

تحلیل فقهی کارکردهای پول‌های رمزنگاری شده (مورد مطالعه بیت کوین)

تاریخ پذیرش: ۱۳۹۷/۰۴/۰۹

تاریخ دریافت: ۱۳۹۷/۰۲/۰۱

علیرضا نواب پور *

احمدعلی یوسفی **

محمد طالبی ***

چکیده

از سال ۲۰۰۹ شکل نوینی از پول در عرصه اقتصاد دنیا تحت عنوان «پول رمزنگاری شده» به وجود آمد. این وسیله مبادله از دسترس سیستم بانکی و بانک مرکزی خارج است و تنها از طریق فضای مجازی منتقل می‌شود. با فراگیر شدن این نوع پول در رفتارها و روابط اقتصادی، یک تحول جدی در ماهیت و کارکرد اقتصادی پول ایجاد می‌شود. تغییر در ماهیت و کارکرد اقتصادی ممکن است کارکرد فقهی متفاوتی نسبت به پول بانکی به دنبال داشته باشد؛ بنابراین لازم است دستگاه فقه ماهیت و کارکردهای اقتصادی این پدیده را با دقت شناسایی نماید و احکام مجاز و غیر مجاز به کارگیری آن را در روابط اقتصادی روشن کند. در پژوهش حاضر ابتدا موضوع شناسی پول‌های رمزنگاری شده صورت پذیرفته، سپس ابعاد فقهی موضوع با دو رویکرد فقه فردی و حکومتی و همچنین در دو سطح معامله و معدن کاوی تبیین گشته است. در آخر نیز با استفاده از روش تحقیق اجتهاد چندمرحله‌ای و نظر خبرگان مالی اسلامی و مراجع عظام تقلید شروط جواز استفاده از پول‌های رمزنگاری شده احصا گردیده است. بر این اساس یکی از انواع این پول‌ها (بیت کوین) با شروط تطبیق داده و وجود شبهه «لا ضرر»، استفاده از آن را با اشکال فقهی روبه‌رو نموده است.

واژگان کلیدی: پول رمزنگاری شده، زنجیره بلوکی، بیت کوین، بلاک چین.

طبقه‌بندی JEL: E49

*. کارشناسی ارشد رشته معارف اسلامی و مدیریت مالی دانشگاه امام صادق (ع) (مقاله مستخرج از پایان‌نامه

Email: alireza.navabpour@gmail.com.

کارشناسی ارشد) (نویسنده مسئول).

Email: economy.islamic@gmail.com.

***. دانشیار پژوهشگاه فرهنگ و اندیشه اسلامی.

***. دانشیار دانشکده معارف اسلامی و مدیریت مالی دانشگاه امام صادق (ع).

Email: mohammad63.mt@gmail.com.

مقدمه

پس از بحران ۲۰۰۸ در سال ۲۰۰۹ فرد یا گروهی ناشناس با اسم مستعار ساتوشی ناکاماتو پولی کاملاً مجازی (غیر فیزیکی) و خصوصی بدون نیاز به نهاد ناظر، واسط و مرکزی به نام بیت‌کوین - یک نوع پول رمزنگاری شده - را به دنیا معرفی کرد.

ویژگی اصلی این پول این است که هیچ نفر سوم در سازوکار پولی آن دخالت ندارد اعم از خلق پول و اعمال انواع سیاست‌های پولی دیگر که گاهی به ضرر عموم مردم است و ارزش پول مردم را کاهش می‌دهد. این ویژگی پول رمزنگاری شده تداعی‌کننده نظام پولی طلا و نقره است. در واقع پول رمزنگاری شده یک سیستم خصوصی و فردبه‌فرد برای تسهیل انجام مبادلات بین افراد است، بدون آنکه نیازی به حضور نهاد مرکزی و واسط باشد (He et al, 2016, p.5).

پول‌های رمزنگاری شده با پول دیجیتال سنتی موجود در حساب بانکی افراد نیز به لحاظ خاصیت ضد تورمی بیت‌کوین که توسط سرمایه بازار ۲۱ میلیونی پشتیبانی می‌شود تفاوت دارد. بسیاری از اقتصاددانان بر این باورند که این مزیت بزرگی است؛ زیرا این سبب می‌شود که قدرت خرید معمولاً بالا رود (Caetano, 2015). در این سیستم خلق پول از طریق قرض‌دهی و قرض‌گیری نهاد سپرده‌پذیر نیز وجود ندارد؛ چراکه فلسفه این پول بر مبنای حذف شخص ثالث بنا شده و اگر فرض شود که چنین نهادی تأسیس گردد ماهیت موضوع تغییر خواهد کرد. هم اکنون نیز در دنیا، تجهیز و تخصیص منابع در نظام پول رمزنگاری شده به صورت فردبه‌فرد انجام می‌شود.

در حال حاضر پول‌های رمزنگاری شده و فناوری مرتبط با آن (زنجیره بلوکی) به سرعت در حال فراگیر شدن هستند و ارزش بازار آنان به ۵۶۰ میلیارد دلار رسیده است*؛ لذا بر همه مسلمانان و بالخصوص شیعیان لازم است که تکلیف شرعی خود را در قبال استفاده از این فناوری و پول‌های نوین بدانند.

این پژوهش از مطالعات آغازین در حوزه بررسی فقهی پول‌های رمزنگاری شده در جهان تشیع محسوب شده که با روش اجتهاد چندمرحله‌ای و استفاده از نظر خبرگان مالی

*. این آمار مربوط به تاریخ ۱۳۹۶/۱۱/۰۲ است.

اسلامی و مراجع تقلید اقدام به استخراج حکم فقهی این پدیده مستحدثه نموده است. مقاله پیش رو پس از بررسی پیشینه پژوهش و بیان اجمالی واژه‌شناسی پول‌های رمزنگاری‌شده به تبیین سازوکار فنی آنها پرداخته و در آخر، این پدیده مستحدثه از منظر فقه شیعه مورد مذاقه قرار گرفته است.

پیشینه پژوهش

مرکز پژوهش‌های مجلس (۱۳۹۳) در گزارش خود پس از بیان اجمالی تاریخچه بیت‌کوین به بیان سازوکار آن بدون نیاز به بانک مرکزی پرداخته و در آخر تجربه قانونگذاری سه کشور آمریکا، آلمان و چین را بیان نموده است که در قوانین خود بیت‌کوین را به مثابه یک کالا در نظر گرفته‌اند.

سیدحسینی و دعایی (۱۳۹۳) در مقاله خود پس از بیان تاریخچه و تبیین مبانی فنی بیت‌کوین به فرصت‌ها و چالش‌های پول رمزنگاری‌شده پرداخته‌اند. آنان مهم‌ترین چالش این پول‌ها را بحث قانونگذاری دانسته و کشورها را بر اساس رویکرد خویش نسبت به بیت‌کوین به چهار دسته تقسیم‌بندی نموده‌اند: دسته اول، کشورهایی که منع قانونی ندارند و عمدتاً در حال تدوین قوانین و مقررات هستند؛ مانند قاره آمریکا به جز مکزیک؛ دسته دوم، کشورهایی که نسبت به بیت‌کوین بدبین بوده و مردم را از آن نهی کرده و به دنبال وضع قوانینی جهت جلوگیری از آن هستند؛ مانند مکزیک؛ دسته سوم، کشورهایی هستند که استفاده از بیت‌کوین را غیر قانونی شمردند؛ مانند ویتنام و ایسلند و دسته چهارم نیز کشورهایی هستند که هنوز موضع مشخصی در این خصوص نگرفته‌اند؛ مانند ایران.

سلیمانی‌پور (۱۳۹۶) ابتدا به موضوع‌شناسی پول مجازی پرداخته سپس آن را مورد بررسی فقهی قرار داده است. او با پذیرش نظریه «اعتباری بودن پول» به استفاده از پول‌های رمزنگاری‌شده مشروعیت داده و تنها نقطه چالش‌برانگیز آن را ایجاد اختلال در اقتصاد معرفی می‌کند. با این توضیح که اگر استفاده از این پول‌ها منجر به صدمه به اقتصاد عمومی کشور شود بر اساس قاعده «لا ضرر» استفاده از آن از دیدگاه فقه جایز نخواهد بود.

ایوانز (۲۰۱۵) در مقاله اخیر خود به بررسی جایگاه بیت‌کوین در بانکداری اسلامی پرداخته است. اعتقاد وی بر این است که بیت‌کوین با قاعده «ممنوعیت ربا» در اسلام

نسبت به پول‌های حاکمیتی تطابق بیشتری دارد. او بیان می‌کند در پول‌های حاکمیتی با پدیده خلق پول و به تبع آن کاهش ارزش پول مواجه هستیم و این امکان وجود ندارد که اگر کسی صد دلار قرض نماید به همان میزان پس دهد؛ چراکه ارزش صد دلار با مرور زمان و خلق پول توسط دولت تغییر نموده است؛ اما این مسئله (خلق پول و کاهش ارزش پول) در بیت‌کوین وجود ندارد و فقط با مرور زمان استخراج می‌گردد - همانند طلا - و اصل منبع آن یعنی ۲۱ میلیون ثابت است و خاصیت ضد تورمی دارد.

برگستر (۲۰۱۵) در مقاله خود پس از بیان الزامات مالی اسلامی که متشکل از پنج اصل ممنوعیت ربا، ضرر، غرر، اکل مال به باطل و وجود شیء حقیقی در دو طرف معامله است، دو مطلب را بیان می‌دارد: اول، آنکه با توجه به معین بودن تعداد کل بیت‌کوین‌ها (۲۱ میلیون) پرداخت بهره در این سیستم موضوعیتی نخواهد داشت؛ دوم، آنکه عملیات معدن‌کاوی در بیت‌کوین به هیچ وجه شبیه به قمار نیست.

مفتی فراز آدم (۲۰۱۷) در یک گزارش که در سایت خود منتشر کرده است (<http://darulfiqh.com/>) تحت عنوان «تحقیق بر روی پول و بیت‌کوین بر اساس قوانین اسلامی و اقتصاد» به بررسی این سؤال پرداخته است که آیا بیت‌کوین بر اساس معیارها و قوانین اسلامی به عنوان یک پول مورد پذیرش قرار می‌گیرد یا خیر؟ او در پاسخ به این نتیجه می‌رسد که بر اساس قوانین اسلامی در حوزه پول، می‌توان بیت‌کوین را یک پول اسلامی محسوب نمود. وی در نهایت بیت‌کوین را به عنوان یک پول که همه شاخصه‌های یک پول اسلامی را داراست، می‌پذیرد و به گسترش ابزارهای مالی اسلامی بر اساس بیت‌کوین توصیه می‌کند.

میرزاخانانی (۱۳۹۶) در گزارش خود معتقد است برای بررسی بیت‌کوین از منظر فقه باید آن را در دو سطح شخصی و حکومتی مورد تحلیل قرار داد. به اعتقاد وی آنچه در زمینه صحت شرعی بیت‌کوین بیشتر مورد اهمیت است، جنبه‌های فقه حکومتی از جمله قواعد فقهی لاضرر، اختلال نظام، اتلاف و عدالت است که باید آنها را در خصوص بیت‌کوین مورد تأمل قرار داد. وی با استناد به قواعد مذکور نتیجه گرفته است تا زمانی که سامانی از طرف حاکمیت برای کنترل پول‌های مجازی در اقتصاد واقعی ترتیب داده نشده است، باید از ورود پول‌های مجازی در دنیای حقیقی جلوگیری گردد.

ابوبکر (۲۰۱۸) در بررسی فقهی خود به بیان سیر تکاملی پول پرداخته سپس پول رمزنگاری شده را به عنوان جدیدترین نوع پول مورد مطالعه قرار داده است. وی در تحلیل فقهی خود به تبیین نظر اسلام در خصوص مالیت پرداخته و مالیت بیت‌کوین را بر این اساس اثبات کرده است. در آخر این گزارش نیز وی به تمام شبهات مخالفان پاسخ داده و استفاده از بیت‌کوین را حلال می‌شمارد (blossomfinance.com/bitcoin).

تفاوت اصلی پژوهش حاضر با مطالعات پیشین در وجود روش تحقیق علمی و قابل اتکا و همچنین بررسی جامع ابعاد فقهی پول‌های رمزنگاری شده است.

روش تحقیق

در این پژوهش از روش تحقیق اجتهاد چندمرحله‌ای استفاده شده است. در این روش بعد از تحلیل تفصیلی موضوع، ابعاد فقهی مسئله به وسیله پژوهشگر بررسی می‌شود؛ سپس با شناسایی خبرگان مالی اسلامی، نظرهای تخصصی فقهی درباره مسئله مورد نظر دریافت شده و پس از پردازش اطلاعات، بحث‌ها جمع‌بندی می‌شود و در صورت اختلاف نظر، پژوهشگر به تبادل نظر بین خبرگان می‌پردازد. زمانی که پژوهشگر به اطمینان کافی رسید، با بیان نکته‌های حساس، مسئله را جهت استفتا به مراجع تقلید عرضه می‌کند و در صورت تأیید مراجع، پاسخ نهایی فقهی درباره مسئله مورد نظر به دست می‌آید. مراحل این روش عبارت‌اند از: موضوع‌شناسی، تعیین ابعاد فقهی، بررسی مستندات فقهی، تطبیق ابعاد فقهی موضوع با مستندات فقهی، انتخاب خبرگان فقهی - مالی، گردآوری و جمع‌بندی نظرات خبرگان فقهی و مالی و دریافت آرای مراجع عظام تقلید (موسویان و خوانساری، ۱۳۹۵).

مبانی نظری

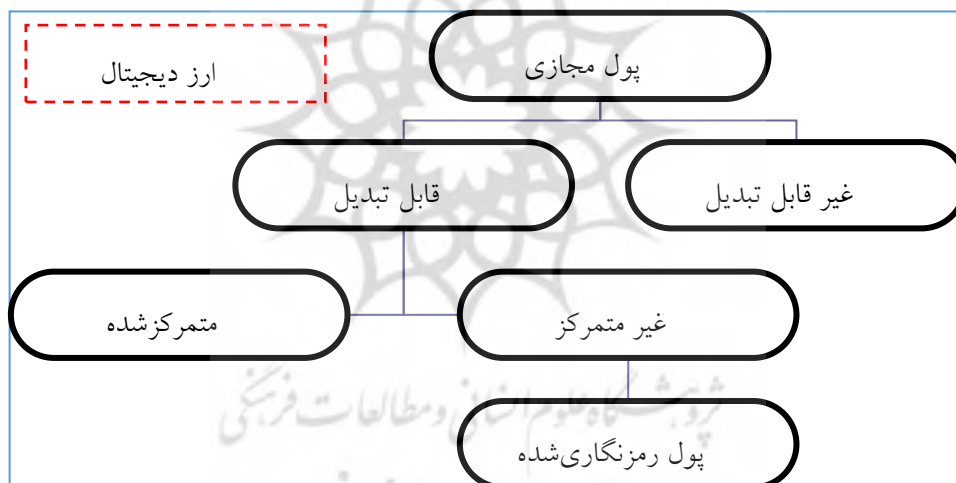
اولین قدم برای بررسی فقهی یک پدیده مستحدثه، موضوع‌شناسی است. بدین منظور در ادامه ابتدا به جایگاه پول رمزنگاری شده در میان انواع پول‌های دیجیتال پرداخته شده و سپس سازوکار فنی آن به‌طور تفصیلی بیان می‌گردد.

۱. انواع پول مجازی

با گسترش فناوری اطلاعات، پول الکترونیکی (دیجیتال) پا به عرصه اقتصاد گشود که ماهیت آن همان اسکناس‌های کاغذی است؛ اما از حالت فیزیکی و ملموس به یک سری اعداد و ارقام داخل کامپیوتر و شبکه تبدیل شده است؛ به عبارتی پول‌های الکترونیک یا دیجیتال، مکانیسمی جدید در پرداخت اسکناس‌های متداول بانکی هستند؛ اما در سال‌های اخیر، انواعی از پول‌ها پدید آمدند که ذاتاً با اسکناس‌های بانکی بدون پشتوانه (Fiat Money) تفاوت می‌کنند و یک واحد سنجش جدید را با سازوکاری کاملاً متفاوت و منحصر به فرد به نام «پول‌های مجازی» با خود به همراه آورده‌اند (Chuen, 2015, p.8).

پول مجازی یک مفهوم عام برای انواع گوناگونی از پول‌ها است که در شکل زیر شمای کلی آن آمده است.

شکل ۱. انواع ارز مجازی (IMF Staff, 2016, p.82)



همان‌گونه که در شکل ۱ مشخص است پول مجازی که غیر ملموس است ارز دیجیتال محسوب می‌شود و وجه تمایز آن بدین صورت است که پول دیجیتال نماینده اسکناس‌های بانکی می‌باشد که فقط سازوکار آن غیر فیزیکی است؛ در حالی که پول مجازی هیچ‌گونه ارتباطی با پول بانکی نداشته و یک پول جدید با سازوکار خاص است. البته گاهی در مقالات علمی به جای پول مجازی، پول دیجیتال به کار برده می‌شود؛ چراکه واژه «مجازی»، مفهوم منفی را در مقابل «حقیقی» به ذهن متبادر می‌کند (Chuen, 2015, p.8)؛ همچنین شکل ۱ گویای این مطلب است که پول مجازی به دو دسته «قابل تبدیل»

(Convertible) و «غیر قابل تبدیل» (Non-convertible) تقسیم می‌شود؛ پول‌های مجازی غیر قابل تبدیل به هیچ عنوان امکان تبدیل به پول‌های بانکی را ندارند؛ همانند پول‌هایی که در بازی‌های رایانه‌ای یا موبایلی کسب می‌شوند و فقط امکان خرج در همان بازی را دارند و اصطلاحاً به آنان «سکه بازی» (Game Coin) می‌گویند. این ارزها صرفاً به صورت متمرکز (Centralized) هستند یعنی یک نهاد مرکزی (به‌طور مثال سازنده بازی) آن را انتشار می‌دهد، قانون‌گذاری می‌نماید و دفتر کل را نزد خود نگاه می‌دارد که «E-gold» معروف‌ترین مثال از این دسته می‌باشد؛ اما در مقابل پول مجازی «قابل تبدیل» امکان تبدیل به پول‌های حقیقی و بالعکس را دارد و از آن برای خرید کالا و خدمات حقیقی و مجازی می‌توان بهره برد. این نوع از پول‌ها، رشد یافته‌ترین نمود از پول‌های مجازی است و بلوغ پول‌های مجازی را نشان می‌دهد (Chow and Guo, 2008, pp.2-4). این پول به دو دسته متمرکز و غیر متمرکز (Decentralized) تقسیم شده است. متمرکز بدین معناست که انتشار و کنترل ارز توسط یک نهاد مرکزی مانند «وب‌مانی» (Web Money) صورت می‌پذیرد. در مقابل پول مجازی غیرمتمرکز، به معنای انتشار و کنترل پول فارغ از کنترل و مدیریت نهاد مرکزی بوده و توسط کلیه افراد موجود در شبکه با به‌کارگیری علم رمزگذاری مدیریت می‌شود. به همین جهت به پول مجازی قابل تبدیل غیرمتمرکز، «پول رمزنگاری شده» می‌گویند؛ چراکه کلیه فرآیندهای آن از جمله ثبت و تأیید تراکنش‌ها به جای اینکه توسط نهاد مرکزی انجام گیرد از طریق افراد و با سازوکار علوم ریاضی و رمزنگاری صورت می‌پذیرد؛ تأمین امنیت این شبکه پولی غیرمتمرکز که فارغ از هرگونه نظارت و کنترل است، نیاز به یک سازوکار رمزنگاری شده دارد تا اعتماد افراد به آن جلب شود؛ به عبارت دیگر در سازوکار این پول نیاز به اعتماد به هیچ نهادی نیست و الگوریتم‌های ریاضی و رمزگذاری صحت معاملات را تأیید می‌نمایند و هیچ کاربری نمی‌تواند در شبکه تغییر ایجاد نماید.*

* جهت مطالعه بیشتر رک به:

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S; Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016 /Vasek, M.; The Age of Cryptocurrency, 2015.

می‌توان گفت یکی از انگیزه‌های اصلی اختراع این پول، غیر متمرکز بودن آن است؛ چراکه این پول در پی نارضایتی از دخالت نهاد مرکزی و ناظر در سیستم اقتصادی پدید آمد. بدین جهت مخترعان این پول در صدد آن بودند تبادلات مالی به صورت فردبه‌فرد، بدون دخالت هیچ نهاد واسطی انجام پذیرد که در این صورت هم هزینه مبادلات کاهش می‌یابد و هم سرعت انتقال افزایش پیدا می‌کند و مهم‌تر از همه کسی نمی‌تواند اقدام به چاپ بی‌رویه پول برای منافع خود نماید و ارزش پول را کاهش دهد. راه‌حل این مسئله اختراع یک پول غیر متمرکز، بر پایه انتقال فردبه‌فرد و متن‌باز (Open Source) بود که تحت نظارت و کنترل هیچ نهادی نباشد (Financial Action Task Force, 2014, p.5). نمونه موفق این پول، «بیت‌کوین» (BitCoin) است که ارزش بازار آن در تاریخ ۱۳۹۶/۱۱/۰۲، ۲۰۰ میلیارد دلار می‌باشد (https://coinmarketcap.com).

جدول ۱. واژه‌شناسی پول مجازی (Financial Action Task Force, 2014, p.8)

غیر متمرکز	متمرکز	
این پول هیچ نهاد مرکزی ندارد و نیاز به اعتماد به شخص ثالث نیست و استفاده‌کنندگان از این پول می‌توانند آن را از طریق صرافی‌ها به اسکناس بانکی تبدیل نمایند؛ مثال: پول رمزنگاری شده؛ مثال: بیت‌کوین و لایت‌کوین (Litecoin).	این پول دارای یک نهاد مرکزی است و استفاده‌کنندگان از این پول می‌توانند آن را از طریق صرافی‌ها به اسکناس بانکی تبدیل نمایند؛ مثال: وب مانی (Web Money).	قابل تبدیل
در حال حاضر وجود ندارد.	این پول دارای یک نهاد مرکزی است و استفاده‌کنندگان از این پول نمی‌توانند آن را به اسکناس بانکی تبدیل نمایند؛ مثال: سکه بازی (World of Warcraft).	غیر قابل تبدیل

۲. سازوکار فنی

بیت‌کوین همانند سایر پرداخت‌های دیجیتال همانند پی‌پل (PayPal) نیست که همان پول بدون پشتوانه (Fiat) را با مکانیسم دیجیتال منتقل و پرداخت کند؛ بلکه پول رمزنگاری شده به خودی خود پولی است که پشتوانه آن ملموس و فیزیکی نیست و در فضای دیجیتال

رقم می‌خورد که به نوعی کارکردهای اصلی اقتصادی پول را می‌تواند ایفا نماید (صندوق بین‌المللی پول، ۲۰۱۶).

در جدول زیر تفاوت‌های بیت‌کوین با پول حاکمیتی و شباهت آن با طلا ذکر شده است.

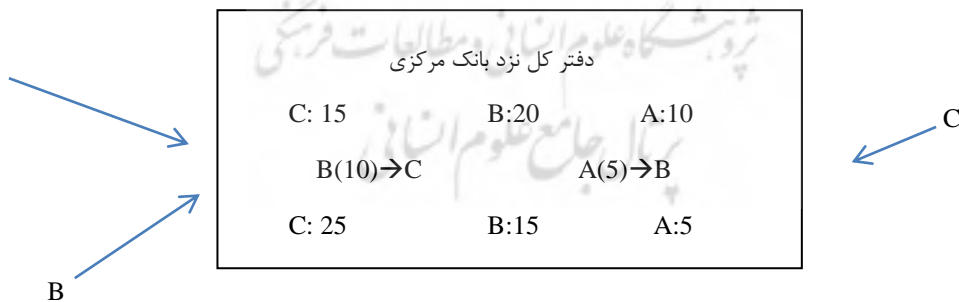
جدول ۲. تفاوت پول رمزنگاری‌شده با پول بانکی و شباهت آن با طلا

شباهت با طلا	تفاوت با پول بانکی
عدم وجود نهاد مرکزی، واسط و ناظر	عدم نیاز به نهاد مرکزی برای جابه‌جایی پول
محدود بودن منابع	عدم توانایی دخالت دولت در تولید و خلق پول
تولید پول به وسیله عملیات استخراج	مخفی ماندن هویت فرستنده و گیرنده
دولت هیچ دخالتی در خلق آن ندارد	تحت حمایت دولت نیست و پشتوانه دولتی ندارد
قیمت آن به وسیله عرضه و تقاضا کشف می‌شود	هزینه عملیاتی ناچیز در سطح بین‌المللی
	سرعت انتقال بالا در سطح بین‌المللی

۳. مشخصات فنی بیت‌کوین

برای فهم بهتر وجه تمایز پول بانکی با پول رمزنگاری‌شده به شکل زیر توجه شود.

شکل ۲. سازوکار نظام متمرکز



همان‌طور که در شکل بالا مشخص است، همه تراکنش‌ها در سیستم سنتی در یک دفتر کل تحت نظارت بانک مرکزی ثبت می‌شود و کسی نمی‌تواند پولی را که ندارد خرج کند و در سیستم‌های ثبتی تغییری ایجاد نماید؛ به‌طور مثال اگر A می‌خواهد پنج واحد پولی به B

بدهد ابتدا نهاد مرکزی بررسی می‌کند که آیا A در سابقه تراکنشی خود چنین پولی دارد یا خیر و اگر موجود بود، آن پول را از او کسر کرده و به B منتقل می‌کند. حال این وظیفه مهم یعنی ثبت، تأیید تراکنش و به‌روزرسانی حساب‌ها در نظام غیر متمرکز چگونه انجام خواهد شد؟

برای جبران نبود نهاد مرکزی در پول‌های رمزنگاری‌شده از دو ابزار فناوری اطلاعات استفاده شده است: اول، علم رمزنگاری (Encryption) برای تأیید صحت تراکنش‌ها و دوم، فناوری زنجیره بلوکی برای ثبت و به‌روزرسانی حساب‌ها است.

در بیت‌کوین کلیه تراکنش‌ها در یک دفتر کل نوشته می‌شود. این دفتر کاملاً شفاف بوده و در اختیار همگان قرار دارد و هر کسی در هر زمانی می‌تواند کلیه تراکنش‌های بیت‌کوین را از این طریق ردیابی کند. به این دفتر که برای همگان در دسترس است زنجیره بلوکی می‌گویند؛ این در حالی است که طرفین معامله با اسم واقعی خود در دفتر کل قابل ردیابی نیستند؛ بلکه از طریق رشته‌ای از حروف و اعداد نمایان هستند. دفتر کل توسط کلیه اعضای بیت‌کوین به‌روزرسانی می‌شود (Chuen, 2015).

وقتی یک تراکنش انجام می‌شود در دفتر کل، اطلاعات مقدار بیت‌کوین و فرستنده و گیرنده ثبت می‌شود که آدرس طرفین معامله به صورت رشته‌ای از ۲۶ الی ۳۵ حرف مشخص شده است. زمانی که فردی قصد دارد پرداخت خود را از طریق بیت‌کوین انجام دهد، اطلاعات تراکنش (مقدار بیت‌کوین و آدرس فرستنده) به همراه امضا* و کلید خصوصی (Private Key) به شبکه ارسال می‌شود؛ هرچند صد تراکنش (به اندازه یک مگابایت) در یک بلوک قرار می‌گیرند که به‌طور تصادفی یکی از تراکنش‌ها به عنوان «سر تیترا (Header)» معین می‌شود که باید به سایر بلوک‌ها اضافه شود؛ اما قبل از اتصال به سایر بلوک‌ها باید تأیید شود؛ این تأیید در سیستم سنتی توسط نهاد مرکزی صورت می‌پذیرفت و ابتدا حساب شما را بررسی می‌نمود که آیا موجودی کافی برای این تراکنش دارید یا خیر؛ در صورت وجود موجودی کافی، آن مبلغ از حساب شما کاسته و به حساب گیرنده

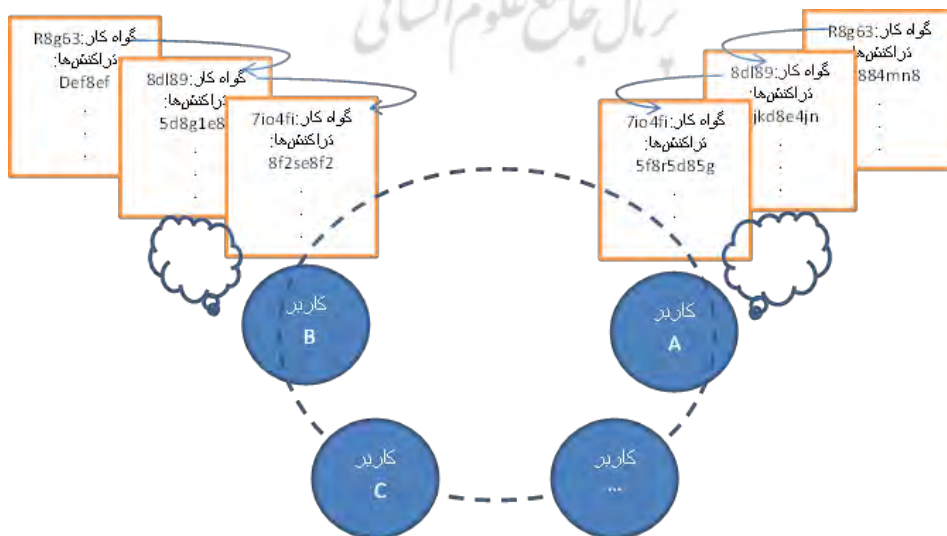
*. یک خلاصه‌سازی دیجیتالی است که با کدهای خصوصی و عمومی تولید شده تا گواهی باشد بر اینکه نقل‌وانتقال بیت‌کوین از یک آدرس خاص آمده است.

اضافه می‌گردید؛ اما در این سیستم معدن‌کاوان (Miners) می‌بایست سه عنصر را یعنی سر تیر، کد بلوک قبلی (کاراکترهای حاصل از عملیات هش) و به علاوه یک سری اعداد و ارقام دلخواه (Nonce) با عملیات درهم سازی (Hash) به یک سری اعداد و ارقام با طول مشخص و ویژگی مشخص تبدیل کنند. برنامه سیستم به گونه‌ای است که هر دفعه این مشخصات را معین می‌کند - مثلاً کاراکتری هفده رقمی باشد و با پنج تا صفر شروع شود که به تناسب شرایط شبکه، مشخصات آسان و سخت می‌شود به گونه‌ای که سرعت حل مسئله در محدوده ده دقیقه بماند - معدن‌کاوان برای اینکه بتواند هشی با آن ویژگی تولید نماید نمی‌تواند اطلاعات تراکنش‌ها و یا کد بلوک قبلی را تغییر دهد؛ بلکه باید آن اعداد دلخواه (Nonce) را آنقدر تغییر دهد تا به هش مورد نظر دست یابد و این می‌شود همان حل مسئله ریاضی که در بیت‌کوین مطرح می‌شود. اولین فردی (معدن‌کاوی) که بتواند تابع هش مورد نظر را بسازد یا به عبارت بهتر بتواند آن کاراکترهای «Nonce» را تشخیص دهد و معما را حل کند برنده پاداش بیت‌کوین خواهد بود (Kelly, 2014).

۲۲۳

در سیستم بیت‌کوین برای اینکه افراد انگیزه لازم را برای حل معما (معدن‌کاوی) و به تبع آن حفظ امنیت شبکه را داشته باشند به اولین کسی که معما را حل کند ۲۵ بیت‌کوین پاداش می‌دهد در واقع این سازوکار تولید و خلق بیت‌کوین جدید می‌باشد (اولین بیت‌کوین توسط خود برنامه ایجاد شد و پس از آن طبق همین سازوکار گسترش یافت). پاداش بیت‌کوین هر چهار سال یک‌بار نصف می‌شود تا مجموع بیت‌کوین‌ها در عدد ۲۱ میلیون متوقف گردد و بدین صورت منابع بیت‌کوین محدود است.

شکل ۳. ساختار زنجیره بلوکی



با توجه به مطالب فوق، در این سیستم همواره آخرین وضعیت دارایی افراد مشخص است و اگر بخواهد تغییری رخ دهد در قالب بلوک بعدی که توسط افراد «تأیید» شده است به بلوک‌های قبلی اضافه می‌گردد این تغییر پس از تأیید اکثریت در دفتر کلیه افراد اعمال می‌شود. تأیید بلوک منوط به سازگاری آن با بلوک‌های قبلی که حاوی مالکیت‌های افراد است می‌باشد (Chuen, 2015).

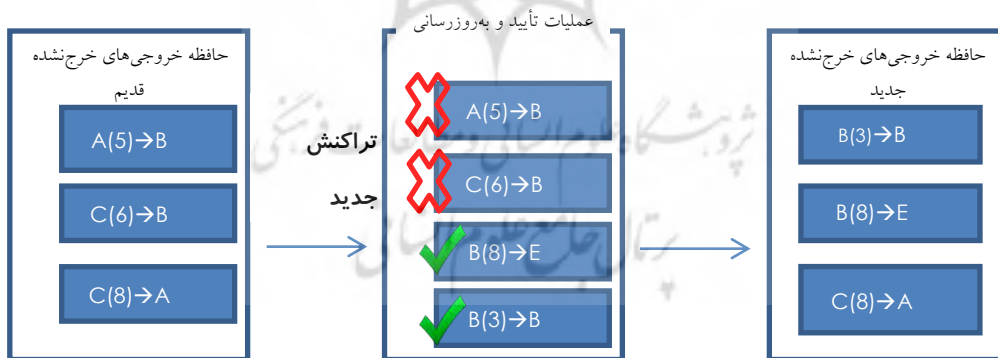
حال این سؤال مطرح می‌شود که چگونه تراکنش‌های مندرج در بلوک تأیید می‌شوند؟ همان‌طور که بیان شد، در این سیستم هویت فرستنده نامعلوم است؛ پس چگونه وقتی که می‌خواهد تراکنشی صورت بگیرد می‌توان بررسی نمود که آن شخص موجودی کافی برای پرداخت وجه را دارد یا خیر؟

در جواب این سؤال باید گفت در کنار زنجیره بلوکی، گره‌ها (Nodes) - که همان افراد مشارکت‌کننده در شبکه بیت‌کوین هستند - پایگاه داده‌ای دیگر به نام «حافظه خروجی‌های تراکنش‌های خرج نشده» را نگهداری می‌کنند. این پایگاه دفتر معینی است که وجوه موجود روی هر آدرس را ثبت و ضبط می‌کند. در اصل این پایگاه داده به عنوان ذخیره‌سازی موقت برای زنجیره بلوکی عمل می‌کند. این پایگاه داده بیشتر به پایگاه داده‌های مرکزی شبیه است که در قلب اکثر سیستم‌های متمرکز وجود دارد؛ البته روش ثبت در این پایگاه داده کاملاً با روش ثبت سیستم‌های سنتی مرکزی متفاوت است. در سیستم سنتی همیشه آخرین وضعیت دارایی افراد در آن به‌طور خالص (Net) مشخص است و هر تراکنشی که صورت می‌گیرد در دفتر کل بر خالص دارایی‌هایش اعمال می‌گردد؛ اما در سیستم غیر متمرکز بیت‌کوین، خروجی‌ها به‌طور مجزا ثبت می‌شوند.

به زبان ساده هر فردی در این سیستم یک کلید عمومی و خصوصی دارد. کلید عمومی همانند آدرس ایمیل است و مانعی برای فاش شدن آن نیست و کلید خصوصی همانند رمز ایمیل هست که فقط در اختیار صاحب حساب است و مجوز استفاده از حساب را می‌دهد. هنگامی که فردی خواهان واریز پول به فردی دیگر است، اطلاعات درخواست خود را شامل

مقدار بیت‌کوین و آدرس فرد مقابل (هش کلید عمومی)* به سیستم ارسال می‌کند. وقتی که این تراکنش جدید از طرف گره به شبکه ارسال می‌شود - و شامل مقدار بیت‌کوین، آدرس مقصد و کلید عمومی فرستنده که به وسیله کلید خصوصی رمز شده و کلید عمومی فرستنده به‌طور آزاد، می‌شود- نزدیک‌ترین گره، باید اعتبار آن را از دو جنبه تأیید کند: اول اینکه فرد فرستنده واقعاً خودش هست یا هکر؛ دوم اینکه آیا فرستنده چنین پولی در حساب خود دارد یا خیر؟ برای کار اول، آن گره می‌بایست ابتدا توسط کلید عمومی، رمز اطلاعات ارسالی را باز نماید، اگر در اطلاعات رمزگشایی شده آدرس کلید عمومی فرستنده موجود بود یعنی خود صاحب اصلی و دارنده کلید خصوصی آن را فرستاده است؛ چراکه تنها با کلید خصوصی می‌تواند از کلید عمومی رمزی (هش) ساخت که با کلید عمومی بتوان آن را رمزگشایی کرد و در آن کلید عمومی باشد؛ سپس اعتبار آن تراکنش را با توجه به حافظه خروجی‌های تراکنش‌های خرج‌نشده که نزد خود دارد بررسی می‌کند و اگر فرد ارسال‌کننده خروجی خرج‌نشده‌ای به اندازه ورودی تراکنش جدید داشت آن را تأیید می‌کند و به شبکه ارسال می‌نماید. در این لحظه پایگاه داده مزبور به‌روزرسانی شده و خروجی استفاده‌شده را حذف و خروجی جدید را ثبت می‌نماید.

شکل ۴. سازوکار ثبت در بیت‌کوین



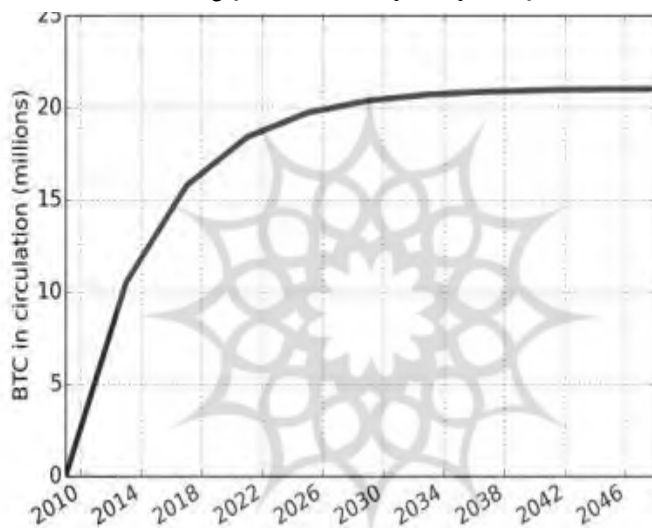
*. آدرس که همان هش کلید عمومی است همیشه ثابت است؛ ولی نمی‌توان از آدرس به کلید عمومی رسید و هویت اصلی نامعلوم می‌ماند.

پس از این فرآیند نوبت به معدن‌کاوان (استخراج‌گران) می‌رسد که تراکنش‌های تأییدشده را در قالب بلوک دریاورند و به واسطه عملیات اثبات گواه کار آن بلوک را در زنجیره بلوکی قرار دهند و از پاداش بیت‌کوین بهره‌مند شوند.

۴. پروتکل زمان‌بندی بیت‌کوین

شکل زیر پروتکل زمان‌بندی تولید بیت‌کوین را نشان می‌دهد. تعداد کل بیت‌کوین‌ها مقدار ثابتی معادل ۲۱ میلیون است. همان‌طور که قبلاً اشاره شد، بیت‌کوین‌هایی که به عنوان

نمودار ۱. برنامه نظری زمان‌بندی بیت‌کوین



پاداش به معدن‌کاو برنده داده می‌شود حدوداً هر چهار سال نصف می‌شود تا اینکه این تعداد به صفر می‌رسد.

مطابق نمودار فوق یکی از تفاوت‌های اصلی بیت‌کوین (پول رمزنگاری‌شده) با پول بانکی بدون پشتوانه خاصیت ضد تورمی آن است. راه تولید بیت‌کوین‌های جدید توسط کد منبع بیت‌کوین برنامه‌نویسی شده است. حداکثر تعداد بیت‌کوین‌های صادرشده حدود ۲۱ میلیون خواهد بود. این عرضه پولی ثابت، خاصیت ضد تورمی خواهد داشت.

البته مدل ضد تورمی بیت‌کوین توسط اقتصاددانان جریان اصلی رد می‌شود. با این استدلال که اگر بیت‌کوین خود را به عنوان یک جایگزین برای پول‌های بدون پشتوانه مطرح کند، این می‌تواند بانک‌های مرکزی را از اجرای سیاست‌های پولی منع کرده و باعث

کاهش درآمد تولیدشده توسط دولت از طریق چاپ پول شود و در نتیجه، عدم پایداری به وجود آمده در سیستم مالی منجر به یورش جهت فروش بیت‌کوین خواهد شد؛ از سوی دیگر، اقتصاددانان مکتب اتریشی به‌طور کلی مدل ضد تورمی بیت‌کوین را به عنوان یک نتیجه مثبت مشاهده می‌کنند؛ به این ترتیب که بیت‌کوین از توسعه اعتباری مرتبط با افزایش در عرضه پول در چرخه کسب‌وکار جلوگیری می‌کند. مدل ضد تورمی بیت‌کوین برای اینکه بتواند ویژگی نایاب بودن را به بیت‌کوین اعطا کند تا آن ارزشمند شود، بیشتر به عنوان یک ضرورت انتخاب شده است تا اینکه یک ویژگی از آن باشد (Smiling Dave, 2013).

تجزیه و تحلیل

برای استخراج ابعاد فقهی پول‌های رمزنگاری شده پس از موضوع شناسی که در بخش‌های پیشین گذشت، از منظر فقه فردی شامل احکام ثمن و مثن، اصول چهارگانه معاملات (ممنوعیت ضرر، غرر، اکل مال به باطل و ربا) حفظ مالکیت فردی، امانت‌داری و اصل آزادی در معاملات و همچنین فقه حکومتی شامل اصول لاضرر و لاضرار، نفی سبیل، عدالت و مبارزه با ظلم در دو سطح معامله و معدن‌کاوی مورد بررسی قرار گرفته و در قالب سؤالات زیر مشخص شد؛ سپس این سؤالات در اختیار خبرگان مالی اسلامی قرار گرفته و نتایج زیر با اکثریت آرا استخراج شد:

۱. آیا رویکرد فقه شیعه در مواجهه با پول، تأییدی و امضایی است؟ آیا صرف اینکه مردم به چیزی به عنوان وسیله مبادله اعتبار دهند و آن شیء مخالفتی با اصول اسلامی نداشته باشد کافی است؟ به‌طور کلی رویکرد فقه در مواجهه با مسائل مستحدثه مالی از جمله «پول رمزنگاری شده»، تأییدی است؛ به‌طوری‌که اگر مسئله جدید با موازین شرع مغایرت نداشته باشد، توسط فقه تأیید می‌شود چنانچه در خصوص طلا و نقره نیز توسط اسلام تأیید شدند نه اینکه آن را تأسیس کرده باشد. این مسئله نیز در زمان مبادله کالا به کالا وجود داشته است و هر چیزی می‌توانست وسیله مبادله قرار گیرد به شرط اینکه ممنوعیتی از جانب شرع وجود نداشته باشد؛ به‌طور مثال آلت قمار نمی‌تواند وسیله مبادله شود؛ پس در مرحله اول اعتبار عرف عقلاً نسبت به آن شیء مهم است و در مرحله بعد بررسی اینکه آیا استفاده از آن تخطی از موازین اسلامی است یا خیر؟ به‌طور مثال استفاده از پول مرسوم

به دلیل تبعاتی که دارد از جمله کاهش ارزش پول (سرقت عمومی از جیب مردم) و تطابق با نظام ربوی خالی از اشکال نمی‌باشد. پول رمزنگاری شده شرط اولیه را که اعتبار نزد عرف عقلا می‌باشد را داراست و هر روز استفاده از آن در زندگی عرف و عقلا فراگیرتر می‌شود و همچنین در مرحله بعد با هیچ یک از اصول عمومی مبادلات همانند ممنوعیت ضرر، غرر، ربا، اکل مال به باطل، ظلم و غیره ناسازگار نیست.

۲. آیا پول مورد تأیید فقه شیعه فقط منحصر به نقدین می‌باشد؟ پول مورد تأیید فقه شیعه منحصر به نقدین نیست؛ همچنان‌که اسلام مبادله کالا به کالا را تأیید نموده است و می‌توان از هر کالایی که با موازین شرع مخالفتی نداشته باشد جهت انجام مبادله استفاده نمود.

۳. از منظر فقه، ارزش و مالیت ناشی از چیست؟ ارزش و مالیت یک شیء ناشی از مطلوبیت آن میان عرف عقلاست که برای به دست آوردن آن به رقابت با هم می‌پردازند. در پول الکترونیک (بانکی) ارزش ناشی از اعتماد عرف به دولت است و در پول رمزنگاری شده ناشی از اعتماد مردم به بستر امن و سازوکار زنجیره بلوکی.

۴. آیا وسیله مبادله باید فی‌نفسه دارای ارزش مصرفی باشد؟ در شروط عوضین، مالیت داشتن جزء شروط است؛ اما هیچ قیدی مبنی بر اینکه آن مالیت حاصل از ارزش مصرفی باشد وجود ندارد؛ همچنان‌که در پول بانکی متداول خود برگه اسکناس هیچ ارزش مصرفی ندارد و کلیه مراجع بر جایز بودن استفاده از آن هم‌نظر هستند؛ در نتیجه این امکان وجود دارد که ارزش و مالیت چیزی برخاسته از اعتماد و مقبولیت عمومی نسبت به آن باشد.

۵. آیا پول رمزنگاری شده مالیت دارد؟ پول رمزنگاری شده مالیت دارد؛ طبق آمارهای موجود هر روز بر تعداد متقاضیان، استفاده‌کنندگان و پذیرندگان پول رمزنگاری شده افزوده می‌شود؛ لذا بر اساس ضوابط مالیت‌پیدا کردن یک شیء نزد عرف و عقلا، این پول مالیت دارد؛ بدین معنا که هم بین عرف و عقلا مطلوب است و هم برای تحصیل آن به رقابت با هم می‌پردازند.

۶. آیا بحث «پشتوانه» جایگاهی در مباحث فقهی دارد؟ آیا لازم است پول رمزنگاری شده پشتوانه داشته باشد؟ ضرورت داشتن پشتوانه پول یک امر اقتصادی تاریخی

است و ارتباطی با دستگاه فقه ندارد. بحث پشتوانه در اقتصاد به این دلیل اهمیت دارد که منجر به تعیین میزان مالیت آن پول می‌شود و گرنه پول، مالیت خود را در ازای خدمت و فایده‌ای که مردم و دولت برای آن جعل کرده‌اند (ذخیره ارزش، وسیله مبادله و محاسبه) به دست می‌آورد؛ البته میزان ارزش و مالیت آن تابع میزان حجمش در ارتباط با کالاها و خدمات قابل مبادله با آن است؛ اما اگر بنا شد که پول کاغذی پشتوانه فیزیکی همانند طلا و نقره نداشته باشد باید تبعات آن از منظر فقه بررسی شود. این مسئله که اسکناس کاغذی مالیت خود را از اعتبار دولت - یا از هر راه دیگر مورد قبول عرف - بگیرد، از منظر فقه بلا اشکال است؛ اما تبعات آن از قبیل کاهش ارزش پول (نوعی سرقت خاموش)، خیانت در امانت توسط سیاست‌های اشتباه دولت و تطابق نظام خلق پول با ربا، خالی از اشکال نخواهد بود. در پول رمزنگاری شده نیز همانند اسکناس بانکی هیچ پشتوانه فیزیکی وجود ندارد و مالیت خود را از مطلوبیت میان عقلا - به دلیل فراهم آوردن بستری امن و سریع برای انتقال دارایی - و محدود بودن گرفته است به طوری که عقلا برای به دست آوردن آن با هم به رقابت می‌پردازند؛ فلذا مالیت دارد و نیازی به بحث درباره پشتوانه نیست؛ البته همانند اسکناس و سایر پول‌های بانکی میزان ارزش و مالیت آن تابع میزان حجم آن در برابر کالاها و خدمات قابل مبادله است.

۲۲۹

۷. اگر عوامل مؤثر بر ارزش و مالیت پول رمزنگاری شده متفاوت از عوامل مؤثر بر ارزش و مالیت پول متعارف موجود باشد، تأثیری در حکم شرعی استفاده از آن دارد؟ مسئله مهم، مالیت بالفعل و مقبولیت عرفی و عمومی آن است.

۸. آیا فیزیکی بودن وسیله مبادله جزء شروط فقهی است؟ فیزیکی بودن عوضین جزء شروط فقهی نمی‌باشد؛ همچنین بعید است منظور از قبض در احکام مختلف فقهی، قبض فیزیکی باشد؛ بلکه به معنای تسلیم نمودن و تحویل دادن شیء است؛ چنان‌که در پول الکترونیک متداول بانکی نیز هیچ وجه فیزیکی وجود ندارد و مورد تأیید مراجع نیز هست.

۹. آیا معامله با بیت‌کوین از مصادیق معاملات غرری محسوب می‌گردد؟ شبهه غرر از این منظر که اصل وجود، اعتباردهنده، هدف از انتشار و ارزش آن همگی مبهم است. خیر، غرری بودن معامله بدین معناست که یکی از ارکان اصلی معامله برای طرفین مجهول باشد. در خصوص بیت‌کوین اگرچه امکان دارد طرفین از سازوکار فنی درونی آن اطلاع

نداشته باشند؛ اما اجمالاً نسبت به کارکرد آن آگاهی کامل دارند و همین امر منجر به تقاضای آن می‌شود.

۱۰. در سیستم بیت‌کوین راه برای مصادیق «اکل مال به باطل» همانند پول‌شویی، باج‌افزارها و همچنین تأمین مالی گروه‌های معاند - در تضاد با قاعده نفی سبیل - باز است و این امور را تسهیل می‌کند؛ همچنین فرار مالیاتی از جمله کارکردهایی است که با بیت‌کوین می‌توان به راحتی انجام داد و در سرتاسر دنیا این مسئله مشاهده می‌شود. چنانچه فرض شود سیستم اخذ مالیات، عادلانه است و در صورت عدم پرداخت آن، امور مسلمین مختل می‌گردد، آیا استفاده از این پول با ویژگی‌های فوق‌الذکر از منظر فقه شیعی جایز است؟ اولاً، این پول همانند سایر پول‌ها دارای منافع و معایبی است که در صورت استفاده صحیح هیچ ضرری بر آن مترتب نخواهد بود. البته اگر این مسائل (اقدامات مجرمانه) به‌طور غالب در استفاده از بیت‌کوین مطرح باشد به‌گونه‌ای که بدین کارکردها در میان مردم معروف باشد، استفاده از آن بدون اشکال نخواهد بود؛ ثانیاً، این مسئله در رابطه با کل پول‌های رمزنگاری‌شده صحیح نیست و در برخی از آنها به دلیل وجود عملیات احراز هویت راه برای کارهای مجرمانه همانند پول‌شویی و فرار مالیاتی هموار نیست؛ لذا طبیعتاً زمانی که جایگزین‌هایی سالم‌تر با همان منافع و بدون معایب مذکور وجود دارند استفاده از جایگزین با اصل احتیاط سازگارتر است.

۱۱. یکی از شبهات مهم در رابطه با پول رمزنگاری‌شده، شبهه ضرر و عدم رعایت مصلحت عامه است؛ بدین معنا که اولاً، احتمال می‌دهند شاید برنامه به‌گونه‌ای طراحی شده باشد که پس از رسیدن به مرحله‌ای به‌طور کامل منحل شود؛ ثانیاً، مطرح می‌شود که شاید این پول توسط دولت آمریکا درست شده و بیش از پنجاه درصد شبکه دست آمریکا باشد و با رشد قیمتی آن در صدد تسویه بدهی‌های جهانی خود است. آیا این مسئله از منظر فقه دارای اشکال است؟ در خصوص شبهه ضرر و عدم رعایت مصلحت عامه پول‌های رمزنگاری‌شده، اولاً برنامه‌های این پول‌ها از جمله بیت‌کوین «متن‌باز» هستند و هر فردی می‌تواند پروتکل اجرایی در آن را از صفر تا صد ببیند و به مراتب شفاف‌تر از سیستم پولی کنونی است. به علاوه باید توجه داشت که این مسئله فقط مختص به یکی از نمونه‌های

پول‌های رمزنگاری شده یعنی بیت‌کوین است؛ درحالی‌که هدف، استخراج حکم کلی پول‌های رمزنگاری شده است.

۱۲. برخی ادعا می‌کنند که احتمال دارد یکی از انواع پول‌های رمزنگاری شده؛ مثلاً بیت‌کوین خریداری شود و بعد از مدتی این نوع پول توسط دولت‌ها غیر قانونی اعلام شود و یا یک نوع پول رمزنگاری شده جذاب‌تری عرضه شود و دیگر کسی بیت‌کوین را نپذیرد و چون بیت‌کوین ارزش ذاتی ندارد در این حالت کل سرمایه دارندگان بیت‌کوین نابود شده و متضرر می‌شوند. آیا این مسئله مصداق ضرر و ضرار است؟ در خصوص امکان صفرشدن ارزش بیت‌کوین در صورت پدید آمدن رقیب بهتر، باید گفت این مطلب محتمل است؛ اما هدف از این پژوهش استخراج حکم کلی استفاده از پول‌های رمزنگاری شده است و نه مصداق آن.

۱۳. این شبهه مطرح است که در پول رمزنگاری شده دولت نمی‌تواند سیاست‌های پولی و مالی خود را پیاده نماید و این مسئله به ضرر عامه مردم تمام می‌شود. آیا این شبهه وارد است؟ در خصوص عدم توانایی دولت در اعمال سیاست‌های پولی و مالی خود باید گفت که دولت کماکان می‌تواند سیاست‌های پولی و مالی خود را پیاده نماید و صرفاً ابزار خلق پول را که اغلب بر خلاف مصلحت عامه می‌باشد از دست می‌دهد.

۱۴. آیا در عملیات معدن‌کاوی شبهه قمار وجود دارد؟ شباهت فرآیند معدن‌کاوی به قمار این است که در زودتر حل کردن مسئله و یافتن جواب، شانس دخیل است و کسی که تجهیزات قوی‌تری دارد صرفاً شانس بیشتری دارد دقیقاً همانند بلیت‌های بخت‌آزمایی؛ البته اگر این فعالیت به صورت یک کار مستمر دیده شود که هر ده دقیقه اتفاق می‌افتد عملاً «شانس» به صفر میل می‌کند به طوری که در طی یک ماه، فردی که از تجهیزات با قدرت محاسبه دو برابر نسبت به فرد دیگر استفاده می‌کند با احتمال بالا، درآمد دو برابری خواهد داشت. از طرفی تفاوت آن با قمار این است که حاصل این عملیات برای امنیت شبکه الزامی است و بدون آن هیچ کس به این سیستم اعتماد نخواهد نمود؛ چراکه به راحتی با یک حمله کامپیوتری می‌شود کل سیستم را تخریب نمود و به نوعی می‌توان آن را پاداش تأمین‌کنندگان امنیت شبکه در قالب جعاله شرعی دانست که جعل در برابر تأمین امنیت شبکه است. گویا اعلام می‌شود که هر کس امنیت این سیستم را با عملیات گواه‌کار تأمین

کند و زودتر پاسخ سؤال را بیابد فلان مبلغ را دریافت می‌کند؛ درحالی‌که در قمار مبلغ دریافتی در برابر منفعت عقلایی و ارائه خدمت مفیدی نیست. از طرف دیگر در این فرآیند شخص برنده، پاداش خود را از سیستم می‌گیرد و نه از ثروت سایرین؛ همانند چیزی که در قمار وجود دارد؛ ضمن اینکه برخی فقها از جمله مرحوم شیخ حسین حلی معتقدند قمار الزاماً باید در قالب بازی صورت گیرد که در این فرآیند هیچ‌گونه بازی وجود ندارد.

۱۵. آیا مهم است که مخترع پول رمزنگاری شده کیست و هدف او چه بوده است؟ مثلاً آیا اسرائیل مخترع آن است و در پی اهداف مجرمانه است؟ در خصوص اهمیت مخترع و بازی‌گردانان پول رمزنگاری شده باید گفت که اگر احتمال عقلایی در خصوص پدیدآمدن خسارت بزرگی وجود داشته باشد احتیاط، لازم است که تاکنون هیچ دلیلی برای وجود چنین احتمالی توسط متخصصین بیان نشده است.

۱۶. آیا وجود نهاد ناظر و واسط در فقه الزامی است؟ بدون وجود چنین نهادی، دولت نمی‌تواند بر اموال مردم نظارت داشته باشد و از آنان مالیات اخذ کند. وجود نهاد ناظر و واسط در فقه الزامی نیست. در نظام طلا و نقره هم که مورد قبول اسلام است چنین نهادی وجود نداشت و ضمن وجود احکام زکات، خمس و خراج در آن زمان هیچ سازوکاری برای نظارت بر اموال و تفتیش آنها نبود. به علاوه وجود نهادهای متعدد با اصل آزادی معاملات منافات دارد.

۱۷. آیا اینکه امکان هک‌شدن سیستم وجود دارد مشکل شرعی ایجاد می‌کند؟ امکان هک‌کردن شبکه پول‌های رمزنگاری شده با توضیحات فنی که در فصل قبل ذکر شده است به مراتب مشکل‌تر از هک‌کردن حساب‌های بانکی و به اعتقاد برخی متخصصان فناوری اطلاعات غیر ممکن است. البته گفتنی است در صورت هک‌شدن سیستم بانکی، دولت و بانک‌ها ضامن آن خواهند بود؛ اما در بیت‌کوین هیچ متولی وجود ندارد؛ در هر صورت این ریسک، قابل بررسی در ملاحظات سرمایه‌گذاری افراد است و ارتباطی با دستگاه فقه ندارد.

۱۸. آیا سیستم موجود در پول رمزنگاری شده با نظام پولی مطلوب اسلامی سازگارتر از وضعیت پولی و بانکی جاری است؟ به دلیل اینکه تغییرات ارزش در پول رمزنگاری شده یا در برخی از انواع آن کمتر اتفاق می‌افتد و از نظر شرعی معیار ارزش هرچه با ثبات‌تر باشد

مبادله و معامله با آن به عدالت نزدیکتر است؛ بنابراین از این جهت با موازین شرعی سازگارتر است.

۱۹. آیا پول رمزنگاری شده مثلی است؟ پول‌های رمزنگاری شده «مثلی» هستند؛ چراکه هر یک از واحدهای پول رمزنگاری شده همانند بیت‌کوین در میزان رغبت و تمایل افراد به آن مساوی هستند.

۲۰. آیا نگاه عرف و عقلا به پول‌های رمزنگاری شده طریقی است یا استقلالی؟ نگاه عرف به پول‌های رمزنگاری شده «طریقی» است؛ زیرا دارای ارزش ذاتی نیستند که به خودی خود برای مردم مطلوبیت داشته باشند؛ بلکه کارکردهای آن از جمله ذخیره ارزش، وسیله محاسبه و مبادله مطلوب است.

۲۱. آیا پول‌های رمزنگاری شده، با فرض اینکه مال باشند، با سایر مال‌ها و کالاها تفاوت دارند؟ چه تفاوتی؟ پول رمزنگاری شده مال است و مال بودن آن برای سهولت در امر معاملات، اعتبار شده است و تفاوتی با دیگر اموال ندارد؛ به همین سبب مورد رغبت مردم واقع می‌شود و به عنوان مال، موضوع احکام فقهی قرار می‌گیرد.

۲۲. آیا پول‌های رمزنگاری شده، پدیده مستحدثه محسوب می‌شوند؟ این پدیده اگر مصداق پول محسوب شود، قبلاً وجود نداشته است؛ بنابراین هرچند وظایف پول را بر عهده گرفته است؛ اما به لحاظ مصداق مستحدثه است.

۲۳. آیا در مطالبات مدت‌دار، همانند دین، قرض، مهریه، غصب، سرقت و اتلاف، کاهش و افزایش ارزش پول‌های رمزنگاری شده بر عهده ضامن است؟ این نوع پول از جهت ضمانت کاهش و افزایش ارزش آن در مطالبات مدت‌دار همانند دین، قرض، مهریه، غصب، سرقت و اتلاف است و فرقی با سایر پول‌های بانکی ندارد.

۲۴. آیا حکم فقهی پول‌های رمزنگاری شده به لحاظ تعلق زکات، کنز، خرید و فروش، وقف، به عنوان سرمایه در مضاربه و تعلق خمس به افزایش ارزش اسمی آن با پول‌های بانکی فرق دارد؟ وقتی پول رمزنگاری شده مالیت پیدا کند و وظایف سه‌گانه پول در روابط مالی را بر عهده گیرد و از نظر عرف و عقلا مورد اقبال گیرد به لحاظ تعلق زکات، کنز، خرید و فروش، وقف، به عنوان سرمایه در مضاربه و تعلق خمس به افزایش ارزش اسمی، حکم فقهی آن با پول‌های بانکی فرقی ندارد.

۲۵. آیا با توجه به اختلاف مذاهب اسلامی و نیز با عنایت به ویژگی‌های پول‌های رمزنگاری‌شده، مسلمانان و نیز کشورهای اسلامی می‌توانند آن را به عنوان پول مشترک در روابط مالی و پولی خود مورد استفاده قرار دهند؟ از آنجایی که پول رمزنگاری‌شده اختصاص به یک کشور خاص ندارد و به عنوان پول بین‌المللی محسوب می‌شود، مسلمانان و کشورهای اسلامی می‌توانند آن را به عنوان پول مشترک در روابط اسلامی مورد استفاده قرار دهند و اختلافات جزئی در نظرات فقهی مانعی برای این امر ایجاد نمی‌کند.

بعد از این مرحله، نتایج بررسی‌ها در اختیار مراجع قرار گرفته و حکم استفاده از پول‌های رمزنگاری‌شده استفتا گردید. با بررسی پاسخ ۱۳ تن از مراجع عظام تقلید می‌توان شروط اصلی حلیت استفاده از پول رمزنگاری‌شده را موارد ذیل دانست:

۱. در فرآیند خلق اعتبار کار نامشروعی انجام نگیرد: همان‌گونه که بررسی شد و به تأیید خبرگان رسید در فرآیند خلق اعتبار و عملیات معدن‌کاوی هیچ شبهه‌ای از جمله قمار وارد نمی‌باشد.

۲. کار نامشروعی با آن صورت نپذیرد: این مسئله یک حکم فردی است و نمی‌توان به کل مفهوم تعمیم داد؛ فلذا اگر کسی از این پول برای قاچاق استفاده کند حرام است و اگر کسی برای پرداخت صدقه استفاده کند حلال است.

۳. این اعتبار در قالب عقد صلح به یکدیگر منتقل شود: این مسئله به نیت افراد بستگی دارد و مقلدین آن مرجع می‌توانند نیت مصالحه نمایند.

۴. حفظ استقلال اقتصادی مملکت و با موافقت مقام معظم رهبری: این مورد از مهم‌ترین و چالش‌برانگیزترین مسائل هست که باید توسط متخصصان اقتصادی کشور مورد ارزیابی و اظهار نظر قرار گیرد. به‌طور نمونه بیت‌کوین ریسک‌ها و خطرات بسیاری برای اقتصاد کشور دارد؛ فلذا این مورد می‌تواند حلیت استفاده از بیت‌کوین را تحت تأثیر قرار دهد؛ اما خدشه‌ای به نوع پول‌های رمزنگاری‌شده وارد نمی‌سازد؛ چراکه در انواع دیگر این پول ممکن است اثرات مخرب بر اقتصاد کشور نداشته باشد؛ مثال بارز آن پول

رمزنگاری شده ملی می باشد که توسط دولت‌های روسیه و ونزوئلا ایجاد شده است (کریپتوروبل و پتروکوبل). این پول نه تنها اثر منفی بر اقتصاد کشور ندارد؛ بلکه نارسایی سیستم پولی کنونی را نیز برطرف می‌سازد و کشور را از سلطه دلار و همچنین اثرات مخرب چاپ بی‌رویه پول رها می‌سازد.

۵. خلاف قانون نباشد: استفاده از پول رمزنگاری شده در ایران برای آحاد مردم خلاف قانون نیست؛ اگرچه طبق دستورالعمل بانک مرکزی، بانک‌ها و سایر مؤسسات تحت نظارت از خرید و فروش آن منع شده‌اند.

۶. طرفین معامله آن را به عنوان پول و یا چیزی که دارای اعتبار و ارزش است قبول نموده و با آن معامله انجام دهند: این مسئله در میان بازار باید احراز شود که افزایش روز-به‌روز تقاضا و قیمت انواع پول‌های رمزنگاری شده و توانایی خرید از فروشگاه‌های معتبر بین‌المللی اثبات‌کننده این مطلب می‌باشد.

۷. اگر پشتوانه و اعتبار داشته باشد: پول رمزنگاری شده پشتوانه و اعتبار دارد با این تفاوت که پشتوانه و اعتبار آن به جای دولت، بستر امن زنجیره بلوکی می‌باشد.

۸. با جمع‌بندی نظرات خبرگان و مراجع می‌توان این‌گونه بیان کرد که اگر استفاده از رمزینارزها پیامدهای منفی در اقتصاد نداشته باشند بر اساس اصل لا ضرر و لا ضرار جایز است.

جمع‌بندی و نتیجه‌گیری

پول رمزنگاری شده یک نوع پول خصوصی است که متعلق به هیچ دولت یا حکومتی نیست و نیازی به نهادهای واسط مانند بانک مرکزی ندارد. این پول دیجیتال و مجازی، غیر متمرکز بوده و هیچ واسطه‌ای برای نقل و انتقال و جوه وجود ندارد؛ به همین خاطر است که دربردارنده مزیت‌هایی همچون سرعت بالای انتقال و هزینه پایین تراکنش می‌باشد. با حذف نهادهای مرکزی از این نظام پولی باید دو وظیفه مهم شامل ثبت مالکیت‌ها در دفتر کل و تأیید تراکنش‌ها، به روشی دیگر صورت می‌پذیرفت که بدین منظور فناوری زنجیره

بلوکی مورد استفاده قرار گرفته است. فناوری زنجیره بلوکی علاوه بر تأمین امنیت این سیستم با استفاده از علم رمزنگاری، کلیه تراکنش‌ها را در دفاتر کل توزیع شده میان افراد شبکه، ثبت می‌نماید.

با محبوب شدن این پدیده مستحدثه و گسترش استفاده از آن، این سؤال در ذهن مسلمانان به وجود آمد که آیا از منظر شریعت، خرید و فروش و استفاده از پول رمزنگاری شده جایز است؟ برای پاسخ به این شبهه، در پژوهش حاضر با بهره‌گیری از روش تحقیق «اجتهاد چندمرحله‌ای»، محورهای فقهی با رویکرد فقه فردی و حکومتی استخراج شده و با استفاده از نظر خبرگان مالی اسلامی و فتوای مراجع عظام تقلید نتیجه ذیل حاصل گردید:

ابتدا پول رمزنگاری شده را باید فارغ از انواع آن بررسی نمود. پول رمزنگاری شده یک نوع پول خصوصی شبیه به نظام طلا و نقره است که نهاد متولی و ناظر در آن وجود ندارد و افراد می‌توانند بدون نیاز به شخص ثالث اقدام به مبادله و انتقال پول نمایند. این تمرکززدایی و انحصار شکنی (اصل آزادی در معاملات) به نظام نقدین در صدر اسلام نزدیک‌تر است و هیچ فرد و دولتی نمی‌تواند به خاطر منافع شخصی خود بر دارایی‌های سایر مردم اثر بگذارد؛ چیزی که در سیاست‌های پولی غلط کشورها مشاهده می‌شود و همچنین اثری که سیاست‌های آمریکا به واسطه دلار بر دیگر پول‌ها می‌گذارد؛ لذا در قدم اول می‌توان گفت فلسفه و هدف این پول مورد تأیید اسلام و مشابه نظام طلا و نقره است؛ چراکه مانع از تأثیر دیگران بر دارایی‌های افراد بدون اجازه و اختیار آنان می‌شود و افراد در فضایی آزاد می‌توانند به نقل و انتقال پول بپردازند؛ بدون اینکه بالاجبار هزینه یا کارمزدی به شخص ثالث بدهند و بدون اینکه حریم خصوصی و اطلاعات آنان فاش گردد. البته به دلیل اینکه حفظ حریم خصوصی افراد گاهی به انجام تخلفات می‌انجامد، در برخی از انواع این پول، سازوکاری دیده شده است که یک نهاد معتمد بتواند از هویت فرستنده و گیرنده آگاهی یابد و این نقص برطرف شده است. همانند پول رمزنگاری شده ملی با پشتوانه طلا یا نفت. حال باید به نحوه تحقق این نظام پولی پرداخته شود که آیا در مرحله اجرا با موازین اسلامی تطابق دارد یا خیر؟ برای پاسخ ناگزیر باید یکی از انواع این پول مورد مذاقه قرار گیرد که در این پژوهش، بیت‌کوین انتخاب شد.

مطابق بررسی انجام شده، چنانچه استفاده از بیت کوین پیامدهای منفی در اقتصاد واقعی نداشته باشد بر اساس اصل «لا ضرر و لا ضرار» جایز می‌باشد؛ این در حالی است که استفاده از بیت کوین ریسک‌های معتناهی برای افراد و کل جامعه در بردارد. مهم‌ترین این خطرات به شرح زیر می‌باشد:

➤ **نوسانات قیمتی و عدم حفظ ارزش:** این پول ارزش ذاتی ندارد و مبنای ارزش‌گذاری آن صرفاً عرضه و تقاضا می‌باشد؛ لذا در طول عمر خود شاهد نوسانات بسیار زیاد بوده و خواهد بود و در این بین بسیاری از افراد سرمایه‌های خود را از دست می‌دهند.

➤ **تهدید اقتصاد واقعی و گسترش بخش غیر رسمی اقتصاد:** در نظام پولی بیت کوین، دائماً به اقتصاد دنیا، پولی خارج از کنترل و به‌طور نامحدود - به دلیل وجود انشعاب‌ها - تزریق می‌شود که تبعات منفی جدی برای اقتصاد به دنبال خواهد داشت.

۲۳۷

➤ **تسهیل فرار مالیاتی، پول شویی، باج‌گیری از طریق باج‌افزارها و تأمین مالی گروه‌های خلافکار:** بیت کوین در شرایط کنونی غالباً برای اقداماتی همچون فرار مالیاتی، باج‌افزارها و تأمین مالی گروه‌های تروریستی استفاده می‌شود و این مسئله یک خطر جدی برای جامعه جهانی است و بسیاری از افراد را متضرر می‌کند.

➤ **تهدید پول‌های رمزنگاری شده با تکنولوژی قوی‌تر و فناوری کامپیوترهای کوانتومی:** همچنین در خصوص تهدید رقبا باید گفت که ممکن است هر لحظه یک پول رمزنگاری شده جدید با ویژگی‌های مطلوب‌تر وارد بازار شود؛ چنانچه در حال حاضر نیز رقاباتی بسیار متریقی‌تر و با ویژگی‌های بهتر همچون اتریوم (Ethereum) و آیوتا (IOTA) و ریپل (Ripple) وجود دارند و بسیار محتمل است که در آینده‌ای نزدیک سرمایه‌گذاران از بیت کوین به سمت این پول‌ها حرکت نمایند و ارزش بیت کوین به صفر میل کند؛ همچنین از دیگر عواملی که در صورت عرضه توسط شرکت‌های کامپیوتری، ارزش بیت کوین را در لحظه صفر می‌نماید، کامپیوترهای کوانتومی هستند که توانایی محاسباتی بالایی دارند و می‌توانند در مدت زمان کوتاهی شبکه بیت کوین را رمزگشایی نموده و امنیت آن را از بین ببرند.

➤ **فقدان مستند قانونی و عدم توانایی طرح دعوی و پیگیری حقوقی:** هویت افراد در بیت کوین مشخص نبوده و هیچ نهاد حکومتی و قضایی در آن دخیل نیست؛ فلذا

مستندات نقل و انتقالات در این نظام پولی قابل ارائه در محاکم قضایی نمی‌باشد و این مسئله منجر به بروز تنش‌ها و اختلافات بسیاری خواهد شد.

➤ **عدم امکان تجهیز و تخصیص منابع به فعالان اقتصادی:** عدم وجود واسطه مالی همانند بانک در سیستم پول رمزنگاری شده سبب می‌شود امکان سپرده‌گذاری در نهاد مالی مشخصی وجود نداشته باشد و به تبع آن تجهیز و تخصیص منابع به فعالیت‌های اقتصادی میسر نخواهد بود. در این شرایط استفاده بهینه از منابع خرد و کلان صورت نپذیرفته و رشد اقتصادی از این طریق با مشکل مواجه می‌شود.

➤ **خروج ارز از کشور:** در شرایط کنونی ایران که تمامی پول‌های رمزنگاری شده باید به دلار خریداری شوند، خرید آنها منجر به خروج ارز از کشور خواهد شد و این یک تهدید جدی برای اقتصاد کشور محسوب می‌گردد.

➤ **تهدید رقبا و غیر قانونی شدن توسط دولت‌های بزرگ:** احتمال دارد استفاده از بیت‌کوین توسط دولت‌های بزرگ از جمله چین و آمریکا غیر قانونی اعلام شود و دیگر هیچ پذیرنده‌ای آن را نپذیرد و سرمایه مردم به هیچ تبدیل شود؛ چراکه بیت‌کوین ارزش اعتباری دارد نه ذاتی و اگر پذیرنده‌ای نباشد در واقع فاقد ارزش می‌شود.

بنابراین بیت‌کوین اگرچه از منظر فقه فردی و احکام ثمن و مثن دارای اشکال نمی‌باشد؛ اما به دلیل خطرات و ریسک‌های مذکور، اقتصاد کشور و سرمایه مسلمان را تهدید و دارای شبهه ضرر و ضرار است؛ لذا استفاده از بیت‌کوین از منظر شریعت و فقه حکومتی بدون اشکال نمی‌باشد؛ این در حالی است که سایر رمزینهارها مانند اتریوم و ریپل باید به‌طور مجزا با همین روش و مدل پژوهش بررسی شوند و این امکان وجود ندارد که برای کلیه آنها حکم واحدی اعلام نمود؛ به‌طور مثال «رمزینهارز منطقه‌ای با پشتوانه طلا یا نفت» ریسک‌ها و خطرات مربوط به بیت‌کوین را نخواهد داشت و به دلیل ماهیت غیر ربوی آن و عدم امکان چاپ پول بدون پشتوانه به نظام پولی اسلامی نزدیک‌تر است.

منابع و مأخذ

۱. سلطانی، محمد و حمید اسدی؛ «ماهیت حقوقی پرداخت در پول الکترونیک»؛ پژوهشنامه حقوق اسلامی؛ س ۱۶، ش ۴۱، ۱۳۹۴.
۲. سلیمانی پور، محمد و همکاران؛ «بررسی فقهی پول مجازی»، دوفصلنامه تحقیقات مالی اسلامی؛ ش ۱۲، ۱۳۹۶.
۳. سیدحسینی، میرمیثم و میثم دعایی؛ «بیت کوین، نخستین پول مجازی»، ماهنامه بورس؛ ش ۱۱۴ و ۱۱۵، ۱۳۹۳.
۴. میرزاخانی، رضا؛ بیت کوین و ماهیت مالی - فقهی پول مجازی (گزارش)؛ تهران: مرکز پژوهش، توسعه و مطالعات اسلامی سازمان بورس و اوراق بهادار، ۱۳۹۶.
5. Andersen, T. G., Bollerslev, T., Diebold, F. X., & Labys, P; Modeling and forecasting realized volatility , **Econometrica**; No.71(2) , 2003.
6. Appel, M. S.; **Canada, Can You Take A Security Interest In Bitcoin?**; Retrieved from <http://www.mondaq.com>, 2014.
7. Bank of Mexico; **Warnings on the use of virtual assets as substitutes for means of payment in legal tender**; Retrieved from: <http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf>.
8. Böhme, R., Christin, N., Edelman, B., & Moore, T.; Bitcoin: Economics, technology, and governance , **The Journal of Economic Perspectives**; 2015.
9. Cian, H., & Li, Z. H. E; The Role Decentralised Non-Regulated Virtual Currencies Play in Facilitating Unlawful Financial Transactions , **Master of Science Thesis in KTH university**; NO.80, 2016. Retrived from: <http://www.diva-portal.org>; 2016.

10. Chuen, D. L. K.; Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data , **Academic Press**, 2015.
11. Cuthbertson, A.; **Cryptocurrency Round-Up: Bolivian Bitcoin Ban, IOS Apps & Dogecoin at McDonald's** , Retrieved from ibtimes.co.uk.; 2014.
12. Dibrova, A.; Virtual Currency: New Step in Monetary Development”, **Procedia-Social and Behavioral Sciences**; 229, 2016.
13. European Central Bank; **Virtual currency schemes—a further analysis** ; retrieved from: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesenn>.
14. European Banking Authority (EBA); **EBA Opinion on virtual currencies**. Retrieved from <https://www.eba.europa.eu/.../EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>; 2014.
15. Financial Crimes Enforcement Network; **Bank Secrecy Act Regulations**; 76, 2011.
16. Financial Action Task Force; Virtual currencies: key definitions and potential AML/CFT risks , **Financial Action Task Force (FATF) Report**; June 2014.
17. García, C. A; Trading with bitcoin is illegal: Superfinanciera , **El Tiempo**; Retrieved from <http://www.eltiempo.com>, 2014.
18. Halaburda, Hanna; Beyond Bitcoin ,**Palgrave Macmillan**; 2016.

19. Hartge-Hazelman, B.; Glenn Stevens says Bitcoins show promise, but so did tulips , **The Australian Financial Review**; 2013.
20. He, D., Habermeier, K. F., Leckow, R. B., Haksar, V., Almeida, Y., Kashima, M & Yepes, C. V.; Virtual Currencies and Beyond: Initial Considerations , **International Monetary Fund**; No. 16/3, 2016.
21. Helbling, Philipp; Virtual Currency Schemes an Assessment of Bitcoin in Respect to the Properties of Money and the Real Economy , **master seminar in university of Basel**; Retrieved from: http://watchthemgo.org/wp-content/uploads/2016/02/Virtual_Currency_Schemes_Bitcoin.pdf, 2014.
22. Jingzhi Guo and Angelina Chow; Virtual Money Systems: a Phenomenal Analysis , in: Proc. IEEE Joint Conf. on E-Commerce Technology (IEEE CEC'08) and Enterprise Computing, E-Commerce and E-Services (EEE'08), IEEE Computer Society (Washington D.C., USA, July 21-24); 2008.
23. Kelly, B.; **The Bitcoin Big Bang: How alternative currencies are about to change the world**; John Wiley & Sons, 2014.
24. Knutsen, E.; Bitcoin, an experimental digital currency, has gained a toehold in the Middle East”, **The Daily Star**; p. 5; 2014.
25. Krause, M.; Bitcoin: Implications for the Developing World , **CMC Senior Theses**; Paper 1261. Retrived from: http://scholarship.claremont.edu/cmc_theses/1261, 2016.
26. Lo, S., & Wang, C.; Bitcoin as money? , **Federal Reserve Bank of Boston**; 2015.

27. MacCarthy, Mark.; What Payment Inter- mediaries Are Doing about Online Liability and Why It Matters , **Berkeley Technology Law Journal**; 25(2), 2010.
28. McAleer, M., & Medeiros, M. C.; Realized volatility, A review , **Econometric Reviews**; 27(1-3), 2008.
29. Mishkin, F. S.; **The economics of money, banking, and financial markets**; Pearson education, 2007.
30. Moore, T.; The promise and perils of digital currencies , **IJCIP**; 6(3-4), 2013
31. Nakamoto, S.; Bitcoin: A peer-to-peer electronic cash system , available at: <http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf>, 2008.
32. Pärilstrand, E., & Rydén, O.; Explaining the market price of Bitcoin and other Cryptocurrencies with Statistical Analysis; Department of Mathematics. University of Kungliga Tekniska Högskolan. Retrived from: <http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A814478&dswid=-4217>, 2015.
33. Reserve Bank of New Zealand; **Notes and Coins Frequently Asked Questions**; Retrieved from rbnz.govt.nz, 2013.
34. Rubinfeld, S.; Canada Enacts Bitcoin Regulations , **Risk and Compliance Journal**; 2014.
35. Stanley-Smith, J.; **Finland recognises Bitcoin services as VAT exempt**; Retrieved from **International Tax Review**: <http://www.internationaltaxreview.com/>, 2014.

36. Surda, P.; **Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?**; dev. economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf, 2012.
37. Szczepański M.; Bitcoin: Market, economics and regulation **European Parliamentary Research Service**; 2014.
38. The Law Library of Congress, Global Legal Research Center; **Regulation of Bitcoin in Selected Jurisdictions**; Retrieved from <http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>; 2014.
39. Yermack, D.; Is Bitcoin a real currency? An economic appraisal , **National Bureau of Economic Research**; No. w19747, 2013.
40. Zivot, E., & Wang, J.; Rolling analysis of time series. In *Modeling Financial Time Series with S-Plus* , **Springer New York**; 2003.