Comparative Studies in Jurisprudence, Law, and Politics

Bitcoin and Cryptocurrency: Challenges, Opportunities, and Future Strategies

1. Masoud Rezaei: PhD Student, Department of Private Law, Go.C., Islamic Azad University, Gorgan, Iran
2. Zahra Tajari Moazzeni*: Assistant Professor, Department of Law, Go.C., Islamic Azad University, Gorgan, Iran. Email: moazen509@gmail.com (Corresponding Author)
3. Akram Tajik: Department of Law, Az.C., Islamic Azad University, Azadshahr, Iran

ABSTRACT

Bitcoin and other cryptocurrencies have garnered significant attention over the past few years. Recognized globally as digital coins and virtual currencies, these cryptocurrencies are generated and traded within the blockchain system. The blockchain technology adopted for the use of cryptocurrencies has stimulated interest among banking sectors, governments, stakeholders, and individual investors. The emergence of cryptocurrencies in this decade, following the introduction of Bitcoin in 2009, has disrupted financial markets. Cryptocurrencies are predicted to be the future of currency, with the potential to replace current paper-based currencies worldwide. Despite attracting widespread user attention, many remain unaware of the associated opportunities, disadvantages, and future challenges. Comprehensive research on cryptocurrencies is still lacking and remains in its nascent stages. In an effort to provide guidance and meaningful insight to the academic community and users, this article discusses the opportunities of cryptocurrencies, such as the security of its technology, low transaction costs, and high investment returns. The core focus of this paper revolves around legal regulations, high energy consumption, the potential for crashes and speculative bubbles, and network attacks. Future commitments and applications of cryptocurrencies are systematically examined in this article.

Keywords: *cryptocurrency, blockchain, mining, investment*.

How to cite: Rezaei, M., Tajari Moazzeni, Z., & Tajik, A. (2025). Bitcoin and Cryptocurrency: Challenges, Opportunities, and Future Strategies. *Comparative Studies in Jurisprudence, Law, and Politics*, *7*(2), 130-145.

© 2025 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 06 December 2024
Revise Date: 28 December 2024
Accept Date: 10 January 2025
Publish Date: 24 July 2025

پژوهش‌های تطبیقی فقه، حقوق و سیاست

بیت کوین و ارز رمزنگاری شده: چالش‌ها، فرصت‌ها و تدابیر آینده

۱. مسعود رضایی: دانشجوی دکتری، گروه حقوق خصوصی، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران
۲. زهرا تجری مؤذنی*: استادیار، گروه حقوق خصوصی، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران. پست الکترونیک: moazen509@gmail.com (نویسنده مسئول)
۳. اکرم تاجیک: گروه حقوق، واحد آزادشهر، دانشگاه آزاد اسلامی، آزادشهر، ایران

چکیده

بیت کوین و سایر ارزهای رمزنگاری شده از چند سال گذشته مورد توجه بسیاری قرار گرفته است. در سطح جهانی که به عنوان سکه دیجیتال و ارز مجازی شناخته می‌شود، این ارز رمزنگاری شده در سیستم بلاک چین به دست آمده و مورد معامله قرار می‌گیرد. فناوری بلاک چین که در استفاده از ارز رمزنگاری شده به تصویب رسیده است، بخش‌های بانکی، دولت، ذینفعان و سرمایه‌گذاران فردی را برانگیخته است. ظهور ارزهای رمزنگاری شده در این دهه از زمان ظهور بیت کوین در سال ۲۰۰۹ بازار را متلاطم کرده است. ارز رمزنگاری شده به عنوان ارز آتی پیش بینی می‌شود که ممکن است جایگزین ارز کاغذی فعلی در سراسر جهان شود. با وجود اینکه توجه کاربران را به خود جلب کرده است، بسیاری از فرصت‌ها، معایب و چالش‌های آینده آن آگاه نیستند. تحقیقات کاملی در مورد ارزهای رمزنگاری شده هنوز وجود ندارد و در مراحل اولیه خود است. در ارائه راهنمایی و دیدگاه قابل توجه به حوزه دانشگاهی و کاربران، این مقاله درباره فرصت‌های موجود در ارز رمزنگاری شده مانند امنیت فناوری آن، هزینه معاملات پایین و بازده سرمایه گذاری بالا بحث می‌کند. محوریت این مقاله پیرامون قانون و مقررات، مصرف زیاد انرژی، احتمال سقوط و حباب و حملات به شبکه است. تعهدات آینده ارزهای رمزنگاری شده و کاربرد آن به طور سیستماتیک در این مقاله مورد بررسی قرار می‌گیرد.

واژگان کلیدی: ارز رمزنگاری شده، بلاکچین، ماینینگ، سرمایه گذاری

نحوه استناددهی: رضایی، مسعود.، تجری مؤذنی، زهرا.، و تاجیک، اکرم. (۱۴۰۴). بیت کوین و ارز رمزنگاری شده: چالش‌ها، فرصت‌ها و تدابیر آینده. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، *۷*(۲)، ۱۴۵-۱۳۰.

© ۱۴۰۴ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۱۶ آذر ۱۴۰۳
تاریخ بازنگری: ۷ دی ۱۴۰۳
تاریخ پذیرش: ۲۰ دی ۱۴۰۳
تاریخ چاپ: ۲ مرداد ۱۴۰۴

مقدمه

از زمان ترویج و انتشار پول فیات (بدون پشتوانه) تاکنون که، مردم از آن برای معاملات روزمره استفاده می‌کنند، تجارت و معامله بسیار ساده‌تر بوده است. در سال ۲۰۰۹، پس از سقوط جهانی سال ۲۰۰۸، اولین شکل ارزهای رمزنگاری شده به شکل بیت کوین ظاهر شد. اولین بار توسط ناکاموتو (۲۰۰۸)، یک گروه یا فرد ناشناس بیت کوین را به عنوان اولین ارز دیجیتال برای انجام آسان‌تر تراکنش‌های روزانه از فردی به فرد دیگر معرفی کردند. بیت کوین بدون واسطه مانند بانک‌ها و موسسات پولی کار می‌کند. این یک نوع معامله همتا به همتا (پایاپا) است، بدون نیاز به افشای هویت فرد برای انجام یک معامله. برخلاف روش فعلی، بانک به عنوان واسطه یا واسطه عمل می‌کند، هویت خریدار و فروشنده را می‌داند، بنابراین مسائل مربوط به حفاظت از اطلاعات شخصی ایجاد می‌شود. پلتفرم بیت کوین تجارت و معامله ارزهای رمزنگاری شده را بسیار ساده‌تر و مستقل‌تر کرده است، بدون اینکه اطلاعات و جزئیات شخصی را به خطر اندازد. برای برخی، انتخاب این روش معامله به آن‌ها این امکان را می‌دهد که آزادانه و ناشناس معامله کنند.

بیت کوین اولین ارز دیجیتال در جهان است که از بستر بلاکچین استفاده کرده است. این در یک گزارش تراکنش با رایانه‌های شرکت شده در یک شبکه ایجاد می‌شود (Böhme et al., 2015). این بلاکچین دارای یکی از بالاترین سیستم‌های امنیتی است، زیرا به کلاهبرداران اجازه نمی‌دهد بیش از یک بار از این ارز استفاده کنند. پروتکل بلاکچین در عین این که بر اثبات کار متکی است، تضمین می‌کند که ماینرها به این ساختار همگرا می‌شوند. عملیات محاسباتی به عنوان هشینگ شناخته می‌شود که در آن اصطلاح توان هش به قدرت محاسباتی استخراج ارزها اشاره دارد (Kiayias & Panagiotakos, 2015).

سیستم موجود در بازار ارزهای رمزنگاری شده، حتی برای کنشگران این صنعت و محققانی که در این زمینه مطالعاتی انجام می‌دهند، بسیار پیچیده و کاملاً دشوار است (Fry & Cheah, 2016). بسیاری از محققان مزایای بیت کوین را این گونه برشمرده‌اند: امنیت (Bariviera et al., 2017)، هزینه پایین تراکنش (Kim, 2017)، بازده بالا (Hong, 2017) و در مورد ابزار جایگزین برای مکانیسم نجات یک کشور (Becker et al., 2013; Bentov et al., 2014) و استفاده از آن برای دستمزد کارکنان (Angel & McCabe, 2015) با وجود این، محققانی نیز به خطرات و معایب استفاده از این سکه دیجیتالی از لحاظ عدم وجود مقررات اشاره می‌کنند (Cheung et al., 2015)، قبض برق بالا به دلیل مصرف انرژی (Hayes, 2017)، عدم امنیت (Bradbury, 2013) و مسائل دیگر مانند ناشناس ماندن و تغییر هزینه (Luther & Salter, 2017) در ادامه لازم است تا پیشینه‌ای از ارز رمزنگاری شده بیان شود تا موضوع روشن‌تر شود.

ناکاموتو بیت کوین را در سال ۲۰۰۹ معرفی کرد و در ابتدا ۵۰ بیت کوین را در گردش عرضه کرد. در این مرحله اولیه، تبلیغات فقط از طرفداران کامپیوتر در سراسر جهان بی اهمیت گرفته شد (Vranken, 2017). در سال ۲۰۱۰، Mt Gox، یک شرکت ژاپنی، پلتفرمی را برای استفاده از بیت کوین به عنوان مکانیزم معاملاتی با ۲۰ کوین به قیمت ۴.۹۵۱ سنت طراحی کرد. حجم کل تقریباً یک دلار آمریکا بود. با افزایش استفاده از بیت کوین، قیمت به شدت افزایش یافت و در زمان نگارش این مقاله، قیمت به شدت افزایش یافت و به دلار آمریکا ۶،۷۷۷ رسید (Bitcoin Chart, 2018).

اساس ارزش بیت کوین بر اساس کمیابی است. این به عنوان پایه‌ای برای ارزش گذاری به هر شکل از پول عمل می‌کند. در روش فعلی استفاده از ارز فیات، مقام پول یا بانک مرکزی را حفظ کرده است. بانک مرکزی یک کشور قدرت تنظیم گردش پول و مقدار مطلق آن را دارد.

این بانک تنها می‌تواند مقدار محدودی از این پول کاغذی را برای تنظیم اقتصاد مالی یک کشور تولید نماید، بنابراین کمبود ایجاد می‌کند. این کمیابی در حسابداری بانک ثبت می‌شود و طبق قوانین قانونی حفظ می‌شود.

سوال اساسی که با معرفی بیت کوین ایجاد می‌شود این است که آیا این ارزهای رمزنگاری شده به عنوان پول واقعی در نظر گرفته می‌شوند؟ تاریخ مشخص کرده است که پول باید معیارهای زیر را داشته باشد: (۱) ذخیره بها. این یک قدرت خرید است که کاربران می‌توانند برای خرید کالا در زمان حال و آینده آن را استفاده کنند. (۲) وسیله مبادله. نوعی توانایی پرداخت و (۳) واحد محاسبه. ارزش قابل اندازه گیری برای هر کالایی برای فروش. از نظر تئوری پول باید تمام این معیارها را برآورده کند اما همیشه این طور نیست. با تجزیه و تحلیل بیت کوین و سایر ارزهای رمزنگاری شده به شکل فعلی، هر سه معیار قابل بحث هستند. می‌توان ادعا کرد که به دلیل توانایی پرداخت، قدرت خرید دارد، اما به دلیل عدم اطمینان، نمی‌توان تخمین زد که آیا بیت کوین می‌تواند در آینده همان طور که در حال حاضر استفاده می‌شود مورد استفاده قرار گیرد. برای مبادله، برخی می‌توانند توجیه کنند که ارز رمزنگاری شده می‌تواند به عنوان وسیله مبادله استفاده شود، اما برای دیگران کالاهای قابل مبادله محدود هستند.

اگر هر سه این معیارها به عنوان یک پیش نیاز برای هرگونه کالایی برای تعیین سطح پول تعیین شده اند، بنابراین باید در چارچوب استفاده و کاربرد آن پذیرفته شود. سیگار در زمان سخت جنگ جهانی دوم همه این معیارها را داشت، جایی که زندانیان در اردوگاه‌های جنگی از آن برای معامله استفاده می‌کردند. در گذشته، نمک پخت و پز را می‌توان در زمان امپراتوری روم که دستمزد نیروها با نمک پرداخت می‌شد، ارزشمند دانست. در مورد ارزهای رمزنگاری شده، می‌توان آن را برای افرادی که از رایانه و اینترنت استفاده می‌کنند، پول دانست. مشکل در این واقعیت نهفته است که تنها بخش کوچکی از مردم جهان به دستگاه‌های اینترنتی دسترسی دارند. بنابراین، در این زمینه، مشابه زندانیان در اردوگاه جنگ و سربازان رومی، ارزهای رمزنگاری شده فقط محدود به کسانی است که به اینترنت دسترسی دارند. فقط حدود ۲۰۰۰۰ دارندگان بیت کوین در انگلستان با تنها ۳۰۰ تراکنش در روز وجود دارد در حالی که این تعداد در کشورهای در حال توسعه به دلیل عدم دسترسی به اینترنت حتی کمتر خواهد بود.

ارزهای رمزنگاری شده، به ویژه بیت کوین، بیشتر به دلیل اینکه زمان واقعی آن قابل تبدیل به یک ارز معمولی با ارزش ثابت است، بیشتر بستری برای پرداخت است تا ارز. این ارز رمزنگاری شده از نظر تجزیه و تحلیل سبد سهام، مدیریت ریسک و تجزیه و تحلیل احساسات با سایر دارایی‌ها متفاوت است (Dyhrberg, 2016). در مقایسه با دارایی‌های دیگر مانند طلا، دارایی، سهام و حقوق صاحبان سهام، ارزهای رمزنگاری شده دارای سبد مشابهی از نظر ارزش خاص هستند. با این حال، ارز رمزنگاری شده شبیه احساسات مردم است، زمانی که ارزش آن افزایش می‌یابد و افراد بیشتری مایل به پذیرش آن‌ها به عنوان پرداخت هستند. این تفاوت‌ها فرصت‌های مختلفی را برای بازار ایجاد می‌کند که در آن سرمایه گذاران و سهامداران می‌توانند از آن سود ببرند. بنابراین، تصدیق ارز رمزنگاری شده به عنوان جایگزین پول فیات در اقتصاد امروز هنوز زود است و نیاز به درک بیشتری از نظر تئوری و عملی دارد.

استخراج و سیستم بلاکچین

ارز دیجیتال در ابتدا چگونه به دست آمد یا دریافت شد؟ در مورد پول فیات، این پول توسط بانک مرکزی صادر می‌شود، در حالی که ارز رمزنگاری شده با استخراج از طریق بلاکچین با استفاده از فناوری رمزنگاری ایجاد می‌شود. این روش صدور رمزارز جدید است. سیستم بلاکچین شامل کاربران، توسعه دهندگان، استخراج کنندگان، نگهدارندگان گره و تعاملاتی است که عملکرد دفتر کل توزیع شده را تضمین

می‌کند (Dos Santos, 2017). چنین فرآیند استخراج مستلزم آن است که ماینرها برای خرید نرم افزار و سخت افزار هزینه سرمایه‌ای داشته باشند. این نرم افزارها شامل GUIMiner، BFGminer و CGminer هستند که در استخراج بیت کوین استفاده می‌شوند و سخت افزارها AntMiner، Avalon و ASICMiner هستند. استخراج سایر ارزها که از الگوریتم‌های مختلف استفاده می‌کند، مستلزم استفاده از کارت‌های گرافیکی سطح بالا و سریع است. برای یک ماینر جدید، باید یک کیف پول و یک بانک رمزگذاری شده آنلاین ثبت شود که بتواند ارز رمزنگاری شده را ذخیره و قبول کند (Kiayias & Panagiotakos, 2015). هنگامی که یک ماینر بتواند معمای سیستم بلاکچین را حل کند، ارزهای دیجیتالی پاداش می‌گیرند و به کیفی که قبلاً از قبل تعیین شده بود منتقل می‌شود.

طبق بسیاری از پروتکل‌های ارزهای رمزنگاری شده، روش کار ماینینگ با اعتبار تراکنش با پیوند دادن به بلاک قبلی پذیرفته می‌شود (O'Dwyer & Malone, 2014). فناوری بلاک چین هر تراکنش را در واحد خود ثبت می‌کند (Eyal & Sirer, 2014). یک شناسه منحصر به فرد در هر بلوک و بلوک قبل از آن اختصاص داده شده است. به این می‌گویند پروتکل اثبات کار. اثبات کار پروتکل تأیید یک معامله و اطلاع دیگران در مورد آن است. کاربران یا ماینرها باید در تأیید یا اثبات هویت واقعی خود کار کنند. این آثار حول الگوریتم و پازلی حل می‌شود که می‌توان آن‌ها را با فرایند ریاضی رایانه حل کرد (Tschorsch & Scheuermann, 2016). اثبات کار منطبق بر اصل کار با ارز رمزنگاری شده، جایگزینی سیستم پرداخت متمرکز است که توسط سیستم بانکی اعمال شده است. اساس اصلی این سیستم دریافت هزینه از کاربر یعنی درخواست کننده خدمات در حل مشکلی است که حل آن در مقایسه با تأیید آن مشکل است (Becker et al., 2013). با این کار، اثبات اصل کار می‌تواند دسترسی به هر سرویس معینی را در استخراج و تجارت ارز رمزنگاری شده محدود کند.

ماینرها باید معمای تعبیه شده در بلوک را حل کنند، که شامل هش بلوک قبلی، هش تراکنش بلوک فعلی و نشانی است که پس از حل معما به آن پاداش داده می‌شود. این اساس فرآیند استخراج است. این به نوبه خود یک زنجیره بلوک ایجاد کرده که اثری از تراکنش می‌باشد که اتفاق افتاده است. این فناوری بلاکچین با دستکاری معاملات در دفتر کل، مانع از آن می‌شود که کلاهبرداران دو برابر پول رمزنگاری خود را خرج کنند (Vranken, 2017).

انتقادات وارد بر ارز رمزنگاری شده

انتقادات قابل توجهی به ارز رمزنگاری شده وارد شده است، یکی از آن‌ها این است که آیا این ارز نوعی دارایی است یا خیر. در شکل فعلی خود، با داشتن توانایی انجام معاملات پولی، بیت کوین و ارزهای رمزنگاری شده بسیار به هم نزدیکتر هستند و با تعریف ارز مطابقت دارند. اگرچه ارزهای رمزنگاری شده دارای معیارهای کاملی از سه ویژگی اصلی ارز هستند که عبارتند از ارزش ذخیره، واحد محاسبه و ابزار معامله، اما اکثر عناصر را دارد.

فرصت‌ها و مزایا

به عنوان یک کالای نسبتا جدید، فرصت‌های رمزنگاری امیدوارکننده به نظر می‌رسد. علیرغم افزایش قیمت و ارزش آن، ثمرات و فرصت‌های آینده هنوز دنبال آن هستند. موارد زیر در مورد فرصت‌های واقعی ارزهای رمزنگاری شده برای کاربران، سرمایه گذاران و از جمله دولت بحث می‌کند.

فناوری ایمن

از زمان کشف اینترنت، بلاک چین یکی از بهترین پلتفرم‌ها و پیچیده‌ترین فناوری محسوب می‌شود. این از نظر امنیت و محرمانه بودن برای معاملات آنلاین کارآیی ایجاد می‌کند. ینگ و همکاران (۲۰۱۸) در مطالعه موردی خود به این نتیجه رسیدند که علاوه بر امکان استفاده از ارزهای رمزنگاری شده، بلاک چین می‌تواند از اطلاعات محرمانه محافظت کند و همچنین واسطه گری را از هر موسسه‌ای حذف کند. حتی اگر گزارش‌هایی وجود داشته باشد که نشان می‌دهد بیت کوین ۴۰ درصد از هویت کاربر را فاش می‌سازد (Androulaki et al., 2013). این گزارش پس از پیروی کاربران از توصیه بیت کوین ادعا شد. این موضوع درباره حریم خصوصی هویت بر اساس ویژگی‌های ارز رمزنگاری شده که با غیرمتمرکز کردن سیستم از مشخصات کاربر محافظت می‌کند، اهمیت دارد. دو ایراد در این مطالعه وجود دارد: ایراد اول این که از سیستم بلاکچین واقعی استفاده نمی‌کند بلکه از شبیه سازی استفاده می‌کند و شبیه سازی فقط در یک دانشکده و تنها مشتمل بر دانشجویان انجام شد. به غیر از این، هیچ مطالعه دیگری تا زمان مطالعه نویسنده وجود نداشته است که اشکالات استفاده از بیت کوین و ارزهای رمزنگاری شده را نشان دهد که خطر افشای اطلاعات شخصی کاربر را آشکار می‌کند.

یکی از خطرات در مالکیت ارزهای دیجیتال معاملات مضاعف است، بدین معنا که شخصی می‌تواند با اعطای ارز یکسان به دو گیرنده مختلف، دو تراکنش موازی صادر کند (Tschorsch & Scheuermann, 2016). در مورد معاملات متمرکز و آنلاین، سیستم عملیاتی بانک قادر به تشخیص چنین فعالیت مشکوکی است. فناوری بلاک چین بسیار امن است. کلاهبرداران قادر به ارتکاب چنین جنایاتی نخواهند بود زیرا نمی‌توان چندین دفترکل را به طور همزمان تغییر داد یا اعتبار بخشید (Bariviera et al., 2017). اگر کلاهبرداران بتوانند مقدار زیادی از سهم اثبات قدرت هش کار را کنترل کنند، امنیت ارز رمزنگاری شده می‌تواند شکسته شود. قدرت هش قابلیت کنترل توان محاسباتی است. قدرت هش قدرت مورد نیاز شبکه ارزهای رمزنگاری شده برای عملکرد مداوم است. قدرت هش به طور متوسط در ۱۰ دقیقه که مصرف می‌شود محاسبه می‌شود. با کنترل اکثریت سهام در اثبات کار، کلاهبرداران می‌توانند با تهیه مخفیانه شعبه بلاکچین، قبل از پخش آن در شبکه زنجیره ای، در همان بلوک دو برابر هزینه کنند. از لحاظ نظری، تقلب را می‌توان در مقیاس وسیع انجام داد به شرطی که کلاهبرداران بتوانند درصد خاصی از قدرت هش را کنترل کنند. از طریق الگوریتم بیت کوین به صورت تصادفی دو نفره، در صورت کنترل ۵۱ درصد از قدرت محاسباتی، کلاهبردار می‌تواند هزینه‌ها را دو برابر کند (Shi, 2016). در پروتکل اثبات کار، تأیید اینکه آیا معامله مضاعف وجود دارد یا خیر، صرفاً براساس قدرت هش است، در عوض امکان هویت‌های جعلی متعدد وجود دارد (Tschorsch & Scheuermann, 2016). این اطمینان حاصل شده است که موضوع کلاهبرداران که مسئله کنترل حداکثری قدرت هش توسط کلاهبرداران با تأیید روش دیگر به جای تکیه تنها بر قدرت هش، تضعیف می‌شود. فرض بر این است که کنترل حداکثری قدرت هش سیستم بسیار دشوارتر از کنترل هویت اکثریت است. الگوریتم ارز رمزنگاری شده ایمن‌تر است و بهتر از استفاده از کارت‌های اعتباری است. حتی اگر هنوز مورد مطالعه قرار نگرفته است، ارز رمزنگاری شده با تراکنش مطمئنی که ارائه می‌دهد هزینه پردازش بسیار کمتری دارد. وان آلستین این گونه توضیح داد که استفاده از ارز رمزنگاری شده هنگام انجام معاملات امن‌تر است. مکانیسم انتقال ارز رمزنگاری شده با احراز هویت توسط خریداران و فروشندگان صورت می‌پذیرد. احراز هویت بین هر دو طرف از جعل هر گونه معامله جدید یا تأخیر در بازپرداخت معامله جلوگیری می‌کند. در مقایسه با کارت اعتباری، این جعل‌ها به دلیل مکانیزم آن اتفاق افتاده و ادامه خواهد داشت. فناوری نهفته در تراکنش کارت اعتباری برای دارنده کارت، بازرگان، بانک تجاری، شبکه کارت اعتباری و بانک صادر کننده خدمات ارائه می‌دهد (Papadimitriou, 2009). برای هر معامله واحد، فرآیند

پیچیده‌تر از چیزی است که به نظر می‌رسد. قبل از نهایی شدن معامله، باید به همه این واحدها مراجعه شود. فرصت ارتکاب کلاهبرداری در هر یک از این مراحل وجود دارد. حتی اگر اقدامات خاصی برای کاهش تقلب در کارت اعتباری انجام شده باشد، این سیستم در مقایسه با بلاکچین آسیب پذیرتر است. سیستم مورد استفاده در فناوری کارت اعتباری هنوز ایمن نیست، زیرا فناوری رمزنگاری دارای ارز رمزنگاری شده است. البته برخی اظهار داشته‌اند که علیرغم پیچیدگی الگوریتمی، سیستم بلاکچین پیچیده نیست. پیچیدگی فقط در گره و معمای ریاضی وجود دارد که با فرآیند استخراج حل می‌شود. به غیر از این، فناوری بلاک چین عملکردهای مفیدی را برای همه کاربران فراهم می‌کند. اسناد و مدارک دیجیتالی آنلاین و شناسایی در حال حاضر و در آینده نزدیک در سیستم بلاک چین به خوبی نهفته شده است.

هزینه معامله

در طول تاریخ، مردم از نوعی پول برای معاملات روزانه استفاده می‌کرده اند. در سیستم تجاری، سیستم مبادلات تجاری با استفاده از توافق دو طرف، تجارت را آغاز کرد، جایی که مردم کالاهای خود را مبادله پایاپا می‌کردند. با گذشت زمان، پول فیات برای مردم طراحی شده است تا بتوانند به راحتی و بدون نیاز به حمل کالاهای بزرگ به تجارت بپردازند. با ورود جهان به قرن ۲۱، ارز رمزنگاری شده بازار را متحول کرده و شرکت‌های چند ملیتی بزرگی از آن استفاده کرده اند. به عنوان هزینه فعلی معامله، هزینه‌های تراکنش ارز رمزنگاری شده و بیت کوین در مقایسه با سایر ارزهای معمولی کمتر است. با ویژگیهای بارز ارز رمزنگاری شده، غیر متمرکز و مقررات زدایی، هزینه کم تراکنش آن محاسبه می‌شود (Kim, 2017). مسائل قابل توجهی در سیستم پرداخت فعلی وجود دارد که توسط کارت‌های اعتباری و حقوق و دستمزد اعمال می‌شود. بهره‌ای که برای کاربرانی که در پرداخت‌های خود پیش فرض انجام می‌دهند بسیار زیاد است و می‌تواند یک کاربر را به ناامیدی مالی برساند (Angel & McCabe, 2015). این امر در مورد ارزهای رمزنگاری شده صادق نیست، جایی که معاملات زمانی اتفاق می‌افتد که کاربران نهایی توافق کرده باشند و تنها در این صورت حواله پول صادر می‌شود.

علاوه بر این، ارزهای رمزنگاری شده می‌توانند ۲۴ ساعت در روز و ۷ روز در هفته در طول سال کار کنند. قیمت گذاری داده‌ها فوراً در دسترس است که به موجب آن هر کس در جهان می‌تواند بدون هیچ هزینه‌ای تجارت کند تا زمانی که اینترنت در دسترس باشد (Pieters & Vivanco, 2017). از آنجا که جهان با توسعه اخیر اینترنت اشیا و تکیه بر داده‌های بزرگ بمباران شده است، داشتن قابلیت تجارت بدون محدودیت زمانی برای کاربران آسان است. این روش پرداخت برای نسل جوان که در آینده انتظار می‌رود صاحب مشاغل شوند و در چارچوب زمانی خاص خود کار کنند، بدون آنکه به ساعات کار معمولی وابسته باشد، تسهیل می‌شود. این روش معاملاتی نیز برای کاربران اینترنتی که نیازی به دریافت هزینه اضافی ناشی از استفاده از سایر سیستم‌های پرداخت ندارند مناسب است.

بازده بالا

ویژگی‌های متمایز ارز رمزنگاری شده و قابلیت مطابقت آن با عملکرد اقتصادی، آن را به یک دارایی منحصر به فرد تبدیل می‌کند. تاریخ نشان می‌دهد که بیت کوین یک ارز بسیار ناپایدار است اما بازده قابل توجهی برای سرمایه گذاران دارد. به غیر از این، ریسک بیت کوین به دلیل نسبت آن در سبدهای مختلف و متنوع کم است. همان طور که برای سرمایه گذاران شناخته شده است، به دست آوردن سود از سرمایه گذاری با خرید هر کالایی با قیمت پایین و فروش بالا است. برای کسانی که بیت کوین را در روزهای اولیه معرفی خود نگهداری می‌کردند، ممکن است ۱۰۰۰ تا ۱۰۰۰۰ درصد از سود سرمایه گذاری شده خود را جمع آوری کرده و از آن سود ببرند (Böhme et al., 2015).

استفاده از ارزهای رمزنگاری شده مانند استفاده از پول فیات یا استفاده از کارت‌های اعتباری در خرید کالاهای قانونی از خرده فروشان است. محبوبیت ارزهای رمزنگاری شده، به ویژه بیت کوین، به دلیل چندین رویداد خاص که بر کاربرد آن دلالت داشت، افزایش یافت، مانند بحران بانکی در قبرس از ۲۰۱۲ تا ۲۰۱۳ و بحران بدهی دولتی اروپا. قبرس با استفاده از مالیات بر سپرده‌های بانکی، گام‌هایی را در استفاده از ارزهای رمزنگاری شده برای دریافت کمک مالی برداشته است. این به دلیل عدم امنیت استفاده از سپرده‌های سنتی است (Luther & Salter, 2017).

یک برنامه ژنتیکی در ارزیابی الگوی سود در سرمایه گذاری ارزهای رمزنگاری شده تطبیق داده شد که حاکی از این بود که سیگنال‌های مکرر و سودآوری در الگوی حاصل از تجزیه و تحلیل وجود داشته است. معاملات با این الگو بیشتر شبیه سازی شد و سیگنال‌ها نشان می‌دهد که می‌تواند برای هر مجموعه‌ای از ارزهای رمزنگاری سودآور باشد. همچنین نظر به اهمیت بازگشت بیت کوین با استفاده از حرکت سری زمانی، به مدت ۸ هفته پیوسته مشخص شد که بازگشت قوی بیت کوین وجود دارد. براساس نظریه‌های دارایی مشهور، پیش بینی با شواهد ادامه بازگشت تجربی و معکوس با قابلیت پیش بینی سری‌های زمانی ثابت شد. همان طور که گفته شد، به دلیل نوسانات ارزهای رمزنگاری شده، طول و بازگشت بیت کوین در مقایسه با دارایی دیگر کوتاه‌تر بود. سرمایه گذاران نهادی می‌توانند با سرمایه گذاری در بیت کوین و در نظر گرفتن سبد سهام خود، سود کسب کنند (Hong, 2017).

چالش‌ها

با وجود فرصت‌های موجود در زمینه ارزهای رمزنگاری شده، هنوز چالش‌های زیادی در مواجه شدن با این نوع ارز مورد انتظار است. فعالان و سرمایه گذاران جدید احتمالاً گامی محتاطانه برداشته اند تا سرمایه گذاری سنگین انجام دهند یا خیر؛ زیرا احتمالا خطرات و چالش‌هایی که در معاملات و سرمایه گذاری در ارزهای رمزنگاری شده ایجاد می‌شود.

حقوق

در مورد پول فیات، استفاده از آن برای کاربران ایمن است، زیرا توسط بانک مرکزی یک کشور تنظیم می‌شود.

سیاست و نتیجه پولی یک کشور در اختیار کامل بانک مرکزی است. در مورد ارز رمزنگاری شده، هرکسی می‌تواند چندین حساب داشته باشد، بدون ایجاد هیچ گونه هزینه ای. بدون روشهای متمرکز صحیح بررسی و همچنین استفاده از نام واقعی آنها اجباری نیست (Böhme et al., 2015). این فرآیند در جایی مبهم است که تصور از فعالیت‌های غیرقانونی در ورای همه ثبت‌ها و معاملات ارزهای رمزنگاری شده به نوعی یک فریب نهفته باشد. ناشناس بودن در وب زمینه مناسبی برای بزهکاران و کلاهبرداران در ارتکاب اقدامات خود است. مجرمان سایبری از این بستر تجاری برای انجام فعالیت‌های نامشروع خود از جمله کلاهبرداری و تقلب استفاده می‌کنند. ارزهای رمزنگاری شده بیشتر توسط بزهکاران اقتصادی از جمله کلاهبرداری، پولشویی و قاچاق مواد مخدر استفاده می‌شوند. علیرغم اینکه فناوری بلاکچین برای سهولت کاربران در سراسر جهان ابداع شده است، مجرمان همیشه راه‌هایی برای کسب سود پیدا می‌کنند.

پیش از این، برخی از مقامات نظارتی از تایید بیت کوین به عنوان ارز به عنوان مثال در چین خودداری کرده بودند. چین استفاده از بیت کوین یا هر ارز دیجیتالی دیگر را در موسسات مالی و هر نوع تجارت ممنوع کرده بود. این اقدام توسط مقامات قابل درک است، زیرا معاملات و فعالیت‌های تجاری ارزهای رمزنگاری شده را نمی‌توان در بستر معاملاتی آن و ناشناس بودن پرسنل درگیر ردیابی کرد. با وجود اینکه برخی

کشورها از استفاده از ارزهای دیجیتالی حمایت می‌کردند، چین ممکن است آن را به دلیل پتانسیل آن در رشد اقتصادی و به عنوان یکی از ابرقدرت‌های اقتصادی جهان ممنوع کرده باشد (Cheung et al., 2015).

صورتحساب برق

صرف نظر از هزینه اولیه سرمایه گذاری در سخت افزار، هزینه اصلی دیگر که یک ماینر باید بپردازد، مصرف انرژی است. مشخص شده است که استخراج ارز دیجیتال قبوض برق بیشتری در مقایسه با پاداش‌هایی که با حل یک بلوک داده می‌شود، گرفته است. استخراج ارز رمزنگاری شده انرژی عظیمی گرفته است. هزینه استخراج با عملکرد سخت افزار متفاوت است. تولید برق از استخراج ارزهای رمزنگاری شده بین ۱۰ مگاوات (معادل یک نیروگاه کوچک) تا ۳-۶ گیگاوات (انرژی برآورد شده توسط کشورهای کوچک تا متوسط مانند بنگلادش و دانمارک مصرف می‌شود (Vranken, 2017).

تحقیقات با تاکید بر جنبه پایداری ارزهای رمزنگاری شده حاکی از این است که اثبات کار در استخراج این ارزهای دیجیتالی انرژی زیادی مصرف می‌کند و نیاز به قابلیت‌های رایانه‌ای فشرده و پیچیده دارد. با این وجود، این رایانه‌های پیچیده که شامل CPU، GPU بوده و در استخراج بلاکچین ضروری هستند لازم است تا از هزینه‌های مضاعف که حول جنبه امنیتی می‌چرخد جلوگیری شود. انتظار می‌رود که فعالیت‌های استخراج در دهه آینده کند شود و تنها کسانی که دارای سخت افزار به روز و قابل ملاحظه‌ای هستند در تجارت ارز دیجیتال و توانایی کاهش هزینه مصرف برق پایدار خواهند ماند (Vranken, 2017).

به دلیل اکثریت قریب به اتفاق این ارزها برای اثبات کار، به دلیل کار ریاضی سخت افزار مورد نیاز، نیاز به مصرف مقدار زیادی انرژی دارد. این امر به ویژه در فعالیت‌های ارزی در مقیاس بزرگ مضر است. این امر به نوبه خود منجر به انتشار دی اکسید کربن می‌شود و از طریق گرم شدن کره زمین که حیات را به نابودی می‌کشاند. سودآوری در تعارض با حیات بشری قرار می‌گیرد. اگر ثابت شود که فرآیند استخراج ارز بیشتر از فایده آن آسیب می‌رساند، دولت‌ها یا حتی سازمان ملل متحد باید در این زمینه مداخله کنند تا محیط زیست به خطر نیفتد.

سقوط و حباب

بازار کارآمد جایی است که اطلاعات گذشته در دسترس باشد و بتواند قیمت و تاریخ آن را به طور کامل منعکس کند. گفته می‌شود ارزهای رمزنگاری شده یک کالای ضعیف هستند زیرا سرمایه گذاران نمی‌توانند چشم انداز آینده را پیش بینی کنند و هیچ اطلاعاتی از گذشته در دسترس نیست. این امر از زمان ظهور ارز رمزنگاری شده در سال ۲۰۰۹، تقریباً یک دهه پیش، صادق است. سرمایه گذاری در این مدت کوتاه مطمئناً سوابق گذشته‌ای ندارد و سرمایه گذاران نمی‌توانند برای اطمینان از سودآوری سرمایه گذاری به سابقه اعتماد کنند. اگر ارزهای رمزنگاری شده دارای شکل واقعی حساب و ذخیره ارزش باشند، این قدر ناپایدار نخواهد بود. مانند مواجه شدن با خطر سقوط و حباب. پیش بینی می‌شود که ارزهای دیجیتال در آینده نزدیک به صورت حبابی خود برسند. با وجود این، هیچ حباب واقعی که در نهایت بیت کوین یا هر ارز رمزنگاری شده دیگری را کاهش دهد، واقعاً رخ نداده است.

نوسانات به طور متوسط ماهانه برای ارزهای رمزنگاری شده شدید است، زیرا در بیت کوین طلا بسیار ارزشمند است. از سوی دیگر، بیشترین نوسانات ماهانه طلا و سایر ارزها از کمترین نوسانات ماهانه بیت کوین بیشتر است. این بی‌ثباتی در بیت کوین نشان می‌دهد که ارز رمزنگاری شده برای سرمایه گذاری بلند مدت یک کالای غیرقابل اعتماد است. با توجه به این روند بی‌ثبات، این فرصت را ایجاد می‌کند که حباب و

سقوط رخ دهد. بیت کوین از سال ۲۰۱۱ تا ۲۰۱۳ دچار سه حباب بزرگ شده است که از ۶۶ به ۱۰۶ روز افزایش یافته است. بزرگترین رسوایی در این فاجعه حبابی، برای صرافی Mt Gox هزینه دربرداشت (Cheung et al., 2015).

تحقیقات قبلی نشان داده بود که حدس و گمان می‌تواند منجر به بی ثباتی دارایی‌ها شود. نوسانات قیمت بیت کوین نشان می‌دهد که معاملاتی است که به دلیل بروز حدس و گمان خدشه دار شده است. احتمالاً گمانه زنی می‌تواند وضعیت آن را به عنوان ارز قابل اجرا حذف کند. قیمت بیت کوین در قیمت معاملاتی اولیه آن تنها چند سنت بود و تا پایان سال ۲۰۱۳ به ۱۱۳۲،۲۶ دلار افزایش یافته بود. چند ماه بعد قیمت آن تقریباً ۶۰ درصد سقوط کرد. این نشانه بارز حباب دارایی بود. با توجه به اینکه افراد محدودی امروزه از بیت کوین به عنوان ارز رمزنگاری شده اصلی استفاده می‌کنند، ارزیابی آن به عنوان یک ارزش عادلانه دشوار است. برای معامله بیت کوین بدون هیچ گونه نرخ بهره، هیچ حسابی لازم نیست. در سراسر جهان، تقریباً کمتر از ۹۰۰۰ خرده فروش وجود دارد که بیت کوین را به عنوان روش پرداخت قبول می‌کنند. این کاربرد نامشخص بیت کوین ممکن است منجر به کلاهبرداری و طرح دیگری شود که می‌تواند منجر به از دست دادن سرمایه گذاری پولی شود. سرمایه گذاران می‌خواهند از ارزهای دیجیتال سود ببرند و به دنبال این هستند که آن‌ها را از خطرات احتمالی نجات دهند (Yermack, 2013). پیش بینی می‌شود که حباب‌ها در نهایت زمانی رخ می‌دهند که مقامات و سیاست‌های اقتصادی با عدم حمایت از ارز رمزنگاری شده مداخله می‌کنند، همان طور که از حباب جزئی بیت کوین در چندین مورد گزارش شده در بالا مشهود است.

حمله به شبکه

کِشتری ۲۰۱۷ اظهار داشت که فناوری بلاک چین دارای ویژگی غیر متمرکز و از حساسیت و امنیت پایینی برخوردار است. این موضوع راه را برای تقلب و جعل باز می‌کند. فناوری بلاکچین از نظر هویت و سیستم مدیریت دسترسی مربوط به اینترنت اشیا چالش‌های زیادی دارد. فعالیت‌های ماینری با استفاده از ایجاد مخزن در برابر دو نوع حمله آسیب پذیر هستند. این کار یا توسط اعضای مخرب مخزن یا اپراتورهای مخزن انجام می‌شود. اپراتورهای مخرب مخزن با ترکیب منابع موجود در مجموعه خود می‌توانند حمله سیبل[1] را در شبکه انجام دهند. در حالی که اعضای مخرب مخزن می‌توانند به طور بالقوه قدرت محاسباتی را در مخزن‌های ماینری خاص و بعداً در آینده افزایش دهند، آن را بی ثبات کنند. این کاربران به منظور تخریب بازده استخراج مخزن‌ها و جلوگیری از اثربخشی بلوک استخراج شده، از یک مخزن به مخزن دیگر می‌روند (Conte de Leon et al., 2017).

یکی دیگر از کاستی‌های ارزهای رمزنگاری شده، حمله به برنامه‌های کدگذاری شده است. کدنویسی شبکه توسط ناکاموتو، برای حمله باز است. این شبکه اکنون توسط یک گروه اصلی در منبع باز از طریق Github نگهداری می‌شود. حمله‌ای در ژوئن ۲۰۱۳ اتفاق افتاده بود، جایی که گره‌های بیت کوین توسط مهاجمی ناشناس در مسیر خود مورد حمله قرار گرفتند و اطلاعات را در شبکه منتقل کردند که در فعالیت‌های ماینری دخالت نداشت (Bradbury, 2013). همان طور که سوابق نشان داد، حمله آینده به شبکه بلاکچین نزدیک است. گرچه بزهکاران تا کنون موفق بوده اند، در صورتی که به طور جدی به این مسئله آسیب پذیری رسیدگی نشود، در نهایت راهی برای حمله به شبکه رمزنگاری بلاکچین پیدا خواهند کرد.

انتقادات پیرامون ارز رمزنگاری شده از اولین روز آغاز به کار آن مطرح بوده است. اتهام فعالیت غیرقانونی ارزهای رمزپایه زمانی مشخص شد که رسوایی جاده ابریشم توسط FBI متوقف شده است. جاده ابریشم یک بازار محبوب بود که کاربران در آن با استفاده از بیت کوین تجارت

[1]. Sybil.

می‌کردند. جاده ابریشم به عنوان بستری برای مشاغل مربوط به مواد مخدر و سایر فعالیت‌های غیرقانونی در مظان اتهام قرار گرفت. اما، طبق گفته الستین[1] تعطیلی جاده ابریشم تقصیر بلاکچین و ارزهای رمزنگاری شده نبود. در عوض، این بزهکاران بودند که از این فناوری برای انتفاع خود سوء استفاده کرده بودند، درست مانند سکوی دیگر که می‌تواند به نفع آن‌ها باشد. دومین مورد مشابه Mt Gox بود که سرمایه آن تا ۳۵۰ میلیون دلار سقوط کرد. می‌توان تصور کرد، قبل از توسعه کامل سیستم و تبدیل شدن به یک فناوری قابل اعتماد و قوی، عامل زمان یک آیتم مهم است. ارزهای رمزنگاری شده قبل از استفاده توسط توده مردم در سراسر جهان به زمان زیادی نیاز دارند. حتی Paypal، سیستم پرداخت الکترونیکی که در سال ۱۹۹۹ معرفی شد چندین بار مورد هدف مجرمان قرار گرفت. این سیستم پس از استحکام کامل حداقل ۵ بار مورد حمله قرار گرفته و به عنوان یک سیستم پرداخت الکترونیکی کارآمد و قابل اعتماد در جهان شناخته شده است (Jackson & Grey, 2014).

با توجه به سابقه بیت کوین، حباب‌ها تحت تاثیر گمانه زنی قرار می‌گیرند و افت قیمت تحت تأثیر مداخله دولت و سازمان‌های مرکزی پولی قرار می‌گیرد. بنابراین، برای علاقه مردم در پیش‌بینی مزایای ارز رمزنگاری شده، دولت باید سیاست‌ها و مقررات مناسبی را وضع کند که بتواند از منافع عمومی و همچنین کنشگران اصلی بازار اقتصادی محافظت کند. یک بازار تثبیت شده تضمین می‌کند که سیاست مالی یک کشور می‌تواند بدون تسلط بر تعامل بانک مرکزی متعادل شود. همه اینها بستگی به نحوه عملکرد دولت در بازار ارزهای رمزنگاری شده فعلی دارد، یا از وجود آن برای یک بار برای همیشه حمایت می‌کند یا آن را کاهش می‌دهد.

بهبود و کار در آینده بر روی ارزهای رمزنگاری شده

غیرقابل انکار است که ظهور ارز رمزنگاری شده نقش مهمی در ساختار اقتصادی جهان ایفا خواهد کرد. این واقعیت است که هر اقتصاددان، محقق و سرمایه گذار باید به طور کلی اقدامات لازم را برای تقویت دانش خود در مورد فناوری بلاکچین انجام دهد. از آنجایی که ارز رمزنگاری شده از نظر بازه زمانی هنوز به بلوغ نرسیده است، باید مطالعات بیشتری در مورد فناوری، پتانسیل و ریسک آن انجام شود تا اطمینان حاصل شود که فرصت‌ها فقط یک اتفاق ساده نیستند. همچنین، چالش‌های پیش رو، ذینفعان را در رکود ناشی از شکست‌های مالی قرار نمی‌دهد.

تحقیقات آینده در مورد کاهش ۵۱ حمله به شبکه استخراج بلاکچین باید بیشتر تقویت شود (Shi, 2016). پروتکل امنیتی باید بهتر از سیستم متداول بانکداری متداول در حفاظت از دارایی‌های پولی مشتری باشد. جنبه امنیتی کاربران، گواهی بی نظیر کنشگران این صنعت جدید را می‌طلبد تا با اطمینان و اعتماد نسبت به فناوری بلاک چین به کاربران اجازه دهد در انجام معاملات روزانه خود از طریق اینترنت به عنوان یک قاعده معمول عمل کنند.

در کاهش هزینه استخراج ارز، اثبات سهام می‌تواند مصرف انرژی کمتری در استخراج این ارزهای دیجیتالی ارائه دهد.. برای اثبات روش شناسی سهام، شخص باید ارزهای متعلق به خود و مقدار دارایی را تایید کند. فرد باید معامله‌ای از ارزهای خود را ایجاد کند که به عنوان پاداش با اطلاعات درصد از پیش تعیین شده به حساب خود ارسال می‌کند. اثبات سهام شبیه طرح قرعه کشی است که شانس یکسانی را برای همه ماینرها فراهم می‌کند. علاوه بر این، یک روش ترکیبی که شامل اثبات کار و اثبات سهام است، با پاداش بخشی از اثبات کار به تمام گره‌هایی که فعال هستند پیشنهاد شده است و در عین حال شرط تعیین کننده بلیط به دست آمده برای همه قرعه‌کشی است. برخی از

[1]. Alstyne.

پژوهشگران، اثبات فعالیت را پیشنهاد کردند که ترکیبی از اثبات کار و اثبات سهام است. در اثبات فعالیت، اصطلاح فعالیت به کاربران فعال اطلاق می‌شود که گره آنلاین کامل را حفظ کرده و پاداشی دریافت می‌کنند. در مقابل، برای اثبات سهام، کاربران آفلاین هنوز می‌توانند ارزها را در طول زمان جمع آوری کنند و این می‌تواند منجر به دو برابر هزینه همان بلوک شود. اثبات فعالیت امنیت بسیار بهتری در مواجهه با تهدیدات آینده ارز دیجیتال ارائه می‌دهد. فضای ذخیره سازی بیشتری دارد و ارتباطات شبکه مجازات کمتری را مجاز می‌داند. به علاوه، اثبات فعالیت همچنین هزینه‌های معاملاتی پایینی دارد، انرژی کمتری مصرف می‌کند و توپولوژی شبکه را می‌توان بداهه کرد (Bentov et al., 2014). بنابراین، جایگزین اثبات فعالیت به دلیل توانایی آن در جلوگیری از هزینه‌های مضاعف و مهمتر از همه هزینه برای دستیابی به ارز رمزنگاری شده در مقایسه با اثبات کار، بستر بهتری برای ارزهای رمزنگاری شده است.

اثبات شده است که داشتن دانش قابل توجهی در زمینه فناوری بلاک چین در کنترل تأثیر منفی استفاده از ارز رمزنگاری شده در فعالیت‌های روزمره ضروری است. بنابراین، تخصص در این زمینه باید با سیاست گذاران و نهادهای دولتی در تنظیم مقررات و سیاست‌های مربوط به موضع یک کشور در استفاده از ارزهای رمزنگاری شده همکاری کند. مدیریت دانش در میان کنشگران و محققان صنعت باید افزایش یابد تا مردم از پتانسیل و خطرات استفاده از ارزهای رمزنگاری شده مطلع شوند. حتی کارشناسان موسسه آموزش عالی باید با مردم در ارتباط باشند زیرا آن‌ها دارای منابع دانش هستند که جامعه را در داشتن دانش بهتر در مورد برخی مسائل تسهیل می‌کند.

نتیجه‌گیری

ارزهای رمزنگاری شده برای ماندن آمده‌اند. آینده تجارت به خوبی در فناوری‌های نوظهور جدیدی که می‌توانند به نفع بشر باشند، نهفته است. بدیهی است که کاربران و کنشگران صنعت می‌توانند ارزیابی کنند که آیا ارزهای رمزنگاری شده قادرند با توجه به اهداف و چشم اندازهای خود در تملک آن، به آن‌ها سود یا زیان برساند. بیت کوین و سایر ارزهای دیجیتال، تحول عمیقی در شیوه‌ی تراکنش‌های مالی ایجاد کرده‌اند و مفاهیمی چون تمرکززدایی، شفافیت و سرعت را به عرصه‌های مالی وارد کرده‌اند. با این حال، این فناوری همچنان با چالش‌های عمده‌ای روبرو است؛ از مسائل قانونی، مالیات و عدم تطابق با مقررات تا مشکلات امنیتی مانند هک و پول‌شویی و همچنین اثرات زیست‌محیطی بالای برخی شبکه‌های استخراج.

چالش‌ها شامل نبود چارچوب‌های حقوقی پایدار و یکپارچه، مشکلات در امنیت سایبری و مسائل فنی از جمله مقیاس‌پذیری و مصرف انرژی است. این چالش‌ها موجب شده‌اند که برخی کشورها استفاده از ارزهای دیجیتال را محدود یا ممنوع کنند.

فرصت‌ها نیز شامل امکان دسترسی به خدمات مالی برای افراد بدون دسترسی به بانک‌ها، ایجاد بسترهای مالی بدون مرز و امکان کاهش هزینه‌های تراکنشی است. بیت کوین و ارزهای رمزنگاری‌شده می‌توانند در رفع این موانع کمک کنند و تحولی در نظام مالی بین‌المللی ایجاد کنند.

تدابیر آینده نیز باید چندوجهی باشد. در سطح جهانی، به چارچوب‌های قانونی شفاف و یکپارچه‌ای نیاز است تا ضمن تسهیل نوآوری، حقوق کاربران و ثبات مالی حفظ شود. بهره‌گیری از فناوری‌های جدید برای کاهش مصرف انرژی و بهبود مقیاس‌پذیری نیز از دیگر اقدامات ضروری است.

در نهایت، آینده بیت کوین و ارزهای رمزنگاری‌شده در گروی یافتن تعادل میان فرصت‌ها و چالش‌ها است و نیازمند همکاری نزدیک میان سیاست‌گذاران، توسعه‌دهندگان فناوری و کاربران است تا این حوزه بتواند به عنوان یک جزء پایدار از نظام اقتصادی جهانی به رشد خود ادامه دهد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

Cryptocurrencies, particularly Bitcoin, have revolutionized the way individuals and institutions conceptualize currency, exchange, and financial autonomy in the digital era. Introduced in 2009 by the pseudonymous figure Satoshi Nakamoto, Bitcoin emerged as a decentralized, peer-to-peer system, independent of traditional financial intermediaries and resistant to conventional forms of state control. This innovation, underpinned by blockchain technology, ensures transactional integrity through consensus mechanisms and cryptographic validation. Unlike fiat currencies that rely on central bank authority and are governed by inflationary pressures and regulatory oversight, Bitcoin's architecture embodies scarcity, transparency, and distributed verification, giving rise to a system where trust is replaced by algorithmic assurance. Despite its relative infancy, Bitcoin has catalyzed broader developments in the cryptocurrency space, including the creation of myriad alternative digital assets. Yet, it also raises theoretical questions about the very definition of money. For an asset to be recognized as currency, it must function as a store of value, a medium of exchange, and a unit of account. Bitcoin and its counterparts fulfill these criteria only partially, as their volatility and adoption barriers limit their universality and practical application as stable financial instruments. Nonetheless, for digitally literate populations with internet access, cryptocurrencies present a new modality of economic agency, echoing past alternatives such as salt or cigarettes used as currency in times of crisis. However, adoption remains uneven globally, and access disparities further problematize their utility as universal monetary tools (Böhme et al., 2015; Fry & Cheah, 2016; Kiayias & Panagiotakos, 2015).

From a technological standpoint, blockchain—the foundational infrastructure of cryptocurrency networks—has been hailed as a breakthrough in digital security and transparency. The process of mining, which validates transactions and introduces new coins into circulation, is governed by the "proof-of-work" protocol, wherein computational puzzles must be solved to confirm and record transaction blocks. This decentralized ledger system prevents double-spending and ensures consensus without the need for a central authority (Dos Santos, 2017; Eyal & Sirer, 2014; O'Dwyer & Malone, 2014). Miners who successfully validate blocks are rewarded with cryptocurrency, incentivizing participation and sustaining network operations. However, this process demands significant energy and computational resources, often requiring investment in specialized software and hardware, such as ASIC miners and advanced GPUs. While the cryptographic nature of the blockchain enhances its security, particularly against tampering and fraudulent transactions,

concerns persist regarding the potential for malicious actors to accumulate over 51% of hashing power, thereby compromising network integrity and enabling attacks such as double spending. Theoretical models demonstrate that should this threshold be surpassed, attackers could alter transaction history or block legitimate transactions, highlighting the tension between decentralization and security in proof-of-work systems (Shi, 2016; Tschorsch & Scheuermann, 2016). These vulnerabilities underscore the importance of continued innovation in consensus mechanisms and the exploration of hybrid models that combine efficiency, accessibility, and resistance to centralization.

The promise of cryptocurrency lies not only in its technological architecture but also in its practical advantages over traditional financial systems. Key among these is the reduction in transaction costs, as cryptocurrencies eliminate intermediaries and operate independently of centralized banking institutions. This allows for direct peer-to-peer transactions, enabling financial inclusion, especially in underbanked regions. Moreover, transactions are processed quickly and globally, unbound by geopolitical borders or the operating hours of conventional banks. For investors and traders, the potential for high returns is another alluring feature, given Bitcoin's historical performance and rapid appreciation in value since its inception (Angel & McCabe, 2015; Kim, 2017; Pieters & Vivanco, 2017). Cryptocurrencies also offer an alternative store of value in times of economic instability, as demonstrated during the European debt crisis and Cyprus banking collapse. In such scenarios, Bitcoin provided a hedge against institutional risk, prompting broader interest among institutional investors and hedge funds. Additionally, the transparent and immutable nature of blockchain appeals to users wary of systemic corruption or opaque financial systems. With round-the-clock availability and global accessibility, cryptocurrencies enable users to transact at any time, further enhancing their appeal in a digitally integrated world economy. Their integration with big data and the Internet of Things signals a paradigm shift in transactional infrastructure, moving toward a decentralized financial future governed by code rather than bureaucracy (Bariviera et al., 2017; Hong, 2017; Luther & Salter, 2017).

Despite these opportunities, the cryptocurrency landscape is fraught with complex legal and regulatory challenges. Unlike fiat currencies, which are subject to oversight by central banks and international financial institutions, cryptocurrencies operate within legal gray zones in many jurisdictions. The anonymity and decentralization of transactions make it difficult to enforce anti-money laundering (AML) regulations or prevent illicit activities such as fraud and drug trafficking. Regulatory responses vary significantly across countries: while some embrace cryptocurrencies and integrate them into financial systems, others—such as China—have imposed strict bans on their use in financial institutions due to concerns over volatility, capital flight, and untraceable transactions (Bradbury, 2013; Cheung et al., 2015). Moreover, the absence of a unified legal framework complicates cross-border enforcement and investor protection, heightening the risk for retail participants. Energy consumption is another pressing issue. Cryptocurrency mining is notoriously power-intensive, with estimates indicating that the global Bitcoin network consumes as much energy as small countries. This raises environmental concerns, particularly regarding carbon emissions and sustainability. If the environmental costs outweigh the financial benefits, governments may be compelled to intervene with regulations or outright bans to protect ecological integrity (Hayes, 2017; Vranken, 2017). Thus, the long-term viability of cryptocurrencies may hinge on the development of energy-efficient consensus mechanisms such as proof-of-stake or proof-of-activity, which promise to maintain network security while significantly reducing energy usage (Bentov et al., 2014).

Beyond energy and legal considerations, the volatility and speculative nature of cryptocurrencies pose further risks to their widespread adoption. Unlike traditional assets with historical performance data and market stability, cryptocurrencies are relatively new and subject to dramatic price swings. Bitcoin, for instance, has experienced multiple boom-and-bust cycles within short time frames, contributing to perceptions of it being a speculative bubble rather than a stable currency. These fluctuations are exacerbated by the lack of intrinsic value and the role of public sentiment in driving prices. Studies suggest that speculative behavior, rather than fundamental valuation, dominates cryptocurrency markets, making them vulnerable to manipulation and sudden crashes (Yermack, 2013). The infamous Mt. Gox collapse exemplifies the consequences of poorly regulated exchanges and the fragility of early infrastructure. While price volatility creates profit opportunities for experienced traders, it also introduces considerable risk for average users and investors. As such, the potential for market crashes undermines cryptocurrencies' utility as reliable stores of value or mediums of exchange, particularly for those seeking long-term financial security. The challenge, then, is to create a regulatory and technological environment that mitigates these risks while preserving the decentralized ethos that makes cryptocurrencies revolutionary (Becker et al., 2013; Conte de Leon et al., 2017; Jackson & Grey, 2014).

In conclusion, the evolving ecosystem of cryptocurrencies represents a profound transformation in global financial structures, offering alternatives to traditional currency systems and expanding the horizons of digital economic interaction. Bitcoin and similar digital assets have opened new possibilities for decentralized transactions, financial autonomy, and technological innovation, yet their path forward remains contested. Balancing innovation with regulation, minimizing environmental impact while maintaining network security, and ensuring broader inclusion without sacrificing decentralization are critical challenges. As governments, developers, and users navigate this uncharted terrain, a collaborative, informed, and adaptive approach will be essential in shaping a future where cryptocurrency can become a stable and inclusive component of the global economic order.

References

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. International Conference on Financial Cryptography and Data Security,

Angel, J. J., & McCabe, D. (2015). The ethics of payments: Paper, plastic, or Bitcoin? *Journal of Business Ethics*, *132*(3), 603-611. https://doi.org/https://doi.org/10.1007/s10551-014-2354-x

Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and its Applications*, *484*, 82-90. https://doi.org/https://doi.org/10.1016/j.physa.2017.04.159

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. The Economics of Information Security and Privacy,

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34-37. https://doi.org/https://doi.org/10.1145/2695533.2695545

Bitcoin Chart. (2018). *Bitcoin chart*. https://charts.bitcoin.com/

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

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security*, *2013*(11), 5-8. https://doi.org/https://doi.org/10.1016/S1361-3723(13)70101-5

Cheung, A., Roca, E., & Su, J. J. (2015). Crypto-currency bubbles: an application of the Phillips-Shi-Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, *47*(23), 2348-2358. https://doi.org/https://doi.org/10.1080/00036846.2015.1005827

Conte de Leon, D., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 286-300. https://doi.org/https://doi.org/10.1108/APJIE-12-2017-034

Dos Santos, R. P. (2017). On the Philosophy of Bitcoin/Blockchain Technology: Is it a Chaotic, Complex System? *Metaphilosophy*, *48*(5), 620-633. https://doi.org/https://doi.org/10.1111/meta.12266

Dyhrberg, A. H. (2016). Hedging capabilities of bitcoin. Is it the virtual gold? *Finance Research Letters*, *16*, 139-144. https://doi.org/https://doi.org/10.1016/j.frl.2015.10.025

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. International conference on financial cryptography and data security,

Fry, J., & Cheah, E. T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, *47*, 343-352. https://doi.org/https://doi.org/10.1016/j.irfa.2016.02.008

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, *34*(7), 1308-1321. https://doi.org/https://doi.org/10.1016/j.tele.2016.05.005

Hong, K. (2017). Bitcoin as an alternative investment vehicle. *Information Technology and Management*, *18*(4), 265-275. https://doi.org/https://doi.org/10.1007/s10799-016-0264-6

Jackson, E., & Grey, C. (2014). *Bitcoin is the new Paypal*. http://tcrn.ch/1fqELeT

Kiayias, A., & Panagiotakos, G. (2015). Speed-Security Tradeoffs in Blockchain Protocols. https://eprint.iacr.org/2015/1019

Kim, T. (2017). On the transaction cost of Bitcoin. *Finance Research Letters*, *23*, 300-305. https://doi.org/https://doi.org/10.1016/j.frl.2017.07.014

Luther, W. J., & Salter, A. W. (2017). Bitcoin and the Bailout. *The Quarterly Review of Economics and Finance*, *60*, 50-56. https://doi.org/https://doi.org/10.1016/j.qref.2017.01.009

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint. 25th IET Irish Signals and Systems Conference and China-Ireland International Conference on Information and Communications Technologies (ISSC/CIICT 2014),

Papadimitriou, O. (2009). *How Credit Card Transaction Processing Works: Steps, Fees & Participants*. https://wallethub.com/edu/credit-card-transaction/25511/

Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, *39*, 1-14. https://doi.org/https://doi.org/10.1016/j.infoecopol.2017.02.002

Shi, N. (2016). A new proof-of-work mechanism for bitcoin. *Financial Innovation*, *2*(1), 31. https://doi.org/https://doi.org/10.1186/s40854-016-0045-6

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *Ieee Communications Surveys & Tutorials*, *18*(3), 2084-2123. https://doi.org/https://doi.org/10.1109/COMST.2016.2535718

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, *28*, 1-9. https://doi.org/https://doi.org/10.1016/j.cosust.2017.04.011

Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal. https://doi.org/10.3386/w19747