Journal of
Management, Economics & Entrepreneurship
www.JMEK.ir

Volume 6, Issue 1, 2025

The Imperative of Adopting Blockchain-Based Digital Currency as a Substitute for the SWIFT System

Hossein Asadi Gorji*[1] Homayoun Asadi[2]

1. PhD student in Economics, Faculty of Economics, Ferdowsi University, Mashhad, Iran. (Corresponding Author) Email: hosseinasadigorji@gmail.com
2. PhD in Entrepreneurship, Faculty of Management, Sari Branch, Islamic Azad University, Sari, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 1-11

Corresponding Author's Info
Email:
hosseinasadigorji@gmail.com

Keywords:
Digital currency, Blockchain technology, SWIFT system, Economic sanctions, Decentralized banking.

ABSTRACT

The global financial system and the SWIFT network have increasingly become strategic tools for the United States to impose and monitor economic sanctions against nations such as Iran. Following the September 11 attacks, the US gained covert access to SWIFT transaction data, transforming this network into the primary, lowest-cost mechanism for detecting sanctions violations. While global powers like China and Russia are actively developing alternative financial messaging systems to mitigate these risks, Iran has yet to implement an effective strategy to bypass this critical vulnerability. This study aims to elucidate the necessity of replacing the SWIFT system with blockchain technology and digital currencies. Employing a descriptive-analytical methodology, the research examines SWIFT's structural vulnerabilities to US surveillance and evaluates the robust security mechanisms inherent in blockchain and cryptocurrencies. The findings indicate that digital currencies, characterized by their decentralized nature, transparency, high security, and elimination of political intermediaries, can establish a secure framework for Iran's international transactions. Furthermore, this technology inherently prevents foreign entities from monitoring financial flows while significantly reducing transaction costs. Consequently, the study concludes that to neutralize the impact of sanctions and mitigate systemic financial risks, the Central Bank of Iran must urgently design and deploy a national blockchain-based digital currency. This strategic shift will preserve Iran's monetary sovereignty and successfully route international trade transactions away from US-monitored financial bottlenecks.

How to Cite This Article: Asadi Gorji, H. and Asadi H. (2025). The Imperative of Adopting Blockchain-Based Digital Currency as a Substitute for the SWIFT System. Management, Economics and Entrepreneurship Studies, 6(1): 1-11. Doi: 10.22034/jmek.2026.601929.1207

فصلنامه مطالعات مدیریت، اقتصاد و کارآفرینی
www.JMEK.ir

دوره ٦، شماره ١ ، بهار ١٤٠٤

لزوم استفاده از ارز دیجیتال با بهره‌گیری از فناوری بلاک‌چین به‌عنوان جایگزینی برای سوئیفت

حسین اسدی گرجی[1]* همایون اسدی[2]

۱. دانشجوی دکتری اقتصاد، دانشکده اقتصاد ، دانشگاه فردوسی، مشهد، ایران.

۲. دکتری کارآفرینی، دانشکده مدیریت، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۱-۱

اطلاعات نویسنده مسئول

ایمیل:

hosseinasadigorji@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۳/۰۹/۱۵

تاریخ ویرایش: ۱۴۰۳/۱۱/۰۳

تاریخ پذیرش: ۱۴۰۳/۱۲/۱۰

تاریخ انتشار: ۱۴۰۴/۰۱/۰۱

واژگان کلیدی:

ارز دیجیتال، فناوری بلاک‌چین، سیستم سوئیفت، تحریم‌های اقتصادی، بانکداری غیرمتمرکز.

چکیده

نظام مالی جهانی و سیستم سوئیفت به یکی از ابزارهای راهبردی ایالات متحده برای اعمال و رصد تحریم‌های اقتصادی علیه کشورهایی نظیر ایران تبدیل شده است. پس از حوادث ۱۱ سپتامبر، دسترسی پنهانی آمریکا به اطلاعات تراکنش‌های مالی سوئیفت، این شبکه را به اصلی‌ترین و کم‌هزینه‌ترین ابزار کشف نقض تحریم‌ها بدل کرده است. در حالی که قدرت‌هایی مانند چین و روسیه به دنبال راه‌اندازی پیام‌رسان‌های مالی جایگزین هستند، ایران هنوز تدبیر مؤثری برای دور زدن این وابستگی خطرناک نیاندیشیده است. هدف از پژوهش حاضر، تبیین ضرورت جایگزینی سیستم سوئیفت با فناوری بلاک‌چین و ارزهای دیجیتال است. روش تحقیق در این مقاله، توصیفی-تحلیلی است که با بررسی ساختار سوئیفت، آسیب‌پذیری‌های آن در برابر نظارت آمریکا، و سپس تشریح مکانیزم‌های امنیتی بلاک‌چین و ارزهای رمزنگاری‌شده انجام شده است. یافته‌ها نشان می‌دهد که ارزهای دیجیتال به دلیل ماهیت غیرمتمرکز، شفافیت، امنیت بالا و حذف واسطه‌های سیاسی، می‌توانند بستری امن برای مبادلات بین‌المللی ایران فراهم کنند. همچنین این فناوری امکان رصد مبادلات را از نهادهای خارجی سلب می‌کند و هزینه‌های مبادلاتی را به شدت کاهش می‌دهد. در نهایت، این پژوهش نتیجه می‌گیرد که برای خنثی‌سازی تحریم‌ها و کاهش ریسک‌های سیستمی، بانک مرکزی ایران باید هرچه سریع‌تر نسبت به طراحی و انتشار ارز دیجیتال ملی مبتنی بر بلاک‌چین اقدام نماید تا ضمن حفظ حق حاکمیت پولی، مبادلات تجاری را از گلوگاه‌های تحت نظارت آمریکا خارج سازد.

۱- مقدمه

سوءاستفاده از اطلاعات مالی شبکه سوئیفت توسط ایالات متحده آمریکا، تقریباً تمامی کشورهای جهان را به فکر یافتن جایگزینی مطمئن برای این سامانه انداخته است. در دوران اعمال تحریم‌های ظالمانه غرب علیه جمهوری اسلامی ایران، آمریکا با قطع اتصال بانک‌های ایرانی به شبکه سوئیفت، عملاً اجازه تبادل پیام‌های مالی را از ایران سلب نمود. در سال ۲۰۱۲، تنها راه دریافت درآمدهای نفتی ایران، حواله‌های بانکی سنتی بود، اما تعداد بسیار کمی از بانک‌ها حاضر به همکاری در این چارچوب بودند. اگرچه برخی از بانک‌های محروم از خدمات سوئیفت توانستند با اجاره خطوط تلفن و دورنگار از همتایان خود در کشورهایی مانند امارات، ترکیه و چین به انتقال پول بپردازند یا از بانک‌های تحریم‌نشده ایرانی به‌عنوان واسطه استفاده کنند، اما این فرآیند با کندی شدید و هزینه‌های گزاف انجام می‌شد. درواقع، این وابستگی باعث شد درآمدهای نفتی ایران از ۹۲.۵ میلیارد دلار در سال ۲۰۱۱ به ۵۲ میلیارد دلار در سال ۲۰۱۲ سقوط کند و این افت درآمد تا سال تصویب برجام نیز ادامه یافت.

کاربرد اصلی سوئیفت برای بانک‌ها به این گونه است که در مبادلات بین‌المللی و حتی داخلی، پیام‌های دستوری برای جابه‌جایی پول بین حساب‌های مختلف از طریق این پیام‌رسان ارسال می‌شود. ازآنجاکه برای ارسال این دستورات باید اطلاعات و جزئیات کامل مبادلات ثبت شود، این پیام‌ها هم قابل‌ارائه به مراجع قضایی داخلی و بین‌المللی هستند و هم حاوی اطلاعات دقیق نقل‌وانتقال، دارنده حساب‌های مبدأ و مقصد و دلیل جابه‌جایی می‌باشند. سوئیفت دارای دو سرور اصلی است؛ یکی در اروپا و دیگری در آمریکا، که اطلاعات نقل‌وانتقالات پولی تمام بانک‌های متصل در هر دوی این سرورها ثبت می‌شود. پس از افشای این مسئله و موضع‌گیری شدید کشورهای اروپایی، مقرر شد اطلاعات تراکنش‌های مالی اشخاص و شرکت‌های اروپایی به‌جز موارد خاص، دیگر در اختیار آمریکا قرار نگیرد؛ اما واشنگتن همچنان به اطلاعات سوئیفت سایر اشخاص و بانک‌ها در کشورهای غیراروپایی جهان، نظیر تمام کشورهای آسیایی، دسترسی کامل دارد. آمریکا از محل جریمه شرکت‌ها و مؤسسات مالی به دلیل همکاری با کشورهای تحریم‌شده و به‌خصوص ایران، تاکنون حدود ۱۵ میلیارد دلار درآمد کسب کرده است.

بنابراین، سوئیفت به پاشنه آشیل متقاعد کردن شرکت‌های خارجی برای ادامه حضور در ایران و یا ادامه صادرات نفت و دریافت وجوه ارزی تبدیل شده است، چراکه تمام اطلاعات ثبت‌شده در آن در اختیار آمریکا قرار گرفته و از این داده‌ها برای جریمه بانک‌ها و شرکت‌ها استفاده می‌کند. متأسفانه در دوره‌ای حتی بانک‌های داخلی نیز برای انتقال پیام بین‌بانکی میان خود از سوئیفت استفاده کرده‌اند که این امر دسترسی سازمان سیا و وزارت خزانه‌داری آمریکا به این اطلاعات را در کنار اطلاعات مبادلات خارجی، تسهیل نموده است. لذا باید توجه داشت حتی اگر آمریکا از برجام خارج نمی‌شد، تکیه بر سوئیفت برای مخابره پیام‌های مالی همچنان مانعی بزرگ در برابر تجارت خارجی ایران بود و حرکت به سمت ایجاد یک سامانه پیام‌رسان موازی یک ضرورت اجتناب‌ناپذیر محسوب می‌شد.

مسئله دیگری که در دنیای مالی امروزه مطرح است، بحران اعتماد به سیستم‌های مالی متمرکز می‌باشد. در سال ۲۰۰۸، اقتصاد جهان دچار سقوط شد و بانک‌ها پولی را که با اعتماد مردم در اختیارشان قرار داشت، به‌صورت بسیار نامناسبی مدیریت کردند. در همان سال، بیت‌کوین در حال ایجاد شدن بود تا قدرتی را که بانک‌ها و دولت‌ها بر زندگی مردم دارند، حذف کرده و به افراد بازگرداند. امروزه گسترش مقبولیت ارزهای دیجیتالی، نفوذ فناوری در عرصه خدمات مالی و بروز فناوری‌های جدید زیرساختی مانند بلاک‌چین، در کنار پیشرفت در هوش مصنوعی و کلان‌داده‌ها، بانک‌های مرکزی را به گذر از پول اعتباری به پول دیجیتالی ترغیب می‌کند. در این مقاله، ابتدا به بررسی پرمصرف‌ترین سیستم پیام‌رسان مالی یعنی

سوئیفت، مزایا و معایب آن پرداخته و سپس به تشریح فناوری بلاک‌چین و نخستین پول دیجیتال غیرمتمرکز، یعنی بیت‌کوین، به‌عنوان جایگزینی راهبردی خواهیم پرداخت.

۲. چارچوب نظری و پیشینه تحقیق

نظام مالی جهانی برای تسهیل مبادلات بین‌المللی، دهه‌ها به سیستم‌های پیام‌رسان متمرکز متکی بوده است. سوئیفت (SWIFT) که در سال ۱۹۷۳ در بلژیک تأسیس شد، به‌عنوان یک مؤسسه تعاونی غیرانتفاعی، استاندارد اصلی ارتباطات مالی بین بیش از ۹۷۰۰ مؤسسه مالی در ۲۰۹ کشور جهان است. این سیستم با ارائه خدمات شبانه‌روزی، سرعت بالا و قابلیت اطمینان ۹۹/۹۹ درصدی، پیام‌های دستوری جابه‌جایی پول را با استفاده از کدهای شناسایی بانک (BIC) مخابره می‌کند. بااین‌حال، ماهیت متمرکز سوئیفت و ذخیره‌سازی پیام‌ها در سرورهای واقع در اروپا و آمریکا، آن را در معرض دسترسی نهادهای اطلاعاتی و سیاسی قرار داده است. این آسیب‌پذیری ساختاری، سوئیفت را از یک ابزار فنی صرف، به ابزاری راهبردی برای اعمال و رصد تحریم‌های اقتصادی تبدیل کرده است که دور زدن آن از طریق روش‌های متعارف بانکی با هزینه‌های گزاف و ریسک‌های بالا همراه است.

در مقابل این پارادایم متمرکز، فناوری بلاک‌چین (Blockchain) به‌عنوان یک دفتر کل توزیع‌شده و غیرمتمرکز، الگوی جدیدی را ارائه می‌دهد. بلاک‌چین شبکه‌ای است که تحت پروتکل‌های اینترنت عمل می‌کند، اما برخلاف اینترنت که با داده‌های نفوذپذیر سروکار دارد، بر پایه مقادیر رمزگذاری‌شده‌ای استوار است که تراکنش‌های مالی را به‌صورت تغییرناپذیر ذخیره می‌کنند. در این ساختار، هر تراکنش ابتدا توسط توابع درهم‌سازی (Hash Functions) به کدهای یکتا تبدیل می‌شود. این کدها برای تضمین امنیت، از سه آزمون مقاومت‌سنجی عبور می‌کنند: مقاومت پیشا تصادم (سنجش سختی تولید هش)، مقاومت در برابر تصادم ضعیف (بررسی برابری هش با هش‌های دیگر) و مقاومت در برابر تصادم قوی (بررسی هم‌زمان دو تراکنش مشابه برای جلوگیری از خرج مضاعف). پس از تأیید، این هش‌ها در ساختاری سلسله‌مراتبی به نام «درخت مرکل» (Merkle Tree) ترکیب شده و به زنجیره بلوک‌های قبلی افزوده می‌شوند. این مکانیزم، هرگونه دستکاری در داده‌های گذشته را از نظر محاسباتی غیرممکن می‌سازد.

ارزهای رمزنگاری‌شده (Cryptocurrencies) مانند بیت‌کوین، تجلی عملی این فناوری هستند. این ارزها که فاقد پشتوانه فیزیکی یا کنترل متمرکز دولتی هستند، با تکیه بر الگوریتم‌های ریاضی و مکانیزم اجماع (مانند استخراج یا Mining)، اعتماد را نه از طریق نهادها، بلکه از طریق شفافیت و رمزنگاری تأمین می‌کنند. ویژگی‌هایی نظیر حذف واسطه‌های مالی، کاهش هزینه‌های مبادله، سرعت انتقال چندثانیه‌ای و عدم وابستگی به نظام ارزی رایج، بلاک‌چین را به نامزدی ایده‌آل برای جایگزینی سوئیفت در مبادلات بین‌المللی کشورهای تحت تحریم تبدیل می‌کند. با وجود این مزایا، مبانی نظری حاکی از آن است که ارزهای رمزنگاری‌شده با چالش‌هایی نظیر نوسانات قیمتی، کثرت تهدیدات سایبری (مانند باج‌افزارها، کیف‌پول‌های تقلبی و کلاه‌برداری‌های ICO) و فقدان چارچوب حقوقی مدون در بسیاری از کشورها مواجه هستند. این معایب، ضرورت طراحی ارز دیجیتال بانک مرکزی (CBDC) را به‌عنوان راهکاری میانه که هم از مزایای بلاک‌چین بهره‌مند باشد و هم نظارت کلان اقتصادی را حفظ کند، دوچندان می‌سازد.

مرور ادبیات پژوهش نشان می‌دهد که گذار از پول اعتباری به پول دیجیتال و الکترونیکی، موضوعی است که از دهه‌های گذشته مورد توجه محققان حوزه اقتصاد و فناوری اطلاعات قرار گرفته است. در داخل کشور، ذوالفقاری (۱۳۹۰) به تبیین

مفاهیم اولیه پول الکترونیکی و زیرساخت‌های آن پرداخت. کیهانی راست‌گو و همکاران (۱۳۹۲) تجارت و پول الکترونیک در ایران را بررسی کرده و چالش‌های پیاده‌سازی آن را تبیین نمودند. شمسایی (۱۳۸۴) و جانو سپاه و عشوریان (۱۳۸۷) نیز به ارائه روش‌های امن برای سیستم‌های پرداخت سکه الکترونیکی و پیاده‌سازی نرم‌افزاری سیستم‌های پول دیجیتال مبتنی بر برندهای معتبر پرداخته‌اند. نصیری احمدآبادی (۱۳۸۷) نیز تأثیر پول و بانکداری الکترونیکی بر اقتصاد کلان را مورد واکاوی قرار داد و دعایی (۱۳۹۳) بیت‌کوین را به‌عنوان نخستین پول مجازی موفق در فضای اقتصادی ایران معرفی کرد.

در سطح بین‌المللی، ریشه‌های نظری بلاک‌چین به پژوهش‌های هابر و استورنتا (۱۹۹۱) بازمی‌گردد که شبکه‌ای برای ثبت زمان‌گذاری اسناد دیجیتال با امضای الکترونیکی غیرقابل نفوذ را معرفی کردند. متعاقباً، دای (۱۹۹۸) با معرفی مفهوم b-money، ایده پول الکترونیکی غیرمتمرکز را پیش برد. نقطه عطف این تحولات، انتشار مقاله ساتوشی ناکاموتو (۲۰۰۸) با عنوان «بیت‌کوین: یک سیستم پول الکترونیکی همتا به همتا» بود که مکانیزم اجماع را برای حل مشکل اعتماد در شبکه‌های غیرمتمرکز ارائه داد. گو و چو (۲۰۰۸) تحلیل پدیده‌شناختی سیستم‌های پول مجازی، نشان دادند که این سیستم‌ها پتانسیل ایجاد ساختارهای مالی جدید خارج از کنترل متمرکز دولتی را دارند. راسکین (۲۰۱۳) نیز در بررسی موردی میلیونرهای بیت‌کوین، به رشد سریع و جذب سرمایه در این اکوسیستم جدید اشاره کرد. جری بریتو (۲۰۱۱) نیز تأکید کرد که بیت‌کوین به‌عنوان پول نقد آنلاین، پتانسیل به چالش کشیدن انحصار دولت‌ها و بانک‌ها را دارد. از سوی دیگر، بومه و همکاران (۲۰۱۵) در مقاله جامع خود با عنوان «بیت‌کوین: اقتصاد، فناوری و حکمرانی»، ابعاد فنی و اقتصادی این ارز را واکاوی کرده و چالش‌های نظارتی و نوسانات قیمتی آن را به‌عنوان موانع اصلی پذیرش گسترده شناسایی نمودند. جان کلهر (۲۰۱۴) نیز فرآیند استخراج بیت‌کوین و مصرف انرژی آن را به‌عنوان یکی از جنبه‌های مهم فنی این سیستم تشریح کرد.

بااین‌حال، مرور پیشینه نشان می‌دهد که اکثر پژوهش‌های انجام‌شده، یا بر جنبه‌های فنی و الگوریتمی بلاک‌چین متمرکز بوده‌اند یا به بررسی کلیات اقتصادی ارزهای دیجیتال پرداخته‌اند. شکاف پژوهشی موجود، عدم تمرکز کافی بر کاربرد راهبردی و عملیاتی ارزهای دیجیتال و فناوری بلاک‌چین به‌عنوان یک جایگزین ساختاری برای سیستم سوئیفت، به‌ویژه در شرایط تحریمی کشورهایی مانند ایران، است. این پژوهش با پر کردن این شکاف، به تبیین ضرورت و مکانیزم این جایگزینی می‌پردازد.

۳. روش تحقیق

پژوهش حاضر از نظر هدف، در زمره پژوهش‌های کاربردی قرار می‌گیرد، زیرا به دنبال ارائه راهکارهای عملی برای حل یک چالش واقعی در نظام مالی کشور، یعنی وابستگی آسیب‌زا به سیستم سوئیفت و تأثیر تحریم‌های اقتصادی است. از نظر ماهیت و روش، این مطالعه توصیفی-تحلیلی است. در این راستا، برای دستیابی به اهداف پژوهش که همانا تبیین ضرورت جایگزینی سیستم سوئیفت با فناوری بلاک‌چین و ارزهای دیجیتال در شرایط تحریمی است، از روش گردآوری داده‌ها به شیوه کتابخانه‌ای و اسنادی استفاده شده است. انتخاب این روش به آن دلیل است که موضوع پژوهش نیازمند بررسی عمیق مفاهیم نظری، ساختارهای فنی پیچیده و سوابق تاریخی سیستم‌های مالی جهانی و فناوری‌های نوین است. بهترین راه دسترسی به این دانش، مطالعه دقیق اسناد، مقالات علمی-پژوهشی، گزارش‌های تحلیلی مؤسسات مالی بین‌المللی و منابع معتبر دیجیتال می‌باشد.

قلمرو موضوعی این پژوهش، بررسی تطبیقی سیستم پیام‌رسان مالی سوئیفت و فناوری بلاک‌چین با تمرکز ویژه بر ارزهای رمزنگاری‌شده (به‌ویژه بیت‌کوین) و ارز دیجیتال بانک مرکزی به‌عنوان جایگزینی راهبردی و امن است. قلمرو زمانی پژوهش، بازه‌ای از تاریخ تأسیس سوئیفت در دهه ۱۹۷۰ میلادی و حادثه

۱۱ سپتامبر (که نقطه عطف دسترسی آمریکا به داده‌ها شد) تا تحولات اخیر در حوزه فناوری‌های مالی غیرمتمرکز و ظهور ارزهای دیجیتال را در بر می‌گیرد. قلمرو مکانی نیز با تمرکز بر نظام مالی جهانی و به‌طور ویژه، چالش‌های نظام بانکی جمهوری اسلامی ایران در مواجهه با تحریم‌های یک‌جانبه آمریکا و وابستگی به زیرساخت‌های متمرکز مالی تدوین و محدود شده است.

برای گردآوری اطلاعات و داده‌های مورد نیاز، از منابع دست‌اول و دست‌دوم معتبر و متنوع استفاده شده است. این منابع شامل کتاب‌های تخصصی در حوزه اقتصاد دیجیتال و رمزنگاری، مقالات علمی منتشرشده در نشریات داخلی و خارجی، گزارش‌های تحلیلی نهادهای مالی، اسناد تاریخی مرتبط با نحوه عملکرد سوئیفت و دسترسی نهادهای اطلاعاتی آمریکا به داده‌های آن، و همچنین مستندات فنی منتشرشده توسط توسعه‌دهندگان فناوری بلاک‌چین (مانند مقاله بنیادین ساتوشی ناکاموتو در مورد بیت‌کوین) می‌باشد. در این فرآیند، تلاش شده است تا با غربالگری دقیق و نقادانه منابع، از اعتبار و روایی داده‌ها اطمینان حاصل شود و تنها از اطلاعاتی استفاده گردد که از نظر علمی و فنی مورد تأیید جامعه دانشگاهی و متخصصان این حوزه باشند.

پس از گردآوری داده‌ها، از روش تحلیل محتوای کیفی و مطالعه تطبیقی برای پردازش اطلاعات استفاده شده است. در این مرحله، مؤلفه‌های کلیدی سیستم سوئیفت (شامل ساختار متمرکز، هزینه‌های بالای مبادله، زمان‌بر بودن انتقال، و میزان آسیب‌پذیری در برابر نظارت‌های سیاسی و جریمه‌های دلاری) با ویژگی‌های ذاتی فناوری بلاک‌چین (شامل غیرمتمرکز بودن، شفافیت، امنیت رمزنگاری‌شده از طریق توابع درهم‌سازی و درخت مرکل، و حذف واسطه‌ها) مورد مقایسه دقیق قرار گرفته‌اند. این تحلیل تطبیقی به پژوهشگر این امکان را می‌دهد تا نقاط قوت و ضعف هر یک از دو سیستم را به‌طور عینی شناسایی کرده و بر اساس آن، امکان‌سنجی فنی و اقتصادی جایگزینی سوئیفت با شبکه‌های مبتنی بر بلاک‌چین را ارزیابی نماید. همچنین، برای تحلیل داده‌ها از رویکرد استنتاجی استفاده شده است؛ بدین معنا که با تکیه بر مبانی نظری موجود در مورد ماهیت پول، اعتماد در سیستم‌های مالی و مکانیزم‌های رمزنگاری، به نتایج کلی در مورد ضرورت گذار از پول اعتباری متمرکز به پول دیجیتال غیرمتمرکز یا نیمه‌متمرکز (ارز دیجیتال بانک مرکزی) دست یافته‌ایم.

مراحل اجرای پژوهش:

فرآیند انجام این پژوهش در چند مرحله نظام‌مند و پیوسته صورت گرفته است:

۱. تبیین مسئله و شناسایی شکاف پژوهشی: در گام نخست، با بررسی وضعیت تحریم‌های مالی علیه ایران و نقش ابزاری سوئیفت در تشدید این تحریم‌ها (مانند افت درآمدهای نفتی از ۹۲/۵ به ۵۲ میلیارد دلار در سال ۲۰۱۲)، ضرورت یافتن یک جایگزین مطمئن و غیرقابل‌ردیابی توسط نهادهای خارجی مورد تأکید قرار گرفت.

۲. مطالعه و آسیب‌شناسی سیستم سوئیفت: در این مرحله، تاریخچه، ساختار فنی، مزایا (مانند استاندارد بودن و قابلیت اطمینان ۹۹/۹۹ درصدی) و معایب حیاتی سوئیفت (به‌ویژه تمرکزگرایی و دسترسی آسان آمریکا به داده‌های تراکنش‌ها و کسب درآمد ۱۵ میلیارد دلاری از جریمه‌ها) به‌طور دقیق واکاوی شد.

۳. تبیین مبانی نظری فناوری بلاک‌چین و ارزهای دیجیتال: در گام سوم، مکانیزم‌های فنی بلاک‌چین، از جمله توابع درهم‌سازی (Hash Functions)، درخت مرکل، آزمون‌های سه‌گانه مقاومت‌سنجی (پیشا تصادم، تصادم ضعیف و تصادم قوی) و فرآیند استخراج و اعتبارسنجی تراکنش‌ها در بازه زمانی ۱۰ دقیقه‌ای، به‌زبان علمی تشریح گردید تا پایه‌های فنی جایگزینی پیشنهادی مستحکم شود.

٤. تحلیل تطبیقی و امکان‌سنجی: در این مرحله، داده‌های حاصل از بررسی سوئیفت و بلاک‌چین در کنار یکدیگر قرار گرفتند تا مشخص شود که چگونه ویژگی‌هایی مانند حذف واسطه‌های سیاسی، کاهش هزینه‌های مبادله، افزایش سرعت

تراکنش‌ها به چند ثانیه، و غیرقابل‌دسترس بودن داده‌ها برای نهادهای نظارتی خارجی، بلاک‌چین را به گزینه‌ای برتر برای دور زدن تحریم‌ها تبدیل می‌کند.

۵. نتیجه‌گیری و ارائه راهکارهای سیاستی: در نهایت، با جمع‌بندی یافته‌ها و با در نظر گرفتن معایب احتمالی ارزهای دیجیتال (مانند نوسانات قیمتی، کثرت تهدیدات سایبری و چالش‌های نظارتی)، راهکارهای عملیاتی برای بانک مرکزی جمهوری اسلامی ایران جهت طراحی و پیاده‌سازی ارز دیجیتال ملی (CBDC) مبتنی بر بلاک‌چین ارائه شده است.

این ساختار روش‌شناسی تضمین می‌کند که پژوهش حاضر از پشتوانه علمی و فنی کافی برخوردار بوده و نتایج آن نه بر اساس حدسیات، بلکه بر پایه تحلیل دقیق داده‌های مستند و مقایسه نظام‌مند پارادایم‌های مالی قدیم و جدید استوار است.

٤. یافته‌ها

یافته‌های پژوهش حاضر بر اساس تحلیل محتوای اسناد، بررسی‌های کتابخانه‌ای و مطالعه تطبیقی سیستم سوئیفت و فناوری بلاک‌چین، در چند محور اصلی و به‌هم‌پیوسته قابل دسته‌بندی است که ضرورت، امکان‌سنجی و چالش‌های جایگزینی را به‌طور جامع تبیین می‌کند.

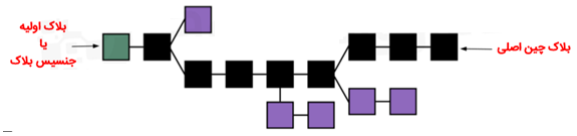
یافته‌های مربوط به آسیب‌شناسی ساختاری و عملکردی سوئیفت: بررسی‌های عمیق نشان می‌دهد که سوئیفت علیرغم ادعای استاندارد بودن، قابلیت اطمینان ۹۹/۹۹ درصدی و ارائه خدمات شبانه‌روزی، دارای یک نقطه ضعف ساختاری بنیادین و اجتناب‌ناپذیر است: تمرکزگرایی. این سیستم دارای سرورهای مرکزی (در اروپا و آمریکا) است که تمامی پیام‌های دستوری و جزئیات مبادلاتی بانک‌های عضو در آن‌ها ذخیره و بایگانی می‌شود. این ویژگی ذاتی باعث شده است که داده‌های مالی حساس کشورها به‌سادگی و با کمترین هزینه در دسترس نهادهای اطلاعاتی و سیاسی ایالات متحده قرار گیرد. یافته‌ها حاکی از آن است که آمریکا از این دسترسی نامتقارن برای رصد دقیق مبادلات کشورهای تحریم‌شده و اعمال جریمه‌های سنگین مالی (با درآمدی حدود ۱۵ میلیارد دلار تاکنون) استفاده کرده است. علاوه بر این، فرآیند انتقال وجه از طریق سوئیفت به‌دلیل نیاز به بانک‌های واسطه متعدد، زمان‌بر (۲ تا ۳ روز کاری) و پرهزینه (کارمزد ۲۰ تا ۶۰ دلار به علاوه هزینه‌های پنهان تبدیل ارز) است که کارایی مبادلات بین‌المللی را به‌شدت کاهش می‌دهد و پاشنه آشیل تجارت خارجی کشورهایی مانند ایران محسوب می‌شود.

یافته‌های مربوط به مکانیزم فنی و لایه‌های امنیتی بلاک‌چین: تحلیل فنی نشان می‌دهد که فناوری بلاک‌چین به‌عنوان یک دفتر کل توزیع‌شده و غیرمتمرکز، الگویی کاملاً متفاوت و انقلابی از سیستم‌های متمرکز ارائه می‌دهد. در این شبکه، تراکنش‌ها از طریق توابع درهم‌سازی (Hash Functions) به کدهای یکتا، طولانی و غیرقابل‌بازگشت تبدیل می‌شوند. برای تضمین امنیت مطلق این کدها، یافته‌ها تأیید می‌کنند که تابع رمزنگاری هش باید از سه آزمون مقاومت‌سنجی پیچیده عبور کند: نخست، «مقاومت پیشا تصادم» که سختی لازم و زمان محاسباتی برای تولید یک هش خاص را می‌سنجد؛ دوم، «مقاومت در برابر تصادم ضعیف» که احتمال برابری یک هش جدید با هش‌های از پیش موجود را بررسی و رد می‌کند؛ و سوم، «مقاومت در برابر تصادم قوی» که احتمال ثبت هم‌زمان دو تراکنش مشابه (مانند تلاش هکرها برای خرج مضاعف) را به صفر می‌رساند. پس از تأیید نهایی، این هش‌ها در ساختاری سلسله‌مراتبی و درختی به نام «درخت مرکل» (Merkle Tree) با یکدیگر ترکیب می‌شوند تا بلوک جدیدی را تشکیل دهند. این بلوک جدید با ارجاع به هش بلوک قبلی، به زنجیره متصل می‌شود، به‌طوری‌که هرگونه تغییر، حتی در یک بیت از داده‌های گذشته، کل زنجیره را نامعتبر می‌سازد و هک کردن یا دستکاری شبکه را از نظر محاسباتی و ریاضیاتی تقریباً غیرممکن می‌کند.

یافته‌های مربوط به مزایا و معایب راهبردی ارزهای رمزنگاری‌شده: یافته‌های پژوهش نشان می‌دهد که ارزهای

رمزنگاری‌شده مزایای راهبردی و کلان‌اقتصادی متعددی دارند. نخست، کاهش چشمگیر هزینه‌ها و کارمزدهای خدمات بانکی و حذف واسطه‌های مالی، که منجر به کاهش خلق پول از کانال بانک‌های سنتی می‌شود. دوم، شفافیت کامل؛ به‌طوری‌که هر کاربر می‌تواند تمامی تراکنش‌های انجام‌شده در شبکه را مشاهده و راستی‌آزمایی کند، بدون آنکه نیازی به اعتماد کورکورانه به شخص ثالث یا نهاد مرکزی باشد. سوم، دسترسی جهانی و فراگیر؛ این شبکه‌ها پذیرای تمام افراد، از جمله حدود دو میلیارد نفری هستند که به دلایل مختلف از خدمات بانکی سنتی محروم‌اند. چهارم، خودتنظیمی هوشمند بازار از طریق الگوریتم‌های پیچیده ریاضیاتی و عدم وجود ضریب فزاینده پولی، که در بانکداری سنتی در مواقع بحران، وضعیت تورمی را وخیم‌تر می‌کند. پنجم، استقلال از نظام ارزی رایج؛ به‌طوری‌که واحد پولی پرداخت‌کننده اهمیتی ندارد و این ویژگی، ارزهای دیجیتال را به پناهگاهی امن و ذخیره‌ای باارزش برای کشورهای با اقتصاد بی‌ثبات یا تحت تحریم تبدیل می‌کند. با این حال، یافته‌ها معایب و چالش‌های جدی این فناوری را نیز به‌وضوح شناسایی کرده‌اند: ناپایداری و نوسانات قیمتی شدید، جذابیت ذاتی برای مجرمان و تروریست‌ها به دلیل ماهیت شبه‌گمنام، کثرت تهدیدات سایبری نوین، و فقدان چارچوب حقوقی و نظارتی مدون بین‌المللی. این معایب باعث شده است که برخی کشورها رویکردی سلبی اتخاذ کرده و تجارت این ارزها را غیرقانونی اعلام کنند، زیرا در صورت عدم کنترل و نظارت مؤثر، می‌تواند ثبات مالی و حاکمیت پولی کشورها را به‌شدت تهدید نماید.

یافته‌های مربوط به برتری بلاک‌چین به‌عنوان جایگزین سوئیفت: مطالعه تطبیقی به‌دست‌آمده نشان می‌دهد که بلاک‌چین در مقایسه با سوئیفت، از برتری‌های انکارناپذیری برخوردار است. در حالی که دور زدن تحریم‌ها از طریق روش‌های متعارف و پرهزینه (مانند تأسیس شرکت‌های صوری، استفاده از پرچم کشورهای ثالث، یا مبادلات پیچیده پایاپای) همواره با ریسک‌های بالا همراه است، بلاک‌چین بستری رایگان از حیث عدم سوءاستفاده از داده‌ها و کاملاً مصون از تحریم‌های سیاسی فراهم می‌کند. استفاده از ارزهای دیجیتال امکان انتقال مستقل، مستقیم و با سرعت چند ثانیه‌ای را فراهم می‌آورد و زیان ناشی از نوسانات نرخ ارز و کارمزدهای مکرر بانک‌های واسطه را به‌طور کامل حذف می‌کند. مهم‌تر آنکه، با به‌کارگیری این فناوری، اطلاعات حساس بانک‌های ایرانی در اختیار شخص ثالث (آمریکا) قرار نمی‌گیرد و بانک‌های متوسط اروپایی می‌توانند بدون هراس از جریمه‌های سنگین وزارت خزانه‌داری آمریکا، با ایران تبادل مالی داشته باشند. این مکانیزم نوین، عملاً فرآیند بانکی جهانی را که دهه‌ها تحت مدیریت و انحصار سیستم فدرال رزرو آمریکا بوده است، دور می‌زند.



شکل ۱- نحوه شکل‌گیری زنجیره اصلی و بلاک‌های جانبی در بلاک‌چین

یافته‌های مربوط به بیت‌کوین و چالش‌های امنیتی لایه کاربردی: بررسی موردی بیت‌کوین به‌عنوان شاخص‌ترین و نخستین ارز دیجیتال غیرمتمرکز، نشان می‌دهد که این سیستم با ترکیب هوشمندانه دو اصل «اعتماد» (از طریق امنیت شدید رمزنگاری و شفافیت شبکه) و «کمیابی» (با سقف عرضه ثابت ۲۱ میلیون واحد)، توانسته است رقیبی جدی و پایدار برای سیستم بانکی رایج شود. یافته‌ها علل اصلی افزایش قیمت و مقبولیت روزافزون آن را شامل فشار تقاضا ناشی از عرضه محدود، به رسمیت شناختن قانونی توسط کشورهایی مانند ژاپن و اتحادیه اروپا، گسترش دایره استفاده جهانی، ورود فعالان بازارهای موازی به دلیل بن‌بست‌های تحریمی، و کاهش شدید اعتماد عمومی به دولت‌ها و بانک‌های مرکزی

(تا ۵۵ درصد طبق نظرسنجی ادلمن در ۲۰۱۷) عنوان می‌کنند. با این وجود، تحلیل داده‌ها ۱۵ روش عمده و رایج سرقت بیت‌کوین را شناسایی کرده است که موانع امنیتی مهمی در لایه کاربردی محسوب می‌شوند. این روش‌ها عبارتند از: باج‌افزارها، کیف‌پول‌های تقلبی، کلاه‌برداری شرکت‌های عرضه اولیه سکه (ICO)، هک کردن استخرهای استخراج (Mining)، کپی کردن کلیدهای خصوصی، کلاه‌برداری ایمیلی، سرقت گذرواژه‌های ایمیل، وب‌سایت‌های تقلبی، کازینوهای بیت‌کوین تقلبی، طرح‌های هرمی، ارزهای رمزی تقلبی (مانند OneCoin)، سرقت از فروشگاه‌های آنلاین، ضعف امنیتی توسعه‌دهندگان، کلاه‌برداری در تبادلات همتا به همتا (P2P)، و کلاه‌برداری از طریق خودپردازهای بیت‌کوین. این یافته‌ها به‌وضوح نشان می‌دهد که اگرچه زیرساخت ذاتی بلاک‌چین از امنیت ریاضیاتی بالایی برخوردار است، اما لایه‌های کاربردی، نرم‌افزاری و رفتاری کاربران همچنان در معرض تهدیدات سایبری جدی و نیازمند ارتقای سواد دیجیتال قرار دارند.

۵. بحث و نتیجه‌گیری

پژوهش حاضر با هدف تبیین ضرورت گذار از سیستم متمرکز سوئیفت به فناوری غیرمتمرکز بلاک‌چین و ارزهای دیجیتال، به‌منظور خنثی‌سازی تحریم‌های اقتصادی علیه ایران انجام شد. یافته‌های تحقیق به‌وضوح نشان داد که سوئیفت، علیرغم ارائه خدمات استاندارد و قابلیت اطمینان بالا، به دلیل تمرکز سرورها و دسترسی نامتقارن نهادهای اطلاعاتی آمریکا به داده‌های تراکنش‌ها، از یک ابزار فنی صرف به یک سلاح راهبردی برای اعمال تحریم‌های ثانویه تبدیل شده است. این وابستگی ساختاری، پاشنه آشیل تجارت خارجی و درآمدهای ارزی کشور محسوب می‌شود و هزینه‌های مبادلاتی و ریسک‌های مسدودسازی دارایی‌ها را به‌شدت افزایش می‌دهد. در نقطه مقابل، فناوری بلاک‌چین با اتکا به دفتر کل توزیع‌شده، توابع درهم‌سازی و ساختار امنیتی درخت مرکل، الگویی انقلابی ارائه می‌دهد که در آن اعتماد از طریق ریاضیات و رمزنگاری تأمین می‌شود، نه نهادهای واسطه.

نتیجه‌گیری نهایی این پژوهش آن است که استراتژی‌های سنتی دور زدن تحریم‌ها (نظیر استفاده از صرافی‌ها، شرکت‌های صوری یا پیام‌رسان‌های مالی واسط) دیگر کارایی و پایداری لازم را ندارند. راهکار بنیادین و راهبردی برای جمهوری اسلامی ایران، حرکت شتابان به سمت طراحی، پیاده‌سازی و انتشار ارز دیجیتال بانک مرکزی (CBDC) مبتنی بر بومی‌سازی فناوری بلاک‌چین است. این گذار فناورانه، مزایای بی‌شماری از جمله حذف واسطه‌های سیاسی و بانکی، کاهش چشمگیر کارمزدها، افزایش سرعت انتقال وجه به چند ثانیه، و از همه مهم‌تر، سلب امکان رصد و رهگیری تراکنش‌ها توسط وزارت خزانه‌داری آمریکا را به همراه دارد. همچنین، این پژوهش تأیید می‌کند که ورود غول‌های فناوری و شبکه‌های اجتماعی به عرصه ارزهای دیجیتال می‌تواند کاتالیزوری قدرتمند برای مقبولیت عمومی این دارایی‌ها باشد. بنابراین، انفعال در این حوزه می‌تواند به انزوای بیشتر نظام بانکی کشور در اکوسیستم مالی نوظهور جهانی منجر شود. بااین‌حال، با توجه به چالش‌هایی نظیر نوسانات ذاتی ارزهای رمزی عمومی، تهدیدات سایبری در لایه کاربری و فقدان چارچوب‌های حقوقی بین‌المللی، ضروری است که ایران با الگوبرداری از تجربیات جهانی و تدوین مقررات دقیق داخلی، ضمن مدیریت ریسک‌های پولشویی، بستر پذیرش این فناوری نوین را در نظام اقتصادی کشور فراهم آورد تا حاکمیت پولی و استقلال مالی خود را در عرصه جهانی تثبیت نماید.

هر مطالعه علمی با محدودیت‌هایی مواجه است که می‌تواند بر دامنه تعمیم‌پذیری یافته‌ها تأثیر بگذارد. مهم‌ترین محدودیت این پژوهش، ماهیت کیفی و توصیفی–تحلیلی آن است که امکان آزمون‌های آماری، مدل‌سازی‌های اقتصادسنجی و شبیه‌سازی‌های کمی (مانند برآورد دقیق میزان صرفه‌جویی در هزینه‌های مبادلاتی در شبکه بلاک‌چین در مقایسه با سوئیفت)

را محدود ساخته است. محدودیت دوم، عدم دسترسی به داده‌های دقیق، محرمانه و دست‌اول از میزان خسارات وارده به اقتصاد ایران ناشی از نشت اطلاعات مالی در بستر سوئیفت و هزینه‌های پنهان دور زدن تحریم‌هاست؛ چراکه این اطلاعات به دلایل امنیتی و راهبردی توسط نهادهای ذی‌ربط منتشر نمی‌شوند.

علاوه بر این، سرعت خیره‌کننده تحولات در حوزه فناوری‌های مالی و ظهور مداوم پروتکل‌های جدید بلاک‌چینی، نسل دوم و سوم اینترنت ارزش، باعث می‌شود که برخی از یافته‌های فنی در بازه‌های زمانی کوتاه نیازمند بازنگری و به‌روزرسانی باشند. محدودیت دیگر، تمرکز مقاله بر ابعاد کلان اقتصادی و فنی بود که موجب شد روان‌شناسی رفتار مصرف‌کننده و میزان تمایل فعالان اقتصادی خرد و کلان داخلی به پذیرش و استفاده از ارزهای دیجیتال در مبادلات روزمره مورد غفلت واقع شود. در نهایت، فقر ادبیات پژوهشی بومی و مدل‌های عملیاتی موفق در زمینه طراحی ساختار ارز دیجیتال ملی در داخل کشور، از دیگر چالش‌های پیش روی محقق در تبیین دقیق الزامات اجرایی این جایگزینی بوده است.

با عنایت به یافته‌های این پژوهش و محدودیت‌های مطرح‌شده، مسیرهای زیر برای پژوهش‌های آتی پیشنهاد می‌گردد:

۱. انجام پژوهش‌های کمی و شبیه‌سازی: پیشنهاد می‌شود محققان آینده با استفاده از مدل‌سازی‌های ریاضی و شبیه‌سازی‌های شبکه‌ای، به مقایسه دقیق هزینه‌های مبادلاتی، سرعت پردازش، مصرف انرژی و مقیاس‌پذیری شبکه‌های مبتنی بر بلاک‌چین در مقایسه با سیستم سوئیفت در سناریوهای مختلف تجاری بپردازند.

۲. بررسی ابعاد حقوقی و فقهی: انجام مطالعات تطبیقی در زمینه تدوین چارچوب‌های رگولاتوری و بررسی تطابق ارزهای دیجیتال با موازین فقهی و حقوقی ایران، به‌منظور ارائه راهکارهایی برای مدیریت ریسک‌های پولشویی و فرار مالیاتی در بستر ارز دیجیتال ملی.

۳. مطالعات تطبیقی بین‌المللی: واکاوی عمیق تجربه کشورهای پیشرو و تحت تحریم (مانند یوان دیجیتال چین، روبل دیجیتال روسیه یا پترو ونزوئلا) در زمینه راه‌اندازی ارز دیجیتال بانک مرکزی و استخراج الگوهای بومی‌سازی‌شده و قابل‌اجرا برای نظام بانکی و تجاری ایران.

۴. ارتقای امنیت لایه کاربری: تحقیق در زمینه توسعه پروتکل‌های امنیتی نوین، طراحی کیف پول‌های سخت‌افزاری بومی و راهکارهای ارتقای سواد سایبری کاربران برای مقابله با تهدیدات لایه کاربری (مانند فیشینگ، کیف پول‌های تقلبی و باج‌افزارها) که از مهم‌ترین موانع پذیرش عمومی این ارزها محسوب می‌شوند.

۵. دیپلماسی مالی و شبکه‌های منطقه‌ای :بررسی امکان‌سنجی فنی و اقتصادی ایجاد یک شبکه پیام‌رسان و تسویه حساب مالی منطقه‌ای مبتنی بر بلاک‌چین میان کشورهای همسو (مانند اعضای بریکس یا سازمان همکاری شانگهای) به‌منظور جایگزینی تدریجی و چندجانبه سوئیفت در مبادلات دوجانبه.

ملاحظات اخلاقی: کلیه اصول اخلاق در پژوهش، همچنین امانت‌داری علمی در استفاده از منابع، استنادها و ارجاعات موردتوجه قرار گرفته و رعایت شده است.

تعارض منافع: نویسندگان اعلام می‌دارند که تدوین و انتشار این مقاله فاقد هرگونه تعارض منافع بوده است.

سهم نویسندگان: نگارش و تدوین مقاله به‌صورت مشترک و با مشارکت برابر تمامی نویسندگان انجام شده است.

تشکر و قدردانی: بدین‌وسیله از تمامی افرادی که در تهیه و تکمیل این مقاله همکاری و مساعدت داشته‌اند، قدردانی می‌شود.

تأمین اعتبار پژوهش: این پژوهش بدون دریافت هرگونه حمایت یا تأمین مالی انجام شده است.

فهرست منابع

جانو سپاه، و عشوریان، م. (۱۳۸۷). پیاده‌سازی نرم‌افزاری یک سیستم پول دیجیتالی مبتنی بر روش برند. *دومین کنفرانس جهانی بانکداری الکترونیکی*، موسسه مطالعات بهره‌وری و منابع انسانی.

ذوالفقاری، م. (۱۳۹۰). آشنایی با پول الکترونیکی. *اولین همایش ملی فناوری اطلاعات و ارتباطات*، دانشگاه جامع علمی کاربردی واحد ابهر.

شمسایی، م. (۱۳۸۴). ارائه روشی امن جهت سیستم‌های پرداخت سکه الکترونیکی. *سومین کنفرانس انجمن رمز ایران*، دانشگاه صنعتی اصفهان.

کیهانی راست‌گو، ح.، حبیب‌زاده مریان، ح.، و حسینی، س. م. (۱۳۹۲). بررسی تجارت و پول الکترونیک در ایران. *اولین کنفرانس ملی نوآوری در مهندسی کامپیوتر و فناوری اطلاعات*، موسسه آموزش عالی شفق.

نصیری احمدآبادی، م. (۱۳۸۷). بررسی چگونگی تأثیر پول و بانکداری الکترونیکی بر اقتصاد کلان. *دومین کنفرانس جهانی بانکداری الکترونیکی*، موسسه مطالعات بهره‌وری و منابع انسانی.

دعایی، م. (۱۳۹۳). بیت‌کوین، نخستین پول مجازی. *ماهنامه بورس*، (۱۱۵-۱۱۴).

Bayer, D., Haber, S & „Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In Sequences II: Methods in Communication, Security and Computer Science (pp. 329–334). Springer . https://doi.org/10.1007/978-1-4613-9323-8_24

Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brito, J. (2011, April 16). Online cash Bitcoin could challenge governments, banks. Time Magazine.

Dai, W. (1998). B-money. Retrieved from http://www.weidai.com/bmoney.txt

Edelman. (2017). Edelman Trust Barometer 2017. Edelman. Retrieved from https://www.edelman.com/trust/2017-trust-barometer

Guo, J., & Chow, A. (2008). Virtual money systems: A phenomenal analysis. In 2008 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services (pp. 267–272). IEEE. https://doi.org/10.1109/CEC-EEE.2008.40

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99–111. https://doi.org/10.1007/BF00204002

Kelleher, J. (2014, April). What is Bitcoin mining? Investopedia. Retrieved from https://www.investopedia.com/terms/b/bitcoin-mining.asp

Massias, H., Avila, X. S., & Quisquater, J.-J. (1999). Design of a secure timestamping service with minimal trust requirements. In 20th Symposium on Information Theory in the Benelux.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Raskin, M. (2013, April 10). Meet the Bitcoin millionaires. Bloomberg Businessweek.