۳۰۰ مؤسسهٔ مالی در روسیه، بلاروس، ارمنستان، تاجیکستان، قرقیزستان،

63. Retrieved from: http://www.pbc.gov.cn/en/3688110/3688172/4437084/4664821/2022092314120713992.pdf, Last accessed on July 5, 2024.

64. Wong, *International Financial Messaging Systems*, 14.

65. Barry Eichengreen, *Sanctions, SWIFT, and China's cross-border interbank payments system*. Center for Strategic and International Studies (CSIS), 2022.

66. Ibid.

67. System for Transfer of Financial Messages (SPFS)

قزاقستان، کوبا و حتی آلمان (شعب بانک‌های روسیه در آلمان) به آن پیوسته‌اند.[۶۸] این سامانه استانداردهای ISO 20022 را که قبلاً به آن اشاره شد و سوئیفت بر مبنای آن کار می‌کند پذیرفته است و بر اساس آنچه مقامات روسیه ادعا کرده‌اند، هزینه‌های استفاده از این سامانه یک‌سوم هزینه‌های سوئیفت است[۶۹] که علی‌القاعده هزینه‌ها برای این پایین آورده شده‌اند که سامانهٔ مزبور برای بانک‌های مختلف در سطح دنیا جذابیت داشته باشد. با این حال، سوئیفت به‌طور شبانه‌روزی و ۲۴ ساعته در طول هفت روز هفته قابل استفاده است اما سامانهٔ روسیه فقط در ساعات کاری قابل استفاده است. ضمن اینکه سرعت انتقال شبکهٔ سوئیفت ۱۰ مگابایت بر ثانیه است اما سرعت انتقال سامانهٔ روسیه ۲۰ کیلوبایت بر ثانیه است که نشان‌دهندهٔ تفاوت قابل‌توجهی است.[۷۰] در اکتبر ۲۰۱۴ رسانه‌های خبری روسیه و چین گزارش دادند که برنامه‌ای بین دو دولت برای اتصال سامانه‌های پیام‌رسانی مالی آن‌ها در دست پیگیری است و حتی خبر از این دادند که سامانهٔ مشابهی که توسط هند در دست طراحی است نیز به این دو سامانه اضافه خواهد شد. بر این اساس به نظر می‌رسد که کشورهای یادشده به دنبال ایجاد جایگزینی برای سوئیفت هستند که امریکا و اتحادیهٔ اروپا از آن به‌عنوان اهرم فشار سیاسی استفاده می‌کنند. همان‌طور که ملاحظه شد، سیستم‌های پیام مالی توسعه داده‌شده توسط هر کشور، نقاط قوت و ضعف خود را دارند. اتصال این سیستم‌ها به یکدیگر می‌تواند به رفع نقاط ضعف یا حداقل کمترشدن آن‌ها کمک کند اما در عین حال، خالی از دشواری‌های فنی و عملیاتی نخواهد بود.

۴-۳. پیام‌رسانی مالی مبتنی بر بلاکچین

با ایجاد و توسعهٔ فناوری *بلاکچین*، برخی شرکت‌ها و اشخاص فعال در این زمینه در صدد بر آمده‌اند که از *بلاکچین* برای پیام‌رسانی مالی استفاده کنند. معتقدین به استفاده از *بلاکچین* برای پیام‌رسانی مالی بر این باورند که این نوع پیام‌رسانی دارای مزیت‌های متعددی است. نخست اینکه امنیت و قابلیت اتکای این نوع پیام‌رسانی در مقایسه با تمامی راهکارهای جایگزین بیشتر است و ریسک تقلب و دسترسی غیرمجاز در آن وجود ندارد. دوم اینکه این نوع پیام‌رسانی مالی کارایی بیشتری دارد چرا که نیاز به وجود واسطه میان فرستنده و دریافت‌کنندهٔ پیام را از بین می‌برد و پیام به‌طور مستقیم از فرستنده به گیرنده منتقل می‌شود و باعث صرفه‌جویی در زمان و هزینه‌ای می‌شود که صرف پردازش پیام از طریق واسطه می‌شود. سوم اینکه در این مکانیزم پیام‌رسانی شفافیت بیشتری وجود دارد و فرستنده و گیرندهٔ پیام بلافاصله کلیهٔ اطلاعات مربوط به پیام را دریافت

68. Murillo Oliviera Dias, Leonardo Jose Dias Periera and Patricia Dos Santos Viera, "Are the Russian Banks Threatened with Removal from SWIFT. A Multiple Case Study on Interbank Financial Messaging Systems." *International Journal of Scientific Research and Management*, 10, 3 (2022) 3137-44.

69. Ibid.

70. Ibid.

می‌کنند و در نهایت، چهارمین مزیت این نوع پیام‌رسانی مالی این است که ردیابی پیام در آن با سهولت بیشتری امکان‌پذیر است و *بلاکچین* از هر تراکنش، سابقه‌ای می‌سازد که در زنجیرهٔ پیام‌ها باقی مانده و قابلیت راستی‌آزمایی دارد.

در حال حاضر، پیشنهادها و ابتکارات متعددی برای استفاده از *بلاکچین* در پیام‌رسانی مالی وجود دارند که به اختصار به برخی از آن‌ها اشاره می‌شود. نخستین نمونه، *ریپل*[۷۱] نام دارد که شرکت فناوری مالی ثبت‌شده در کالیفرنیا است. این شرکت یک شبکهٔ پرداخت مبتنی بر بلاکچین به نام *ریپل نت* راه‌اندازی کرده است. بر اساس آنچه در وبسایت *ریپل نت* ادعا شده است، تمامی پرداخت‌ها در این شبکه، ظرف سه ثانیه قابل انجام است. این شبکه بیش از ۵۵ کشور را تحت پوشش قرار می‌دهد و بیش از ۱۲۰ ارز در آن قابل انتقال هستند.[۷۲] لازم به ذکر است که *ریپل نت* فقط مکانیزم پیام‌رسانی مالی نیست بلکه پرداخت و انتقال وجه را نیز انجام می‌دهد و از این حیث، یک نظام تسویهٔ مالی نیز به حساب می‌آید و تفاوت آن با نظام‌های سنتی تسویه این است که نیاز به سیستم پیام‌رسانی مالی جداگانه ندارد. البته فعالیت *ریپل* در امریکا بدون مانع و مشکل نبوده است. در دسامبر ۲۰۲۲ کمیسیون اوراق بهادار امریکا اعلام کرد که به دلیل فروش و معاملهٔ بدون مجوز XRP که نوعی دارایی دیجیتال *ریپل* است، علیه آن طرح دعوا نموده است. رابطهٔ XRP و *ریپل نت* در این است که *ریپل نت* از همان زیرساخت‌های XRP استفاده می‌کند و نیز امکان پرداخت این نوع دارایی به جای پول‌های ملی کشورها در این مکانیزم وجود دارد. *ریپل* پاسخ داده است که دارایی مزبور نوعی رمزارز است و مشمول مقررات کمیسیون اوراق بهادار نیست.[۷۳] با این حال، نفس وجود این پرونده نشانگر آن است که این نوع فعالیت‌ها می‌توانند با توجه به تازه و بدیع بودن فناوری زیربنایی و محصولات آن از یک سو و نبود قوانین و مقررات در غالب کشورها (یا وجود قوانین مجمل و مبهم) با نااطمینانی‌های حقوقی قابل‌توجهی روبه‌رو شوند.

یکی دیگر از شبکه‌های پرداخت مبتنی بر *بلاکچین*،[۷۴] *لینک* نام دارد که در ۲۰۱۷ توسط بانک *جِی پی مورگان* راه‌اندازی شد. *جی پی مورگان* مدعی است که بیش از ۴۰۰ مؤسسهٔ مالی از این شبکهٔ پرداخت استفاده می‌کنند. این مکانیزم به منظور انتقال ایمن، کارآمد و شفاف اطلاعات مالی تهیه شده است و برای انجام تراکنش‌ها، تأیید هویت و پرداخت‌های فرامرزی قابلیت استفاده دارد. این مکانیزم مبتنی بر فناوری دفتر کل غیرمتمرکز بوده و امکان تبادل اطلاعات میان بانک‌ها را

71. Ripple

72. Retrieved from: https://cointelegraph.com/learn/ripplenet-the-decentralized-network-of-banks, Last accessed on July 5, 2024.

73. Wong, *International Financial Messaging Systems*, 8.

۷۴. *لینک*(Liink) نام تجاری جدید شبکهٔ پرداخت مبتنی بر *بلاکچین* است که *جی‌پی مورگان* آن را راه‌اندازی کرد. در ابتدا این شبکه به‌عنوان(IIN) "Interbank Information Network" شناخته می‌شد، اما در اکتبر ۲۰۲۰ به *لینک* تغییر نام داد تا برند جدیدی برای این شبکه ایجاد شود. *لینک*، بخشی از پلتفرم بلاکچین *جی‌پی مورگان* به نام Onyx است.

فراهم می‌سازد. همچنین ادعا شده است که این مکانیزم منحصر به پیام‌رسانی مالی نبوده و به‌عنوان مرکزی برای ارائهٔ فناوری‌های نوظهور همانند قراردادهای هوشمند و تحلیل داده‌ها عمل می‌کند.

آنچه تا کنون گفته شد، در رابطه با آن دسته از مکانیزم‌های پیام‌رسانی مالی مبتنی بر *بلاکچین* بود که پیام‌های مربوط به پول‌های ملی متعارف و سنتی از طریق آن‌ها جابه‌جا می‌شوند. در کنار این مکانیزم‌ها، رمزارزها (شامل رمزارزهای غیردولتی و رمزارزهای بانک‌های مرکزی) وجود دارند که سیستم تسویه و پیام‌رسانی آن‌ها کاملاً متفاوت با پول ملی کشورهاست و به نوعی نیازمند سیستم‌های پیام‌رسانی مالی سنتی نیستند و بحث از آن‌ها از حدود این مقاله خارج است. در مجموع به نظر می‌رسد فناوری‌های مالی مبتنی بر *بلاکچین* تا کنون به‌طور نظام‌مند توسط دولت‌ها برای مقابله با تحریم‌های حوزهٔ پیام‌رسانی مالی مورد استفاده قرار نگرفته‌اند و عمدهٔ ابتکاراتی که در این زمینه صورت گرفته در کشورهای غربی و با هدف سرمایه‌گذاری و کسب سود برای شرکت‌های فعال در این حوزه‌ها بوده است. این امر می‌تواند دو علت داشته باشد. نخست اینکه فناوری *بلاکچین* عمدتاً بر رمزارزها متمرکز است و رمزارزها ماهیتاً به نوعی هستند که به یک شیوهٔ پیام‌رسانی مستقل احتیاجی ندارند. دوم اینکه علی‌رغم رشد و گسترش رمزارزها، هنوز هم ارزهای سنتی کشورها نقش غالب را در تجارت بین‌الملل دارند و کشورهایی که مشمول تحریم‌ها یا در معرض آن‌ها هستند، بیشتر به دنبال این هستند که مکانیزم‌هایی را برای انتقال پیام‌های مالی و با شباهت فنی هر چه بیشتر با سوئیفت طراحی کنند که بانک‌های کشورهای مختلف با سهولت بیشتر قانع شوند که از آن‌ها استفاده کنند. به نظر می‌رسد استفادهٔ دولت‌ها از فناوری *بلاکچین* در سال‌های آینده بیشتر متمرکز بر طراحی و انتشار پول‌های دیجیتال بانک‌های مرکزی باشد تا پیام‌رسانی مالی جایگزین سوئیفت. با این حال، با توجه به قابلیت‌های فناوری *بلاکچین*، امکان استفاده از این فناوری به‌عنوان جایگزینی برای سوئیفت در پیام‌رسانی مالی تراکنش‌های مربوط به پول‌های ملی وجود دارد. فناوری *بلاکچین* با فراهم‌کردن امنیت بالا، شفافیت و کاهش هزینه‌های تراکنش، می‌تواند به بانک‌ها و فعالان اقتصادی در دورزدن تحریم‌ها کمک کند. شبکه‌هایی مانند *ریپل نت* و *لینک* که بر اساس *بلاکچین* عمل می‌کنند، به بانک‌ها این امکان را می‌دهند که تراکنش‌های بین‌المللی را بدون نیاز به واسطه‌های سنتی و با سرعت بیشتری انجام دهند. این شبکه‌ها با ارائهٔ راه‌حل‌های امن و کارآمد برای انتقال پول و اطلاعات مالی، می‌توانند جایگزین مناسبی برای سوئیفت باشند و در شرایط تحریمی نقش مهمی ایفا کنند.

نتیجه

با توجه به مطالبی که در این مقاله بیان شد، ملاحظه می‌شود که سوئیفت علی‌رغم برخی تهدیدات و مخاطرات فنی نظیر دسترسی غیرمجاز و کلاهبرداری، همچنان جایگاه خود را به‌عنوان مهم‌ترین شبکهٔ پیام‌رسانی مالی بین‌المللی حفظ کرده است. با این حال، استفادهٔ واضعان تحریم‌های بین‌المللی از اطلاعات سوئیفت برای ردیابی موارد نقض تحریم‌ها از یک سو و اعمال فشار به بانک‌ها و مؤسسات مالی کشورهای هدف از سوی دیگر، باعث شده است که برخی از دولت‌ها که نقش قابل‌توجهی در اقتصاد جهانی دارند، نسبت به تداوم امکان استفاده از سوئیفت دچار تردید شده و به دنبال طراحی و عملیاتی‌سازی راهکارهای جایگزین برآیند، خصوصاً که تبعیت سوئیفت از تحریم‌های فراسرزمینی از منظر حقوق بین‌الملل قابل دفاع نیست و سوئیفت به‌عنوان شرکت اروپایی ملزم به اجرای تحریم‌های ایالات متحدهٔ امریکا نیست. تلاش‌های سوئیفت برای مشروعیت‌بخشی به همکاری‌های انجام‌شده با دولت‌های واضع تحریم نیز از منظر حقوقی قابل دفاع به نظر نمی‌رسد و این توافقات نمی‌تواند به زیان اشخاص ثالث مورد استناد قرار گیرد ولی فقدان مرجع بین‌المللی مستقل و دارای صلاحیت برای رسیدگی به نقض تعهدات سوئیفت در مقابل اعضا و اعمال تبعیض، باعث شده است که از منظر حقوقی امکان برخورد با سوئیفت و الزام آن به تغییر سیاست سوئیفت وجود نداشته باشد؛ لذا مؤثرترین راهکار، طراحی و اجرای راهکارهای جایگزین سوئیفت است که در این مقاله به برخی از آن‌ها اشاره شد. هرچند راهکارهای جایگزین سوئیفت هنوز تا رسیدن به نتیجهٔ مطلوب فاصله دارند، انتظار می‌رود کشورهای وضع‌کنندهٔ تحریم‌های خارجی با ملاحظهٔ قوت‌گرفتن مکانیزم‌های رقیب، در سیاست خود مبنی بر استفادهٔ حداکثری از سوئیفت به‌عنوان ابزار تحریمی تجدیدنظر کنند و همکاری و تعامل بین‌المللی باید آن گونه باشد که کشورهای تحریم‌کننده را وادار به تجدیدنظر در تصمیمات خود کند. البته راهکارهای فعلی موجب بی‌نیازی کامل به سوئیفت نمی‌شوند اما به‌عنوان راهکارهای اولیه، مثبت و مفید بوده و انتظار می‌رود که در آینده به نتایج مفیدتر و جامع‌تری منتهی شوند.

منابع:

الف. فارسی

ـ کتاب

۱. منصوری رضی، ایوب. *رژیم حقوقی حاکم بر سوئیفت*. تهران: انتشارات شهر دانش، ۱۳۹۸.

۲. فیروزبخت، فهیمه. *حقوق انتقال الکترونیکی وجوه*. تهران: انتشارات مجد ۱۳۹۸.

۳. زاراته، خوان. *جنگ خزانه‌داری امریکا*. تهران: ترجمهٔ ادارهٔ مطالعات و نوآوری بانک انصار، انتشارات دانشگاه جامع امام حسین، ۱۳۹۸.

۴. احمدی، سیدمحمود و مهدی خندان سویری. *نظام‌های پرداخت و بانکداری الکترونیک در ایران*. تهران: انتشارات پژوهشکدهٔ پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، ۱۳۹۴.

ـ مقاله

۱. عزیزی، محمود و جمشید شریفیان، «بایسته‌های سوئیفت و آسیب‌شناسی آن در حقوق تجارت ایران در پرتو تحریم»، *مجلهٔ پژوهش و مطالعات علوم اسلامی* ۲، شمارهٔ ۱۶(۱۳۹۹).

۲. قنبری، حمید، «کشف رمز غیرقانونی: سوئیفت چگونه با امریکا همکاری می‌کند؟»، *تجارت فردا*، شمارهٔ ۶۰، ۱۳ (۱۳۹۲).

۳. قنبری، حمید، «عیارسنجی ۳ باور ضد برجام»، *دنیای اقتصاد*، شمارهٔ ۳۵۸۷ (۱۳۹۴/۷/۱).

ب. انگلیسی

- Books

1. Bamford, Colin. *Principles of international financial law*. Oxford University Press, USA, 2011.
2. Lowenfeld, Andreas F. *International Economic Law*. 2nd ed. Oxford University Press, 2008.

- Articles

1. Cipriani, Marco, Linda S. Goldberg, and Gabriele La Spada. "Financial sanctions, SWIFT, and the architecture of the international payment system." *Journal of Economic Perspectives* 37, no. 1 (2023): 31-52.
2. Oliveira Dias, Murillo, Leonardo Jose Dias Pereira, and Patricia Dos Santos Viera. "Are the Russian Banks Threatened with Removal from SWIFT? A Multiple Case Study on Interbank Financial Messaging Systems." *International Journal of Scientific Research and Management*, 10, no. 3 (2022), 3137-44.

3. Scott, Susan V., and Markos Zachariadis. "Origins and development of SWIFT, 1973–2009." *Business History* 54, no. 3 (2012): 462-482.
4. Scott, Susan V., and Markos Zachariadis. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community*. Taylor & Francis, 2014.
5. Wong, Liana. *International financial messaging systems*. Congressional Research Service, 2021.