بسمه تعالی

پایان‌نامه برای دریافت درجه کارشناسی ارشد

فقه مقارن و حقوق خصوصی اسلامی

"مطالعه تطبیقی رمزارزها از دیدگاه مذاهب اسلامی و قوانین پولی بانکی ایران"

استاد راهنما: جناب آقای دکتر محمدحسین مختاری
استاد مشاور: جناب آقای دکتر حامد رستمی

نگارش:
کوثر بابایی

زمستان ۹۸

تقدیر و تشکر

برخود لازم می‌دانم از همه کسانی که در مسیر علم‌آموزی همراه و راهنمایم بوده‌اند، علی‌الخصوص پدر و مادر مهربانم و همسر و فرزند عزیزم که همواره حامی و مشوقم در تمام مراحل زندگی بوده‌اند تشکر کنم. همچنین از تمام ا ساتید و معلمانم در مقاطع مختلف تح صیلی و به‌خ صوص ا ساتید فرهیخته‌ام که در انجام این پژوهش راهنمایم بودند، جناب آقای دکتر مختاری و جناب آقای دکتر رستمی کمال تشکر را دارم.

چکیده

با ظهور بیت کوین[1]در سال ۲۰۰۸ میلادی، کارشناسان حوزه مالی، خبر از تولد پدیده‌ای تحول‌ساز می‌دادند. پدیده‌ای که در عمر کوتاه خود نهاد بانک و مرکزیت در مبادلات مالی را هدف قرار داده بود و با وجود مخالفت دولت‌ها و رگولاتوری‌های سخت‌گیرانه با قدرت به مسیر رشد خود ادامه داد. یکی از نکات قابل توجه در مورد پدیده رمزارزها و به‌طور خاص بیت‌کوین، تکنولوژی بستر آن بود، فناوری بلاک‌چین یا زنجیره‌بلوک که توانسته بود با بکارگیری ابزار ریاضیات و رمزنگاری به‌صورت بهینه مساله عدم اعتماد را در شبکه همتا به همتا حل کند و معماری منحصربه‌فردی را پیشنهاد کند که بدون نیاز به وجود ناظر، تراکنش‌ها تایید شده و شبکه پایدار بماند.

در این پژوهش که به روش توصیفی و تحلیلی انجام شده، ابتدا مروری بر تاریخچه فناوری زنجیره‌بلوک و رمزارزها و ادبیات موضوعه خواهیم داشت. در ادامه پدیده رمزارزها و به‌طور خاص بیت‌کوین را از منظر فقه مذاهب اسلامی مورد بررسی قرار می‌گیرد و فرآیندهای ذیل این پدیده از قبیل استخراج را با عقود فقه معاملات تطبیق داده می‌شود، در بخش دیگری از پژوهش، ظرفیت‌های قوانین جمهوری اسلامی از قبیل قانون تجارت الکترونیک، قانون مبارزه با پولشویی و ... جهت پذیرش این پدیده نوظهور در چارچوب قوانین موجود بررسی می‌شود. نهایتاً در فصل آخر و پس از جمع‌بندی موارد مذکور، مطالعات فقهی و حقوقی در مورد قراردادهای هوشمند به‌عنوان محصول نسل دوم فناوری زنجیره‌بلوک پیشنهاد شده است.

کلید واژگان: زنجیره‌بلوک، رمزارز، بیت‌کوین، رمزنگاری، فقه مذاهب اسلامی

---

[1] Bitcoin

[2] Cryptocurrency

فهرست مطالب

فهرست تصاویر

کلیات و مفاهیم تحقیق

تبیین مسأله

رمزارز چیست؟ پول، کالای دیجیتال، سهامی از یک پروژه فناوری اطلاعات؟

این پدیده نوظهور از منظر فقه مذاهب اسلامی چه احکامی دارد؟

از زمان بعثت رسول اکرم (ص)، رویکرد شریعت و فقه اسلامی راجع به پدیده‌های نوظهور امضایی بوده، طبیعتا همه پدیده‌ها توسط اسلام تاسیس نشده‌اند و برخی از آن‌ها سابقه‌ای تاریخی داشته‌اند و برخی هم بعد از اسلام متولد شده‌اند. مسلمین و متشرعین همواره به دنبال یافتن موضع نهاد دین پیرامون پدیده‌ها بوده اند و بر آن اساس با آن پدیده برخورد کرده‌اند. شاید بتوان از فتوای حرمت تنباکو میرزای شیرازی بعنوان مثال معروف معاصر در این رابطه نام برد. البته مشابه این موضوع را در اعلام نظر مراجع پیرامون اپراتور سوم به یاد داریم. اعلام موضعی که آینده اپراتور سوم را دستخوش تغییر اساسی کرد. در این پژوهش به موضوعی خواهیم پرداخت که مولود تلاقی اقتصاد و فناوری است. رمزارزها[۱]نام شناخته شده‌ای برای همگان نیستند و شاید عموم با نام بیت‌کوین[۲]بیشتر آشنا باشد. رمزارزها که خود شعبه‌ای از ارزهای دیجیتال[۳]هستند با چند رمزارز مطرح و قدیمی تر یعنی بیت‌کوین و اتریوم[۴]شناخته می‌شوند در حالی که امروزه بیش از ۲۰۰۰ رمزارز در بازارهای مالی دنیا موجودند و حجم بازار رمزارزها حدود ۱۵۰ میلیارد دلار است. در ابتدای امر، اقتصاددانان بیت‌کوین را جدی نگرفتند تا اینکه این پول جدید از پس حوادث متعددی برآمد و دولت‌ها را ناچار به پذیرش و قانون گذاری پیرامون خود کرد. کشور ما هم از این موضوع مستثنی نیست و فرآیند گنارش[۵]رمز ارزها در دست انجام است و نهادهایی از قبیل، مرکز ملی فضای مجازی، بانک مرکزی، قوه قضاییه، مرکز پژوهش‌های مجلس شورای اسلامی، پلیس فتا و .... درگیر آن شده‌اند. بخشی از کندی فرآیند قانون‌گذاری رمزارزها در کشورمان به عدم اظهار نظر صریح و شفاف نهاد دین در این خصوص برمی‌گردد. ابتدا لازم است که زوایا و خفایای این پدیده نوظهور مشخص شود و پس از لیست کردن سوالات فقهی و استفتاء از مراجع عظام تقلید، موضع شریعت در این باره مشخص شود. بسترسازی جهت روشن شدن زوایا و خفایای این پدیده و مقدمات لازم بر عهده دانشگاه‌ها و حوزه‌های علمیه و مراکز پژوهشی و در قالب پایان نامه ها و مقالات است. مراکز اسلامی بین‌المللی در کشورهای اندونزی، ترکیه، آفریقای جنوبی، مصر و ... تحقیقاتی را پیرامون رمزارزها انجام داده‌اند که بعنوان منابع تحقیقی فقه فرق اسلامی از آن‌ها بهره خواهیم گرفت.

---

۱ Cryptocurrency

۲ Bitcoin

۳ Digital Currency

۴ Etherium

۵ Regulation

پدیده رمزارزها

کمی به قبل باز میگردیم، پس از اینکه اینترنت در دهه ۱۹۷۰ میلادی از مدل آزمایشگاهی تبدیل به مدلی جهانی شد تا سالهای دهه ۹۰ میلادی که همه دنیا را فراگرفت همواره این سوال وجود داشت که در این دنیای گسترده و بدون مرز مجازی چه پدیده ای نقش پول را ایفا خواهد کرد؟ وقتی خرید یک کالا از قاره‌ای دیگر با بستر اینترنت مقدور شده پس باید پولی جهان‌روا و امن که مورد قبول طرفین معامله است هم وجود داشته باشد. در همین راستا تلاش‌های گسترده‌ای صورت گرفت و در سال‌های دهه ۹۰ میلادی پول‌های دیجیتالی از قبیل دیجی‌کش[۱]و ای گلد[۲]ظهور کردند. اما این پول‌ها دو ایراد عمده داشتند اول اینکه بصورت متمرکز اداره می‌شدند و دوم اینکه در برابر تورم مقاوم نبودند. متخصصین فناوری اطلاعات و رمزنگاری[۳]دست به کار شدند تا پولی غیرمتمرکز،[۴] بدون پشتوانه و فوق‌العاده امن را ارائه کنند. حاصل این تلاش‌ها در سال ۲۰۰۹ میلادی نتیجه داد و بیت‌کوین متولد شد. پولی که از فناوری زنجیره‌بلوک[۵]بهره می‌برد و به معنی واقعی کلمه امن، غیرمتمرکز، ضد تورم و بدون پشتوانه‌های رایج است.

اهمیت و ضرورت تحقیق

رمزارزها پدیده‌ای است که در عمر کمتر از ۱۰ ساله خود اکثر دولت‌ها را وادار به پذیرش و قانون‌گذاری پیرامون خود کرده است. بازاری با حجم بالغ بر ۲۰۰ میلیارد دلار و روند گسترش چشمگیر آن، ایجاب می‌کند تا از منظر فقه مذاهب اسلامی بررسی شود و پاسخی کامل و جامع به شبهات مسلمین در زمینه رمزارزها داده شود. امروزه تعدادی از مسلمین با استخراج رمزارزها امرار معاش می‌کنند، برخی مشغول معاملات رمزارزها هستند و ... پس ارائه احکام صریح و شفاف فقه اسلامی در زمینه رمزارزها حیاتی است.

اهداف تحقیق

باتوجه به موارد مذکور در توصیف اهمیت این پژوهش، اجمالا می‌توان گفت، در این پژوهش یک هدف اصلی و چند هدف فرعی دنبال خواهد شد که:

- **هدف اصلی**

✓ نگاه به پدیده رمزارزها از منظر حاکمیت اسلامی با تحلیل دقیق این پدیده، که زمینه ساز رگولاتوری دقیق خواهد شد.

---

[۱] DigiCash
[۲] E-gold
[۳] Cryptography
[۴] Decentralized
[۵] Blockchain

- **اهداف فرعی**

✓ پاسخ به سوالات و شبهات فقه فردی در زمینه رمزارزها که مسلمین فعال در این حوزه با آن‌ها روبه‌رو خواهند شد.

✓ بررسی نظرات علمای مذاهب اسلامی پیرامون پدیده رمزارزها.

✓ بررسی ظرفیت‌های این پدیده جهت همکاری‌های اقتصادی و تجاری کشورهای مسلمان.

سؤالات تحقیق

- **سوال اصلی**

✓ احکام رمزارزها از دیدگاه فقه مذاهب اسلامی و حقوق جمهوری اسلامی ایران چیست؟

- **سوالات فرعی**

✓ سرمایه گذاری در عرضه اولیه رمزارزها از منظر فقه مذاهب اسلامی و حقوق جمهوری اسلامی ایران چه احکامی دارد؟

✓ کسب درآمد از طریق استخراج رمزارزها از نگاه فقه مذاهب اسلامی و حقوق جمهوری اسلامی ایران چه حکمی دارد؟

✓ خرید وفروش و معاملات رمزارزها در صرافی ها از منظر فقه مذاهب اسلامی و حقوق جمهوری اسلامی ایران چگونه تفسیر می شود؟

پیشینه تحقیق

پژوهش‌های صورت گرفته پیرامون بررسی فقهی رمزارزها در مراکز دانشگاهی و حوزوی، بسیار محدودند و طبق بررسی‌های انجام شده یک مورد پایان نامه کارشناسی ارشد در دانشگاه امام صادق (ع) انجام شده که نتیجه آن بعنوان کتاب در صف انتشار است که البته رویکرد آن بیشتر متوجه اقتصاد اسلامی است. همچنین پایگاه مجلات تخصصی نور، وبسایت مقالات حوزه علمیه، سایت تبیان و .... در این خصوص بررسی شده و کار پژوهشی با موضوع مطروحه (مطالعه تطبیقی رمزارزها از دیدگاه فقه مذاهب اسلامی و حقوق جمهوری اسلامی ایران) در ابعاد پایان نامه کارشناسی ارشد یافت نشد.

مقالاتی با عناوین ارزهای دیجیتال، پول مجازی و ... در نشریات مختلف منتشر شده که از این مقالات بعنوان منابع پژوهش استفاده شده است.

یکی از مهمترین منابع این پژوهش کار تحقیقی وزینی است که توسط مفتی محمدابوبکر در موسسه اقتصاد اسلامی بلاسوم اندونزی در سال ۲۰۱۸ انجام شده که از ماحصل این پژوهش هم استفاده کرده ایم.

نوآوری تحقیق

خرید و نگهداری رمزارزها، معاملات رمزارزها، استخراج رمزارزها و سرمایه‌گذاری در عرضه اولیه رمزارزها مواردی است که جامعه اسلامی دچار آن شده است و طبق آمار رئیس کمیسیون اقتصادی مجلس شورای اسلامی، حدود ۲ میلیارد دلار از انواع مختلف رمزارزها توسط هموطنانمان خریداری شده است. در این شرایط با بررسی دقیق و موشکافانه فرآیندهای فنی موارد فوق الذکر و تطبیق با عقود فقهی و بررسی خیارات از منابع فقهی مذاهب اسلامی سعی بر ایجاد سندی قابل استفاده در این زمینه خواهیم داشت. در ادامه پژوهش پدیده رمزارزها را از منظر فقه حکومتی بررسی خواهیم کرد این پدیده را با قواعد نفی سبیل و لاضرار و ... تطبیق می دهیم و سعی می‌کنیم تا جایگاه حاکمیت اسلامی نسبت به پدیده رمزارزها تبیین شود با این توضیح که حکومت اسلامی در جایگاه قانون گذاری، نظارت، آموزش و آگاه‌سازی شهروندان و حمایت از کسب و کارهای مبتنی بر رمزارزها مسئولیت خواهد داشت. مسائل فوق الذکر بصورت جامع و یکجا تاکنون موضوع اصلی هیچ پایان نامه یا پروژه پژوهشی دانشگاهی نبوده‌اند.

کارهایی که تاکنون در این حوزه صورت گرفته یا معطوف به مسائل فنی و تکنولوژی رمزارزها بوده یا با رویکرد اقتصادی رمزارزها را تحلیل و بررسی کرده‌اند و بررسی فقهی جامع این پدیده نوظهور تاکنون مغفول مانده است. طبق استعلام صورت گرفته از ایرانداک، پژوهشی با این موضوع تا به حال صورت نگرفته است.

در آخر با توجه به شان تقریبی دانشگاه مذاهب اسلامی، ظرفیت های رمزارزها بعنوان تکنولوژی بستر برای ایجاد یک سامانه پولی چندجانبه بین دولت‌های اسلامی بررسی خواهد شد.

کاربردهای تحقیق

تامین محتوای لازم برای دستگاه های تصمیم‌گیر در زمینه قانون‌گذاری رمزارزها از قبیل شورای فقهی بانک مرکزی، کمیسیون اقتصادی و مرکز پژوهش‌های مجلس شورای اسلامی، مرکز ملی فضای مجازی، قوه قضاییه، سازمان امور مالیاتی و ... را می‌توان از کاربردهای اصلی نتایج این تحقیق برشمرد. علاوه بر آن باتوجه به بررسی پدیده رمزارزها از منظر فقه فردی در این پژوهش، نتایج به‌دست آمده برای مسلمانان فعال در زمینه رمزارزها نیز قابل استفاده خواهد بود.

روش تحقیق

روش تحقیق در این پژوهش، توصیفی- تحلیلی خواهد بود و روش جمع آوری اطلاعات کتابخانه ای است. به این منظور، شاکله اصلی پژوهش از کتب و مقالات جدید که در بخش منابع ذکر شده، استخراج خواهد شد. همچنین جهت تکمیل و غنای پژوهش از نظر کارشناسان رمزارها استفاده خواهد شد که این بخش بصورت مصاحبه شفاهی انجام شده و پس از پیاده سازی و تطبیق با منابع، به پایان نامه اضافه خواهد شد.

ساختار تحقیق

ما در این پژوهش، در فصل اول، پس از ذکر مقدمات و ادبیات موضوعه حوزه رمزارزها به موضوع پر اهمیت رگولاتوری از منظر دولت‌های مختلف خواهیم پرداخت، تاثیر این پدیده نوظهور را در اقتصاد بررسی می‌کنیم و با توجه به شناخت حاصل از این پدیده در بخش‌های قبلی و فرصت‌ها و چالش‌های پیش‌روی این پدیده مقدمات لازم را جهت ارائه چارچوب رگولاتوری رمزارزها در قالب قوانین جمهوری اسلامی در فصل‌های آتی فراهم خواهیم کرد. در فصل دوم، با این پیش‌فرض که پدیده رمزارزها یک محصول حوزه مالی و اقتصاد است، به تعریف مال و شروط مالیت از منظر فقه اسلامی خواهیم پرداخت و در ادامه با مرور عقود و خیارات فقه معاملات زمینه را برای پدیده‌شناسی فقهی و بررسی صحت معاملات رمزارزها در فصل سوم مهیا خواهیم کرد. در فصل سوم از این پژوهش، با رجوع به مقدمات پیش‌گفته مسائل فقه فردی رمزارزها از قبیل، معاملات رمزارزها در بازارهای بین‌المللی، مسئله استخراج رمزارزها و سرمایه‌گذاری در عرضه اولیه سکه را مورد بررسی و تطبیق با عقود فقه معاملات قرار خواهیم داد. سپس به مسائل رمزارزها از منظر فقه حکومتی و بررسی ظرفیت قوانین جمهوری اسلامی ایران از قبیل قانون مدنی و قوانین تجارت الکترونیک خواهیم پرداخت. در فصل چهارم با رویکرد تطبیقی به ارائه نظر کارشناسان و علمای مذاهب اسلامی در مورد پدیده رمزارزها پرداخته‌ایم و با این مقدمه، پیشنهاد پیمان پولی چندجانبه بین دولت‌های اسلامی جهت تسهیل در مبادلات اقتصادی و بازرگانی مستقل از هژمون دلار را ارائه کرده‌ایم. در این پیشنهاد ایجاد یک رمزارز با پشتوانه دارایی‌های کشورهای اسلامی، از قبیل نفت و گاز، جهت تسویه مالی مبادلات اقتصادی، ارائه شده است. در بخش آخر این پژوهش، پس از جمع‌بندی موارد مذکور در فصول قبلی و ارائه یک نظر جامع در مورد پدیده رمزارزها به ارائه یک موضوع چالشی که زمینه کار پژوهشی حول آن وجود دارد، خواهیم پرداخت. در نهایت در بخش مراجع، فهرستی از کتب و مقالاتی که در این پژوهش از آن‌ها بهره برده‌ایم ارائه شده است.

مقدمه

پس از تولد بیت کوین در سال ۲۰۰۸ میلادی، جهان با پدیده ای رو به رو شد که ادعا می کرد که تمام شئون زندگی بشر را دستخوش تغییرات عمده ای خواهد کرد. پول دیجیتال[۱]، ارز مجازی[۲] رمزارز و ... مفاهیمی بودند که در پی تلاش های محققین و دانشمندان حوزه های فناوری اطلاعات و فناوری های مالی، نهایتاً با ظهور بیت کوین عینیت پیدا کرده بودند. اهدافی از قبیل: حذف نهاد ناظر، حذف بانک های مرکزی، پول جهانی بدون مرز و ... همگی به جذابیت این پدیده جدید می‌افزود، اما در کنار تمام فرصت‌هایی که بیت‌کوین به ارمغان آورده بود، با توجه به ناشناس بودن طرفین معامله و عدم نظارت هیچ نهاد ناظر دولتی بر معاملات این ارز، همواره به‌عنوان یک تهدید و یک حوزه جرم‌خیز برای حاکمیت‌ها به حساب می‌آمد و کارشناسان آن را ابزاری مناسب برای جرائم کلانی از قبیل: پولشویی، تأمین مالی جرائم سازمان یافته، تامین مالی تروریسم، معاملات قاچاق انسان و قاچاق مواد مخدر و ... می‌دانستند. تاریخ پرفراز و نشیب بیت‌کوین و قضایایی چون فروشگاه اینترنتی راه ابریشم[۳]با مالکیت راس اولبریخت[۴]که به فروش بی‌واسطه مواد مخدر بصورت ناشناس اقدام کرده بود یا ورشکستگی صرافی‌های بزرگ بیت‌کوین و نابودی سرمایه تعداد زیادی از مردم، برای مثال ماجرای صرافی مت‌گاکس[۵]و ... همگی تاییدکننده این ادعاست که بیت‌کوین ظرفیت فوق العاده‌ای برای اقدامات مجرمانه و خرابکارنه محسوب می‌شود. از همین رو حاکمیت‌ها برآن شدند تا با اشراف و تسلط بر این حوزه و قانون‌گذاری، گُنارش[۶]و نظارت بر این حوزه از خطرات و تهدیدات آن کاسته و از مزایای این فناوری بهره لازم را ببرند. بسیاری از کشورها قوانین جدیدی به این منظور تصویب کردند، برخی دیگر این موضوع را ذیل قوانین موجود از قبیل قوانین مربوط به مالیات[۷] پولشویی[۸]و عرضه اوراق بهادار گنجانده‌اند و برخی از کشورها اقدام به ایجاد رمزارز ملی منحصر به خود کرده‌اند، در همین راستا در داخل کشور مراکزی از قبیل: معاونت فناوری‌های نوین بانک مرکزی، مرکز پژوهش‌های مجلس شورای اسلامی، مرکز ملی فضای مجازی، مرکز فناوری اطلاعات قوه قضاییه ... اقداماتی را در شناخت این تکنولوژی و گُنارش رمزارزها انجام داده اند و هدف اصلی نهادهای حاکمیتی از تمرکز بر این پدیده، استفاده از آن در راستای دور زدن تحریم ها علیه کشورمان و پیشگیری از وقوع جرائم[۹]در این حوزه است.

---

۱ Digital Currency
۲ Virtual Currency
۳ Silk Road
۴ Ross Ulbricht
۵ Mt Gox
۶ Regulation
۷ Tax
۸ Money Laundring
۹ Crimes

فصل اول

معرفی رمزارزها

۱-۱- فلسفه پیدایش، تاریخچه رمزارزها

۱-۱-۱- رمزارزها ماقبل بیت کوین

در این بخش به سیر تکوین رمزارزها خواهیم پرداخت. همانطور که هر محصول فناوری یک شبه طراحی و تولید نمی‌شود، توسعه رمزارزها هم حاصل سال‌ها تلاش و همفکری و هم‌افزایی جمعیت بزرگی از متخصصین فناوری اطلاعات، ریاضیات و آمار، امنیت و رمزنگاریست. در این بخش سعی شده به اکثریت چهره‌های تاثیرگذار در روند شکل‌گیری رمزارزها و بطور خاص بیت‌کوین هرچند کوتاه و اجمالی، پرداخته شود و کارهای بزرگی که در عمر ۱۰ ساله بیت‌کوین و کمی قبل از آن واقع شده را مرور می‌کنیم. اینکه در بخش‌های مختلف این پژوهش تاکید ویژه‌ای بر بیت‌کوین داریم از این‌جهت است که بیت‌کوین با توجه به سابقه و ویژگی‌هایش نماینده مناسبی از مجموعه رمزارزهاست. اولین معاملات از طریق اینترنت در سال‌های دهه ۷۰ میلادی و به روش‌های فوق‌العاده کند و سنتی انجام شد. از همان سال‌ها کارشناسان فناوری اطلاعات به فکر ارائه درگاه‌های پرداخت اینترنتی و روشی برای جابه‌جایی پول در فضای مجازی افتادند. بدون شک دیوید چاوم[۱] یکی از شخصیت‌های مهم این عرصه است، او مقالات زیادی را در زمینه پول‌های الکترونیکی منتشر کرده بود اما در مقاله ای که در سال ۱۹۸۳ منتشر نمود،[۲] ایده یک پول الکترونیکی تحت عنوان دیجی‌کش[۳] را منتشر کرد، دیجی‌کش بعنوان یک شرکت در سال ۱۹۹۰ بطور رسمی ثبت شد، و اینطور که در منابع آمده حتی تا پای امضای قرارداد با سیتی‌بانک[۴] و مایکروسافت[۵] پیش رفت، گویا مایکروسافت پیشنهادی ۱۸۰ میلیون دلاری به چاوم داده بود که از دیجی‌کش در ویندوز ۹۸ استفاده کند اما به دلایل مبهمی این قرارداد ثبت نمی‌شود. نهایتا دیجی‌کش در سال ۱۹۹۸ بطور کامل ورشکست شده و تعطیل اعلام می شود. اما دلایل عدم اقبال گسترده به دیجی‌کش را میتوان در چند مورد ذکر کرد، اول اینکه دیوید چاوم شخص شناخته شده‌ای نزد دولت بود و طبیعتا باید درصورت درخواست دولت اطلاعات کاربران را دراختیار نهادهای امنیتی می‌گذاشت که این موضوع ابدا به ذائقه سایفرپانک[۶]ها و رمزنگارها و حامیان حریم خصوصی

تصویر ۱ - دیوید چاوم خالق دیجی‌کش

---

۱ David Chaum

۲ Blind signature for untraceable payments in book ”Advanced in Cryptology ”

۳ Digicash

۴ Citibank

۵ Microsoft

۶ Cypherpunk

خوش نمی‌آمد، در ضمن راهکاری که چاوم ارائه کرده بود به هیچ وجه قابلیت مقیاس پذیری نداشت، تایید صحت تمام تراکنش‌ها به عهده شرکت متمرکزی به عنوان دیجی‌کش با مدیریت شخص دیوید چاوم بود که نیاز به رفع این نقیصه بعدها زمینه ساز سیستم‌های غیرمتمرکز شد. یکی دیگر از دلایل شکست دیجی‌کش بدون شک اوج‌گیری و محبوبیت پی پال[۱] در سال‌های آخر دهه ۹۰ بود. در همین سال‌ها داگلاس جکسون[۲] اولین ارز اینترنتی با پشتوانه طلا را پایه‌گذاری کرد، ای‌گولد[۳] که متولد سال ۲۰۰۵ بود تا سال ۲۰۰۹ به فعالیت خود ادامه داد اما در همان سال جکسون به اتهام پولشویی و انجام کسب و کار اینترنتی بدون مجوز بازداشت شد و به حصر خانگی محکوم شد.

ای‌گولد در دوران اوج خود پس از پی‌پال رتبه دوم سرویس‌های پرداخت آنلاین را به خود اختصاص داده بود. برخی کارشناسان دلایل شکست ای‌گولد را عدم همکاری با سرویس مخفی ایالات متحده مطرح کرده اند که از طریق موسسات مانی‌گرام و وسترن یونیون به نوعی ای‌گولد تحریم شده بود. جکسون پس از پایان مدت محکومیت تلاش‌هایی را در راستای احیای ای‌گولد انجام داد که بی‌نتیجه بود و ای‌گولد هیچگاه به جایگاه قبلی خود بازنگشت. در سال ۲۰۰۸، نیک زابو[۴] بیت‌گولد[۵] را معرفی کرد، بیت‌گولد هم از نظر تاریخ تولد و هم از نظر معماری و تکنولوژی بسیار شبیه بیت کوین است از همین روست که به عقیده برخی کارشناسان یکی از از کاندیداهای هویت واقعی ساتوشی ناکاموتو است. بیت‌گولد برخلاف دیجی‌کش و ای‌گولد غیرمتمرکز بود، برای حل مساله ژنرال‌های بیزانسی[۶] راه حل گواه اثبات کار[۷] را ارائه کرده بود. ضعف بیت‌گولد این بود که در گواه اثبات کار به‌جای توان پردازش نودها، تعداد اکانت ها را مبنا قرار داده بود که همین امر باعث آسیب پذیری آن در برابر حملات سیبیل[۸] شده بود. بیت‌گولد هیچ‌گاه در مقیاس بزرگی عملیاتی نشد. نیک زابو که یک رمزنگار و متخصص امنیت به حساب می‌آمد، در سال ۱۹۹۹ یک مقاله با عنوان پروتکل خدا[۹] منتشر کرده بود که از مقالات بی‌مانی[۱۰] وی‌دای[۱۱] که در سال ۱۹۹۸ در فهرست پستی سایفرپانک‌ها[۱۲] منتشر شده بود الهام گرفته بود. دو نکته اساسی در مقاله معرفی بیت کوین، غیرمتمرکز بودن و مقاومت در برابر تورم است که هردو در مقالات وی‌دای و نیک‌زابو مطرح شده بودند.

---

۱ Pay Pal
۲ Douglas Jackson
۳ Egold
۴ Nick szabo
۵ Bit Gold
۶ Byzantine Generals Problem
۷ Proof of work
۸ Sybil Attack
۹ God Protocol
۱۰ Bmoney
۱۱ Wei Dai
۱۲ Cypherpunks mailing list

یکی دیگر از شخصیت‌های تاثیرگذار تاریخ بیت‌کوین هال فینی[۱]است، فینی یکی از رمزنگاران مطرح دوره خود بوده که نام او هم در زمره کاندیداهای هویت واقعی ساتوشی قرار می‌گیرد. یکی از دلایل این گمان، دریافت اولین تراکنش بیت کوین توسط هال فینی از حساب ساتوشی ناکاموتوست. شخص تاثیر گذار بعدی آدام بک[۲]مخترع پروتکل هش‌کش[۳]و از توسعه دهندگان هسته بیت‌کوین[۴]بوده که اوهم در زمره کاندیداهای هویت ساتوشی قرار دارد. با همه این اوصاف هویت ساتوشی همچنان مجهول است. هفته نامه نیوزویک در یک ویژه نامه مدعی شده بود که ساتوشی ناکاموتو فردی به نام دوریان پرنتیس[۵]است که در خانه‌ای کوچک در کالیفرنیا زندگی می‌کرد. البته به محض انتشار این مقاله در نیوزویک، ساتوشی در فهرست پستی سایفرپانک‌ها اعلام کرد که من دوریان نیستم. به عنوان جمع‌بندی و قبل از شروع دوران بیت‌کوین، می‌توان گفت که ابهام در هویت ساتوشی یک اقدام فوق هوشمندانه و جزئی از معماری بیت‌کوین بوده که با توجه به تجربه شناخته شده بودن دیوید چاوم و مشکلاتی که برای دیجی‌کش پیش آمده بود قابل تحلیل است. در این مقطع تاریخی هیچ‌کدام از دولت‌ها یا به عرصه رگولاتوری رمزارزها نگذاشته بودند و این پدیده به‌صورت زیرزمینی توسعه می‌یافت.[۶]

۱-۱-۲- تولد بیت کوین

سرانجام در سوم ژانویه ۲۰۰۹ بیت‌کوین بصورت عملیاتی آغاز به کار کرد و اولین تراکنش در تاریخ ۱۲ ژانویه ۲۰۰۹ بین ساتوشی و هال فینی انجام شد و در بلوک پیدایش[۷]قرار گرفت. بیت کوین ۰/۰۰۰۷۶ دلار قیمت گذاشته شد و مبنای قیمت‌گذاری مصرف برق جهت استخراج[۸]بود. خیلی از کاربران اولیه بیت‌کوین به قیمت بالای آن اعتراض داشتند. اولین معامله واقعی و خرید کالا در تاریخ ۲۲ می ۲۰۱۰ صورت گرفت که در آن ۱۰۰۰۰ بیت‌کوین در قبال دریافت یک پیتزا پرداخت شد. در این روز که بین علاقه مندان بیت‌کوین به روز پیتزا[۹]معروف شده، بعضی پیتزافروشی‌هایی که با بیت‌کوین کار می‌کنند، پیتزای رایگان ارائه می‌دهند. در جولای ۲۰۱۰ اولین

---

۱ Hal finney

۲ Adam Back

۳ Hash Cash

۴ Bitcoin Core Developer

۵ Dorian Prentice

۶ یان دی‌مارتینو، راهنمای بیت‌کوین، ۲۰۱۳، ترجمه پیمان رحمانی و سایرین، تهران، انتشارات موسسه شبکه عصر تراکنش، ۱۳۹۶

۷ Genesis Block

۸ Mining

۹ Pizza Day

صرافی[۱]متمرکز بیت‌کوین تحت عنوان مت گاکس[۲]شروع به کار کرد و همین موضوع سبب جهش قیمت بیت کوین تا ۰/۰۶ دلار شد. در تاریخ ۹ فوریه ۲۰۱۱ قیمت هر بیت‌کوین به ۱ دلار آمریکا رسید که موجب پوشش رسانه‌ای گسترده و شناخت بیشتر این رمزارز شد. در ۲۶ جولای ۲۰۱۱ یک مشروب فروشی در برلین به‌عنوان اولین مجموعه‌ای که در ازای خدمات، بیت‌کوین دریافت می‌کند اعلام موجودیت کرد. قیمت بیت‌کوین در مارس ۲۰۱۳ به ۱۰۰ دلار و ارزش بازار به حدود ۱ میلیارد دلار رسیده بود. بیت‌کوین در حال اوج‌گیری بود که صرافی مت گاکس ورشکسته شد و اولین شوک بزرگ به جمعیت طرفداران بیت‌کوین وارد شد. پس از ماجراهای مت گاکس بیت‌کوین دچار افت قیمت شد اما از سال ۲۰۱۵ دوباره روند صعودی را در پیش گرفت. قیمت بیت‌کوین در اوایل ۲۰۱۵ به ۴۵۰ دلار رسید و این روند ادامه داشت تا بیت‌کوین در اواخر ۲۰۱۷ قیمت ۱۹ هزار دلاری را تجربه کرد.

۱-۱-۳- فلسفه پیدایش رمزارزها

پس از بررسی تاریخ رمزارزها قبل و بعد از تولد بیت‌کوین، یک سوال مهم باقی می‌ماند، اصلا چه شد که محققان و توسعه دهندگان به فکر توسعه رمزارزها و بطور خاص بیت‌کوین افتادند؟ چه کمبود و خلاء بزرگی در سیستم‌های مالی سنتی آن‌ها را مجاب کرده بود تا به فکر توسعه یک جایگزین متمایز بیافتند؟ در پاسخ به این سوال می‌توان گفت، وجود نهاد متمرکز قدرتمندی به‌عنوان بانک مرکزی که بواسطه داشتن انحصار در چاپ پول و نظارت بر تراکنش‌ها، قدرت بلامنازع سیستم مالی سنتی بود گروهی را برآن داشت تا به فکر ارائه یک سیستم مالی غیرمتمرکز بدون وجود نهاد مرکزی باشند. این گروه که در قالب جنبش سایفرپانک‌ها[۳] و گروه کریپتوآنارشیست‌ها[۴] خود را معرفی می‌کردند، رمزنگاری و ریاضیات را بهترین ابزار برای ایجاد امنیت در یک شبکه غیرمتمرکز می‌دانستند. این گروه در دهه ۸۰ میلادی یک بیانیه تحت عنوان مانیفست کریپتوآنارشیسم منتشر کرده و اصول و اهداف خود را در آن ارائه کردند. از مهمترین بندهای مانیفست کریپتوآنارشیست‌ها می‌توان به این جمله اشاره کرد، ما طبیعت اعتماد[۵]و اعتبار[۶]را تغییر خواهیم داد، از افراد مهم و تاثیرگذار این جریان می‌توان به تیموتی می[۷] مهندس بازنشسته اینتل اشاره کرد که یکی از سه نگارنده اصلی مانیفست کریپتو آنارشیسم بود.[۸]

---

۱ Exchange

۲ Mt Gox

۳ Cypherpunk

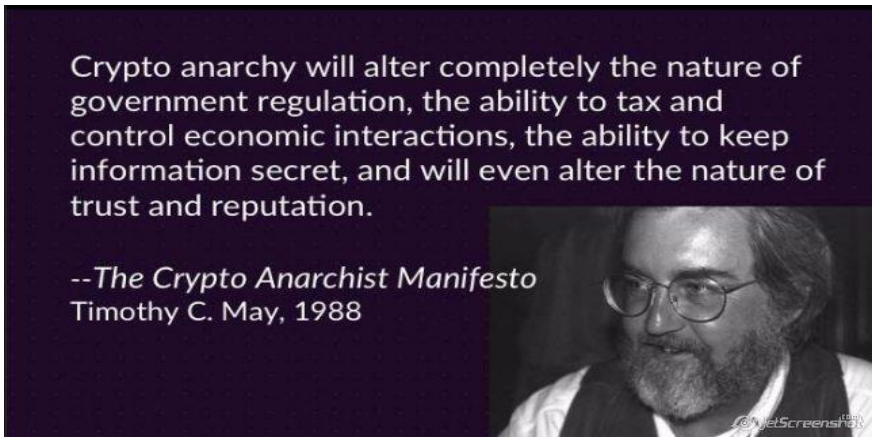
۴ Crypto Anarchist

۵ Trust

۶ Reputation

۷ Timothy May

۸ یان دی‌مارتینو، راهنمای بیت‌کوین، ۲۰۱۳، ترجمه پیمان رحمانی و سایرین، تهران، انتشارات موسسه شبکه عصر تراکنش، ۱۳۹۶



تصویر ۲ - بخشی از مانیفست کریپتو آنارشیسم

۱-۲- ادبیات موضوعه در رمزارزها

با توجه به اینکه فناوری بلاک‌چین و پدیده رمزارزها، حوزه‌ای نو محسوب می‌شود و مملو از تعاریف و مفاهیم فنی است، در ادامه لیستی از مهمترین مفاهیم کاربردی این حوزه به ترتیب حروف الفبا ارائه شده است.

آدرس[۱]

یک آدرس بیت کوین برای دریافت و ارسال نقل و انتقال روی شبکه بیت کوین به کار می‌رود. این آدرس شامل یک رشته از حروف الفبایی و اعداد است، اما همچنین می‌تواند به صورت یک کد QR و قابل اسکن درآید.

اجماع[۲]

به توافق صورت گرفته بین بخشی قابل توجهی از یک جامعه بلاک‌چینی اشاره می‌کند. برای شکل‌گیری یک اجماع می بایست حداقل ۵۱ درصد از کل افراد آن جامعه با یک دیگر هم نظر باشند. اجماع بخش بسیار مهمی از ساختار رمز ارز ها را تشکیل می‌دهد. این توافق تضمین کننده‌ی معتبر بودن داده‌های بلاک‌چین است و اصولا موضوعی حیاتی برای پیاده سازی سیستم های غیر متمرکز می‌باشد.

استخر[۳]

مجموعه‌ای از موکلین استخراج که به طور اشتراکی یک بلوک را استخراج می‌کنند و سپس پاداش را بین خودشان تقسیم می‌کنند. استخرهای استخراج روش مفیدی برای افزایش احتمال موفقیت استخراج یک بلوک است خصوصا همچنان که سطح دشواری افزایش می‌یابد.

---

۱ Address

۲ Consensus

۳ Pool