EGHTESAD–E ISLAMI (A Quarterly Journal on Islamic Economics)
Vol.24 / No.95 / Autumn 2024
ISSN: 1735-3262
https://eghtesad.iict.ac.ir
JEL classification: K290, K230.

Evaluating the Gambling-likeness of Bitcoin's Distributed Ledger with Emphasis on Imam Khomeini's Jurisprudence thought

Seyyed Mohammad Kazem Rajaei
Professor of Economics Department of Imam Khomeini Educational and Research Institute.
Email: rajaee_smk@ yahoo.co.uk

Gholamali Masoumi Nia
Associate Professor, Department of Economics, Kharazmi University.
Email:masuminia@khu.ac.ir

Mahdi Noori
Associate Professor, Department of Economics, University of Tehran.
Email: mahdinouri@ut.ac.ir

Saeed Ebrahimi (Corresponding Author)
Qom seminary lecturer and Islamic economics researcher.
Email: s_e1386@yahoo.com

Use your device to scan and read the article online

Citation Seyyed Mohammad Kazem Rajaei, Gholamali Masoumi Nia, Saeed Ebrahimi [Evaluating the Gambling-likeness of Bitcoin's Distributed Ledger with Emphasis on Imam Khomeini's Jurisprudence thought (Persian)].EGHTESAD–E ISLAMI (A Quarterly Journal on Islamic Economics). 2024; 24 (95): 151-186
10.22034/iec.2024.2027891.2747

Received: 01 May 2024 , Accepted: 27 August 2024

Abstract

The structure of Bitcoin as the first cryptocurrency is based on the three foundations of cryptography, decentralization and irreversibility of transactions. The lack of concentration in cryptocurrencies leads to the creation of distributed ledgers, and encryption and irreversibility each lead to the improvement of the security of cryptocurrencies. The legitimacy of using Bitcoin and other cryptocurrencies depends on the legitimacy of the laws governing the cryptocurrency ledger and avoiding red lines such as gambling, which is the focus of this research. There are different views among the jurists regarding the restrictions and conditions of gambling. These differences and diversity of thoughts have led to the formation of various conclusions about gambling, which may be effective in the case of the title of gambling on Bitcoin. The current research, with a descriptive and analytical method and with an emphasis on Imam Khomeini's (RA) opinions, explained the concept of gambling in the ledger of Bitcoin as the oldest and most important cryptocurrency, and while explaining the fundamental concepts of Bitcoin and the laws governing it, reached this conclusion. It was found that the distributed ledger of Bitcoin is not contaminated with gambling, although the investigation of the gambling nature of its secondary transactions requires independent research.

Keywords

Gambling, Bitcoin, distributed ledger, consensus algorithm, jurisprudence.

فصلنامه علمی اقتصاد اسلامی
سال بیست و چهارم/ شماره نودوپنج/ پاییز ۱۴۰۳
ISSN: 1735-3262
نوع مقاله: علمی ـ پژوهشی
https://eghtesad.iict.ac.ir
طبقه‌بندی JEL: K290, K230.

ارزیابی قمارگونه بودن دفتر کل توزیع‌شده بیت‌کوین با تأکید بر اندیشه فقهی امام خمینی (ره)

سیدمحمدکاظم رجایی
استاد گروه اقتصاد مؤسسه آموزشی و پژوهشی امام خمینی (ره) Email: rajaee_smk@yahoo.co.uk.
غلامعلی معصومی‌نیا
دانشیار گروه اقتصاد، دانشگاه خوارزمی. Email: masuminia@khu.ac.ir
مهدی نوری
استادیار گروه اقتصاد، دانشگاه تهران. Email: mahdinouri@ut.ac.ir
سعید ابراهیمی (نویسنده مسئول)
مدرس حوزه علمیه قم و پژوهشگر اقتصاد اسلامی. Email: s_e1386@yahoo.com

Use your device to scan and read the article online
Citation Seyyed Mohammad Kazem Rajaei, Gholamali Masoumi Nia, Saeed Ebrahimi [Evaluating the Gambling-likeness of Bitcoin's Distributed Ledger with Emphasis on Imam Khomeini's Jurisprudence thought (Persian)].EGHTESAD–E ISLAMI (A Quarterly Journal on Islamic Economics). 2024; 24 (95): 151-186
10.22034/iec.2024.2027891.2747
تاریخ دریافت: ۱۴۰۳/۰۲/۱۲، تاریخ پذیرش: ۱۴۰۳/۰۶/۰۶

چکیده

ساختار بیت‌کوین به عنوان اولین رمزارز بر سه پایه رمزنگاری، عدم تمرکز و برگشت‌ناپذیری تراکنش‌ها استوار شده است. عدم تمرکز در رمزارزها به ایجاد دفاتر کل توزیع‌شده منتهی می‌شود و رمزنگاری و برگشت‌ناپذیری نیز هریک به‌گونه‌ای به ارتقای امنیت رمزارزها می‌انجامند. مشروعیت استفاده از بیت‌کوین و دیگر رمزارزها، در گرو مشروع‌بودن قوانین حاکم بر دفتر کل رمزارز مزبور و دوری از خطوط قرمزی مانند قمار می‌باشد که محور این تحقیق را به خود اختصاص داده است. در قیود و شروط تحقق قمار دیدگاه‌های گوناگونی در میان فقها وجود دارد. این اختلافات و گوناگونی اندیشه‌ها، به شکل‌گیری استنباطات مختلفی در مورد قمار انجامیده است که ممکن است در صدق عنوان قمار بر بیت‌کوین مؤثر باشد. تحقیق کنونی با روش توصیفی- تحلیلی و با تأکید بر آرای امام خمینی به تبیین مفهوم قمار در دفتر کل بیت‌کوین به عنوان قدیمی‌ترین و مهم‌ترین رمزارز پرداخته و ضمن تشریح مفاهیم بنیادی بیت‌کوین و قوانین حاکم بر آن، به این نتیجه دست یافت که دفتر کل توزیع‌شده بیت‌کوین آلوده به قمار نیست؛ هرچند بررسی قمارگونه بودن معاملات ثانویه آن نیازمند تحقیقات مستقلی می‌باشد.

واژگان کلیدی
قمار، بیت‌کوین، دفتر کل توزیع‌شده، الگوریتم اجماع، فقه.

مقدمه

پس از اختراع رایانه، اینترنت و ظهور فناوری اطلاعات و در نتیجه تسهیل دسترسی به اطلاعات و پردازش داده‌ها، تحولات عظیمی در سطح دانش‌های مختلف روی داد. مبادلات و تراکنش‌های مالی نیز از این قاعده مستثنی نماندند و فناوری مزبور سبب تغییرات شگرف در بازارهای مالی گردید. پیدایش رمزارزها و رقابت آنها با پول‌های متداول یکی از آثار ورود فناوری اطلاعات به فضای مالی در عصر کنونی است. تمامی رمزارزها از فناوری دفتر کل توزیع‌شده استفاده می‌کنند که دارای سه لایه پروتکل، شبکه و داده می‌باشد. اولین رمزارزی که مبتنی بر این فناوری در سال ۲۰۰۸ وارد بازارهای مالی شد، بیت‌کوین بود و رمزارزهای متعددی بر اساس دفتر کل توزیع‌شده بیت‌کوین شکل گرفتند.

با ورود بیت‌کوین و کوین‌های وابسته‌اش به جوامع اسلامی، سؤالات فقهی متعددی نظیر مالیت، غرری‌بودن معاملات و یا قمارگونه بودن این کوین‌ها مطرح شد. با صرف‌نظر از شبه غرر و یا عدم مالیت بیت‌کوین، شبه قمار را می‌توان در دو سطح در مورد بیت‌کوین مطرح نمود؛ گاه در سطح معاملات بیت‌کوین‌های استخراج‌شده و گاه در مورد ساختار دفتر کل بیت‌کوین مطرح می‌شود. این تحقیق تلاش می‌کند سؤال اخیر را با توجه به عبارات برخی از متخصصان این فناوری که استخراج بیت‌کوین را وابسته به شانس و قمارگونه معرفی کرده‌اند (Antonopoulos, ۲۰۱۷, p.۲۵۰) بررسی کند. البته این شبهه تنها در سطح متخصصان رمزارزها مطرح نمی‌گردد و به سطح قانونگذاران نیز تسری یافته و هیئتی از قانونگذاران انگلستان در ۱۶ می ۲۰۲۳ خواستار دسته‌بندی بیت‌کوین تحت عنوان قمار شده‌اند که می‌توان از مطالبه مزبور به عنوان دکترین حقوقی در این زمینه نام برد. قماربودن بیت‌کوین می‌تواند در دو سطح دفتر کل توزیع‌شده آن و نیز در معاملات ثانویه آن مطرح گردد و این مقاله به بخش نخست یعنی قمارگونه

بودن دفتر کل بیت‌کوین می‌پردازد. برای پاسخ به سؤال قمارگونه بودن این نوع از دفتر کل، باید به سؤالات مطرح در سه زمینه آتی پاسخ داد. آلودگی یا عدم آلودگی رمزارزها به قمار در لایه پروتکل، رخداد قمار در لایه شبکه و در نهایت امکان مطرح‌شدن شبه قمار در لایه داده. به صورت خلاصه قابل پذیرش بودن یا نبودن قمارگونگی دفتر کل رمزارزها در اندیشه فقهای امامیه خصوصاً امام راحل، مسئله اصلی این تحقیق را به خود اختصاص داده است. تحقیق پیش رو بر اساس فیش‌برداری و روش توصیفی، تحلیلی درصدد پاسخگویی به سؤال مزبور است. پاسخ به این دست پرسش‌های فقهی به روشن‌شدن ابعاد فقهی استفاده از رمزارزها می‌انجامد و عرصه را برای تحقیقات حقوقی و تدوین قوانین مناسب در این‌باره فراهم می‌آورد.

پیشینه تحقیق

الف) پیشینه داخلی

مقدس اردبیلی در **مجمع‌الفائده** (اردبیلی، ۱۴۰۳ق، ج۸، ص۴۱)، مرحوم شیخ *انصاری* در **المکاسب** (انصاری، ۱۴۱۱ق، ج۱، ص۱۹۲) و امام خمینی در **المکاسب المحرمة** (امام خمینی، ۱۴۱۵ق، ج۲، ص۸) همانند بسیاری از فقهای عظام از منظر فقهی صرف به تشریح مفهوم قمار اهتمام ورزیده‌اند. در تحقیقات میان‌رشته‌ای مرتبط با بیت‌کوین می‌توان به آثار آتی اشاره نمود. *خردمند* (۱۳۹۸) در مقاله «بررسی فقهی استخراج و مبادله رمزارزها با تمرکز بر شبکه بیت‌کوین» ضمن اشاره گذرا به ساختار بیت‌کوین بحث قمار را بر اساس نظر دو تن از متأخرین مطرح می‌کند و در نهایت عدم تحقق قمار را نتیجه می‌گیرد. لکن مقاله مزبور بین وجود قمار در دفتر کل بیت‌کوین و معاملات ثانویه تفکیک ننموده است و از موضوع‌شناسی عمیق نیز برخوردار نیست. گزارش کارشناسی پژوهشکده پولی و بانکی بانک مرکزی (۱۳۹۹) نیز به صورت گذرا به شبهه قماری‌بودن بیت‌کوین پرداخته

است و بی‌آنکه مستندات فقهی ارائه کند، شبهه مزبور را مردود می‌داند. *رضایی صدرآبادی* و همکاران (۱۳۹۸) در «تحلیل فقهی اقتصادی استخراج ارزهای مجازی در نظام اقتصادی اسلام (مطالعه موردی بیت‌کوین)» بدون عنایت به بحث قمار، عمدتاً از دیدگاه فقه حکومتی و با تأکید بر احتمال تسلط کفار به بحث استخراج بیت‌کوین پرداخته‌اند. *مدرسی* (۱۴۰۱) در کتاب **فقه رمزارزها** توجهی به شبهه قمارگونه بودن رمزارزها ننموده و به مباحثی مانند بررسی شروط عوضین در رمزارزها، شبهه عدم مالیت و جریان ربا در رمزارزها پرداخته است.

ب) پیشینه خارجی

مقالات و تحقیقات مختلفی در مورد مباحث فنی و حقوقی بیت‌کوین منتشر شده است که در ذیل به مهم‌ترین این تحقیقات اشاره می‌شود. *ناکاموتو* (Nakamoto, ۲۰۰۸) معتقد بود که یک نسخه کاملاً همتا به همتا از پول نقد الکترونیکی، این امکان را به ما می‌دهد که پرداخت‌های برخط از یک طرف به طرف دیگر بدون مراجعه به یک مؤسسه مالی ارسال شود. وی سپس ساختار فنی از بیت‌کوین را در این مقاله برای اولین بار منتشر می‌کند.

پینا و رانبرگ (Pinna & Ruttenberg, 2016) ضمن مطرح‌نمودن ساختار دفتر کل توزیع‌شده معتقدند که فناوری دفتر کل توزیع‌شده، به کاربران اجازه می‌دهد بدون نیاز به استفاده از یک سیستم اعتبارسنجی مرکزی که استانداردهای خود را تحمیل می‌کند، اطلاعات خود را تغییر دهند.

بینوس و همکاران (Benos, Garratt & Gurrola, 2017) با نگاهی اقتصادی به مقوله رمزارز معتقدند این فناوری بر سه محور رمزنگاری، عدم اعتماد و عدم تمرکز استوار است و یکی از گونه‌های آن بلاک‌چین است. بلاک‌چین یک پایگاه داده توزیع‌شده تراکنش‌هاست که گره‌های توزیع‌شده در سطح جهانی، توسط یک شبکه ارتباطی همتا به همتا با یکدیگر مرتبط شده‌اند.

گلاسر (Glaser, 2017)، *آنتونوپولوس* (Antonopoulos, 2017) و نیز *بشیر* (Bashir, 2018) به تشریح جزییات فنی بیت‌کوین، الگوریتم اجماع آن و مقولات مرتبط پرداخته‌اند. تحقیقات یادشده عمدتاً مسائل فنی دفتر کل بیت‌کوین را مطرح نموده‌اند و مباحث حقوقی و مفاهیم مرتبط با قراردادهای مالی را بررسی نکرده‌اند. از جمله مقالاتی که به ساختار مباحث فقهی و حقوقی بیت‌کوین توجه کرده‌اند می‌توان به آثار ذیل اشاره نمود.

رشید عوده (۲۰۱۹) در مطالعه «ارزهای مجازی: احکام فقهی آنها و حکم برخورد با آنها» مبادله با بیت‌کوین را قمار می‌داند. همچنین *سمیران* (۲۰۱۹) در مقاله «کنترل فرایند انتشار ارزهای دیجیتال» اعتقاد به آلودگی رمزارزها و خصوصاً بیت‌کوین به قمار دارد. در میان محققان اسلامی، نویسندگان دیگری مانند *اوزیو و یاندیو* (Oziev& Yandiev, 2017) و *طه علی و حق* (Taha Ali & Haq, 2018) به همراه *فبریاندیکا و سوکمانا* ۲۰۱۸) (Febriandika & sukmana در مقالات خود عنوان قمار را بر بیت‌کوین تطبیق کرده‌اند. از دانشمندان دیگر می‌توان *یونلاین* (Yuneline, 2019) را نام برد که در پژوهشی با عنوان «تحلیل ویژگی‌های ارز دیجیتال در چهار منظر» و *ذوالخبری* (Zulkhibri 2019) در مقاله‌ای با نام «ارز دیجیتال حلال و ثبات مالی» همراه با *آمادو و بالله* (Amadu &Billah, 2019) در گزارش تحقیقی که با عنوان «اخلاق در ارزهای دیجیتال» منتشر نمودند، قمار را از جمله ادله ممنوعیت استفاده از بیت‌کوین برشمرده‌اند. نگارندگان، تحقیقی یافت نکردند که با تفکیک دفتر کل از معاملات ثانویه بیت‌کوین و با تأکید بر نظرات امام راحل تلاش نموده باشد که شبهه قمارگونه بودن دفتر کل بیت‌کوین را مورد مداقه قرار دهد.

مفهوم‌شناسی قمار

از بررسی کتب لغت (ازهری، ۱۴۲۱ق، ج۹، ص۱۲۶/ زمخشری، ۱۹۷۹م،

ص۵۲۲/ ابن‌فارس، ۱۴۰۴ق، ج۵، ص۲۶/ مصطفوی، ۱۴۰۲ق، ج۹، ص۳۱۷/ فیروزآبادی، ۱۴۱۵ق، ج۲، ص۲۰۷/ فیومی، ۱۴۱۴ق، ج۲، ص۵۱۵/ حمیری، ۱۴۲۰ق، ج۳، ص۱۷۷۰/ مهنا، ۱۴۱۳ق، ج۲، ص۴۱۶) در معنای قمار این‌گونه نتیجه می‌شود که قمار خواه ریشه در نیرنگ داشته باشد و یا اینکه از معنای سفیدی و یا ماه مشتق شده باشد در نهایت به دو رکن مغالبه و مراهنه یا رهان استوار است. بازی‌کردن هم اگرچه توسط برخی از بزرگان مانند مرحوم *طریحی* (طریحی، ۱۳۷۵، ج۳، ص۴۶۳) و *ابن‌منظور* (ابن‌منظور، ۱۴۱۴ق، ج۵، ص۱۱۵) و نیز جوهری (جوهری، ۱۳۷۶، ج۲، ص۷۹۹) در معنای قمار اخذ شده است، اما این امر مورد پذیرش همه لغویان نیست و نمی‌توان بازی و لعب را بخشی از معنای قمار دانست و از نظر تحقق خارجی هم این دو مفهوم تلازمی باهم ندارند. چه‌بسا اشاره به معنای لعب و بازی، به دلیل کثرت وقوع قمار در قالب بازی می‌باشد؛ نه اینکه قمار در اشکال دیگر قابل تحقق نیست.

حال به واکاوی معنای رهان و مغالبه می‌پردازیم. مغالبه از ریشه غلب و به معنای پیروزی است و مغالبه یعنی تلاش طرفین برای پیروزی در امری واحد و در امور مختلف مانند مباحثات علمی و اعتقادی نیز مفهوم مغالبه استفاده می‌گردد (ابن‌اثیر، ۱۳۶۷، ج۱، ص۳۴۱). مراهنه از ماده رهن می‌آید. **تاج‌العروس** در ماده رهن می‌گوید: هر چیزی که به سبب آن شخصی محبوس شود، رهین فرد محسوب می‌شود و مراهنه و رهان به معنای در خطر قراردادن مال است که در قالب مسابقه در مطلق امور خواه اسب‌دوانی و خواه هر شیء دیگری می‌تواند رخ دهد (زبیدی، ۱۴۱۴ق، ج۱۸، ص۲۵۰)

«خاطره» که توسط صاحب **تاج‌العروس** معادل مراهنه گرفته شده است، به معنای مال را در معرض نابودی قراردادن می‌باشد و با توجه به باب مفاعله حکم به طرفینی‌بودن آن می‌شود؛ یعنی دو طرف به صورت متقابل مال خود را در معرض هلاکت قرار می‌دهند. کلام زمخشری نیز مؤید همین

معناست (جوهری، ۱۳۷۶، ج۲، ص۶۴۸/ زمخشری، ۱۳۸۶، ص۲۲۶).

بنابراین مراهنه نزد اهل لغت به معنای رهن‌گذاری طرفینی و گروگذاری متقابل است که امروزه شرط‌بندی به آن اطلاق می‌شود و طرفین ملتزم می‌شوند در صورت شکست، تعهدی مالی را نسبت به طرف مقابل ایفا کنند و این معنا روشن‌ترین مصداق قمار است. البته امکان تفکیک رهان و مراهنه در معنا و ترجمه رهان به مطلق پاداش وجود دارد و بر این اساس تحقق قمار در زمان پرداخت رهان و در موردی که طرفین برای دست‌یابی به پاداش شخص ثالث با یکدیگر رقابت می‌کنند، ممکن است.

پس از بررسی معنای لغوی قمار، به کلمات فقهای امامیه در دو دوره قدما و متأخرین مراجعه و کلمات مرحوم امام به عنوان نماینده معاصرین به صورت تفصیلی مطرح می‌شود.

قمار در اندیشه فقهای امامیه

مرحوم *مفید* در باب شرایط شاهد می‌فرمایند شهادت قمارباز، بازی‌کننده با شطرنج و دیگر آلات قمار پذیرفته نیست (شیخ مفید، ۱۴۱۳ق، ص۷۲۶). همین‌طور *حلبی* (۱۴۰۳ق، ص۲۸۱)، *سلار* (۱۴۰۴ق، ص۱۷۰)، *ابن‌براج* (۱۴۰۶ق، ص۳۲۵) و شیخ *طوسی* (۱۳۸۷، ج۸، ص ۲۲۱ و ۱۴۰۰، ص۳۲۵) در حکم حرمت، صرف بازی‌نمودن با آلات قمار را کافی دانسته‌اند و عبارتی که حاکی از مفهوم‌شناسی قمار باشد در کلمات آنان یافت نشد؛ اما با دقت در عبارات این بزرگواران می‌توان گفت که ایشان بازی با آلات قمار را دارای حکمی برابر با قمار دانسته‌اند؛ ازاین‌رو شاید نتوان گفت که قدما مفهوم قمار را حتماً شامل معنای بازی‌کردن هم می‌دانند، بلکه ممکن است صرف شرط‌بندی را قمار بدانند که اگر شرط‌بندی با آلات خاص و در قالب بازی محقق شود قطعاً قمار است و اگر بازی بدون شرط‌بندی با آلات قمار صورت گیرد، قمار نیست، اما حرام است.

بااین‌همه حمل مزبور قطعی به نظر نمی‌رسد و می‌توان گفت که

عبارت آلات قمار و بازی با آنها یعنی اینکه در معنای قمار قطعاً بازی نهفته است و این بازی‌ها آلت مخصوص به خود را دارند. درعین‌حال همچنان این احتمال وجود دارد که ایشان صرف شرطبندی را قمار بدانند و این شرطبندی اگر در قالب بازی مطرح گردد نیاز به آلت دارد که به این آلات، آلات قمار گفته می‌شود. شاهدی که بر این ادعا وجود دارد عبارتی است که شیخ *صدوق* ذکر نموده‌اند و قمار و لعب را از هم تفکیک نموده‌اند (صدوق، ۱۴۱۵ق، ج۱، ص ۴۵۷).

اما در طبقه متأخرین نیز مفهوم مشخصی از قمار در کلام بسیاری از بزرگان ارائه نشده است و تنها به بیان حکم قمار بسنده نموده‌اند (ابن‌ادریس حلی،۱۴۱۰ق، ج۲، ص۱۲۱/ کیدری، ۱۴۱۶ق، ص۲۴۶/ محقق حلی، ۱۴۰۸ق، ج۴، ص۱۱۷/ علامه حلی،۱۴۱۰ق، ج۲، ص۱۵۶ و همو ۱۴۲۰ق، ج۵، ص۲۵۰/ عاملی (شهید اول)، ۱۴۱۷ق، ج۲، ص۱۲۶). در این میان کلام مرحوم علامه *حلی* ظهور در عدم اشتراط لعب در معنای قمار دارد (علامه حلی، ۱۴۱۴ق، ج۱۰، ص۳۹۵). علامه *مجلسی* نیز در بیان شرح حدیثی از امیر مؤمنان (ع) کلامی را مطرح نموده‌اند که می‌توان وجود معنای لعب را در آن محتمل دانست (مجلسی، ۱۴۰۶ ق، ج۱۰، ص۱۸۶).

مرحوم *اردبیلی* اولین فقیه متأخری هستند که تعریف روشنی از قمار ارائه نموده‌اند و فرموده‌اند: «قمار به معنای بازی‌کردن با آلات مخصوص به آن است؛ مانند نرد و شطرنج و حتی بازی با انگشتر و ... را نیز قمار گویند»؛ یعنی ایشان پس از ذکر روشن‌ترین فرد قمار در معنای قمار توسعه داده و استفاده از آلات مخصوص به قمار را شرط تحقق قمار نمی‌دانند (اردبیلی، ۱۴۰۳ق، ج۸، ص۴۱).

مرحوم شیخ *انصاری* در مقام بیان مفهوم قمار، سه احتمال ذکر می‌کنند و بدون اینکه قضاوتی نمایند از مفهوم‌شناسی عبور نموده و چهار قسم برای تحقق قمار ذکر می‌کنند و در هر چهار قسم، بازی را در مفهوم قمار

مطرح می‌کنند (شیخ انصاری، ۱۴۱۱ق، ج۱، ص۱۸۵ـ۱۹۲). البته ایشان در جای‌جای عبارت بر وجود مفهوم مغالبه تأکید کرده‌اند و چه‌بسا ذکر بازی توسط جناب شیخ، به عنوان روشن‌ترین و شایع‌ترین مصداق مفهوم مغالبه باشد. دلیل بر این مدعا نیز تصریح ایشان به کفایت مطلق مغالبه در تحقق قمار است و می‌فرمایند: «الأظهر أنه مطلق المغالبة» (همان، ص۱۹۲)؛ بنابراین می‌توان این‌گونه ادعا کرد که در دیدگاه شیخ اعظم بازی خصوصیتی در صدق قمار ندارد و هر جا که مغالبه و رهان و یا حتی مغالبه وجود داشته باشد، می‌توان گفت که قمار صدق می‌کند.

دیدگاه امام راحل در مورد قمار

عبارات مرحوم امام در کتاب **البیع** اشاره‌ای به مفهوم‌شناسی قمار ندارد و حداکثر اشاره‌ای به باطل‌بودن قمار نموده‌اند (امام خمینی، ۱۳۷۹، ص۹۹). ایشان در **المکاسب** به بررسی تفصیلی قمار پرداخته‌اند و در تعریف قمار می‌فرمایند: «بر اساس دیدگاه علمای شیعه قمار زمانی که با آلات مخصوص و رهان صورت پذیرد، اجماعاً حرام است. مفهوم قمار و میسر با این دو قید قطعاً محقق می‌گردد و تفاوتی میان انواع قمار نظیر نرد و شطرنج و حتی بازی‌کردن با گردو و تخم‌مرغ نیست؛ زیرا عرف به تمامی این موارد قمار اطلاق می‌کند؛ ولو دلیل حکم عرف متداول‌بودن قماربازی با گردو و تخم‌مرغ باشد و اگر در صدق قمار بر این موارد شک شود، تردیدی وجود ندارد که این موارد از نظر حکمی به قمار ملحق می‌شوند» (امام خمینی، ۱۴۱۵ق، ج۲، ص۸)؛ اما در مواردی که تنها بازی با آلات قمار و غیر آلات قمار صورت پذیرد و رهان وجود نداشته باشد صدق قمار از نظر معظمٌ‌له محل تأمل است و تنها حکم حرمت را بدون تحقق عنوان قمار بر مورد اول صادق می‌دانند (همان، ص۱۲ـ۱۳).

در خصوص بازی با غیر آلات قمار و با رهان، ایشان اجماع را مدرکی و قول لغوی را نیز دال بر صدق قمار نمی‌دانند (همان، ص۲۳). از نظر ایشان

روایات نیز دال بر تحقق قمار نیستند و تنها حکم حرمت را از مرسله مرحوم *صدوق* استفاده می‌فرمایند (همان، ص۲۵ ـ ۳۵). دلیل دیگر بر حرمت نیز باطل‌بودن این سبب است و در نتیجه این قسم را تحت اطلاق آیه شریفه اکل مال به باطل درج می‌نمایند (همان، ص۲۵ ـ ۲۸)؛ بنابراین قمار تنها در بازی با آلات قمار و در صورت مغالبه و مراهنه محقق است.

البته ایشان در کتاب فوق روایتی از *ابن‌سیابه* (عاملی، ۱۴۰۹ق، ج۲۷، ص۴۱۳) ذکر فرمودند که قمار را قابل توسعه در مطلق بازی‌ها می‌دانست و همین معنا را می‌توان از صحیحه *معمربن‌خلاد* (همان، ج۱۷، ص۳۲۳) و روایت *جابر* (همان، ص۱۶۵) از امام *باقر* (ع) برداشت نمود که امام (ع) آلت را داخل در مفهوم قمار نمی‌داند؛ ازاین‌رو وجه روشنی برای کنارگذاردن این روایات توسط حضرت امام تصور نمی‌شود. شاید به دلیل همین نوع اشکالات است که نظر ایشان در کتاب **تحریرالوسیله** با تغییر همراه است و از قید آلت قمار رفع ید نموده‌اند و صرف لعب به همراه رهان را در صدق قمار کافی می‌دانند (امام خمینی، ۱۴۲۱ق، ص۸۵۲).

همچنین در استفتائاتی که از محضر شریفشان به عمل آمده، ورزش‌هایی مانند والیبال را نیز با وجود رهان در آنها مصداق قمار دانسته‌اند (امام خمینی، ۱۴۰۰، ج۳۶، ص۵۴۲)؛ ضمن اینکه بنا بر ظاهر عبارت معظّم‌له مالی که به عنوان رهان قرار داده شده است نیز لزوماً نباید از سوی طرفین پرداخت شود و صرف بردوباخت اگر با جایزه همراه باشد مفید قمار است (همان، ص۵۴۳). در نهایت می‌توان گفت که امام راحل سه رکن لعب، مغالبه و رهان را برای تحقق قمار لازم دانستند و چون مراهنه دربردارنده معنای مغالبه نیز هست می‌توان گفت که دو قید لعب و رهان در صدق قمار از دیدگاه امام خمینی کافی است.

اما به نظر می‌رسد با توجه به روایات *ابن‌سیابه* و *ابن‌خلاد* و با عنایت به کلام لغویان، کلمات فقهای عظام مانند علامه *حلی* و فهم عرفی از قمار،

مراهنه و مغالبه در تحقق عنوان قمار کافی است و لزومی ندارد که قید بازی در مفهوم قمار اخذ شود. یکی از شاگردان مبرز امام راحل نیز صرف وجود عوض به همراه بردوباخت را در تحقق قمار کافی می‌دانند و مهم‌ترین استدلال را دلالت عرف و لغت بر این مسئله می‌دانند (لنکرانی، ۱۳۹۰، ص۴۷۳). در نظر ایشان در مواردی که طرفین در معرکه‌ای مانند بخت‌آزمایی وارد می‌شوند و برای دستیابی به پاداشی رقابت می‌کنند که تصادف و شانس تعیین‌کننده‌ترین عامل استحقاق است، قمار تحقق می‌یابد؛ کلامی که نمی‌توان به‌سادگی از آن چشم پوشید.

در نهایت و با توجه به آنچه که گفته شد، قمار را می‌توان این‌گونه معنا کرد: «هر نوع فعالیت غیراقتصادی اعم از بازی، شرط‌بندی، بخت‌آزمایی و ... که افراد بدون انجام فعالیت ارزشمند و عقلایی متناسب و تنها بر اساس بخت و اقبال، در پی کسب پاداش و درآمد هستند را قمار می‌نامند». البته اگر معنای لعب در دیدگاه امام راحل را عام بدانیم، نظر ایشان با دستاورد تحقیق از معنای قمار، کاملاً برهم منطبق هستند.

حال برای شناخت موضوع تحقیق، ابتدا به انگیزه ایجاد و اندیشه‌های طرفداران بیت‌کوین اشاره می‌شود؛ سپس به مفاهیم بنیادین بیت‌کوین مانند دفتر کل توزیع‌شده و بخش‌های مختلف آن پرداخته و ضمن تشریح تراکنش‌های مبتنی بر بیت‌کوین، وجود مفهوم قمار در تمامی بخش‌های دفتر کل و معاملات مبتنی بر آن پی گرفته می‌شود.

زمینه‌های فکری پیدایش بیت‌کوین

توانایی پرداخت و انجام تراکنش برخط به صورت گمنام و بی‌واسطه همواره از طرف جوامع خاصی مانند نخبگان فناوری اطلاعات، سایفرپانک‌ها (Cypherpunk) که طرفدار آزادی انتشار اطلاعات هستند، طرفداران غیرمتمرکزسازی و مدعیان آزادی فردی مورد حمایت قرار گرفته است. در تمامی گروه‌های مذکور یک هویت و جهان‌بینی مشترک وجود دارد. آنها

احساس می‌کنند که بخشی از یک خانواده بزرگ تحت تأثیر نظرات متفکرانی مانند *هایک* هستند (وانگ، ۱۴۰۱، ص۲۰). این افراد همواره در تلاش برای روشی برای تبادل آزاد کلیه اقسام اطلاعات بودند که نقش نهادهای تنظیم‌گر را حذف یا به حداقل می‌رساند (همان، ص۲۰). آنان از رمزنگاری به عنوان حافظ حریم خصوصی شهروندان و از بلاک‌چین به عنوان بستری برای کلیه خدمات اجتماعی و دولتی یاد می‌کنند و برخی از آنها فناوری‌های توزیع‌شده را پایان‌بخش دولت‌ها و حاکم‌کننده مطلق بازار آزاد می‌دانند (Atzori, 2015).

مفاهیم بنیادی

رمزنگاری

حفاظت داده‌ها از دسترس افراد فاقد صلاحیت و ایجاد قفل دیجیتالی بر اطلاعات را ایده اصلی رمزنگاری می‌توان دانست. در گذشته رمزنگاری تنها به رمزگذاری و رمزگشایی پیام‌ها با استفاده از کلیدهای مخفی اطلاق می‌شد؛ اما امروزه به صورت سه مکانیزم تعریف می‌شود. به رمز درآوردن به وسیله کلید متقارن، به رمز درآوردن با استفاده از کلید نامتقارن و هشینگ (فروزان، ۱۳۹۵، ص۱۷).

در رمزگذاری با کلید متقارن کلید رمزگشایی و رمزنگاری یکسان است (قادرمرزی، ۱۳۹۸، ص۲۵)؛ اما با رمزگذاری بر اساس کلید نامتقارن، از دو کلید خصوصی و عمومی استفاده می‌شود که از سرعت پایین‌تری در مقایسه با رمزنگاری متقارن برخوردارند (همان، ص۲۴). کلید عمومی قابل دسترسی برای عموم است و همه می‌توانند یک کپی از آن را داشته باشند؛ اما کلید خصوصی به صورت امن نگهداری می‌شود (همان، ص۴۵). با وجود اینکه رمزنگاری بخشی بسیار مهم در دفتر کل توزیع‌شده را به خود اختصاص می‌دهد، اما هیچ ارتباطی بین این مفهوم و قمار متصور نیست.

شبکه همتا به همتای توزیع‌شده

در این شبکه‌ها، کنترل‌کننده مرکزی وجود ندارد و همه شرکت‌کنندگان به صورت مستقیم با هم در ارتباط هستند. این خصوصیت سبب می‌شود که تراکنش‌ها به‌طور مستقیم بین همتایان بدون دخالت شخص ثالثی مانند بانک، انجام شود (Bashir, ۲۰۱۸, p.۱۲).

اجماع توزیع‌شده

ادبیات اجماع توزیع‌شده میان اعضای یک شبکه بیش از سه دهه است که در صنعت و دانشگاه مورد توجه دانشمندان بوده (Ibid, p.30) و در علوم مختلف مانند مهندسی ارتباطات مورد استفاده واقع شده است (Ren and W. Beard, 2008, p.8).

ناکاماتو با تکیه بر این دانش توانست اجماع میان گره‌های شبکه اختراعی بزرگ را به سرانجام رساند. این اجماع به‌طور صریح توسط هیچ شورا و یا رأی‌گیری ایجاد نمی‌شود و هیچ زمان مشخصی را نمی‌توان به عنوان لحظه ظهور اجماع تعیین کرد. این اجماع محصول تعاملات هزاران گره مستقل است و با کمک الگوریتم‌های اجماع ایجاد می‌شود (Antonopoulos, 2017, p.217).

الگوریتم اجماع

بوترین معتقد است در شبکه‌های همتا به همتا، الگوریتم اجماع حق به‌روزرسانی شبکه یعنی رأی‌دادن در مورد حقیقت را تقسیم‌بندی می‌کند (تاپ اسکات و تاپ اسکات، ۱۳۹۹، ص۱۱۸). این الگوریتم روشی است که از طریق آن تمام افراد فعال در شبکه بلاک‌چین به یک توافق مشترک درباره وضعیت کنونی دفتر کل دست می‌یابند. وظایف الگوریتم اجماع به شرح زیر است.

۱. حصول اطمینان از اضافه‌شدن بلاک‌های واقعی و دارای مقبولیت

عمومی.

۲. تصمیم‌گیری در مورد اینکه آیا این تراکنش صلاحیت تأیید و ذخیره در دفتر را دارد یا خیر.

۳. تضمین یکدست‌سازی اطلاعات روی سامانه‌های سرویس‌دهنده به شبکه.

۴. انتخاب گره‌ها برای مدیریت امور روی دفتر کل توزیع‌شده (نواب‌پور، ۱۴۰۰، ص۲۰).

فناوری دفتر کل (DLT)

سیستمی از رکوردهای الکترونیکی است که شبکه‌ای از شرکت‌کنندگان مستقل را قادر می‌سازد اجماعی حول ترتیب معتبری از تراکنش‌هایی که با رمزنگاری تأیید شده‌اند، شکل دهند. داده‌ها در این دفتر به روش دائمی و تغییرناپذیر با تکنیک‌های رمزنگاری ذخیره می‌شوند و به علت وجود مهر زمانی و هش، داده‌ها به‌راحتی قابل حسابرسی هستند (Vestergaard and et al, 2021, p.9).

دفتر کل توزیع‌شده داری انواع مختلفی است که بلاک‌چین یکی از آنها است. بلاک‌چین یک دفتر توزیع‌شده خاص است که در آن داده‌ها در بلوک‌هایی که توسط توابع هش به هم مرتبط شده‌اند سازماندهی می‌شوند (Treiblmaier, 2020, p.102). اعضای شبکه یا همان گره‌ها از طریق ip همدیگر را می‌شناسند و کاربران از طریق کلیدهای عمومی با یکدیگر ارتباط می‌گیرند (Glaser, 2017).

دفتر کل توزیع‌شده را می‌توان از زاویه‌های مختلف بررسی نمود. برخی از کتب، دفتر کل را بر اساس ویژگی‌های هفت‌گانه اساسی توضیح داده‌اند (Treiblmaier, 2020, p.40) اما *راچس* (Rauchs et al, 2018) با نگاهی مفهومی و عمیق‌تر DLT را بر اساس لایه‌های تشکیل‌دهنده آن تقسیم نموده است. با توجه به جامعیت این نگاه، از تقسیم‌بندی مزبور برای تشریح اجزای DLT بهره می‌گیریم.

لایه‌های دفتر کل توزیع‌شده

یک سیستم DLT را می‌توان به سه لایه اساسی به هم وابسته تقسیم کرد. هر لایه از یک یا چند مؤلفه و هر مؤلفه یک مجموعه منطقی از فرایندهای وابسته به هم است. هر فرایند شامل تعدادی از اقدامات است که بازیگران برای رسیدن به یک یا چند هدف خاص انجام می‌دهند. سه لایه دفتر کل شامل پروتکل، شبکه و داده می‌باشند (Ibid, p.۳۳).

لایه پروتکل

لایه پروتکل، پایه و اساس یک سیستم DLT است. این لایه معین‌کننده مجموعه قوانین رسمی است که سیستم را مدیریت و طراحی و معماری آن سیستم را در قالب کد بیان می‌کند. پروتکل را می‌توان به صورت قانون اساسی در نظر گرفت که تمام شرکت‌کنندگان سیستم آن را قبول کرده‌اند (Ibid, p.34).

مؤلفه‌های پروتکل

پروتکل دارای دو مؤلفه است. مؤلفه آغازین و مؤلفه دگرگونی (Ibid, p.38).

در مؤلفه آغازین فرایندهایی که تعیین‌کننده مرزهای سیستم و نحوه ایجاد کد پایه و مدیریت تغییرات در کد پایه معین می‌شود (Ibid, pp.53-54).

در مؤلفه دگرگونی، چگونگی تغییر پروتکل مورد بحث قرار می‌گیرد و نیز این مؤلفه شامل نحوه اتخاذ تصمیمات گروهی در مورد تغییر پروتکل و همچنین نحوه درج نتایج تصمیمات در پروتکل است (Ibid, pp.55-57).

بررسی قماری‌بودن لایه پروتکل

برای اجتناب از پیچیدگی و اطناب در انتهای هر لایه به بررسی حکم لایه مزبور می‌پردازیم. در لایه پروتکل، فرایندهای وابستگی سیستمی و ایجاد کد پایه ارتباط مستقیمی با قمار ندارند و قمار بر مبنای نظر امام راحل و مبنای تحقیق در آنها قابل تصور نیست. فرایند شروع قانون نیز از سه بخش مدیر،

نگهدارنده کد پایه و ابزار شکل گرفته است. روشن است که ساختار قانونی تعیین مدیر و نگهدارنده کد پایه و ابزار اعمال مدیریت نیز ارتباطی با قمار در هر دو معنا ندارند.

اما در بخش مؤلفه دگرگونی فرایند چگونگی تغییر پروتکل مورد بحث قرار می‌گیرد که توسط یک مرکز خاص و یا بر اساس رأی‌گیری و یا بدون قاعده صورت می‌گیرد. در این بخش نیز اساساً رقابت و رهان را نمی‌توان تصور نمود؛ بنابراین بحث قمار در لایه پروتکل چندان قابل طرح نیست.

لایه شبکه

شبکه یک DLT نتیجه مستقیم پیاده‌سازی قوانین پروتکل است. شبکه مجموعه‌ای از گروه‌های بازیگران به‌هم‌پیوسته و فرایندهایی است که به یک استاندارد فناوری پایبندی دارند و به صورت فعال در تبادل داده‌ها مشارکت می‌کنند. لایه شبکه دارای سه مؤلفه ارتباطات، پردازش تراکنش و مؤلفه اعتبارسنجی می‌باشد (Ibid, p.38).

مؤلفه ارتباطات

در مؤلفه ارتباطات سه فرایند دسترسی به شبکه، انتشار داده و شروع تراکنش وجود دارد (Ibid, p.33).

فرایند دسترسی به شبکه: این فرایند همان حق وصل‌شدن به شبکه است (Ibid, p.58).

فرایند انتشار داده: داده‌ها می‌توانند شایعه‌وار میان همه گره‌ها و یا گره‌های خاص و محدودی منتشر شوند (Ibid, p.59).

فرایند شروع تراکنش: تراکنش این‌گونه آغاز می‌شود. یک کاربر پیامی در قالب استاندارد با استفاده از کلید خصوصی خود را امضا می‌کند و جهت ایجاد و ارسال تراکنش به شبکه واسطه‌های متفاوتی مانند انواع کیف پول‌ها در دسترس کاربران نهایی قرار گرفته است (Ibid, p.60).

مؤلفه پردازش تراکنش

مؤلفه پردازش تراکنش شامل فرایندهای پیشنهاد رکورد، قانون حل اختلاف و پردازش تراکنش انگیزشی می‌گردد.

فرایند پیشنهاد رکورد: پیشنهاد رکورد به فرایندی اشاره دارد که در آن تولیدکنندگان رکورد مجموعه‌ای از تراکنش‌های تأییدنشده را انتخاب کرده و کنار هم قرار می‌دهند تا یک رکورد کاندیدا شکل بگیرد (Ibid, p.61).

فرایند قانون حل اختلاف: مشخص می‌کند که اختلافات در مورد نسخه‌های رقیب یا متضاد از رکوردهای معتبر چگونه رفع شود. این قانون به الگوریتم اجماع مورد استفاده بستگی دارد. بیت‌کوین از قانون طولانی‌ترین زنجیره استفاده می‌کند (Ibid, p.62).

فرایند پردازش تراکنش انگیزشی: به مواردی می‌پردازد که تولیدکنندگان رکورد را تشویق می‌کنند تا با تولید و پیشنهاد رکورد در فرایند پردازش شرکت داشته باشند (Ibid).

مؤلفه اعتبارسنجی

به مجموعه فرایندهای مورد نیاز برای اطمینان از اینکه بازیگران هرکدام مستقلاً به نتیجه یکسانی در مورد مجموعه‌ای از رکوردهای معتبر برسند گفته می‌شود (Ibid, p.63).

برای عینیت بیشتر مؤلفه‌ها و فرایندهایشان با اجرای یک معامله فرضی میان الف و ب، کلیه مؤلفه‌ها در سه بخش تراکنش، ثبت در بلاک و ارسال به شبکه و اعتبارسنجی بلاک تعقیب می‌کنیم. برای روشن‌شدن ارتباط این گام‌ها با مؤلفه‌های ذکرشده به صورت مختصر باید گفت که گام اول یا همان انجام تراکش و معامله با رمزارز در مؤلفه ارتباطات قرار داد. اعتبارسنجی تراکنش مربوط به مؤلفه اعتبارسنجی است. ثبت در بلاک و ارسال به شبکه در مؤلفه پردازش تراکنش جای می‌گیرد و در نهایت افزودن

بلاک به شبکه نیز در مؤلفه اعتبارسنجی صورت می‌پذیرد.

گام اول: تراکنش

مرحله اول: انجام معامله با رمزارز

در ابتدا فرض می‌کنیم فرد الف خانه‌ای را به فرد ب می‌فروشد و در ازای آن از شخص مقابل مقداری کوین باید دریافت کند. فرد الف کیف پول خود را باز نموده و دگمه دریافت را فشار می‌دهد و آدرس بیت‌کوینی که کیف پولش به او می‌دهد را در اختیار فرد ب می‌گذارد. وی نیز مقدار کوینی که باید به فروشنده منتقل نماید را به آدرس مزبور می‌فرستد. حال باید دید در کیف پول چه رخ می‌دهد.

ابتدا به بخش خروجی تراکنش می‌پردازیم؛ جایی که کیف پول فرستنده برای فراهم‌کردن مبلغ مورد نیاز باید چند خروجی تراکنش خرج‌نشده را کنار هم قرار دهد. پس از فراهم‌شدن مبلغ، فرستنده اقدام به طراحی بخش خروجی تراکنش و ارسال مبلغ می‌کند. برای ارسال تراکنش‌ها روی شبکه، باید تراکنش‌ها را تبدیل به سریال نمود. این سریال‌ها فرمت داخلی ساختار داده (Datastructher) را تبدیل به فرمتی می‌کند که بتوان آن را بایتی منتقل نمود که به آن «استریم‌بایت» گفته می‌شود. استریم‌بایت‌ها از طریق فرایند بازگشت سریال‌سازی به داده‌های اولیه قابل تبدیل هستند.

هر خروجی تراکنش شامل دو بخش است. یک مبلغ بیت‌کوین بر حسب ساتوشی و دیگری هم یک معمای رمزنگاری که شرایط لازم برای خرج‌کردن خروجی را معین می‌کند. به این معما «اسکریپت قفل‌کننده» یا «اسکریپت شاهد» اطلاق می‌شود. در شکل ۳ کیف پول برای خرج بیت‌کوین، دو تراکنش خروجی ایجاد کرده است که میزان هر کدام مقابل عبارت value درج شده و «ScriptPubKey» نیز معمای رمزنگاری است (Antonopoulos, 2017, pp.119-123).

"vout[:"
}
"value": 0.01500000,
"scriptPubKey": "OP_DUP OP_HASH160 ab-
68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_
EQUALVERIFY
OP_CHECKSIG"
,{
}
"value": 0.08450000,
"scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb-
68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERI-
FY OP_CHECKSIG,"
{

شکل ۳: (Antonopoulos, 2017, p.119)

حال به بخش ورودی تراکنش می‌رویم. هر سریال ورودی شامل ۴ بخش است. بخش نخست هشی که اشاره به خروجی‌های خرج‌نشده‌ای که کنار هم قرار گرفتند، دارد. بخش دوم شماره ترتیبی که محل این خروجی‌های خرج‌نشده در بلاک‌چین را نشان می‌دهد. بخش سوم یک کد اسکریپت یا همان امضای دیجیتال گیرنده و کلید عمومی فرستنده و نیز یک بخش فنی دیگر است که همه اینها تبدیل به سریال می‌گردند. سریال در بخش ورودی در حقیقت پاسخ معمای رمزنگاری مطرح‌شده توسط مالک قبلی است که در اینجا و از طریق امضای دیجیتال مالک جدید حل می‌شود (Antonopoulos, 2017, pp.123-126).

"vin] :"
}
"txid": "7957a35fe64f80d234d76d83a2a8f1a-
0d8149a41d81de548f0a65a8a999f6f18,"
"vout": 0,
"scriptSig: "
3045022100884"d142d86652a3f47ba4746ec719bbfb-
d040a570b1deccbb6498c75c4ae24cb02204
b9f039ff08df09cbe9f6addac960298cad530a863ea8f-
53982c09db8f6e3813 [ALL]
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e-
7ade8416ab9fe423cc5412336376789d1
72787ec3457eee41c04f4938de5cc17b4a10fa336a-
8d752adf,"
{
"sequence": 4294967295
,[

شکل ۴: (Antonopoulos, 2017, p.126)

در شکل ۴ یک شناسه ارجاع به تراکنشی که مبلغ خرج‌نشده مورد نیاز را دارد «txid»، یک اندیس خروجی تراکنش «vout» که مشخص می‌کند در تراکنش منتخب کدام مبلغ مدنظر است و اندیس صفر یعنی اولین مبلغ تراکنش مدنظر است، یک بازکننده قفل «scriptSig» داریم که حل‌کننده معمای رمزنگاری است و در نهایت یک شماره ترتیب «sequence» وجود دارد.

مرحله دوم: انتشار اطلاعات در شبکه

پیام‌ها به شکلی شایعه‌وار منتشر می‌شوند (Nakamoto, 2008). هر گره بیت‌کوین تراکنشی که دریافت می‌کند را قبل از ارسال به دیگران به صورت مستقل اعتبارسنجی می‌کند (Balamurugan et al, 2023, p.79). گره‌ها تراکنش‌ها را بر اساس معیارهای ذیل دسته‌بندی می‌کنند تا تنها تراکنش‌های معتبر در شبکه منتشر شوند.

الف) ساختار دستوری و ساختمان داده تراکنش باید درست باشد و هر تراکنش ورودی باید مبتنی بر خروجی مورد ارجاعی باشد که پیش از این خرج نشده است؛ مگر اینکه از کوین‌هایی که به عنوان پاداش شبکه پرداخت شده‌اند استفاده کنند.

ب) برای هر تراکنش ورودی، اگر خروجی‌ای که توسط این ورودی به آن ارجاع شده در دیگر تراکنش‌های لاگ وجود داشته باشد، آن تراکنش مردود می‌شود.

ج) قابل شناسایی بودن هر پیام به واسطه اثر انگشت دیجیتالی مختص به خود سبب می‌شود که گره‌ها بتوانند به‌سادگی پیام‌های تکراری دریافتی را تشخیص دهند و نادیده بگیرند (Antonopoulos, 2017, p.215).

گام دوم درج تراکنش در بلاک

ساختار بلاک

بلاک یک ساختار داده‌ای است که برای نگهداری مجموعه‌ای از تراکنش‌ها استفاده می‌شود و به تمام گره‌های شبکه توزیع می‌گردد (Balamurugan et al, 2023, p.77). هر گره تراکنش‌های دریافتی را پیش از ثبت در بلاک در مخزن تراکنش‌های تأییدنشده (لاگ) خود ذخیره می‌کند. چنانچه یک بیت‌کوین دوبار خرج گردد، اولین تراکنش بر حسب برچسب زمانی معتبر است و تراکنش‌های دیگر فاقد اعتبار هستند (Nakamoto, 2008).

زمان و مقدار هر تراکنش همراه با آدرس‌های بیت‌کوین آنها به‌طور دائم

در بلاک‌ها ثبت می‌شوند و برای همه رایانه‌ها قابل مشاهده هستند؛ اما اطلاعات شخصی طرفین قابل نمایش نمی‌باشد (Girasa, 2023, p.37).

بلاک‌ها تراکنش‌ها را در بدنه خود ثبت می‌کنند. هر بلاک علاوه بر بدنه، دارای یک شمارنده تراکنش و یک هدر یا همان سرایند است. هر بلاک بدون درج داده دارای ۴ کیلوبایت حجم و سرایند آن ۸۰ بایت حجم دارد. با توجه به اینکه هر تراکنش ۲۵۰ بایت دارد و یک بلاک به‌طور میانگین شامل ۵۰۰ تراکنش می‌باشد، بنابراین سرایند یک‌هزارم بلاک کامل است (Antonopoulos, ۲۰۱۷, p.۱۹۵).

جدول ۵: ساختار یک بلوک

Size	Field	Description
bytes ۴	Block Size	The size of the block, in bytes, following this field
bytes ۸۰	Block Header	Several fields form the block header
bytes ۹ـ۱ ((Varlnt	Transaction Counter	How many transactions follow
variable	Transactions	The transactions recorded in this block

منبع: (Antonopoulos, 2017, p.224)

سرایند بلوک

مجموعه‌ای مرکب از ۵ فراداده است: هش بلوک قبلی، مهر زمانی ایجاد بلوک، سطح دشواری، ریشه درخت مرکل و نانس (Antonopoulos, 2017, p.227).

هش بلوک قبلی این امکان را به ما می‌دهد که پیشینه تراکنش‌ها را در نظر داشته باشیم. مهر زمانی ایجاد بلوک مانع از دوبار خرج کردن می‌شود (Bon-neau, et al, 2015). سطح دشواری بلوک به میزان صفرهای وابسته ابتدای هش گفته می‌شود. سطح دشواری با ارتقای توان پردازش شبکه افزایش می‌یابد تا روند استخراج بیت‌کوین با سرعت ثابت ادامه پیدا کند. به سطح دشواری

بلاک مقدار آستانه و یا مقدار هدف گفته می‌شود (Pinna & Ruttenberg, 2016). ریشه درخت مرکل نیز چکیده تراکنش‌های بلاک است.

هش بلاک قبلی و سطح دشواری بلوک، زمان تشکیل و ریشه درخت مرکل غیرتصادفی هستند؛ ولی نانس یک عدد کاملاً تصادفی است که فقط از طریق آزمون‌وخطا می‌توان به آن دست یافت و باید به‌گونه‌ای باشد که وقتی کنار اعداد دیگر سرایند قرار گیرد، هش مزبور کمتر از سطح دشواری بلوک باشد (Girasa, 2023, p.38). نانس تنها یک‌بار تولید و یک‌بار استفاده می‌شود (Bashir, 2018, p.21).

جدول ۶: ساختار سرایند بلوک

Size	Field	Description
۴bytes	Version	A Version number to track software/ protocol upgrades
۳۲bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
۳۲bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
۴bytes	Timestamp	The approximate creation time of this block ((seconds from Unix Epoch
۴bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
۴bytes	Nonce	A counter used for the Proof-of-Work algorithm

منبع: (Antonopoulos, ۲۰۱۷, p.۲۲۷)

الگوریتم اثبات کار

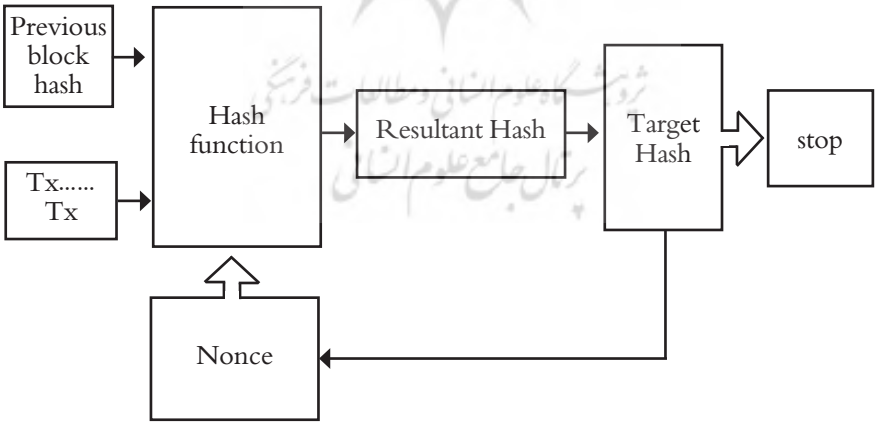
اثبات کار را اولین بار رمزنگار بریتانیایی به نام *آدام* بک در سال ۱۹۹۶ آزمایش کرد تا بتواند با ایمیل‌های اسپم مقابله نماید. اگرچه این نظریه برای ارسال ایمیل با شکست مواجه شد، اما بعدها توسط ساتوشی مورد

استفاده قرار گرفت. اثبات کار از لحاظ اقتصادی هزینه ورود اطلاعات غلط را افزایش می‌دهد (وانگ، ۱۴۰۱، ص۲۸ـ۲۹). این الگوریتم به صورت خلاصه دارای فرایند ذیل است.

تراکنش‌های جدید به تمام گره‌های شبکه پخش می‌شود و پس از دریافت تراکنش‌ها در لاگ گره ذخیره می‌شوند.

- هر گره تراکنش‌ها را در یک بلوک کاندید جمع‌آوری می‌کند.
- گره‌ها بلوک‌های نامزد را به شبکه پیشنهاد می‌کنند.
- ماینرها هش بلوک جدید را ایجاد می‌کنند.
- هش حاصل در برابر مقدار هدف یعنی سختی شبکه بررسی می‌شود (Bashir, 2020, p.171). اگر هش حاصل کمتر از مقدار هدف باشد، آن‌گاه اثبات کار حل شده است، در غیر این صورت نانس افزایش می‌یابد و گره دوباره تلاش می‌کند. این فرایند تا زمانی ادامه می‌یابد که هش حاصل کمتر از هدف پیدا شود.

شکل ۷: الگوریتم اثبات کار



منبع: (Bashir, 2020, p.171)

پرداخت پاداش

همین که یک گره به نانس دست یافت، موفقیت خود را به همگان اعلام می‌کند. گره‌های دیگر ادعای وی را بررسی می‌کنند تا در صورت عدم صحت ادعا، بار دیگر برای یافتن نانس تلاش کنند. زمانی که بیش از پنجاه درصد گره‌ها ادعای وی را تأیید کنند، بلوک ساخته‌شده توسط وی در شبکه ثبت می‌شود و پاداش ساخت بلوک به وی تعلق می‌گیرد (Pinna & Ruttenberg, 2016).

این مفهوم در دفتر کل ذیل فرایند تراکنش انگیزشی از مؤلفه پردازش قرار می‌گیرد. پس از تأیید بلاک جدید، بلافاصله هر گره، تراکنش‌های موجود در لاگ خود را با تراکنش‌های بلاک جدید مقایسه می‌کند و اقدام به حذف موارد تکراری می‌نماید. تراکنش‌های باقیمانده تراکنش‌هایی هستند که هنوز ثبت نشده‌اند و منتظر ثبت‌شدن در یک بلاک جدید هستند (Antonopoulos, 2017, p.224).

گره‌های کامل شروع به ایجاد بلاک نامزد و قراردادن تراکنش‌ها در این بلاک و شروع مسابقه برای یافتن نانس می‌کنند. اولین تراکنشی که در هر بلاک قرار می‌گیرد دربردارنده جایزه استخراج بلاک است که شامل جایزه شبکه برای استخراج بلاک و کارمزد پرداختی توسط طرفین تراکنش است (Balamurugan, et al, 2023, p.140). به این تراکنش، تراکنش کوین بیس گفته می‌شود. تراکنش کوین بیس یک آدرس بیت‌کوین دارد که کل مبلغ این تراکنش را به حساب مالک گره منتقل می‌کند (Antonopoulos, 2017, p.225).

گام سوم: اتصال بلاک‌ها در بلاک‌چین

گره‌های کامل بیت‌کوین برخلاف گره‌های دیگر، یک کپی کامل از بلاک‌چین از اولین بلوک که توسط مخترع بیت‌کوین ایجاد شده تاکنون را نزد خود نگه می‌دارند. با پیدایش بلاک جدید، بلاک‌چین محلی به‌طور

پیوسته به‌روزرسانی شده و زنجیره بلاک‌ها توسعه می‌یابد. با دریافت هر بلاک جدید از شبکه، گره کامل آن را اعتبارسنجی کرده و سپس این بلاک را به بلاک‌چین موجود متصل می‌کند. برای ایجاد اتصال گره کامل باید هش بلاک قبلی را در سرایند بلاک وارده بررسی کند؛ یعنی هشی که در سرایند بلاک جدید به عنوان هش بلاک قبلی قرار گرفته است، باید واقعاً هش بلاک قبلی باشد و در این صورت بلاک جدید توسط گره به انتهای بلاک‌چین خود اضافه می‌شود (Antonopoulos, 2017, p.200).

ممکن است گره دیگری برخی از این تراکنش‌ها و تراکنش‌های دیگر را جمع‌آوری نموده و بلاکی در همین زمان به شبکه ارائه می‌کند و گره‌های مجاور وی نیز آن را تأیید نموده و به شبکه بلاک‌چین خود می‌افزایند. در این حالت شبکه با خطر فروپاشی مواجه می‌شود. دو زنجیره مجزا روی یک بلوک در حال تشکیل است که فرایند اجماع را با خطر نابودی مواجه می‌سازد. بلاک‌چین‌های متعدد برای حل این معضل راهکارهای متعددی ارائه داده‌اند. راهکارهایی نظیر بلندترین زنجیره برای حل این معضل ارائه شده‌اند (درشر، ۱۴۰۱، ص۱۹۱). بلندترین زنجیره اثبات‌کننده کار بیشتر است (Balamurugan, et al, 2023, p.140).

در راهکار بلندترین زنجیره که متداول‌ترین راهکار حل معضل مزبور می‌باشد، هر گروهی که موفق شود اولین بلاک بعدی را بسازد، زنجیره بلندتر را شکل داده و کل گره‌های شبکه موظف هستند که این زنجیره را زنجیره اصلی حساب کنند. به صورت نادر اتفاق می‌افتد که هر دو زنجیره بلوک بعدی را هم باهم استخراج کنند. در این حالت معیار بلندترین زنجیره به ساخت سریع‌تر بلوک بعدی منتقل می‌گردد. در حالتی که زنجیره اصلی تعیین شد، بلاک‌های زنجیره دیگر مردود می‌شوند و تراکنش‌های آنها نیز جزء تراکنش‌های ثبت‌نشده محسوب می‌شوند و به مخزن تراکنش برگردانده می‌شوند (Antonopoulos, 2017, p.240-246).

بررسی قماری‌بودن لایه شبکه

درگام اول که روی‌دادن تراکنش است، فردی ضمن خرید کالا به فروشنده بیت‌کوینی به عنوان ثمن معامله پرداخت می‌کند و با استفاده از کیف پولی که مبتنی بر هش و رمزنگاری عمل می‌کند اقدام به انتقال پول به کیف پول فرد مقابل می‌کند. کیف پول‌ها برای ثبت تراکنش در شبکه و رسمیت‌بخشیدن به این انتقال اطلاعات تراکنش را به شبکه ارسال می‌کنند و تراکنش‌ها پس از اعتبارسنجی بر اساس اصولی که ذکر شد در شبکه به عنوان تراکنش تأییدشده منظور می‌شدند. در هیچ کجای روند تاکنون با مغالبه و تلاش برای پیروزی بر رقیب مواجه نیستیم؛ لذا قمار تا بدین جا قابل طرح نمی‌باشد.

اولین جایی که در معاملات مبتنی بر بیت‌کوین با رقابت مواجه می‌شویم، هنگام تلاش برای ثبت تراکنش‌ها در بلاک‌ها و رقابت بر سر به‌دست‌آوردن نانس می‌باشد. پس عنصر مغالبه یا همان تلاش برای پیروزی بر رقیب وجود دارد؛ اما عنصر مراهنه اگر به معنای گروگذاری و شرط‌بندی طرفینی باشد، در اینجا وجود ندارد؛ چون طرفین در صورت پیروزی به پاداش شبکه و کارمزد اعطایی توسط کاربران می‌رسند، نه مالی که گره‌های رقیب به وی می‌دهند؛ اما بنا بر مبنای نظر امام راحل و تحقیق که رهان به معنای مطلق وجود عوض از سوی هر کسی باشد، این عنصر نیز صادق است؛ اما امام راحل معتقدند که قید لعب نیز باید موجود باشد و در این مورد لعب صادق نیست؛ بنابراین تلاش برای استخراج نانس بنا بر نظر امام راحل مصداق قمار نیست و بنا بر مبنای تحقیق چون ثبت اطلاعات معاملات خدمتی واقعی است، رقابت بر سر آن مصداق جعاله محسوب می‌شود و ارتباطی با قمار ندارد.

در هنگامی که یک گره پولی را خرج کرد و سپس تراکنشی با دستمزد بالاتر انجام داد و هر دو را با زمان اندکی به شبکه فرستاد و تراکنش دوم

پذیرفته شد، در این مورد هم می‌توان بحث فروش مال غیر را مطرح نمود اما ارتباطی با قمار ندارد.

همچنین در صورت بروز انشعاب اگر معیار بلندترین زنجیره را اتخاذ کنیم، با وجود اینکه دو گره استحقاق مساوی دارند و این معیار ممکن است سبب تضییع حق یک یا چند گره گردد، اما به هر صورت در این حالت نیز قمار رخ نمی‌دهد و شاید بتوان مبنای فقهی این انتخاب را قرعه دانست؛ زیرا حل مشکل انشعاب که ناشی از تزاحم حقوق بین دو گره است مبتنی بر تصادف است و قرعه نیز مبتنی بر تصادف مشکلات را حل می‌کند و مورد قرعه به تعبیر امام راحل تنازع و تزاحم در حقوق است (امام خمینی، ۱۳۸۱، ص۳۹۹). نکته‌ای که قابل ذکر است، در قمار بدون وجود تزاحم حقوق از ابتدا بنا بر تصادف پاداش توزیع می‌گردد؛ اما در قرعه فقهی پس از بروز تزاحمات حقوقی در بخش واقعی و نبود هیچ‌گونه راه‌حل مشروع، قرعه لاجرم مطرح می‌گردد.

تلاش هکرها برای پیشی‌گرفتن از توان شبکه در خلق بلوک و ایجاد بلندترین زنجیره نیز فاقد عناصر اصلی قمار است و لذا قمار به حساب نمی‌آید.

لایه داده

لایه پروتکل نحوه عملکرد یک سیستم DLT را مشخص می‌کند. لایه شبکه لایه پروتکل را پیاده‌سازی می‌کند و لایه پروتکل و لایه شبکه در کنار هم پایه و اساس لازم برای لایه داده را تشکیل می‌دهند. این لایه دارای دو مؤلفه عملیات و ژورنال می‌باشد. مؤلفه عملیات شامل تمامی فرایندهایی می‌شود که از طریق آنها ژورنال و در نهایت دفتر کل با همکاری کاربران و در نتیجه تعامل آنها با سیستم ایجاد شده و تغییر می‌کند (Rauchs et al, 2018, p.66-69).

بررسی قماری‌بودن لایه داده

در این لایه مباحث حول منابع مجاز شبکه برای ارسال داده و مباحث مربوط به قراردادهای هوشمند مطرح می‌گردد که در بخش اول قمار اساساً قابل تصور نیست و بخش دوم نیز شامل مباحث قراردادهای هوشمند می‌گردد که ورود به سرفصلی مجزا و بسیار مفصل است که برای رعایت اختصار در این مقاله به آنها پرداخته نمی‌شود. پس بدون درنظرگرفتن مباحث مرتبط با قراردادهای هوشمند، مفهوم قمار در این لایه نیز قابل تصور نیست.

جمع‌بندی و نتیجه‌گیری

بیت‌کوین اولین رمزارزی است که با بهره‌گیری همزمان از مفاهیم شبکه همتا به همتا، اجماع توزیع‌شده، رمزنگاری، اثبات کار و ... توانست رمزارزی کاملاً غیرمتمرکز را ایجاد کند. صرف‌نظر از اینکه این رمزارزها منجر به خروج پول از عرصه مدیریت دولت‌ها می‌گردند و با توجه به سرمایه‌بربودن ایجاد آنها عملاً سرمایه‌داران بزرگ دنیا این‌گونه ارزها را کنترل می‌کنند که در فقه حکومتی و با دیدگاه کلان باید مورد بررسی قرار گیرند، این رمزارزها دارای مزایا و معایب متعددی هستند و پرسش‌های متعددی در مورد ابعاد فقهی آنها مطرح گشته است.

این تحقیق با شرح تفصیلی فرایند استفاده از رمزارزها و نگهداری اطلاعات این تراکنش‌ها به بررسی یکی از ابعاد فقهی در بخشی از رمزارزها که بر الگوریتم اثبات کار استوارند پرداخت و ضمن بررسی لغوی و فقهی مفهوم قمار، تأکید اصلی بخش فقهی تحقیق را بر اندیشه‌های فقهی امام خمینی مبتنی نمود و قمار را در دیدگاه امام راحل لعب به همراه مغالبه برای رسیدن به عوض معنا نمود و بنا بر مبنای تحقیق قید لعب خصوصیتی ندارد و قمار به معنای وسیع‌تری می‌باشد.

در نهایت با بررسی تفصیلی معاملات مبتنی بر بیت‌کوین به این نتیجه

رسید که بر مبنای امام راحل و نیز برداشت نگارنده از مفهوم قمار، در این دست رمزارزها آلودگی به قمار وجود ندارد. البته ممکن است با کنار هم قراردادن مفاهیمی مانند غرر که به معنای در معرض نابودی قراردادن مال از روی جهالت به ارکان ارزش‌گذاری در معامله است و اسراف که نابودکردن مال در اثر مصرف بی‌رویه است به همراه روایاتی که بر حفظ و تنمیه مال تأکید دارند و نیز قمار که در معرض نابودی قراردادن مال در امور بیهوده است، بگوییم که شارع راضی به ورود به هیچ نوع فعالیتی نیست که بدون دربرداشتن پیامد عقلایی و مشروع، سبب اتلاف مال مسلمان گردد و در موارد مانند روی‌دادن انشعاب در زنجیره بلاک‌چین، سبب واردشدن ضرر مالی قابل توجهی به فردی که زنجیره کوتاه‌تر را تشکیل داده است، می‌شود و بر این اساس استفاده از دفتر کل‌های مبتنی بر اثبات کار مشروع نیست؛ لکن ادعای مزبور نیز ارتباطی با قمار در فقه ندارد. درعین‌حال تحقیق در مورد مالیت بیت‌کوین، معاملات قمارگونه بیت‌کوین ناشی از سفته‌بازی بیش‌ازحد در این بازار و یا غرری‌بودن معاملات بیت‌کوین، به همراه بررسی احکام ثانویه در معاملات مبتنی بر این رمزارز بسیار ضروری است و بدون آن تحقیقات نمی‌توان دیدگاه روشنی از حکم فقهی بیت‌کوین را استخراج نمود.

منابع و مآخذ

* قرآن کریم.

ابن‌اثیر، مبارك‌بن‌محمد (۱۳۶۷). *النهایة في غریب الحدیث و الأثر*. قم، اسماعیلیان.

ابن‌فارس، احمدبن‌فارس (۱۴۰۴ق). *معجم مقاییس اللغة*. قم، مکتب الاعلام الاسلامی.

ابن‌منظور، محمدبن‌مکرم (۱۴۱۴ق). *لسان العرب*. ۱۵ج، بیروت، دار صادر.

احمدی، جواد (۱۴۰۱). *فقه رمزارزها* (ماهیت رمزارزها، احکام رمزارزها، بررسی فقهی ارز)؛ (تقریرات درس آیت‌الله سیدمحمدرضا مدرسی طباطبایی). قم، انتشارات حوزه‌های علمیه.

اردبیلی، احمدبن‌محمد (۱۴۰۳ق). *مجمع الفائدة و البرهان*. قم، دفتر انتشارات اسلامی.

ازهری، محمدبن‌احمد (۱۴۲۱ق). *تهذیب اللغة*. بیروت، احیاء التراث العربي.

انصاری دزفولی، مرتضی‌بن‌محمدامین (۱۴۱۱ق). *کتاب المکاسب*. قم، دارالذخائر

تاپ اسکات، دان، و تاپ اسکات، الکس (۱۳۹۹). *انقلاب بلاک‌چین*. ترجمه مازیار معتمدی. تهران، راه پرداخت.

جوهری، اسماعیل‌بن‌حماد (۱۳۷۶ق). *الصحاح*. بیروت، دار العلم للملایین.

حلبی، ابوالصلاح (۱۴۰۳ق). *الکافي في الفقه*. اصفهان، کتابخانه امیرالمؤمنین (ع).

حلّی (علامه)، حسن‌بن‌یوسف (۱۴۱۰ق). *إرشاد الاذهان*. قم، انتشارات اسلامی.

حلّی (علامه)، حسن‌بن‌یوسف (۱۴۱۴ق). *تذکرة الفقهاء*. قم، آل‌البیت (ع).

حلّی (علامه)، حسن‌بن‌یوسف (۱۴۲۰ق). *تحریر الأحکام الشرعیة*. قم، امام صادق (ع).

حلّی، ابن‌ادریس (۱۴۱۰ق). *السرائر*. قم، انتشارات اسلامی.

حلّی، محقق، جعفربن‌حسن (۱۴۰۸ق). *شرائع الإسلام في مسائل الحلال و الحرام*. قم، اسماعیلیان.

حمیری، نشوان‌بن‌سعید (۱۴۲۰ق). *شمس العلوم*. دمشق، دارالفکر.

خردمند، محسن (۱۳۹۸). بررسی فقهی استخراج و مبادله رمزارزها با تمرکز بر شبکه بیت‌کوین. *معرفت اقتصاد اسلامی*، ۱۰ (۲۰).

خمینی، سیدروح‌اللّه موسوی (۱۳۷۹ق). *کتاب البیع*. قم، مؤسسه تنظیم و نشر آثار امام (ره).

خمینی، سیدروح‌اللّه موسوی (۱۴۰۰). *موسوعة الإمام الخمینی*. قم، مؤسسه تنظیم و نشر آثار امام خمینی (ره).

خمینی، سیدروح‌اللّه موسوی (۱۴۱۵ق). *المکاسب المحرمة*. قم، مؤسسه تنظیم و نشر آثار امام (ره).

خمینی، سیدروح‌اللّه موسوی (۱۴۲۱ق). *تحریرالوسیله*. قم، مؤسسه تنظیم و نشر آثار امام (ره).

درشر، دانیل (۱۴۰۱). *مبانی بلاک‌چین، مقدمه‌ای غیرفنی در ۲۵ گام*. ترجمه سیاوش تفضلی. تهران، راه پرداخت.

دیلمی، حمزةبن‌عبدالعزیز سلاّر (۱۴۰۴ق). *المراسم العلویة و الأحکام النبویة*. قم، منشورات الحرمین.

رشید عوده، مرادرایق (۲۰۱۹). العملات الافتراضیه تکییفها الفقهی و حکم التعامل بها. *مجلة الجامعة الإسلامیة للعلوم الشرعیة بالمدینة المنورة*، ۱۸۹.

رضایی صدرآبادی، محسن، موسویان، سیدعباس، نوری، جواد، عیوضلو، حسین (۱۳۹۸). تحلیل فقهی اقتصادی استخراج ارزهای مجازی در نظام اقتصادی اسلام (مطالعه موردی بیت‌کوین). *معرفت اقتصاد اسلامی*، ۱۱ (۲۱).

زمخشری، محمودبن‌عمر (۱۳۸۶). *مقدمة الأدب*. تهران، مطالعات اسلامي دانشگاه تهران.

زمخشری، محمودبن‌عمر (۱۹۷۹م). *أساس البلاغة*. بیروت، دار صادر.

سمیران، محمدعلی صالح (۲۰۱۹م). ضوابط عملیة إصدار النقود العملات الرقمیة. فی کتاب *مؤتمر العملات الافتراضیة في المیزان*، الامارات، جامعه الشارقه.

صدوق، محمدبن‌علی (۱۴۱۵ق). *المقنع*. قم، موسسه امام هادی.

طرابلسی، قاضی ابن‌براج (۱۴۰۶ق). *المهذب*. قم، انتشارات اسلامی.

طریحی، فخرالدین‌بن‌محمد (۱۳۷۵). *مجمع البحرین*. تهران، مرتضوي.

طوسی، ابوجعفرمحمدبن‌حسن (۱۳۸۷ق). *المبسوط فی فقه الإمامیة*. تهران، المکتبة المرتضویة.

طوسی، ابوجعفرمحمدبن‌حسن (۱۴۰۰ق). *النهایة في مجرد الفقه و الفتاوی*. بیروت، دارالکتاب العربي.

عاملی، شیخ حر (۱۴۰۹ق). *وسائل الشیعه*. قم، آل‌البیت.

عاملی، محمدبن‌مکی (۱۴۱۷ق). *الدروس الشرعیة في فقه الإمامیة*. قم، انتشارات اسلامی.

فاضل موحدی لنکرانی، محمد (۱۳۹۰). *تفصیل الشریعة*. تهران، مؤسسه تنظیم و نشر آثار امام خمینی (ره).

فروزان، بهروز (۱۳۹۵). *رمزنگاری و امنیت شبکه*. ترجمه احد درفشی چارطاق. تهران، مرتضی دشت.

فیروزآبادی، محمدبن‌یعقوب (۱۴۱۵ق). *القاموس المحیط*. بیروت، دارالکتب العلمیة.

فیومی، احمدبن‌محمد (۱۴۱۴ق). *المصباح المنیر*. قم، دارالهجرة.

قادرمرزی، امید (۱۳۹۸). *رمزنگاری RSA بر پایه پردازش موازی*. تهران، آفتاب گیتی.

کیدری، قطب‌الدین (۱۴۱۶ق). *إصباح الشیعة*. قم، امام صادق (ع).

مجلسی، محمدباقر (۱۴۰۶ق). *ملاذ الأخیار*. قم، کتابخانه آیةالله مرعشی.

مرتضی زبیدی، محمدبن‌محمد (۱۴۱۴ق). *تاج العروس*. بیروت، دارالفکر.

مصطفوی، حسن (۱۴۰۲ق). *التحقیق في کلمات القرآن الکریم*. تهران، مرکزالکتاب للترجمة والنشر.

مفید بغدادی، محمدبن‌محمد (۱۴۱۳ق). *المقنعة*. قم، کنگره جهانی هزاره.

مهنا، عبدالله علی (۱۴۱۳ق). *لسان اللسان*. بیروت، دار الکتب العلمیة.

میثمی، حسین، بیابانی، زینب (۱۳۹۹). تحلیل ماهیت، استخراج و مبادلهٔ انواع رمزارزها و توکن‌ها از منظر فقه اسلامی و قوانین کشور. تهران، گزارش کارشناسی پژوهشکده پولی و بانکی بانک مرکزی، pdf.۱۲۶/katalog/https://iaif.ir/images/SAADATI۱

نواب‌پور، علی‌رضا (۱۴۰۰). *دارایی دیجیتال، آشنایی با دفتر کل توزیع‌شده، توکن و رمزارز دیجیتال بانک مرکزی*. تهران، راه پرداخت.

وان لین وانگ، آریس (۱۴۰۱). *اقتصاد کریپتو*. ترجمه علی‌رضا نواب‌پور و محمدرضا قدوسی. تهران، راه پرداخت.

Antonopoulos, Andreas M. (2017). *Mastering Bitcoin Programming the Open Blockchain.* Sebastopol, O'Reilly Media.

Atzori, Marcella (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary*?. From https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Balamurugan, B. & Poongodi, T. & Manu, M. R. & Karthikeyan, S. & Sharma, Yogesh (2023).*Convergence of Blockchain, AI and IoT A Digital Platform*. london,CRC Press.

Bashir, Imran (2018). *Mastering Blockchain*. second Edition, Birmingham, packt.

Bashir, Imran (2020). *Mastering Blockchain*. Third Edition, Birmingham, packt.

Benos, Evangelos & Garratt, Rodney & Gurrola-Perez, Pedro (2017). *The economics of distributed ledger technology for securities settlement*. from https://www.researchgate.net/publication/323979798_The_Economics_of_Distributed_Ledger_Technology_for_Securities_Settlement.

Bonneau, Joseph & Millerx, Andrew & Clark, Jeremy & Narayanan, Arvind A. Kroll, Joshua & W. Felten, Edward (2015). *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. from https://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf.

Cindy Vestergaard (2021). *Blockchain for International Security The Potential of Distributed Ledger Technology for Nonproliferation and Export Controls*. Berlin, Springer.

Febriandika, Nur Rizqi, Sukmana, Raditya (2018). *crypytocurrency position in islamic financial system case study of bitcoin*. from https://pdfs.semanticscholar.org/3663/aa6340acc2a36a493fff0ec7843587afb34f.pdf

Girasa, Rosario (2023). *Regulation of Cryptocurrencies and Blockchain Technologies*. Second Edition, London, palgrave.

Glaser, Florian (2017). *Pervasive Decentralisation of Digital Infrastructures, A Framework for Blockchain enabled System and Use Case Analysis*. Frankfurt from https://www.semanticscholar.org/paper/Pervasive-Decentralisation-of-Digital-A-Framework-Glaser/859d0535e16095f274df-4d69df54954b21258a13.

Haq ,Hina Binte, Ali, Syed Taha (2018). *Navigating the Cryptocurrency Landscape: An Islamic Perspective*. From https://arxiv.org/abs/1811.05935

Ma'Sum Billah, Mohd, Mohammed, Amadu (2019). *Shari'ah Code of Ethics in Cryptocurrency*. from https://www.researchgate.net/publication/333846854_Shari'ah_Code_of_Ethics_in_Cryptocurrency.

Nakamoto, Satoshi (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. from https://bitcoin.org/bitcoin.pdf.

Oziev, Gapur , Yandiev, Magomet (2018). *Cryptocurrency Shari'ah Perspective*. from https://www.researchgate.net/publication/330441911_Cryptocurrency_from_a_shari'ah_perspective.

Pinna, Andrea & Ruttenberg, Wiebe (2016). *Distributed ledger technologies in securities post-trading. Revolution or evolution?*. Frankfurt, European Central Bank, European Central Bank, From www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

Rauchs, Michel & Glidden, Andrew & Gordon, Brian & Pieters, Gina & Recanatini, Martino & Rostand, François & Vagneur, Kathryn & Zhang, Bryan (2018). *Distributed Ledger Technology Systems A Conceptual Framework*. Lo Cambridge University Pressndon, from https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf.

Ren, Wei & W. Beard, Randal (2008). *Distributed Consensus in Multi-vehicle Cooperative Control, Theory and Applications*. Berlin, Springer.

Treiblmaier, Horst & Clohessy, Trevor (2020). *Blockchain and Distributed Ledger Technology Use Cases Applications and Lessons Learned*. Berlin, Springer.

Yuneline, Mirza (2019). *Analysis of cryptocurrency's characteristics in four perspectives*. from https://www.researchgate.net/publication/334986357_Analysis_of_cryptocurrency's_characteristics_in_four_perspectives.

Zulkhibri, Muhamed (2019). *Halal Cryptocurrency and Financial Stability*. from https://www.researchgate.net/publication/333852858_Halal_Cryptocurrency_and_Financial_Stability.