

نوع مقاله: ترویجی

موضوع‌شناسی رمزارزها و تحلیل فقهی آنها (مورد مطالعه بیت‌کوین)^۱

mortezaasadianlalimi@gmail.com

majidhabibian@atu.ac.ir

م. مرتضی اسدیان لالیمی / دانش‌آموخته طلبه سطح سه حوزه علمیه قم

مجید حبیبیان نقیبی / استادیار دانشکده اقتصاد دانشگاه علامه طباطبائی

پذیرش: ۱۴۰۰/۰۱/۲۵

دریافت: ۹۹/۰۹/۱۸

چکیده

بیشرفت در حوزه فناوری‌های مالی در دهه‌های اخیر به تغییر شئون مختلف زندگی مردم و دولت‌ها منجر شده و تحولات شگرفی در نظام پولی کشورها ایجاد کرده است. یکی از این فناوری‌ها، ارزهای رمزنگاری شده است؛ با توجه به سرعت همه‌گیری آن در جوامع اسلامی، لازم است تا ماهیت این پدیده نوظهور و تنظیم‌گری آن توسط فقه انجام شود. بنابراین لازم است دستگاه فقه ماهیت و کارکردهای اقتصادی این پدیده را با دقت شناسایی کند تا زمینه برای استنباط حکم شرعی به‌کارگیری آن را در روابط اقتصادی روشن کند. لذا به دلیل نوظهور بودن این مسئله، ابتدا با مراجعه به منابع کتابخانه‌ای، محتوای تحت وب و همچنین ترجمه مقالات بین‌المللی دیگر به موضوع‌شناسی پرداخته شده است و سپس ابعاد فقهی آن، با مراجعه به مبانی غنی فقه شیعه در دو سطح معامله و معدن‌کاوی تبیین شده است. در آخر نیز چالش‌های مطرح‌شده توسط خبرگان مالی اسلامی و مراجع عظام تقلید احصا شده است. براین اساس وجود شبهاتی مانند «لاضرر»، «نفی سییل»، «وجود هک و سایبری» و بسیاری از چالش‌های دیگر که می‌تواند رادعی در مشروعیت آن محسوب شود، مورد بررسی قرار گرفته است.

کلیدواژه‌ها: ارز رمزنگاری شده، رمزارز، ارز دیجیتال، بیت‌کوین، بلاک‌چین.

مقدمه

بلوکی است (هابر میر، ۲۰۱۴، ص ۳) که تحت عنوان ارزهای رمزنگاری شده شناخته می‌شوند. ویژگی اصلی این پول آن است که هیچ نفر سومی در سازوکار پولی آن، اعم از خلق پول و اعمال انواع سیاست‌های پولی دیگر که گاهی به ضرر عموم مردم است و ارزش پول مردم را کاهش می‌دهد، دخالت ندارد. 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. علاوه بر آن، استفاده از این نوع پول سبب می‌شود که قدرت خرید معمولاً بالا رود (ر.ک: کاتبرتسون، ۲۰۱۴). در واقع تاریخ نشان داده که مراجع مرکزی نظیر پادشاهان و بانک‌های مرکزی با در اختیار داشتن قدرت صدور پول حاکم، از این ویژگی در سطوح مختلف سوءاستفاده کرده‌اند. این سوءاستفاده از قدرت، با انتقال قدرت خرید از مردم به خود قدرتمندان و افراد نزدیک آنها انجام می‌شد. بیت‌کوین، پیشنهاد ساتوشی برای درمان این بیماری همه‌گیر بود.

در حال حاضر پول‌های رمزنگاری شده و فناوری مرتبط با آن (زنجیره بلوکی) به سرعت در حال فراگیر شدن هستند و حجم سرمایه در گردش آنان بسیار رشد کرده است؛ به طوری که فقط حجم سرمایه در گردش بیت‌کوین به بیش از ۱۳۱ میلیارد دلار رسیده است. همچنین علاوه بر بیت‌کوین حدوداً ۴۹۸۶ رمزارز دیگر نیز وجود دارند. با توجه به نفوذ گسترده رمزارزها در جوامع اسلامی و افزوده شدن بر محبوبیت آن، به دلایل پیش‌گفته، لازم است تا پژوهش‌های گسترده‌ای ابتدا درباره موضوع‌شناسی آن و شیوه کار، استخراج و حتی شیوه معامله آن، صورت پذیرد؛ تا ابتدا حقیقت این نوع از پول یا دارایی مشخص شود و سپس باید آن را منطبق بر قواعد فقه، پویا ساخت. اما تاکنون تحقیق دقیقی که هم به موضوع‌شناسی این مقوله پرداخته باشد و هم تقریباً تمامی چالش‌های فقهی آن را طرح کرده باشد، صورت نگرفته است. در این پژوهش ابتدا با تکیه بر روش تحقیقی و کتابخانه‌ای به بررسی ماهیت این نوع از پول / دارایی پرداخته خواهد شد و سپس چالش‌هایی را که خبرگان مالی اسلامی و یا مراجع عظام تقلید مطرح کرده‌اند، بررسی خواهد شد.

سال ۲۰۰۸، سال شروع بحران اقتصادی در آمریکا است، که با بحران وام‌های مسکن شروع شد و به سرعت به تمامی ساختار مالی آمریکا و حتی جهان ضربه مهلکی زد. بسیاری یکی از علل رخ دادن این بحران را سفته‌بازی بانک‌های آمریکایی و وال استریت بر روی خرید و فروش اوراق وام‌های مسکن می‌دانند؛ چیزی که باعث شد بانک‌های آمریکایی بسیاری ورشکسته شده و پول مردمی که پس‌اندازهای خود را در بانک‌ها ذخیره کرده بودند، به یک‌باره به سرقت رفته و توان مالی وام‌گیرندگان نیز به شدت کاهش یابد و به دنبال آن حجم زیادی از وام‌های مسکن اعطاشده، سر رسید شد و وام‌گیرندگان نتوانستند بدهی‌های خود را به بانک‌ها بازگردانند و بسیاری خانه و سر پناه خود را به یک‌باره از دست دادند.

دولت آمریکا مثل تمامی دولت‌های دیگر دنیا در زمان چنین بحرانی، با چاپ پول و تزریق نقدینگی جلوی ورشکستگی سیستم مالی را گرفت و این نیز عاملی برای نارضایتی بیشتر از وضعیت موجود و عملکرد دولت آمریکا شد. سفته‌بازی‌ها و سودهای کلان را بانک‌ها و مؤسسات مالی کرده بودند و آنها عامل چنین ضرر بزرگی بودند؛ ولی دولت مردم را تنبیه کرد و با چاپ پول و کاهش ارزش پول در دست مردم ضررهای بانک‌ها را جبران کرد.

در نتیجه، اعتماد به دلار که همیشه فدرال رزرو آمریکا آن را باثبات و قابل اعتماد نشان می‌داد، از بین رفت و مردم عملاً به این نتیجه رسیدند که به این پول‌های کاغذی که توسط دولت‌ها منتشر می‌شوند، اعتماد نمی‌توان کرد.

در همین زمان‌ها بود که شخصی به نام ساتوشی ناکاموتو (Satoshi Nakamoto) مفهوم بلاک‌چین را در سال ۲۰۰۸ معرفی کرد (کاظمی‌تبار، ۱۳۹۶، ص ۴۳).

و این‌گونه بود که جامعه کم‌کم به سمت وسوی استفاده از ابزاری رفت تا بتواند از زیر سلطه بانک‌ها و مؤسسات مالی خارج شود و بتواند ارزش پول خودش را کنترل کند؛ لذا سرعت پیشرفت فناوری، به‌ویژه در حوزه فناوری‌های مالی در دهه‌های اخیر به تغییر شئون مختلف زندگی مردم و همچنین دولت‌ها منجر شد و تحولات شگرفی در نظام پولی کشورها ایجاد کرد.

یکی از این فناوری‌های نوین، ارزهای مبتنی بر فناوری زنجیره

است. لذا لازم است تا به سازوکار فنی آن به‌طور تفصیلی پرداخته شود. در ابتدا باید دانست که ارزهای رمزنگاری‌شده، تحت یک مفهوم عام، به نام «پول مجازی» یا «ارز دیجیتال» قرار دارد، که به دو قسم قابل تبدیل (Convertible) و غیرقابل تبدیل (Non-convertible) تقسیم می‌شود. پول مجازی قابل تبدیل، به دو قسم متمرکز و غیرمتمرکز تقسیم می‌شود و ارزهای رمزنگاری‌شده در واقع از نوع غیرمتمرکز است. پول مجازی غیرقابل تبدیل، مانند سکه‌هایی که در بازی خاصی مانند بازی‌های امروزی (clash of clans) و یا بازی‌های دیگری که توسعه‌دهنده آن بازی‌ها و نرم‌افزارها، سکه‌ها و پول‌های مجازی را در آن بازی‌ها قرار می‌دهند که صرفاً در همان بازی‌ها و پلتفرم‌ها کارایی دارند و نه در هیچ کجای دیگر و قابل تبدیل هم نیستند و کاملاً به صورت متمرکز هستند و توسط توسعه‌دهنده داده می‌شوند؛ آن هم فقط در همان بازی یا همان پلتفرم. در مقابل، پول مجازی وجود دارد که قابل تبدیل به پول حقیقی (غیردیجیتال) است. این مورد به دو قسم متمرکز (یعنی انتشار و کنترل ارز توسط یک نهاد مرکزی صورت می‌پذیرد) و غیرمتمرکز (سیدحسینی و دعایی، ۱۳۹۳، ص ۸۵) تقسیم می‌شود. غیرمتمرکز بودن به این معناست که 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 می‌گویند؛ چراکه کلیه فرایندهای 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؛ به عبارت دیگر، در سازوکار این پول نیاز به اعتماد به هیچ نهادی نیست و الگوریتم‌های ریاضی و رمزگذاری، صحت معاملات را تأیید می‌کنند و هیچ کاربری نمی‌تواند در شبکه تغییر ایجاد کند (نارایانان، ۲۰۱۴، ص ۳۲).

همان‌طور که بیان شد این پول در پی نارضایتی از دخالت نهاد مرکزی و ناظر در سیستم اقتصادی پدید آمد. بدین جهت مخترعان این پول درصدد 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 کند و ارزش پول را کاهش دهد. می‌توان گفت در این راه موفق

کتاب همه‌چیز درباره بیت‌کوین (اخوان، ۱۳۹۸) که حاوی مجموعه مقالاتی به‌منظور آشنایی با بیت‌کوین و بلاک‌چین است، با نگارشی ساده و روان، به چگونگی پیدایش و تاریخچه آن پرداخته است.

پایان‌نامه کارشناسی ارشد *بررسی ماهیت ارزهای رمزنگاری‌شده و تحلیل فقهی معاملات مبتنی بر آن* (اسدیان، ۱۳۹۹)، ابتدا به مسائل فنی ارزهای رمزنگاری‌شده اشاره کرده و آن‌گاه به صورت کامل به ماهیت‌شناسی آن پرداخته و در آخر نیز چالش‌های فقهی را درباره ارزهای رمزنگاری‌شده، متذکر شده است. سیدحسینی و دعایی (۱۳۹۳) در مقاله خود پس از بیان تاریخچه و تبیین مبانی فنی بیت‌کوین به فرصت‌ها و چالش‌های پول رمزنگاری‌شده پرداخته‌اند. آنها مهم‌ترین چالش این پول‌ها را بحث قانونگذاری دانسته و کشورها را براساس رویکرد خویش نسبت به بیت‌کوین به دسته‌های خاصی تقسیم‌بندی کرده‌اند؛ دسته‌هایی چون کشورهایی که آن را پذیرفته‌اند و یا کشورهایی که آن را رد کرده‌اند و یا کشورهایی که مانند ایران فعلاً درباره آن سکوت کرده‌اند.

میرزاخانی (۱۳۹۷) در مقاله 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 تا زمانی که از طرف حاکمیت کنترل پول‌های مجازی در اقتصاد واقعی، سامان‌دهی نشده است، باید از ورود پول‌های مجازی در دنیای حقیقی جلوگیری گردد.

نواب‌پور (۱۳۹۷) در پایان‌نامه کارشناسی ارشد با عنوان *تحلیل فقهی کارکردهای پول رمزنگاری‌شده*، ابتدا به مسائل فنی و سپس به بررسی فقهی کارکردهای این نوع از پول پرداخته است.

مقاله «تحلیل فقهی کارکردهای پول‌های رمزنگاری‌شده؛ مورد مطالعه بیت‌کوین» (نواب‌پور و همکاران، ۱۳۹۷)، به بررسی موضوعی و فقهی این مسئله پرداخته است.

۱. جایگاه رمزارزها

برای بررسی یک پدیده نوظهور، ابتدا باید به موضوع‌شناسی آن پرداخت، و اولین قدم در موضوع‌شناسی طرح مسائل فنی و نظری آن

مرکزی وجود ندارد، این وظیفه یعنی ثبت، تأیید تراکنش و به‌روزرسانی آن حساب‌ها بر عهده دو ابزار قرار گرفته است؛ به این صورت که از علم رمزنگاری (Ecrption) برای تأیید صحت تراکنش‌ها و از فناوری زنجیره بلوکی جهت ثبت و به‌روزرسانی حساب‌ها استفاده می‌شود.

در بیت‌کوین کلیه تراکنش‌ها در یک دفتر کل ثبت 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 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 به روزرسانی می‌شود (چوئن، ۲۰۱۵).

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 که شامل مقدار بیت‌کوین و آدرس فرستنده به همراه امضا و کلید خصوصی (Private Key) است، به شبکه ارسال می‌شود. هر چند صد تراکنش (به اندازه یک مگابایت) در یک بلوک قرار می‌گیرند که به‌طور تصادفی یکی از تراکنش‌ها به‌عنوان «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 می‌کرد 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 اضافه می‌گردید. اما در این سیستم معدن‌کاوان (Miners) می‌بایست سه عنصر را یعنی سر تیترا، کد بلوک قبلی (کاراکترهای حاصل از عملیات هش) و به علاوه یک سری اعداد و ارقام دلخواه (Nonce) با عملیات درهم‌سازی (Hash) به یک سری اعداد و ارقام با طول مشخص و ویژگی مشخص تبدیل کنند. برنامه سیستم به‌گونه‌ای 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 به‌گونه‌ای که سرعت حل مسئله در محدوده ده دقیقه بماند - معدن‌کاوان برای اینکه

هم شده‌اند؛ زیرا توانستند ارزی به نام بیت‌کوین را مطرح کنند که امروزه ارزش بسیاری دارد و مرجع مبادلات بسیاری در جهان نیز قرار می‌گیرد؛ اگرچه هنوز آن‌طور که باید، فراگیر نشده است؛ اما از حجم مبادلات بسیار بالایی برخوردار است؛ زیرا سهولت بسیاری را برای استفاده‌کنندگان به ارمغان آورده، به‌صورتی که اگر بخواهیم دلار و بیت‌کوین را مقایسه کنیم، باید بگوییم دلار قابلیت خرج کردن دارد، اما در کارت ناشناس نیست؛ ۳ تا ۷ روز طول می‌کشد تا از نهادهای واسط به کشوری دیگر منتقل شود؛ قابل جعل و چاپ غیرمجاز است؛ قابل سرقت است؛ تورم آن دارای ثبات نیست؛ غیرمتمرکز نیست؛ قابلیت تقسیم‌پذیری زیاد ندارد؛ هرچقدر بخواهید چاپ می‌شود و تورم ایجاد می‌کند و ارزش را به حداقل می‌رساند؛ بجز خرج کردن هیچ کاربرد دیگری ندارد و بعد از مدتی مندرس شده و یا کثیف می‌شود؛ درحالی‌که ارز رمزنگاری شده هیچ‌کدام از ضعف‌های شمرده شده را نداشته و بسیار قابل اتکاست؛ زیرا کاملاً ناشناس است، قابل جعل نیست، تورم در آن راه ندارد و از ثبات تورمی بهره‌مند است؛ قابلیت تقسیم‌پذیری بسیاری دارد، به‌صورتی که ۱ عدد بیت‌کوین می‌تواند به ۱۰۰ میلیون واحد تقسیم شود. به‌علاوه دارای سختی استخراج و منابع محدود یعنی تنها ۲۱ میلیون عدد می‌باشد (رضادوست و رمضانی شماسی، ۱۳۹۷، ص ۷۹) که این پدیده را کاملاً از پول‌های فیزیکی متمایز می‌کند.

اگر بخواهیم ویژگی‌های اصلی بیت‌کوین و ارزهای رمزنگاری شده غیرمتمرکز را برشمریم، لازم است تا به این موارد اشاره کنیم: عدم نیاز به نهاد مرکزی برای جابه‌جایی پول؛ عدم توانایی دخالت دولت در تولید و خلق پول؛ مخفی ماندن هویت فرستنده و گیرنده؛ تحت حمایت دولت نیست و پشتوانه دولتی ندارد؛ هزینه عملیاتی ناچیز در سطح بین‌المللی؛ سرعت انتقال بالا در سطح بین‌المللی؛ قیمت آن به وسیله عرضه و تقاضا کشف می‌شود؛ تولید پول به وسیله عملیات استخراج؛ محدودبودن منابع (دیفیلی، ۱۳۹۷، ص ۳۸).

۲. مشخصات فنی و شیوه کار

در نظام پولی بانکی همه تراکنش‌ها در سیستم سنتی در یک دفتر کل، تحت نظارت بانک مرکزی ثبت می‌شود (درشر، ۱۳۹۷، ص ۴۹) و کسی نمی‌تواند پولی را که ندارد خرج کند و در سیستم‌های ثبتی تغییری ایجاد کند. اما در ارزهای رمزنگاری شده که نهاد واسط بانک

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 بایستی ابتدا توسط کلید عمومی، رمز اطلاعات ارسالی را باز کند، 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 خرج نشده که نزد خود دارد، بررسی می‌کند و اگر فرد ارسال‌کننده خروجی خرج نشده‌ای به اندازه ورودی تراکنش جدید داشت، آن را تأیید می‌کند و به شبکه ارسال می‌کند. در این لحظه پایگاه داده مزبور به‌روزرسانی شده و خروجی استفاده‌شده را حذف و خروجی جدید را ثبت می‌کند.

پس از این فرایند نوبت به معدن‌کلوان (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.

۳. منابع محدود بیت‌کوین

از آنجاکه فرایند پیدا کردن هش بلاک در شبکه بیت‌کوین مانند پیدا کردن طلا توسط معدن‌چیان است؛ نام استخراج یا ماینینگ را بر روی آن گذاشته‌اند. اما استخراج بیت‌کوین همان فرایند افزودن بلاک‌های جدید به بلاک‌چین است، که توضیح آن گذشت. تعداد کل بیت‌کوین‌ها به ۲۱ میلیون عدد محدود شده است که تاکنون ۱۸,۱۳۵,۲۱۲ BTC استخراج شده است.

تنها راه به دست آوردن بیت‌کوین به صورت استخراج و یا معامله آن است. اما در زمینه استخراج پاداشی که به هر معدن‌کاو داده می‌شود، با در نظر گرفتن دوره حدودی ۴ ساله با هر بار نصف شدن پاداش، سال ۲۱۴۰م آخرین سالی خواهد بود که طبق پروتکل فعلی، استخراج‌کنندگان بیت‌کوین دیگر پاداشی از بابت افزودن بلاک‌های جدید به بلاک‌چین دریافت نخواهند کرد.

یکی از تفاوت‌های اصلی بیت‌کوین (پول رمزنگاری‌شده) با پول بانکی بدون پشتوانه، خاصیت ضد تورمی آن است؛ زیرا راه تولید

بتواند هشی با آن ویژگی تولید کند، نمی‌تواند اطلاعات تراکنش‌ها و یا کد بلوک قبلی را تغییر دهد؛ بلکه باید آن اعداد دلخواه را آن قدر تغییر دهد تا به هش موردنظر دست یابد و این می‌شود همان حل مسئله ریاضی که در بیت‌کوین مطرح می‌شود. اولین فردی (معدن‌کاو) که بتواند تابع هش موردنظر را بسازد یا به عبارت بهتر بتواند آن کاراکترهای «Nonce» را تشخیص دهد و معما را حل کند، برنده پاداش بیت‌کوین خواهد بود (کلی، ۲۰۱۴).

در سیستم بیت‌کوین برای اینکه افراد انگیزه لازم را برای حل معما (معدن‌کاو) 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 یک بار نصف می‌شود، تا مجموع بیت‌کوین‌ها در عدد ۲۱ میلیون متوقف گردد و بدین صورت منابع بیت‌کوین محدود است (چوئن، ۲۰۱۵).

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 به‌عنوان 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.

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 به طور آزاد، می‌شود –

بیت‌کوبین‌های جدید توسط کد منبع بیت‌کوبین برنامه نویسی شده است، این عرضه پولی ثابت و محدود بودن منابع، خاصیت ضد تورمی خواهد داشت (استانلی اسمیت، ۲۰۱۴).

۴. چالش‌های قابل طرح

برای دریافت ابعاد فقهی ارزهای رمزنگاری شده پس از موضوع‌شناسی که در بخش‌های پیشین گذشت، با جست‌وجو و هم‌فکری بسیار با صاحب‌نظران این عرصه، و جست‌وجو در کتب معتبر و مسائل مطرح‌شده از دانش‌پژوهان و دانشمندان، چالش‌های بسیاری مشخص شده و مورد بررسی قرار خواهد گرفت:

۱. آیا ارزهای رمزنگاری‌شده، یک امر مستحدثه و نوظهور محسوب می‌شوند؟

اگر این نوع از ارز از مصادیق پول (سلیمانی‌پور و همکاران، ۱۳۹۶، ص ۱۷۸) محسوب شود، که به این صورت قبلاً وجود نداشته است؛ بنابراین هرچند وظایف پول را برعهده گرفته است؛ اما به لحاظ مصادق مستحدثه است.

۲. مواجهه فقه شیعه با پول تأسیسی است یا امضایی و تأییدی؟ یعنی اگر مردم ارزهای رمزنگاری‌شده را معتبر بدانند و با آن مبادله کنند و مخالف اصول حقه اسلام نباشد، کافی است؟

آنچه از فقه شیعه برمی‌آید به این صورت است که رویکرد فقه شیعه در مواجهه با پول و یا اصلاً بگوییم مسائل مستحدثه مالی، امضایی است؛ مانند طلا و نقره و یا حتی مبادله کالا به کالا که تأسیسی نبوده‌اند؛ بلکه اگر مورد تأیید عرف عقلا باشد و رادعی از جانب شرع نبود آنها نیز می‌توانستند وسیله مبادله قرار بگیرند (توسلی، ۱۳۸۴، ص ۱۲۸). از طرفی دیگر ارزهای رمزنگاری‌شده 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 با توجه به نظرات بسیاری از علما دلیلی برای انحصار معاملات در عقود معین وجود ندارد؛ بلکه هر معامله عقلایی صحیح است، مگر آنکه با دلیلی خاص از شمول ادله عام مانند عموماً «تجاره عن تراض»، «ووفوا بالعقود»، «الناس مسلطون علی اموالهم»، «احل الله البیع» خارج شده باشد و ردعی نیز از جانب شارع نیامده است.

۳. آیا پول مورد تأیید فقه شیعه منحصر در امور نقدیه، مانند اسکناس و مسکوک و یا نقدین (درهم و دینار) است؟

قطعاً انحصاری در کار نیست؛ همان‌گونه که معامله کالا به کالا (که در آن، یکی از کالاها ثمن خواهد بود) تأیید شده است؛ لذا هر پولی که به لحاظ عموماً و اطلاعات و شرایط کلی معاملات منع شرعی نداشته باشد، می‌تواند به‌عنوان ثمن معامله مورد استفاده قرار گیرد.

۴. آیا مهم است که مخترع پول رمزنگاری‌شده، 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 رمزنگاری‌شده، 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 متخصصان بیان نشده است.

۵. 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؛ همچنان که 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.

۶. 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. لذا فقها از نوع رفتار عقلا نسبت به اشیا انتزاع مالیت می‌کنند (صدر، ۱۳۹۰، ص ۲۷۴). در پول‌های رایج فعلی (اسکناس و مسکوک) ارزش ناشی از اعتماد عرف به دولت؛ و در پول رمزنگاری‌شده، ناشی از اعتماد مردم به بستر امن و سازوکار زنجیره بلوکی است. البته پر واضح است که مال باشد یا نباشد، بالاخره معامله‌ای انجام می‌شود؛ اگرچه این نیز مهم است که شارع از آن نهی نکرده باشد؛ به‌علاوه در مالیت هم، باید مفید باشد، کم‌یابی نسبی داشته باشد، که این شرایط را دارد.

۷. اگر عوامل مؤثر بر ارزش و مالیت ارز رمزنگاری‌شده، متفاوت از عوامل مؤثر بر ارزش مبادله‌ای و مالیت پول متعارف موجود باشد، تأثیری در حکم شرعی استفاده از آن دارد؟

مسئله مهم، مالیت داشتن بالفعل و مقبولیت عرفی و عمومی آن نزد عقلا است.

۸. آیا رمز ارز مالیت دارد؟

به عبارت دیگر، اگر کل طلاهای دنیا در بانک مرکزی به‌عنوان پشتوانه جمع شود، ولی تناسب بین کالاها و خدمات قابل مبادله در بازار با متغیر حجم پول تغییر نکند؛ یعنی حجم پول بیشتر شود؛ آیا کاری از طلاهای پشتوانه برمی‌آید؟ حال برعکس، اگر بانک مرکزی یک گرم طلا نداشته باشد، ولی تناسب مذکور حفظ شود، آیا ارزش پول کاهش پیدا می‌کند یا افزایش؟ اگر تناسب به نفع کالاها تغییر پیدا کند، ارزش پول بیشتر هم می‌شود، ولو یک گرم طلا به‌عنوان پشتوانه اضافه نشود. حالا اگر بخواهیم بحث پشتوانه ارزهای رمزپایه را بررسی کنیم، می‌گوییم جریان پشتوانه پول یک اتفاق تاریخی بوده و کسانی که طلا در اختیارشان بوده در انتشار اسکناس زیاده‌روی می‌کردند و موجب ایجاد تورم می‌شدند و ابتدا تصور می‌کردند که اگر ما تناسب بین انتشار اسکناس و پشتوانه آن، که طلا باشد را حفظ کنیم، می‌توانیم تورم را کنترل کنیم به این نحو که ارزش پول کاهش پیدا کرده و تناسب حفظ شود؛ درحالی‌که این نظریه باطل است و پشتوانه ربطی به تناسب مذکور ندارد.

۱۱. آیا رمز ارزها مثلی هستند؟

«مثلی» هستند (یوسفی، ۱۳۹۷، ص ۲۳۱)؛ چراکه هریک از واحدهای رمز ارزها همانند بیت‌کوین در میزان رغبت و تمایل افراد به آن مساوی هستند؛ زیرا در واقع نوعی قدرت خرید است که آثارش در دیون و مبادلات نسبه ظاهر می‌شود.

۱۲. نگاه عرف و عقلا به رمز ارزها طریقی است یا استقلالی؟

نگاه عرف به رمز ارزها «طریقی» است؛ زیرا دارای ارزش ذاتی نیستند که به‌خودی‌خود برای مردم مطلوبیت داشته باشند؛ بلکه کارکردهای آن از جمله ذخیره ارزش، وسیله محاسبه و مبادله مطلوب است. همان‌طور که نگاه عقلا به اسکناس و پول‌های الکترونیکی طریقی است، به این معنا که عقلا این پول را به دست می‌آورند تا از دستش خلاص شوند و آن را خرجش کنند، رمز ارزها نیز چنین هستند.

۱۳. آیا سیستم موجود در رمز ارزها با نظام پولی مطلوب اسلامی

سازگارتر از وضعیت پولی و بانکی جاری است؟

به دلیل اینکه تغییرات ارزش در رمزارزها یا در برخی از انواع آن کمتر اتفاق می‌افتد و از نظر شرعی معیار ارزش هرچه باثبات‌تر باشد، مبادله و معامله با آن به عدالت نزدیک‌تر است؛ بنابراین از این جهت با موازین شرعی سازگارتر است.

۱۴. آیا رمزارزها، با فرض اینکه مال باشند، با سایر مال‌ها و

می‌توان گفت رمز ارزها مالیت دارند. طبق آمارهای موجود هر روز بر تعداد متقاضیان، استفاده‌کنندگان و پذیرندگان آن افزوده می‌شود؛ لذا براساس ضوابط مالیت پیدا 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 باهم می‌پردازند.

۹. 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 کردن و تحویل دادن شیء است؛ چنان‌که در پول الکترونیک متداول بانکی نیز هیچ وجه فیزیکی وجود ندارد و مورد تأیید مراجع نیز هست.

۱۰. آیا لازم است رمز ارز پشتوانه داشته باشد؟ آیا نیاز است

درباره «پشتوانه» در مباحث فقهی بحث شود؟

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، و‌گرنه 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 حجم 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 ارز رمزنگاری‌شده 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؛ به‌طوری‌که عقلا برای به‌دست آوردن آن با هم به رقابت می‌پردازند؛ پس، بنابراین 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.

کالاها تفاوت دارند؟

رمزارز نوعی 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 به‌عنوان مال، موضوع احکام فقهی قرار می‌گیرد. حق این است که مال نیز مانند پول یک مفهوم عرفی است؛ باید دید عرف به چه چیزی مال می‌گوید؟ (وحدتی شبیری، ۱۳۷۹، ص ۶۰) البته می‌دانیم مال از عناوین و مفاهیم عرفیه‌ای است که ممکن است شریعت مقدسه برای آن احکامی جعل کرده و با جعل احکام حدود و ثغوری قرار داده و احیاناً مالیت مورد خاصی را از آن گرفته باشد؛ مانند خمر. خمر در دنیا مال است، ولی شریعت مقدسه آن را حرام اعلام می‌کند و با این کار هر نوع تصرفی را حرام اعلام می‌کند؛ لذا خمر مالیت خود را در جامعه اسلامی از دست می‌دهد. این موارد استثنائی است و بجز موارد استثنائی، شناخت مال دائر مدار عرف است. ارزشهای رمزنگاری‌شده مانند بیت‌کوین می‌توانند ثمن و مومن واقع شوند و حداقل از باب شروط عوضین، این شرط بسیار مهم را دارا می‌باشد و امروزه می‌بینیم که هم ثمن واقع می‌شود و هم مومن. به‌علاوه بیت‌کوین مانند یک انتقال اعتبار است؛ لذا می‌توانیم بگوییم قدرت بر تسلیم نیز درباره آن وجود دارد و مانعی نیز درباره آن وجود ندارد. باید اضافه کنیم که ارزشهای رمزنگاری‌شده تازه به راه افتاده‌اند و نمی‌توان انتظار داشت که عرف تمام جهان از آن استفاده کنند، یا درباره آن بدانند؛ ولی در حد خود امروزه به‌عنوان یک واحد مبادله استفاده می‌شود و با آن خرید و فروش صورت می‌گیرد. آشکار است که ارزشهای رمزنگاری‌شده نشانی از اعتبار دولت و قدرت حاکمه ندارند و صرفاً برای اعتبار جمعی از جامعه، مبنای انتقال ارزش برای همان جمع خاص شده است و طبیعتاً در چنین فرایندی، بنای عقلایی نقشی ندارد. اما پول اعتباری بدون تحقق پشتوانه نیز می‌تواند تحقق پذیرد؛ چون براساس زنجیره بلوکی که سابقاً توضیحات آن داده شد، می‌توان بدون نیاز به قدرت مرکزی، پول اعتباری تولید کرد و نقل و انتقال آن را انجام داد و «ادل‌الدلیل علی امکان شی وقوعه» است که می‌بینیم این مطلب در عالم واقع نیز حادث شده است؛ زیرا اجماع صاحب‌نظران بر کارکردهای سه‌گانه پول مبنی بر واسطه بودن برای مبادله، عیار سنجش ارزش و ذخیره ارزش را می‌توان امری قطعی تلقی کرد. امروزه پول‌های رمزپایه در واقع هم می‌توانند نوعی ذخیره

ارزش باشند و هم می‌توانند وسیله مبادله باشند و هم می‌توانند معیار سنجش قرار بگیرند؛ پس می‌توان به آنها پول اطلاق کرد و با آن صورتی که گفته شد، ادعا کرد که این نوع از ارزش‌های مالیت اعتباریه هستند (توسلی، ۱۳۹۱).

۱۵. آیا با توجه به اختلاف مذاهب اسلامی و نیز با عنایت به ویژگی‌های رمزارزها، مسلمانان و نیز کشورهای اسلامی می‌توانند آن را به‌عنوان پول مشترک در روابط مالی و پولی خود مورد استفاده قرار دهند؟

از آنجاکه رمزارزها اختصاص به یک کشور خاص ندارد و به‌عنوان پول بین‌المللی محسوب می‌شود، مسلمانان و کشورهای اسلامی می‌توانند آن را به‌عنوان پول مشترک در روابط اسلامی مورد استفاده قرار دهند و اختلافات جزئی در نظرات فقهی مانعی برای این امر ایجاد نمی‌کند. به‌علاوه با توجه به اینکه امروزه اکثر کشورهای اسلامی و بخصوص شیعیان و... تحت ظالمانه‌ترین تحریم‌ها قرار دارند، می‌توانند به راحتی و بدون اینکه شناخته شوند، به مبادله بپردازند و مشکلات اقتصادی خویش را مرتفع سازند.

۱۶. آیا در مطالبات مدت‌دار، همانند دین، قرض، مهریه، غصب، سرقت و اتلاف، کاهش و افزایش ارزش رمزارزها 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 و به راحتی و سهولت قابل تبدیل است.

۱۷. آیا حکم فقهی رمزارزها به لحاظ تعلق زکات، کنز، خرید و فروش، وقف، به‌عنوان سرمایه در مضاربه و تعلق خمس به افزایش ارزش اسمی آن با پول‌های بانکی فرق دارد؟

وقتی رمزارزها مالیت پیدا کند و وظایف سه‌گانه پول در روابط مالی را بر عهده گیرد و از نظر عرف و عقلاً مورد اقبال گیرد، به لحاظ تعلق زکات، کنز، خرید و فروش، وقف، به‌عنوان سرمایه در مضاربه و تعلق خمس به افزایش ارزش اسمی، حکم فقهی آن با پول‌های بانکی فرقی ندارد.

۱۸. آیا اینکه امکان هک شدن سیستم وجود دارد، مشکل شرعی ایجاد می‌کند؟

امکان هک کردن شبکه با توضیحات فنی که در مطالب قبل ذکر شده، به مراتب مشکل‌تر از هک کردن حساب‌های بانکی و به

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

۲۲. برخی ادعا می‌کنند که احتمال دارد یکی از انواع رمزارزها؛ مثلاً بیت‌کوین، خریداری شود و بعد از مدتی این نوع پول توسط دولت‌ها غیرقانونی اعلام شود و یا یک نوع 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 اینکه دولت‌ها آن را غیرقانونی اعلام کنند یا خیر، چنین مسئله‌ای دخیل در این ارز نمی‌باشد. به‌علاوه هدف از این پژوهش استخراج حکم کلی استفاده از رمزارزها است و نه مصداق آن.

۲۳. یکی از شبهات مهم، 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 درصدد تسویه بدهی‌های جهانی خود است. آیا این مسئله از منظر فقه دارای اشکال است؟

در خصوص شبهه ضرر و عدم رعایت مصلحت عامه ارزشهای رمزنگاری شده، اولاً برنامه‌های این پول‌ها از جمله بیت‌کوین (متن باز) هستند و هر فردی می‌تواند پروتکل اجرایی در آن را از صفر تا صد ببیند و به مراتب شفاف‌تر از سیستم پولی کنونی است. به‌علاوه باید توجه داشت که این مسئله فقط مختص به یکی از نمونه‌های رمزارزها یعنی بیت‌کوین است؛ درحالی که هدف، استخراج حکم کلی رمزارزها است.

۲۴. در سیستم بیت‌کوین راه برای مصادیق «اکل مال به باطل» همانند پول شویی، باج‌افزارها و همچنین تأمین مالی گروه‌های معاند - در تضاد با قاعده نفی سبیل - باز است و این امور

اعتقاد برخی متخصصان فناوری اطلاعات غیرممکن است. البته گفتنی است در صورت هک شدن 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.

۱۹. آیا وجود نهاد ناظر و واسطه 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 واسطه 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. به‌علاوه وجود نهادهای متعدد با اصل آزادی معاملات منافات دارد.

۲۰. چون دولت نمی‌تواند در رمزارزها سیاست‌های پولی و مالی خود را پیاده‌سازی کند، لذا این مسئله دارای اشکال 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 کند و صرفاً ابزار خلق پول را که اغلب برخلاف مصلحت عامه می‌باشد، از دست می‌دهد.

۲۱. آیا در عملیات معدن‌کاوی شبهه قمار وجود دارد؟

شبهات فرایند 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؛ به‌طوری‌که 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 (موسوی بجنوردی، ۱۳۷۲، ص ۴۰) و بدون آن هیچ‌کس به این سیستم اعتماد نخواهد کرد؛ چراکه به راحتی با یک حمله کامپیوتری می‌شود کل سیستم را تخریب کرد 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 هرکس امنیت این سیستم را با عملیات گواه کار تأمین

چنین پولی با عنوان حرمت روبه‌روست؛ آیا این اشکال صحیح است؟ این مهم در صورتی می‌تواند موجب حرمت باشد که اولاً قرار باشد چنین پولی در اقتصاد واقعی داخل شود و ثانیاً نظارتی بر ورود آن صورت نگیرد و ثالثاً این ورود موجبات ضربه زدن به اقتصاد داخلی را فراهم آورد. اما امروزه آنچه که اتفاق افتاده خلاف این است؛ زیرا اولاً معمولاً این پول وارد اقتصاد داخلی نمی‌شود، یا هنوز نشده است. البته که این پول در بعضی کشورها ورود به دنیای اقتصاد واقعی را داشته است و حتی بعضی کشورها آن را تأیید و سپس بر آن مالیات وضع کرده‌اند و حتی برای آن وام می‌دهند؛ ولی آن‌گونه که کسی بگوید ورود این پول‌ها به‌منزله ضربه به اقتصاد داخلی وارد نشده؛ منتها ممکن است ورود این پول ضربه به اقتصاد داخلی باشد، که می‌توان این جنبه آن را با وضع قوانین دقیق و کارساز مثل بسیاری از کشورها که آن را تأیید کرده‌اند، کارسازی کرد و حتی موجبات شکوفایی اقتصاد داخلی را نیز فراهم آورد؛ مخصوصاً کشورهایی مانند ایران که دائماً تحت شدیدترین تحریم‌ها هستند و نمی‌توانند آن‌گونه که باید و شاید از پول‌های فیات استفاده کنند، به راحتی می‌توانند با وضع قوانین و نظارت مستمر موجبات ارزآوری و تقویت اقتصاد داخلی را با این ارزش‌های رمزنگاری شده پدید آورند. در واقع عمده دلیلی که باعث می‌شود نتوانیم به درستی این‌گونه معامله‌ها را تجویز کنیم، عدم نظارت کافی و وافی است و این خود موجب هزاران فساد در سیستم بانکی و پولی کشورها نیز شده و صرفاً در ارزش‌های رمزنگاری شده، نیست؛ شما بیشترین اختلاس‌ها و اضرار به کشورها و مردم و جامعه را می‌توانید حتی در دلار و پول‌های ملی کشورها نیز ببینید. پس اینکه صرفاً یک امری خودش به دلیل عدم نظارت، موجب یک اتلاف مال می‌شود، نمی‌تواند نفس عمل را از دایره تجویز خارج کند.

۲۷. لزوم حفظ نظام و جلوگیری از اختلال نظام زندگی مسلمین به‌عنوان یک قاعده عقلی و ضروری، از امور مسلمین تلقی می‌شود (مغنیه، ۱۳۷۷، ص ۳۲۸). لذا با عنایت به چالش‌های رمز ارزها، مانند مشکلات امنیتی، تسهیل جرایم اینترنتی، فرار مالیاتی و پول‌شویی که موجب اختلال نظام اقتصادی و حتی سیاسی و اجتماعی جامعه خواهد شد. با توجه به موارد فوق آیا مصلحت اقتضا می‌کند تا حاکم اسلامی تا به سامان رسیدن تولید و جریان این شکل از پول، از ورود آن به اقتصاد واقعی جلوگیری کند؟

را تسهیل می‌کند؛ زیرا هویت متعاملین مشخص نیست و قابل ردیابی نیست. همچنین فرار مالیاتی از جمله کارکردهایی است که با بیت‌کوین می‌توان به راحتی انجام داد. 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) به طور 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 رمزنگاری شده 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.

۲۵. 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 (مصباحی مقدم و رستم‌زاده، ۱۳۸۶، ص ۲۱۳) 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. عده‌ای نیز نوسانات قیمتی آن را موجب تحقق غرر می‌دانند؛ اما بدیهی است که به دلیل حقیقت نوسانات، نمی‌توان بیت‌کوین و ارزش‌های رمزنگاری شده را حرام اعلام کرد. در حقیقت اگر این شرط تعیین‌کننده بود، تجارت طلا، نقره، دلار آمریکا و یورو هم غیرشرعی است؛ چراکه این دارایی‌ها نیز دارای نوسان هستند. برای مثال، دو برابر مقدار طلایی که تاکنون در تاریخ تمدن بشری استخراج شده است، در بازارهای دیجیتال طلا در یک دوره سه ماهه تجارت شده است.

۲۶. براساس قاعده احترام و حرمت تضييع اموال مسلمین، ورود بدون نظارت این نوع از پول‌ها در اقتصاد واقعی موجب تغییر ضرری در حجم پول و ثروت‌های اقتصاد واقعی است که براین‌اساس، تزریق

متأسفانه این مسئله نه تنها در بیت‌کوین و رمزارزها، بلکه در انواع و اقسام پول‌های دیگر نیز وجود دارد و راه چاره‌ساز آن، دخالتی در تجویز یا عدم تجویز این نوع از پول ندارد و به نظر می‌رسد بیشتر در بخش نظارت و بازرسی و شیوه مدیریت باید به دنبال آن گشت.

۳۰. آیا اینکه بیت‌کوین بستر بسیار مناسبی برای سفته‌بازی است - سفته‌بازی، کاری اقتصادی است که به هدف دستیابی به سود از طریق پیش‌بینی تغییرات قیمت کالا، اوراق بهادار یا ارز انجام می‌شود - می‌تواند موجب عدم تأیید آن توسط فقه شیعه شود؟

سفته‌بازان بخشی از ثروت جامعه را به صورت نقد نگهداری می‌کنند (مصباحی‌مقدم و رستم‌زاده، ۱۳۸۶، ص ۱۲۸) تا بتوانند از فرصت‌هایی که برای این منظور در بازارهای مالی پدید می‌آید، بهره‌گیری کنند؛ لذا برای پول، افزون بر تقاضای معاملاتی و احتیاطی، تقاضای سفته‌بازی را نیز مطرح می‌کنند.

در میان صاحب‌نظران اقتصاد اسلامی نیز برخی سفته‌بازی را زیان‌بار می‌دانند؛ زیرا آنچه در اقتصاد به افزایش تولید، اشتغال و رفاه منجر می‌شود، رونق بخش واقعی اقتصاد و نه بزرگ‌شدن بخش پولی است. برخی نیز بر این عقیده‌اند اگر سفته‌بازی به‌گونه‌ای سالم و به دور از احتکار و ائتلاف (تبانی) و انتشار اخبار کذب و معامله‌هایی صورتی و مانند آن انجام شود، اشکال فقهی نخواهد داشت؛ مانند اینکه شخصی مقداری بیت‌کوین را ذخیره کند تا بعدها که قیمت آن رشد بخصوصی پیدا کرد آنها را به فروش برساند و سود کند؛ پر واضح است که اگر این کار موجب خللی در نظام اقتصادی نشود، نمی‌تواند مشکلی بیافریند و موجبات عدم تأیید را فراهم آورد.

نتیجه‌گیری

با توجه به رشد روزافزون اقبال مردم جهان به ارزهای رمزنگاری‌شده، خصوصاً بیت‌کوین، به‌عنوان یک پدیده مستحدثه و گسترش بسیار زیاد استفاده از آن، این سؤال در بسیاری از نهادهای اقتصادی اسلامی و در اذهان بسیاری از شیعیان شکل گرفته که آیا از منظر شریعت حقه اسلام، خرید و فروش و استفاده از این نوع پول جایز است یا خیر؟ در تحقیق حاضر پس از موضوع‌شناسی و مشورت با صاحب‌نظران فقهی اقتصادی و خبرگان صاحب‌نظر، اکثر و بلکه شاید تمامی چالش‌ها و اشکالاتی که در این زمینه وجود داشته‌اند، جمع‌آوری و در این پژوهش ارائه شده است. این پول یک نوع پول

پاسخ این سؤال قبلاً داده شد، که اولاً این پول همانند سایر پول‌ها دارای منافع و معایبی است که در صورت استفاده صحیح، هیچ ضرری بر آن مترتب نخواهد بود؛ ثانیاً این مسئله در رابطه با کل رمزارزها صحیح نیست و در برخی از آنها عملیات احراز هویت وجود دارد که راه برای کارهای مجرمانه، همانند پول‌شویی و فرار مالیاتی می‌بندد. به‌علاوه، اینکه بگوییم وارد اقتصاد واقعی شود نیز محقق نشده است؛ حتی اگر وارد اقتصاد واقعی شود، می‌توان به سرعت با وضع قوانین صحیح و مدبرانه آن را مدیریت کرد.

۲۸. اگر سیاستگذار پولی با عدم رعایت مصلحت و غبطه مسلمین و سیاست‌هایی که موجب تضییع اموال مسلمین است، موجب کاهش ارزش ثروت و تضییع حقوق گردد، مطابق قاعده ائتلاف ضامن است و فعل ضرری او به استناد قاعده احترام و اصل حرمت تضییع اموال مسلمین عنوان حرمت دارد. حال آیا می‌توان گفت که اگر دولت‌ها جلو انتشار رمزارزها را نگیرند، در واقع آنها مرتکب ائتلاف مال غیر شده‌اند و سیاستگذار پولی مکلف است در شرایط فعلی به دلیل وجود ضرر بسیار، مسلمین را از این کار منع کند؟

اولاً عده‌ای هستند که در فضاهای مجازی گروه‌های خاصی دارند که خودشان تحلیل‌های موردنیاز و فن اختصاصی برای معامله را بلد هستند و به دیگران در اصطلاح سیگنال می‌دهند تا آنها نیز بتوانند ارزیابی که آن متخصصان تحلیل کرده‌اند را بخرند و سود ببرند؛ که البته همه آن متخصصان با این وجود نیز مسئولیت سود و یا ضرر را به عهده نمی‌گیرند (دقیقاً مثل کاری که امروزه در بورس‌ها هم شاهد این مسئله هستیم) و تنها می‌گویند ما سیگنال می‌دهیم (یعنی با توجه به تحلیل‌های تخصصی می‌دانیم که کدام ارز رشد می‌کند، آن را به شما می‌گوییم تا بخرید)؛ خواستید بخرید، خواستید نخرید. حال وقتی شخص اقدام می‌کند، با مسئولیت خویش اقدام کرده است؛ و ثانیاً اینکه سیاستگذاران پولی می‌توانند به جای ممنوعیت آن ابزار و سازوکار آموزش کامل آن را در اختیار بگذارند تا از هرگونه ائتلاف جلوگیری شود و چه‌بسا یک ارزآوری بسیار قوی نیز صورت بگیرد و موجبات تقویت اقتصاد داخلی و عدم ائتلاف و ازدیاد سرمایه مسلمین فراهم گردد.

۲۹. آیا توزیع ناعادلانه ثروت که از جمله تهدیدهای بیت‌کوین برای نظام اقتصاد اسلامی است می‌تواند به‌عنوان رادعی در این مسئله عمل کند؛ زیرا مخالف قاعده عدالت است؟

درشر، دنیل، ۱۳۹۷، *مبانی بلاک‌چین؛ مقدمه‌ای غیرفنی در ۲۵ گام*، ترجمه سیاوش تفضلی، تهران، صفحه سفید.

دیفیلیپی، پریماورا آبرون رایت، ۱۳۹۷، *بلاک‌چین و قانون*، ترجمه حامد حیدری و یاسر زندی، تهران، صفحه سفید.

رضادوست، نیما و مژگان رضائی شمایی، ۱۳۹۷، *بررسی block chain و کاربرد آن در حوزه‌های مختلف*، دومین کنفرانس ملی دانش و فناوری علوم مهندسی ایران، ص ۷۰-۸۳.

سلیمانی‌پور، محمدمهدی و همکاران، ۱۳۹۶، «بررسی فقهی پول مجازی»، *تحقیقات مالی اسلامی*، دوره ششم، ش ۲، ص ۱۶۷-۱۹۲.

سیدحسینی، میرمیثم و میثم دعایی، ۱۳۹۳، «بیت‌کوین، نخستین پول مجازی»، *بورس*، ش ۱۱۴-۱۱۵، ص ۸۸-۸۴.

صدر، سیدمحمدباقر، ۱۳۹۰، *الاسلام یقود الحیاة*، بی‌جا، پژوهشگاه علمی - تخصصی شهید صدر.

کاظمی تبار، سیدجواد، ۱۳۹۶، «آسیب‌شناسی بلاک‌چین»، در: *هفتمین همایش ملی بانکداری الکترونیک و نظام‌های پرداخت*.

مصباحی مقدم، غلامرضا و اسماعیل رستم‌زاده، ۱۳۸۶، «غیر در معاملات اختیارات بر روی سهام از دیدگاه فقه امامیه»، *جستارهای اقتصادی*، ش ۸، ص ۲۰۹-۲۲۱.

مغنیه، محمدجواد، ۱۳۷۷، *فقه الامام جعفر الصادق*، چ دوم، قم، اسماعیلیان.

موسوی بخوردی، سیدمحمد، ۱۳۷۲، «نظرخواهی از فقها پیرامون مسائل فقهی و حقوقی ناشی از کاهش ارزش پول»، *ره‌نمون*، ش ۶، ص ۳۱-۴۲.

میرزاخانی، رضا، ۱۳۹۷، «بیت‌کوین و ماهیت مالی - فقهی پول مجازی»، *جستارهای اقتصادی*، دوره پانزدهم، ش ۳۰.

نواب‌پور، علیرضا و همکاران، ۱۳۹۷، «تحلیل فقهی کارکردهای پول‌های رمزنگاری‌شده؛ مورد مطالعه بیت‌کوین»، *اقتصاد اسلامی*، ش ۲، ص ۲۱۳-۲۴۳.

_____، ۱۳۹۷، *تحلیل فقهی کارکردهای پول رمزنگاری‌شده*، پایان‌نامه کارشناسی ارشد، رشته معارف اسلامی و مدیریت مالی، تهران، دانشگاه معارف اسلامی و مدیریت.

وحدتی شبیری، حسن، ۱۳۷۹، *مجهول بودن مورد معامله*، قم، دفتر تبلیغات اسلامی.

یوسفی، احمدعلی، ۱۳۹۷، *ماهیت پول و راهبردهای فقهی و اقتصادی آن*، تهران، پژوهشگاه فرهنگ و اندیشه اسلامی.

Chuen, D. L. K.; 2015, *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data* Academic Press.

Cuthbertson, A, 2014, *Cryptocurrency Round-Up: Bolivian Bitcoin Ban, IOS Apps & Dogecoin at McDonald's*, Retrieved from ibtimes.co.uk

Kelly, B.; 2014, *The Bitcoin Big Bang: How alternative currencies are about to change the world*; John Wiley & Sons.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S; , 2014, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

Stanley-Smith, J.; 2014, *Finland recognises Bitcoin services as VAT exempt*; Retrieved from International Tax Review: <http://www.internationaltaxreview.com/>, 2015.

خصوصی شبیه به نظام طلا و نقره است که نهاد ناظر در آن وجود ندارد و افراد می‌توانند بدون نیاز به شخص ثالث، اقدام به مبادله کنند. این تمرکززدایی و انحصار شکنی (اصل آزادی در معاملات) به نظام نقدی 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. 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 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 می‌گرفت که در این پژوهش، بیت‌کوین به لحاظ فقهی بررسی شد و طبق عناوین اولیه فقهی اشکالی در خرید و فروش آن احراز نشد؛ بدین لحاظ می‌توان ادعا کرد بیت‌کوین آثار و پیامد منفی بر باورها و ارزش‌های دینی ندارد؛ اما به لحاظ پیامدهای منفی اقتصادی که طبیعتاً تحت عناوین ثانویه قرار می‌گیرد، نیازمند بررسی میدانی است. لذا پیشنهاد می‌شود به صورت محدود اجازه خرید و فروش آن داده شود و پیامدهای آن ارزیابی شود تا پیامدهای اقتصادی آن نیز روشن گردد.

منابع.....

اخوان، پیمان، ۱۳۹۸، *همه چیز درباره بیت‌کوین*، تهران، آتی‌نگر.

اسدیان، مرتضی، ۱۳۹۹، *بررسی ماهیت ارزهای رمزنگاری‌شده و تحلیل فقهی معاملات مبتنی بر آن*، پایان‌نامه کارشناسی ارشد، رشته فقه معاملات، قم، حوزه علمیه.

توسلی، محمداسماعیل، ۱۳۸۴، «بررسی و نقد نظریات برخی از اندیشه‌ورزان اسلامی درباره ماهیت پول»، *اقتصاد اسلامی*، ش ۱۹، ص ۱۲۳-۱۵۹.

_____، ۱۳۹۱، «تحلیل ماهیت پول»، *اقتصاد اسلامی*، ش ۴۸، ص ۱۰۷-۱۳۰.