مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه ترکیبیات، رمزنگاری و محاسبات، ص ۵۰ -۴۱

چالش‌های امنیتی رمز ارزهای مطرح و راه‌کارهای امنیتی آن

رحیم اصغری*[۱]، سعیده غفوری[۲]، فاطمه حاجی‌زاده[۳]، حسن خرازی[۴]

۱- استادیار، ۲و۳- دانشجوی کارشناسی ارشد، دانشگاه صنعتی مالک اشتر ۴- استادیار، دانشگاه جامع امام حسین(ع)
(دریافت: ۱۳۹۷/۰۸/۲۵ پذیرش: ۱۳۹۸/۰۷/۰۲)

چکیده

در این مقاله، ابتدا به تشریح زنجیره بلوکی و رمز ارزهای مطرح پرداخته می‌شود و سپس مشکلات و راهکارهای امنیتی آن‌ها را بررسی کرده و نهایتاً رمز ارزهایی که در حوزه امنیت به‌خصوص حریم خصوصی قدمی برداشته‌اند را مورد بررسی قرار می‌دهیم. زنجیره بلوکی در مقایسه با ساختار نگه‌داری پایگاه داده‌ای، داده‌ها را امن‌تر نگه می‌دارد. داشتن یک شبکه غیرمتمرکز مبتنی برداشتن هویت دیجیتالی امن، انتقال داده امن در بستر یک شبکه همتا به همتا، ثبت و داشتن تاریخچه امن و غیرقابل تغییر از داده‌ها ازجمله خواصی است که زنجیره بلوکی به‌طور هم‌زمان آن‌ها را فراهم می‌نماید. در این میان، فناوری‌های جدیدی نیز در حال ظهور هستند که سعی در رفع برخی از مشکلات و محدودیت‌های فناوری زنجیره بلوکی جاری دارند. معایبی نظیر طولانی شدن زمان تایید در زمانی که شبکه خیلی بزرگ شود، یا هزینه‌های برق و پاداش استخراج‌کننده‌ها ازجمله این مشکلات هستند. مطالعه ما نشان می‌دهد که تنگل، فناوری جدیدی است که سعی در ساختن یک شبکه غیرمتمرکز مبتنی بر گراف جهت‌دار غیرمدور دارد و می‌تواند بسیاری از این محدودیت‌ها را برطرف سازد و درعین حال قابلیت‌های جدیدی را نیز به آن اضافه کند.

واژه‌های کلیدی: زنجیره بلوکی، رمز ارز، تنگل، اثبات بادانش صفر، حریم خصوصی، گمنامی

۱- مقدمه

ارز دیجیتال به‌عنوان یک واحد پولی یا واسطه تبادل (جدا از واسطه‌های فیزیکی مانند اوراق بانکی یا سکه) بر پایه اینترنت تعریف می‌شود که ویژگی‌هایی مشابه با پول فیزیکی را داراست، اما تراکنش‌ها در آن به‌صورت آنی و بدون مرز انجام می‌دهد [۱].

در اوایل دهه ۱۹۸۰، دیوید چایم که یک رمزنگار آمریکایی بود، یک الگوریتم ناآگاهانه به جهان معرفی کرد [۲]. الگوریتم ناآگاهانه یک روش در رمزنگاری است که برای تبادل اطلاعات به‌صورت امن و غیرقابل بازگشت استفاده می‌شود؛ که به‌عنوان پول کور نامیده می‌شود. در اواخر دهه ۱۹۸۰، دیوید چایم، دیجی‌کش را که یک سامانه پرداخت الکترونیک بود تأسیس کرد که معاملات آن بر اساس گمنامی انجام می‌شد [۲]؛ اما موفق نبود. این عدم موفقیت دلایل گوناگونی داشت: تقلب، مشکلات مالی و حتی اختلافات کارمندان با رئیسانشان. همه این سامانه‌ها از یک رویکرد شخص ثالث معتمد استفاده می‌کردند.

در سال ۱۹۹۸، یک مهندس نرم‌افزار به نام ویدای[۱] سامانه پول الکترونیکی توزیع‌شده به نام "B-Money" [۲] را اختراع کرد.

نهایتاً در سال ۲۰۰۹ برنامه‌نویس یا گروهی از برنامه‌نویسان گمنام تحت نام ساتوری ناکام وتو[۲] بیت کوین[۳] را معرفی کردند. ساتوشی بیت کوین را سامانه پولی الکترونیکی همتا به همتا تعریف نمود [۳]، اما اکنون بانام رمز ارز[۴] بیت کوین شناخته می‌شود.

رمز ارزها زیرمجموعه‌ای از ارزهای دیجیتال محسوب می‌شوند. به‌طور کلی، رمز ارز نوعی سامانه پرداخت دیجیتالی است که با حل مسائل ریاضی، می‌توان آن را به‌صورت دیجیتالی تولید کرد و به شخص دیگری انتقال داد [۴]. یکی از اصلی‌ترین دلایل موفقیت بیت کوین وجود سامانه غیرمتمرکز همتا به همتا در آن است که توجهات زیادی را به خود جلب کرد چرا که بدون آن، این خدمات از لحاظ فناوری آسان است اما نیاز به اعتماد به یک مدیریت متمرکز دارد. برخلاف سامانه‌های اقتصادی و بانکداری، رمز ارزها غیرمتمرکز هستند و هیچ کنترلی از سوی دولت‌ها بر آن وجود ندارد.

کسانی که به شبکه غیرمتمرکز سرویس می‌دهند را گره[۵] می‌نامند. گره‌های شبکه یک کپی از تاریخچه تراکنش‌ها را

رایانامه نویسنده مسئول: meisam.mathhome@gmail.com

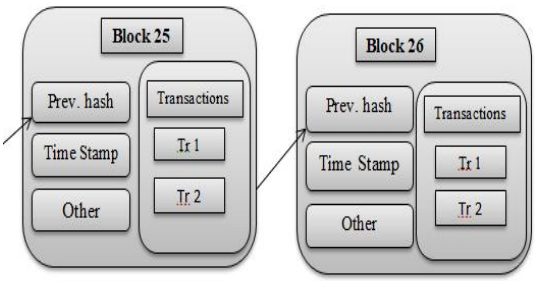
[1] Wie Dai

[2] Satoshi Nakamoto
[3] Bit coin
[4] Crypt currencies
[5] Node

ذخیره می‌کنند. هرگونه تغییری در شبکه، فقط در صورتی انجام می‌شود که تمامی گره‌ها در اتفاق افتادن آن اجماع و توافق داشته باشند. مسئولیت اصلی گره‌ها ثبت تغییرات در زنجیره بلوکی و همچنین انتقال از یک وضعیت به وضعیت دیگر است. وجود گره‌ها یا استخراج‌کننده‌ها[1] در شبکه باعث می‌شود که از هرگونه اشتباه یا تقلب در این شبکه جلوگیری شود؛ بنابراین، ویژگی غیرمتمرکز بودن، باعث تقسیم کنترل پروتکل می‌شود، همچنین تمام تراکنش‌ها به‌صورت عمومی در اختیار تمام گره‌های شبکه قرار می‌گیرد. بیت کوین اولین رمز ارز غیرمتمرکز همتا به همتا است که بر اساس الگوریتم چکیده‌ساز SHA-256 کار می‌کند [۵]. بیت کوین دارای یک فهرست توزیع‌شده[2] عمومی برای ثبت تمام معاملات بیت کوین به نام زنجیره بلوکی[3] نگهداری می‌شود. تا قبل از بیت کوین تجارت اینترنتی به‌جایی رسیده بود که برای پردازش پرداخت‌های الکترونیکی، منحصراً به نهادهای مالی متکی بود که نقش اشخاص ثالث قابل اعتماد را بر عهده داشتند. با این‌که این سامانه برای اکثر تراکنش‌ها کارایی لازم را دارد، همچنان ضعف‌های ذاتی مدل مبتنی‌بر اعتماد[4] را در خود دارد [۶]. انجام تراکنش‌های کاملاً برگشت‌ناپذیر، کاملاً ناممکن بود، چرا که نهادهای مالی نمی‌توانند از وساطت در مشاجرات سرباز زنند. هنگامی‌که امکان بازگشت در معاملات وجود داشته باشد، نیاز به حس اعتماد هم بیشتر می‌شود. در چنین شرایطی، بازرگانان نیز مجبور خواهند بود با مشتریان خود محتاطانه برخورد کنند و از آن‌ها اطلاعاتی را بخواهند که اگر معاملات برگشت‌ناپذیر بودند اصلاً نیازی به آن‌ها نبود [۶]. همچنین، آن‌ها باید بپذیرند که جلوی درصدی از کلاه‌برداری را نمی‌توان گرفت و باید آن را به‌عنوان جزئی از کار پذیرفت. راه‌هایی برای رهایی از عدم قطعیت در معاملات حضوری و استفاده از ارز فیزیکی[5] وجود دارد، اما سازوکاری برای پرداخت از طریق کانال‌های ارتباطی بدون حضور نهادی قابل اعتماد وجود ندارد. در اینجا نیاز به یک سامانه پرداخت الکترونیک احساس می‌شد که در آن مدرک رمزنگاری‌شده[6] جای اعتماد را بگیرد و این امکان را برای دو طرف مایل به انجام معامله فراهم کند که مستقیماً و بدون نیاز به شخص ثالث مورد اعتمادی، تراکنشی را انجام دهند. وقتی تراکنش‌ها از لحاظ محاسباتی[7] عملاً برگشت‌ناپذیر باشند، از حقوق فروشنده حمایت می‌شود. همچنین با استفاده از سازوکارهای ضمانتی عادی می‌توان به سادگی حقوق خریداران را نیز تأمین کرد [۶]. برای رفع مشکل دو بار خرج کردن، ساتوشی ناکاموتو، از یک سرور مهر زمانی[8] توزیع‌شده به‌صورت همتا به همتا استفاده کرده است. این سرور مدرک محاسباتی را از طریق ترتیب زمانی[9] تراکنش‌ها ایجاد می‌کند [۶]. سامانه موردنظر به شرطی امن است که *گره‌های* درست‌کار[10] جمعاً قدرت سی پی یو بیشتری را نسبت به گره‌های حمله‌گر در اختیار داشته باشند [۶]. ساختار این مقاله به این صورت است که در بخش دوم این مقاله مروری بر زنجیره بلوکی شده است. در بخش سوم، انشعابات زنجیره بلوکی مطرح‌شده است. در بخش چهارم رمز ارزهای مطرح بررسی و از جهت کارایی و امنیت باهم مقایسه شده‌اند. در بخش پایانی مقاله هم تحلیل و ارزیابی امنیتی رمزارزهای مطرح با بیان جزئیات مطرح‌شده است.

۲- مروری بر زنجیره بلوکی

زنجیره بلوکی در حقیقت یک پایگاه داده (دفتر کل) توزیع‌شده همتا به همتا است که چکیده هر بلوک جدید به چکیده بلوک قبل از آن اشاره می‌کند. این سامانه از چکیده‌ها، تضمین می‌کند که هیچ تراکنشی درگذشته قابل تغییر نباشد؛ چون اگر یک قسمت از تراکنش تغییر کند، چکیده همان بلوک نیز تغییر می‌کند و درنتیجه چکیده‌های بلوک‌های بعد از آن نیز تغییر خواهند کرد. درنهایت تشخیص تراکنش‌های دست‌کاری‌شده، بسیار ساده خواهد بود. نتیجه این کار بسیار جالب است. چرا که همه افراد روی زنجیره بلوک، تنها نیاز دارند تا روی ۲۵۶ بیت برای تایید حالت زنجیره بلوک توافق کنند. زنجیره بلوکی بیت کوین در حال حاضر بیشتر از ۱۷۰ گیگابایت حجم دارد [۸]، اما در عین حال، مقدار فعلی زنجیره بلوکی آن، یک چکیده شانزده دهی است که با ۲۵۶ بیت نشان داده می‌شود. در شکل (۱)، ساختار کلی زنجیره بلوکی نشان داده می‌شود.

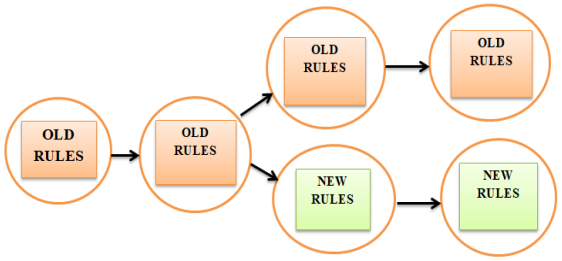


شکل (۱): ساختار کلی یک زنجیره بلوکی

[1] Miners
[2] Distributed ledger
[3] Block chain
[4] Trust-based model
[5] Physical currency
[6] Cryptographic Proof
[7] Computationally
[8] Timestamp server
[9] Chronological order
[10] Honest nodes

۳- انشعابات زنجیره بلوکی

در مقالات متعددی که منتشرشده نیاز به اعمال تغییرات در رمز ارز اولیه و اصلی، یعنی بیت کوین، مورد بحث قرارگرفته است از سال ۲۰۰۹ میلادی که بیت کوین متولد شد تاکنون راه‌حل‌های مختلفی برای آن ارائه شده است که شامل قسمت‌های مختلفی از جمله امنیت، پروتکل‌های اثبات کار، تغییر در ساختار زنجیره بلوکی و ... است. به علت متن‌باز بودن بیت کوین امکان اصلاح و به‌روزرسانی آن وجود دارد بنابراین، بیت کوین انشعابات زیادی را به‌منظور ارتقا و اضافه کردن و یا تغییر ویژگی‌های آن، تاکنون تجربه کرده است. انشعابات به ۲ دسته سخت و نرم تقسیم می‌شوند. انشعابات سخت یک تغییر در پروتکل است که نسخه‌های قدیمی را نامعتبر می‌کند. اگر نسخه‌های قدیمی‌تر نیز همچنان در حال اجرا باشند، نسخه قدیمی‌تر نهایتاً با یک پروتکل متفاوت و با داده‌های متفاوت از نسخه جدید به پایان می‌رسند [۱۰]. مطابق شکل (۲)، در بیت کوین، یک انشعاب سخت برای تغییر پارامترهای مشخص‌شده مانند اندازه بلوک، پیچیدگی پازل رمزنگاری که باید حل شود، محدود کردن اطلاعات اضافی که می‌توان آن‌ها را اضافه کرد و غیره، ضروری است. تغییر در هر یک از این قوانین می‌تواند باعث پذیرش بلوک‌هایی توسط پروتکل جدید شود که توسط نسخه‌های قدیمی‌تر رد می‌شوند [۱۰].



شکل (۲): انشعاب زنجیره بلوکی

برای مثال، در رمز ارز بیت کوین کش[1] که چهارمین رمز ارز پرارزش دنیاست [۱۱]، یک انشعاب سخت از بیت کوین است که در آن محدودیت سایز بلوک از ۱ مگابایت به ۸ مگابایت افزایش یافت، بلوک ۲ مگابایت توسط گره‌هایی که نسخه جدید را اجرا می‌کنند، پذیرفته می‌شود، اما توسط گره‌هایی که نسخه قدیمی‌تر (بیت کوین) را اجرا می‌کنند، رد می‌شوند [۱۰]. هردوی این زنجیرها همچنان ادامه دارند، زیرا آن‌ها از قوانین مختلفی پیروی می‌کنند. بلوک‌ها در زنجیره بیت کوین کش توسط گره‌های زنجیره بیت کوین نامعتبر است و برعکس [۱۲]. انشعابات نرم[2] می‌توانند در کنار نسخه‌های قدیمی‌تر کار کنند. برای مثال، اگر یک پروتکل طوری تغییر یابد که قواعد را سخت‌گیرانه‌تر کند یک تغییر آرایشی را اجرا کند یا یک تابعی اضافه کند که ساختار را به هیچ‌وجه تحت تأثیر قرار نمی‌دهد، آنگاه بلوک‌های نسخه جدید توسط گره‌های نسخه قدیمی پذیرفته خواهند شد [۱۰]. انشعاب نرم نیز قبلاً چندین بار اتفاق افتاده است. برای مثال در ابتدا بیت کوین محدودیت اندازه بلوک نداشت. ایجاد محدودیت ۱ مگابایت، با استفاده از یک فورک نرم انجام شد، چرا که قانون جدید سخت‌گیرانه‌تر از قبل بود [۱۰]. در جدول ۱، مقایسه برخی انشعابات سخت بیت کوین آورده شده است.

	بیت کوین کش	بیت کوین گلد	سگویت2x	بیت کوین
نماد	BCH	BTG	B2X	BTC
حداکثر تعداد سکه	21m	21m	21m	21m
الگوریتم استخراج	SHA 256	Equihash	SHA 256	SHA 256
سخت افزار استخراج	ASIC	GPU	ASIC	ASIC
زمان ساخت بلوک	۱۰	۱۰	۱۰	۱۰
اندازه بلوک	8MG	1MG	2MB	1MB
تنظیم میزان سختی	هر بلوک	هر بلوک	۲ هفته	۲ هفته

جدول (۱): مقایسه انشعابات سخت بیت کوین

۴- بررسی و مقایسه رمز ارزهای مطرح

بیت کوین اولین و پرارزش‌ترین رمز ارز است [۱۱] که توضیحاتی درباره آن داده شد، در ادامه نیز آن را بیشتر بررسی می‌کنیم. اتریوم دومین رمز ارز پرقدرت دنیاست [۱۱]. مانند بیت کوین، اتریوم هم یک زنجیره بلوکی توزیع‌شده عمومی است. اگرچه تفاوت‌های فنی زیادی بین این دو وجود دارد اما مهم‌ترین تفاوت این دو، اهداف و قابلیت‌های آن‌ها است. بیت کوین یک برنامه کاربردی خاص از فناوری زنجیره بلوکی است. درواقع بیت کوین یک سامانه پرداخت جهانی، همتا به همتا و غیرمتمرکز را ایجاد می‌نماید. زنجیره بلوکی بیت کوین برای پیگیری مالکیت پول دیجیتال (بیت کوین) استفاده می‌شود، درحالی‌که زنجیره

[1] Bitcoin Cash
[2] Soft Fork

بلوکی اتریوم برای اجرای کدهای برنامه‌نویسی برنامه‌های غیرمتمرکز طراحی شده است.

اتریوم یک بستر نرم‌افزاری باز است که بر مبنای فناوری زنجیره بلوکی شکل‌گرفته و به توسعه‌دهندگان امکان ایجاد انواع کاربردهای غیرمتمرکز را می‌دهد [۱۳]. بستر اتریوم توسعه‌دهندگان را قادر می‌سازد تا برنامه‌های کاربردی غیرمتمرکز را ایجاد و راه‌اندازی کنند [۱۳]. یک برنامه غیرمتمرکز یا به اختصار Dapp، می‌تواند بدون نیاز به واسطه‌ها و با استفاده از توزیع جمعی یک عمل مخصوص را انجام دهد. برای مثال بیت کوین یک برنامه غیرمتمرکز است که کاربران می‌توانند توسط آن دارایی‌های دیجیتالی به اسم بیت کوین را به‌صورت همتا به همتا منتقل کنند.

قراردادهای هوشمند مهم‌ترین سازه اتریوم است، یک قرارداد هوشمند، یک پروتکل ویژه است که برای مشارکت، تأیید یا اجرای مفاد یک قرارداد خاص، فعال می‌شود [۱۳]. قراردادهای هوشمند معاملات و فرایندها را به‌صورت کاملاً تضمینی و بدون اشخاص ثالث انجام می‌دهند. فعالیت‌ها و اسناد قرارداد هوشمند، قابل‌پیگیری و غیرقابل برگشت هستند [۱۳]. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف‌گذاری‌شده به‌طور خودکار می‌باشند. درواقع ابتدا، دارایی‌ها و شرایط قرارداد، کدگذاری می‌شوند و در بلوکی از زنجیره بلوکی قرار می‌گیرند. این قراردادها بین گره‌های بستر توزیع و کپی می‌شوند و مطابق با شرایط مشخص‌شده اجرا می‌شود. ریپل[1] سومین رمز ارز پرارزش است [۱۱] که در سال ۲۰۱۲ معرفی شد. شبکه ریپل به بانک‌ها و مؤسسات بزرگ متصل می‌شود و انتقال پول یا سایر دارایی‌ها را می‌توان در بستر شبکه انجام داد. تمام تراکنش‌ها در دفتر غیرمتمرکز ریپل[2] ثبت می‌شوند [۱۴]. هر تراکنش در ریپل حداکثر پس از فقط چهار ثانیه انجام می‌شود. لایت کوین پنجمین رمز ارز است [۱۱] که در هفتم اکتبر ۲۰۱۱ معرفی شد. برخلاف بیت کوین که از تابع چکیده‌ساز SHA-256 استفاده می‌کند، چارلی لی از الگوریتم Scrypt در لایت کوین استفاده کرد. این الگوریتم نسبت به الگوریتم بیت کوین دارای امکان محاسبه آسان‌تر، حجم کار کمتر و در نتیجه توانایی تایید سریع‌تر تراکنش‌ها است. در جدول ۲، رمز ارزهای مطرح ازنقطه‌نظر ساختاری مقایسه شده‌اند.

آیوتا[3] نیز یکی از رمز ارزهای پرارزش است که تفاوت جدی با سایر رمز ارزهایی که تاکنون بررسی کردیم دارد در این رمز ارز خبری از محدودیت زنجیره بلوکی نیست. رمز ارز پایه آیوتا برای اینترنت اشیا طراحی شده است. آیوتا رمز ارزی است که هیچ هزینه تراکنشی ندارد و نیز نیاز به هیچ استخراج‌کننده‌ای ندارد تا روند تراکنش‌ها را بررسی کند. به همین دلیل آیوتا به‌طور کامل غیرمتمرکز است با این وجود، نیاز به قدرت محاسباتی برای ثبت یک تراکنش دارد، و آن را تبدیل به یک ابزار مناسب به‌عنوان یک ارز و پروتکل ارتباطات توزیع‌شده برای اینترنت اشیا می‌کند.

هدف اصلی آیوتا حل برخی از مشکلات عمده فنّاوری زنجیره بلوکی است، یکی از اصلی‌ترین آن‌ها این است که زنجیره بلوکی (بزرگ‌ترین و اصلی‌ترین آن بیت کوین)، کند و گران است و همچنین محدود به انتقال پول است.

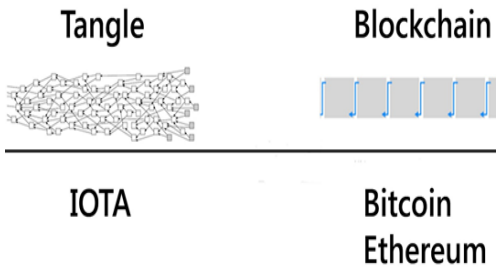
مسئله دیگر زنجیره بلوکی، اندازه آن است، هر چه بلوک‌های بیشتری اضافه شوند، زنجیره بلوکی بزرگ‌تر می‌شود و بنابراین، تعداد کمتری از کامپیوترها می‌توانند آن را استخراج کنند. در حال حاضر بیت کوین بزرگ‌تر از ۱۷۰ گیگابایت است. اگر این اندازه ده برابر افزایش یابد، تعداد بسیار کمی از کامپیوترها قادر خواهند بود تا تمام آن را استخراج کنند [۱۵]. آن‌ها در حال حاضر نیز تقریباً متمرکز شده‌اند. چهارتا از بزرگ‌ترین استخرهای استخراج‌کننده بیت کوین حدود ۵۳ درصد از قدرت چکیده‌ساز را دارند [۱۶].

یکی از تفاوت‌های اصلی این فنّاوری در مقابل زنجیره بلوکی، همان چیزی است که آیوتا آن را " تنگل[4]" می‌نامد. این‌یک روش جدید ذخیره‌سازی تراکنش‌ها از طریق مکانیسمی به نام گراف جهت‌دار غیر دوری[5] یا DAG است. که باعث می‌شود تراکنش‌ها سریع تایید شوند و مقیاس‌پذیر باشد [۱۷]. مقیاس‌پذیری[6] به‌معنای توانایی برای رشد کردن و بزرگ شدن سامانه می‌باشد. درحالی‌که اندازه بلوک در بیت کوین ثابت و یک مگابایت است.

در آیوتا برای ارسال یک تراکنش، باید دو تراکنش دیگر به‌صورت تصادفی تأیید شود. بنابراین، هر کاربر به تأیید و امنیت کمک می‌کند [۱۷]. تراکنش‌ها تا چندین بار توسط کاربران مختلف تأیید می‌شود، یک تراکنش ارسال‌شده در شبکه باید سطح کافی تأیید را جمع‌آوری کند (یعنی باید توسط سایر کاربران تأیید شود) تا میزان اطمینان برای این تراکنش افزایش یابد [۱۶]. آیوتا با کمک هماهنگ‌کننده[7] کار می‌کند که همه تراکنش‌ها را در بازه‌های خاصی تأیید می‌کند. بدون وجود این هماهنگ‌کننده، آیوتا در مراحل اولیه خود به اندازه کافی امن نیست. هنگامی که

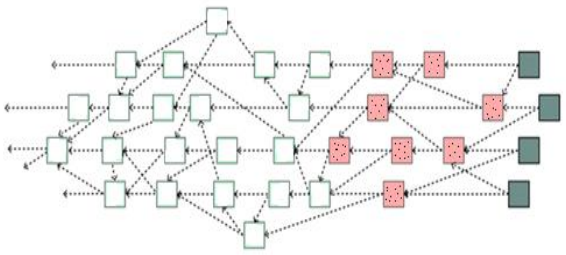
[1] Ripple
[2] XRP Ledger
[3] IOTA
[4] Tangle
[5] Directed Acyclic Graph
[6] Scalability
[7] Coordinator

شبکه به اندازه کافی از جهت مقیاس بزرگ شود، هماهنگ‌کننده آن حذف خواهد شد. یکی دیگر از جنبه‌های مهم تنگل این است که به جای قطعی بودن تعداد تراکنش‌ها مانند زنجیره بلوکی (فقط مقدار X تراکنش در هر ثانیه)، به‌صورت احتمالی است. این بدان معنی است که برخی از تراکنش‌ها ممکن است سریع‌تر از دیگران تأیید شود، زیرا شبکه دو رویداد تصادفی را تأیید می‌کند. درحالی‌که در بیت کوین، همیشه حدود ۱۰ دقیقه (به‌علاوه میزان ازدحام شبکه که به این زمان اضافه می‌شود) طول می‌کشد [۱۶]. در شکل (۳)، مقایسه ساختاری زنجیره بلوکی و تنگل نشان داده شده است.



شکل (۳): مقایسه زنجیره بلوکی و تنگل

هرکدام از مربع‌های نشان داده‌شده در شکل (۴)، نشان‌دهنده تراکنشی است که ارسال شده است. درواقع در تنگل برای هر تراکنش جدید، دو تراکنش تصادفی و تائید نشده باید تائید شود. هر بار اعتبارسنجی تراکنش (n)، احتمال صحیح بودن یک تراکنش را تا رسیدن به آستانه (c) افزایش می‌دهد. در این شکل، مربع‌های خاکستری نشان‌دهنده زمانی است که $n = 0$ یعنی هنوز اعتبارسنجی آغاز نشده است ، مربع‌های خال‌خالی که در آن $n > 0$ است تراکنش‌هایی را نشان می‌دهند که هنوز تعداد کافی تأییدیه دریافت نکرده‌اند و مربع‌های سفید نیز نشان‌دهنده تراکنش‌هایی است که تعداد کافی تأییدیه را دریافت کرده‌اند ($n \geq c$) [۱۸].



شکل (۴): ساختار تراکنش‌ها در زنجیره بلوکی تنگل

در ادامه با ارائه جدول (۲)، رمز ارزهای مطرحی را که در بخش‌های قبلی بررسی‌شده‌اند مورد مقایسه قرار می‌دهیم.

جدول (۲): مقایسه ساختاری رمز ارزهای مطرح

	بیت کوین	اتریوم	ریپل	آیوتا
نماد	BTC	ETH	XPR	IOTA
حداکثر تعداد سکه	21 m	?	100 bil	27 bil
الگوریتم چکیده‌ساز	SHA 256	Ethash	SHA 512	Kerl
پشتیبانی قرارداد هوشمند	ندارد	دارد	دارد	ندارد
ثانیه زمان ساخت بلوک	۶۰۰	۱۵	۴	---
اندازه بلوک	1 MB	متغیر	1 MG	بدون بلوک
سهم بازار	۴۷٪.۶	۱۶٪.۲۱	۶٪.۶۷	٪.۰۹۴

۴-۱- تحلیل امنیتی رمز ارزها

حریم شخصی زنجیره بلوکی به‌ویژه زمانی که زنجیره‌های بلوکی عمومی طراحی‌شده‌اند پیچیده می‌شود چرا که تمام معاملات شفاف هستند و عرضه سکه‌ها به‌صورت عمومی تأیید می‌شود. سازوکارهای حفظ حریم خصوصی باید این اطمینان را حاصل کنند که هر دو این عناصر یعنی، حفظ حریم خصوصی و سازوکار تأییدیه عمومی به‌درستی صورت می‌پذیرد، هرچند که بین این دو مغایرت وجود دارد. قبل از مقایسه رمز ارزها در حوزه حریم شخصی باید مشخص کنیم که چه چیزی به‌معنای حریم خصوصی است. در بعضی از سکه‌ها به این معنی است که اطلاعات معامله پنهان می‌شوند. چه مقداری سکه شما فرستاده‌اید و به چه کسی آن را فرستاده‌اید درحالی‌که بعضی‌ها به‌معنای پنهان کردن آدرس IP شما در شبکه است. حریم خصوصی به‌طور پیش‌فرض به این معنی است که هر تراکنش به‌صورت خودکار خصوصی است. در این بخش تحلیل امنیتی چند رمز ارز مطرح و پرکاربرد مورد بررسی قرارگرفته است.

۴-۲- تحلیل امنیتی بیت کوین

بیت کوین اغلب به‌عنوان پول ناشناس شناخته می‌شود، زیرا امکان ارسال و دریافت بیت کوین‌ها بدون ارائه اطلاعات شناسایی شخصی است. با این حال، رسیدن به گمنامی مناسب و دقیق با بیت کوین می‌تواند بسیار پیچیده باشد و ناشناس بودن کامل ممکن است غیرممکن باشد. بیت کوین مانند نام مستعار است ارسال و دریافت بیت کوین مانند نوشتن تحت نام مستعار است.

اگر نام مستعار نویسنده به هویت آن مرتبط شود، همه چیزهایی که تحت آن نام مستعار نوشته شده است، به آن مرتبط می‌شود [۱۹]. در بیت کوین، نام مستعار شما همان آدرسی است که بیت کوین را دریافت می‌کنید. هر تراکنشی که شامل آن آدرس می‌شود برای همیشه در زنجیره بلوکی ذخیره می‌شود. اگر آدرس شما با هویت شما مرتبط باشد، همه تراکنش‌های شما به شما مرتبط خواهد شد [۱۹]. در مقاله اصلی بیت کوین، به کاربران بیت کوین توصیه می‌شود برای جلوگیری از متصل شدن تراکنش‌ها به یک صاحب مشترک از یک آدرس جدید برای هر تراکنش استفاده کنند. این معادل نوشتن تعداد زیادی کتاب تحت نام‌های مختلف است. اگرچه این راه‌حل خوبی است، اما به دلیل چندین ورودی بودن تراکنش‌ها، برای تضمین کامل گمنامی کافی نیست.

یک تراکنش چند ورودی[1] زمانی اتفاق می‌افتد که شما تراکنش‌های مختلفی را از آدرس‌های مختلف در کیف پول خود دریافت می‌کنید، اما بعد از آن برای یک پرداخت، پول‌ها را از کیف پول خود خارج می‌کنید که بیت کوین‌های آن از چندین آدرس استفاده می‌کنند. بنابراین، تراکنش خروجی شامل آدرس‌های متعدد به‌عنوان ورودی است که اثبات می‌کند همه آن‌ها در یک کیف پول هستند و متعلق به یک موجود واحد هستند. اگر هویت شما به یکی از این آدرس‌ها مرتبط شود، هیچ‌یک از آدرس‌ها گمنامی خود را حفظ نخواهند کرد.

یکی از راه‌های دیگر افزایش گمنامی استفاده از کیف‌های متعدد است. این مانند داشتن چندین شناسه جداگانه است. ساده‌ترین راه برای داشتن چندین کیف پول به‌صورت هم‌زمان استفاده از چند بیتی[2] است. چند بیتی یک کیف پول برای ویندوز، مک و لینوکس است که به شما امکان می‌دهد تا از طریق یک برنامه چندین کیف پول را مدیریت کنید.

یکی از اولین روش‌هایی که برای دست‌یابی به هدف گمنامی صورت گرفت استفاده از معلق‌کننده[3] رمز ارز بود. این کاربر مبنای اصل مخلوط کردن وجوه با دیگران، از طریق ارسال سکه‌ها به افراد دیگر و سپس دادن سکه‌های آن‌ها به شما است [۲۰]. درواقع شما بیت کوین خود را با بیت کوین افراد دیگر با تاریخچه‌های مختلف دست‌به‌دست می‌کنید. برای این کار، آن‌ها بیت کوین‌های شما و بیت کوین‌های بسیاری از کاربران دیگر را در یک استخر قرار می‌دهند. سپس بیت کوین‌ها را به‌صورت تصادفی ارسال می‌کنند تا معلوم نشود کدام ورودی‌ها به کدام خروجی وصل است [۲۰]. بنابراین، اکنون سخت است ثابت کنید که کدام سکه متعلق به چه کسی است و درنتیجه آن سطحی از حریم خصوصی فراهم می‌شود. مخلوط کردن دارای چندین عیب است، شما باید به معلق‌کننده که شخص ثالثی است، اعتماد کنید که سکه‌های شما را به سرقت نمی‌برد.

۴-۳- تحلیل امنیتی رمز ارز مو نرو

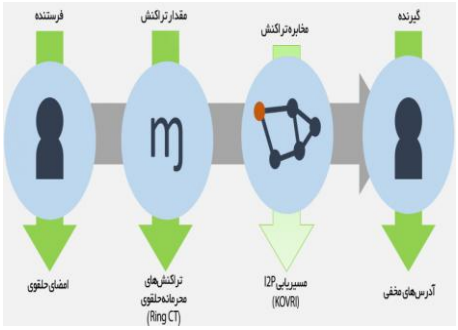
در رمز ارز مو نرو[4] از امضاهای حلقه‌ای[5] استفاده می‌شود که به‌طور قابل توجهی گمنامی را نسبت به انواع طرح‌های مخلوط کردن بهبود می‌بخشد. امضای حلقه از طریق اثبات این‌که معامله را فردی از میان یک گروه از افراد (بدون این‌که مشخص شود چه کسی بوده)، امضا کرده است انجام می‌شود [۲۲]. درواقع با استفاده از امضاهای حلقه‌ای کاربر می‌تواند معامله را انجام دهد و به‌صورت خودکار از خروجی‌های معاملات مشابه دیگر در زنجیره بلوکی برای ورودی‌ها به یک معامله امضای حلقه استفاده کند تا مشخص نشود کدام ورودی متعلق به فردی است که معامله را انجام می‌دهد [۲۲]. این کار به‌صورت خودکار بدون نیاز به مشخص کردن کاربران دیگر که مایل به مخلوط کردن هستند انجام می‌شود و همچنین نیازی به منتظر ماندن برای دیگران برای تأمین بودجه نیست چون این فقط پویش کردن[6] زنجیره بلوکی برای استفاده از آن خروجی‌ها است. از آنجایی که هیچ ترکیب‌کننده‌ای وجود ندارد، نیاز به اعتماد به هیچ ترکیب‌کننده‌ای نیست.

مو نرو همچنین RingCT (معاملات محرمانه حلقه[7]) را پیاده‌سازی کرده است که مبلغ معامله را پنهان می‌کند [۲۲]. اشکال اصلی مو نرو این است که تراکنش‌های آن، به‌ویژه با RingCT، بسیار بزرگ هستند و چند کیلوبایت را اشغال می‌کنند و این به طرز چشمگیری حجم فضای ذخیره‌سازی موردنیاز برای ذخیره زنجیره بلوکی را افزایش می‌دهد.

امضای حلقه که در رمز ارز مو نرو اجرا می‌شوند محدودیت‌هایی در مورد اندازه حلقه (تعداد خروجی‌هایی که شما از آن سکه دریافت می‌کنید) دارد، زیرا اندازه یک تراکنش با افزایش اندازه حلقه به‌صورت خطی افزایش می‌یابد [۲۲]. به همین دلیل است که به‌طور پیش‌فرض مو نرو دارای اندازه نسبتاً کوچک حلقه، یعنی ۴ است. در هر معامله، ناشناس بودن به تعداد شرکت‌کنندگان در حلقه محدود می‌شود. تحلیلگران زنجیره بلوکی اگرچه ممکن است قادر به اثبات ارتباط معاملات نباشد، آن‌ها می‌توانند احتمالات را محاسبه کنند.

در شکل (۵)، حلقه مو نرو نشان داده شده است.

[1] Multi-input transaction
[2] MultiBit
[3] Tumbler
[4] Monero
[5] Ring signatures
[6] Scan
[7] Ring Confidential Transactions



شکل (۵): حلقه مونرو

عیب دیگر مونرو این است که اگر ضعف در اجرای امضای حلقه وجود داشته باشد یا یک کامپیوتر کوانتومی منطقی قوی موجود باشد، تمام تاریخچه زنجیره بلوکی شناسایی و افشا می‌شود؛ که قابل جبران نیست. در حقیقت، پیاده‌سازی ناقص امضای حلقه در یک رمز ارز به نام ShadowCash اجازه داد که زنجیره بلوکی آن به‌طور کامل شناسایی شود.

با وجود این مشکلات، امضای حلقه ثابت کرده است که یکی از فنآوری‌های حفظ حریم خصوصی خوب و مورد بازبینی شده است و تنها مواردی که به‌طور عمومی شناسایی شده است به دلیل پیاده‌سازی نامناسب بوده است مانند ShadowCash یا استفاده از معامله mixin-0 در مو نرو که منجر به ردیابی شدن ۸۷٪ از ورودی‌ها شد. مو نرو بسیاری از مشکلات معلق‌کننده‌های رمز ارزها را حل کرد و گمنامی خوبی را ایجاد کرد اما دارای مشکلات مقیاس‌پذیری در اندازه‌های بزرگ معاملات، غیرقابل هرس شدن زنجیره بلوکی و محدود بودن اندازه حلقه است.

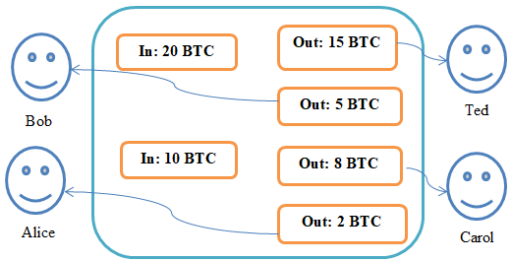
۴-۴- تحلیل امنیتی پروتکل کوین جوین در رمز ارز دش

پروتکل کوین جوین[1] بهبودیافته ایده مخلوط کردن است و امکان دزدیدن سکه‌ها توسط معلق‌کننده را از بین می‌برد. این ویژگی در دارک کوین[2] که در حال حاضر به‌عنوان دش[3] شناخته می‌شود استفاده می‌شد. بااین‌حال، هنوز هم اشکالاتی در این سامانه وجود دارد. شما می‌بایست برای ناشناس ماندن خود به معلق‌کننده اعتماد کنید زیرا ترکیب‌کننده[4] می‌تواند اطلاعات قابل‌شناسایی را ثبت[5] کند و می‌داند که چگونه عمل مخلوط کردن، از طریق آدرس ورودی هر کاربر و آدرس دریافت‌شده سکه‌ها، اتفاق می‌افتد [۲۱]. این مسئله را می‌توان با استفاده از امضاهای دیجیتالی کور[6] حل کرد، اما در این صورت ناشناس بودن کوین جوین به شدت بر امکان اتصال به معلق‌کننده به‌صورت ناشناس، از طریق شبکه تور[7]، متکی می‌شود [۲۱].

برای ترکیب کردن باید افراد شرکت‌کننده در ترکیب حتماً آنلاین باشند. اگر کس دیگری جز شما نخواهد عمل ترکیب کردن را انجام دهد، ترکیب کردن به تأخیر می‌افتد. ناشناس بودن به تعداد افرادی که با آن‌ها عمل مخلوط کردن را انجام می‌دهید بستگی دارد. در حالت عادی یک عمل مخلوط کردن در رمز ارز دش شامل سه شرکت‌کننده می‌شود، البته این کار می‌تواند تکرار شود. تحقیقات نشان می‌دهد که در هنگام پرداخت، حتی با چندین بار مخلوط کردن کوین جوین، کیف پول کاربر قابل شناسایی است اگر آن‌ها مراقب کوکی‌های مرورگر نباشند، زیرا مخلوط کردن فقط ارتباطات تراکنش‌ها با آدرس‌ها را مختل می‌کند، اما به‌طور کامل آن‌ها را نابود نمی‌کند [۲۱].

پیشرفت‌های دیگر مانند CoinShuffle++، نیاز به اعتماد به یک شخص ثالث را حذف کرد، اما همچنان دارای اشکالات دیگر کوین جوین، یعنی یک مجموعه محدود برای گمنامی و نیاز به آنلاین بودن شرکت‌کنندگان است.

مزیت اصلی طرح‌های مخلوط کردن این است که آن‌ها نسبتاً ساده هستند و در رمز ارزها بدون نیاز به استفاده از قوانین خاص اجماع کار می‌کنند. با اقدامات احتیاطی مناسب، کوین جوین می‌تواند گمنامی را در سطح پایه فراهم کند. در شکل (۶) ، نحوه عملکرد پروتکل کوین جوین نمایش داده شده است.



شکل (۶): عملکرد پروتکل کوین جوین در رمز ارز دش

۵-۴- تحلیل امنیتی پروتکل زیروکوین

پروتکل زیروکوین[8] در رمز ارزهای زد کوین[9] و پی آی ایکس[10] پیاده‌سازی شده است. برخلاف طرح‌های گمنامی قبلی که شامل مبهم‌سازی معاملات واقعی با استفاده از سایر ورودی‌ها یا معاملات

[1] CoinJoin
[2] Darkcoin
[3] Dash
[4] Mixer
[5] Log

[6] Blind digital signatures
[7] Tor
[8] Zerocoin
[9] Zcoin
[10] Pivx

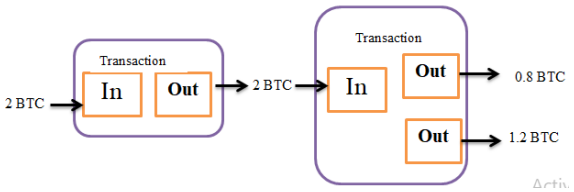
هستند، پروتکل زیروکوین ارتباطات معامله‌ای بین سکه‌ها را از طریق استفاده از اثبات با دانش صفر از بین می‌برد. به عبارت ساده، یک اثبات با دانش صفر، ثابت می‌کند که شما کاری را انجام داده‌اید و یا چیزی را می‌دانید بدون نشان دادن اطلاعات دیگر. به‌عنوان مثال، اثبات این‌که شما رمز عبور را می‌دانید بدون این‌که آن را واقعاً بیان کنید.

زیروکوین با اجازه دادن به شما برای سوزاندن[1] سکه‌ها کار می‌کند که به آن ضرب سکه زیروکوین[2] گفته می‌شود و بعد از آن به همان تعداد سکه جدید (که به‌عنوان یک زیروکوین مصرفی[3] شناخته می‌شود) داده می‌شود [۲۳]. این سکه‌ها بدون سابقه معامله قبلی هستند و شبیه به سکه‌های تازه استخراج شده‌اند [۲۳]. اثبات با دانش صفر برای اثبات این است که شما واقعاً سکه‌ها را بدون آشکار کردن ویژگی‌های سکه‌ها سوزانده‌اید. علاوه‌بر این، با استفاده از اثبات شما مجاز به دریافت تعداد یکسان سکه جدید و تمیز هستید [۲۳].

این بدان معنی است که برخلاف کوین جوین و امضای حلقه که در آن مجموعه گمنامی به تعداد شرکت‌کنندگان یا اندازه حلقه محدود می‌شود، زیروکوین گمنامی بیشتری را فراهم می‌کند. مجموعه گمنامی در آن شامل تمام افرادی است که ضرب سکه زیروکوین انجام داده‌اند. همچنین، سکه‌ها واقعاً ارتباطات[4] معامله‌ای خود را از بین می‌برد، زیرا آن‌ها به‌طور کامل سکه جدیدی ایجاد می‌کنند درحالی‌که در روش قبلی صرفاً مبهم می‌شدند.

با توجه به شکل (۷)، زنجیره یک تاریخچه عادی از تراکنش بیت کوین را نشان می‌دهد که هر تراکنش به تراکنش پیشین خود متصل است ولی در زنجیره زیروکوین، ارتباط بین ضرب و خرج سکه را نمی‌توان از داده‌های زنجیره بلوک به‌دست آورد [۲۳].

این طرح گمنامی هم خالی از اشکال نیست. در عوض مجموعه گمنامی بزرگ و از بین بردن ارتباطات معاملات، زیروکوین برای تولید پارامترهای اولیه نیاز به‌یک‌بار تنظیم اعتماد[5] دارد. تنظیمات قابل‌اعتماد به این معنی است که سازندگان باید برخی پارامترهای اولیه را برای سکه خود تولید کنند و سپس این پارامترها را از بین ببرند. در زیروکوین دو عدد آغازی بسیار بزرگ وجود دارد که باید نابود شوند. دانستن این دو عدد اول بزرگ اجازه می‌دهد که زیروکوین جعلی ساخته شود. برای مقابله با این مشکل، زدکوین از RSA استفاده می‌کند تا امروز، پارامترهای RSA-2048 به‌طور گسترده‌ای مورداستفاده قرار می‌گیرد و حداقل تا زمان ظهور محاسبات کوانتومی تقریباً غیرقابل شکست است [۲۴]. در شکل (۷)، دو نمونه از زنجیره بلوکی نشان داده‌شده است.



شکل (۷): تراکنش بیت کوین [۲۳].

شایان‌ذکر است که دانستن این دو عدد اول گمنامی زیروکوین را به خطر نمی‌اندازد، اما امکان جعل سکه را فراهم می‌کند [۲۴]. علاوه بر این، احتمال وقوع این موضوع با توجه به این‌که عرضه زدکوین قابل حسابرسی است، کاهش می‌یابد، بنابراین، جعل سکه‌ها قابل‌شناسایی است. در حقیقت، به علت یک اشکال در پیاده‌سازی (و نه به خاطر شکست RSA)، جعل *سکه‌ها* به‌طور واقعی در زدکوین رخ داد اما شناسایی و متوقف شد. این نشان می‌دهد که چقدر در *سکه‌های* اثبات بادانش صفر که شامل سوزاندن و ایجاد *سکه‌های* جدید می‌شوند، قابلیت حسابرسی عرضه بسیار مهم است.

یکی دیگر از محدودیت‌های زیروکوین این است که معیار[6] پولی ثابتی باید برای سکه زدن و مصرف آن استفاده شوند و اندازه اثبات بادانش صفر برای زیروکوین مصرفی در مقایسه با معامله RingCT نسبتاً بزرگ و در حدود ۲۵ کیلوبایت است [۲۴]. همچنین استفاده نادرست یا استفاده قابل پیش‌بینی از تراکنش‌های مصرفی و ضرب سکه مانند ضرب سکه و خرج کردن آن در فواصل منظم و یا استفاده از یک آدرس IP مشابه برای ضرب سکه و خرج کردن آن، می‌تواند احتمالاً گمنامی را به خطر اندازد.

به‌طور خلاصه، زیروکوین گمنامی بسیار قوی را با یک مجموعه بزرگ گمنامی بدون هیچ ردی از ارتباط معامله ارائه می‌دهد، اما در حال حاضر نیاز به تنظیمات اعتماد، فضای ذخیره‌سازی اضافی در زنجیره بلوکی و منابع محاسباتی اضافی برای تأیید دارد. تحقیقاتی وجود دارد که نشان می‌دهد حذف تنظیمات اعتماد و کاهش اندازه اثبات کار از طریق پروتکل سیگما در زیروکوین امکان‌پذیر است و گروه Zcoin در حال بررسی و ارزیابی استفاده از آن به همراه سایر روش‌ها است [۲۴].

[1] Burn
[2] Zerocoin mint
[3] Zerocoin spend
[4] Links
[5] Trusted setup
[6] Denomination

۴-۶- تحلیل امنیتی پروتکل زیروکش

طرح نهایی گمنامی بررسی‌شده در این تحقیق، پروتکل زیروکش[1] است که در زی‌کش[2] استفاده می‌شود. زیروکش در ادامه کار زیروکوین ساخته‌شده و به دنبال رفع نقص‌های زیروکوین است. زی‌کش با استفاده از پروتکل زیروکش و استفاده از zkSNARK[3]، اندازه اثبات کار را به ۱ کیلوبایت کاهش داد و تائید آن بسیار سریع است. علاوه بر این، تمامی مبالغ معامله‌ها پنهان هستند و دیگر نیازی به استفاده از معیارهای پولی ثابت در هنگام ضرب سکه نیست. زیروکش همچنین به افراد اجازه می‌دهد تا بدون نیاز به تبدیل، معادل زیروکش از زیروکوین را به یکدیگر انتقال دهند. با نگاهی مختصر به آن، به نظر می‌رسد که زیروکش، زیروکوین را منسوخ می‌کند. بااین‌حال برای رسیدن به این هدف، مجبور است که بین مزایای خاصی که زیروکوین دارد تعادل برقرار کند. اول‌ازهمه، زیروکش فاقد حسابرسی است؛ مانند زیروکوین، زیروکش نیاز به تنظیمات اعتماد دارد، اما تنظیمات زیروکش بسیار پیچیده‌تر است. زی‌کش از شش نفر شخص ثالث استفاده می‌کند، تنها راه برای نشت پارامترها این است که تمام این شش نفر برای حفظ کلیدها باهم تبانی کنند [۲۵]. به‌عبارت‌دیگر، شما باید به همه این شش نفر اعتماد کنید که پارامترهای اولیه را نابود می‌کنند این‌یک مشکل جدی است که زی‌کش درروش جدید تنظیمات قابل اعتمادش دارد.

اگر یک اشکال در کد، یک نقص رمزنگاری یا یک مشکل در تنظیمات اعتماد اشخاص ثالث[4]، وجود داشته باشد، مهاجم احتمالاً می‌تواند به‌طور نامحدود زی‌کش ایجاد کند و برخلاف زیروکوین، این عرضه اضافی قابل‌شناسایی نیست. این در حالی است که به‌خصوص در یک سامانه که با اصول مشابه با زیروکوین عمل می‌کند که اجازه ایجاد *سکه‌های* جدید را می‌دهد، وجود حسابرسی به‌طور فزاینده‌ای مهم است. بنابراین اگرچه زیروکش به‌طور بالقوه بیشترین گمنامی را ارائه می‌دهد، این را با پرداخت *هزینه‌های* نبود حسابرسی به همراه پیچیدگی تنظیمات اعتماد و استفاده از رمزنگاری جدید می‌پردازد. در جدول (۴)، مؤلفه‌های امنیتی رمز ارزهای مطرح مقایسه شده است.

جدول (۴): مقایسه مؤلفه‌های امنیتی رمز ارزها

زیروکوین	مونرو	دش	زد کش	بیت کوین	
XZC	BTC	ZEK	DASH	XMR	نماد
zk-SNARK	zk-SNARK	Coinjoin-based	Zerocoin	ندارد	الگوریتم امنیتی
دارد	دارد	دارد	دارد	ندارد	حریم خصوصی
۱۰ دقیقه	۲/۵ دقیقه	۲/۵ دقیقه	۲/۵ دقیقه	۱۰ دقیقه	ساخت بلوک
دارد	ندارد	دارد	دارد	ندارد	انتقال امن پیام
دارد	دارد	دارد	دارد	ندارد	پنهان سازی تراکنش
ندارد	دارد	دارد	دارد	ندارد	تراکنش شفاف

۵- نتیجه‌گیری

زنجیره بلوکی مانع نفوذ هکرها به شبکه‌های سنتی و از بین بردن یا تغییر داده‌ها می‌شوند. با مطالعات انجام‌شده مشاهده نمودیم که زنجیره بلوکی به علت وجود پاداش‌ها رو به متمرکز شدن می‌رود درحالی‌که ساختار تنگل که در آن خبری از پاداش نیست و تراکنش‌ها را بدون هزینه انجام می‌شود، غیرمتمرکزتر است و همین‌طور با توجه به ساختار آن‌که نیاز به تائید ۲ تراکنش برای انجام هر تراکنش دارد، از سرعت مطلوبی برخوردار است.در بررسی گمنامی رمز ارزهای مطرح نشان دادیم که درحالی‌که حاضر، بهترین پروتکل دارای گمنامی، پروتکل zkSNARK است که شامل یک پروتکل اثبات بادانش صفر بوده و این امکان را ایجاد می‌نماید که تراکنش‌ها به‌صورت رمز شده تائید شوند تا اطلاعات کاربران و مقدار پول انتقال‌یافته محرمانه بماند.

هدف از این مقاله، تحلیل و بررسی ارزهای دیجیتال مطرح ازنقطه‌نظر ساختار، قدرت و امنیت است تا بتوان با استفاده از بهترین ساختار و روش، رمز ارزی تولید کرد که از امنیت و گمنامی بالایی برخوردار باشد تا با توجه به مشکل روز جامعه و وابستگی تجارت به دلار که مشکلات اقتصادی سنگینی را وارد کرده است، امکان مبادله و خرید به‌صورت ناشناس و با استفاده از رمز ارز بومی امکان‌پذیر باشد که کشورهای زیادی ازجمله کشورهای تحت تحریم بر روی آن سرمایه‌گذاری کرده‌اند.

[1] Zerocash
[2] ZCash
[3] Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
[4] Multi-party

۶- مراجع

[1] Moneycrashers, "What is Cryptocurrency - How it Works, History & Bitcoin Alternatives," August 14, 2017. https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives

[2] D. LEE Kuo Chuen, "Digital Currency Bitcoin, Innovation, Financial Instrument and Big Data," 1st Ed, Univ. of Singapore Management, Singapore, vol. 11, 2015.

[3] A. Zameer and P. Kumar Chaurasia, "A Review on crypto-currency," International Journal of Computer Science and Mobile Applications, vol. 6, Issue. 1, pp. 95-100, 2018.

[4] Sh. Shakeel Ahamad, M. Nair, and B. Varghese, "A Survey on Crypto Currencies, 2013.

[5] Amoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] P. Akhavan, "Digital Currency Bitcoin Blockchain," 1st Ed, Univ. of Malek Ashtar University, Iran, pp. 153-157, 2017.

[7] N. Acheson, "hard fork vs soft fork," 2018. https://www.coindesk.com/information/hard-fork-vs-soft-fork.

[8] Bitcoin. Stackexchange, "How can forks coexist even though only one of the is the longest chain?," 2018. https://bitcoin.stackexchange.com/questions/77838/how-can-forks-coexist-even-though-only-one-of-the-is-the-longest-chain/77839#77839.

[9] V. Buterin, "A next generation smart contract and decentralized application platform," 2013.

[10] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," 2014.

[11] A. Efe Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. Gün Sirer, "Decentralization in Bitcoin and Ethereum Networks," Cornell University, January 2018.

[12] S. Popov, "The Tangle," October 2017.

[13] S. Goldfeder, H. Kalodner, and D. Reisman, "Arvind Narayanan," When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Univ. of Cornell, UK, Aug. 2017.

[14] Th. Hernandez-Castro, Julio C, "An Analysis of Bitcoin Laundry Services," Nordic Conference on Secure IT Systems," Tartu, Estonia, pp. 8-10, Nov. 2017.

[15] F. Konstantin Maurer and T. Neudecker, "Anonymous CoinJoin Transactions with Arbitrary Values," Communication and Distributed Systems RWTH Aachen University, 2017.

[16] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, Sh. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, "An Empirical Analysis of Traceability in the Monero Blockchain," Proceedings on Privacy Enhancing Technologies, pp. 143–163, 2018.

[17] I. Miers, Ch. Garman, M. Green, and Aviel D. R. The Johns Hopkins, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," Univ. of Baltimore, USA, 2016.

[18] R. Yap, "How Zcoin's Privacy Technology Compares to the Competition," 2017. https://zcoin.io/zcoins-privacy-technology-compares-competition,

[19] E. en-Sasson, A. Chiesa, Ch. Garman, M. Greenz, I. Miers, E. Tromer, and M. Virzay, "Zerocash: Decentralized Anonymous Payments from Bitcoin," May 2014.