نشریه علمی پدافند غیرعامل

سال دهم، شماره ٤، زمستان ۱۳۹۸، (پیاپی ٤٠): صص ۸۰-۶۹

معرفی بیت‌کوین و چالش‌های امنیتی آن

فاطمه عزیزی[۱]، هادی سلیمانی[۲]*

تاریخ دریافت: ۱۳۹۷/۰۵/۰۹
تاریخ پذیرش: ۱۳۹۸/۰۲/۱۶

چکیده

جهان با روند رشد روزافزون اطلاعات و تراکنش‌ها، نیاز به سامانه سریع با امنیت بالا دارد. به همین دلیل مبحث ارز دیجیتال طی چند سال گذشته توجه پژوهشگران را به خود جلب کرده است. بیت‌کوین اولین ارز دیجیتال ارائه شده است و بر روی بلاک چین عمل می‌کند. در حال حاضر تقاضا برای استفاده از بیت‌کوین به دلیل ویژگی‌های جالبی که دارد، بسیار بالا رفته است. دلیل این امر ویژگی‌های خاص ارزهای دیجیتال است. به‌طور خاص مهم‌ترین ویژگی این ارزها و به‌طور ویژه بیت‌کوین، غیرمتمرکز بودن آن است که به‌موجب آن نیازی به‌واسطه مورد اعتماد برای حفظ امنیت نیست. در این مقاله ضمن معرفی بیت‌کوین و سازوکارهای تولید این ارز دیجیتال، امنیت آن را در مقابل حملات ارائه‌شده، بررسی می‌کنیم. به‌طور خاص در این مقاله چالش‌هایی از قبیل حمله و گمنامی در بیت‌کوین را بررسی می‌کنیم. شناخت چالش‌ها و ویژگی‌های ارزهای دیجیتال و به‌ویژه بیت‌کوین می‌تواند ما را در فهم چالش‌ها و فرصت‌های پیش‌رو، در این حوزه یاری کند. این تحقیق از این جهت در حوزه پدافند غیرعامل ضروری به نظر می‌رسد که شاهد افزایش بی‌نظیر استفاده از بیت‌کوین در کشور می‌باشیم. این امر پتانسیل این را دارد که سبب ضعف اساسی در حمله به بخشی از اقتصاد کشور شود.

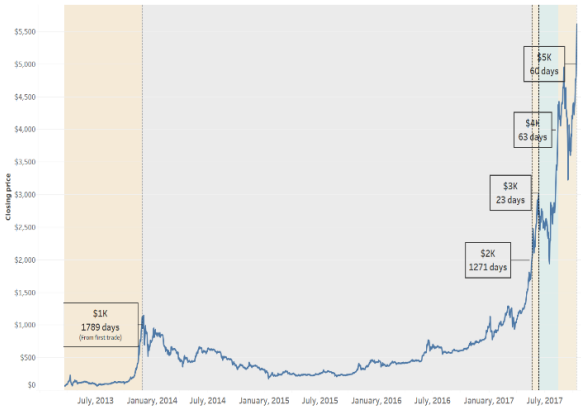
کلید واژه‌ها: بیت‌کوین، ارز دیجیتالی، بلاک‌چین، گمنامی

۱- دانشجوی کارشناسی ارشد، دانشگاه شهید بهشتی، fam_azizi1912@yahoo.com
۲- استادیار پژوهشکده فضای مجازی، دانشگاه شهید بهشتی (h_soleimany@sbu.ac.ir)- نویسنده مسئول

۱. مقدمه

حجم تراکنش‌ها در سراسر جهان به‌طور نمایی در حال رشد است و مطمئناً پیچیدگی، آسیب‌پذیری، ناکارآمدی و هزینه سامانه‌های کنونی برای انجام تراکنش‌ها را شدت خواهد بخشید. به‌خصوص حجم تراکنش‌ها با پدیدار شدن اینترنت اشیا (IOT) به‌صورت انفجاری در حال رشد است. جهان برای مقابله با چنین چالش‌هایی به شبکه پرداختی سریع، دارای سازوکار مورد اعتماد، کم‌هزینه‌تر نیازمند است.

راه‌حلی که برای پاسخ به این موضوع داده‌شده، استفاده از ارزهای دیجیتال است. بیت‌کوین (Bitcoin) اولین ارز دیجیتال ارائه‌شده و رایج‌ترین آن‌ها است. بیت‌کوین یک ارز دیجیتالی است که توسط شخص (اشخاص) بانام مستعار ساتوشی ناکاماتو شناخته می‌شود، در سال ۲۰۰۸ عرضه شد [۱]. پس‌ازآن ارزهای مشابهی عرضه شده است که بعضاً استفاده از آن‌ها رو به رشد است [۲-۴].



شکل (۱): افزایش اعتبار بیت‌کوین [۵].

بیت‌کوین بر زیربنای بلاک‌چین ساخته شده است که به‌عنوان دفتر کل مشترک بیت‌کوین به‌کار می‌رود [۶]. در واقع بلاک‌چین ابزار ثبت تراکنش‌های بیت‌کوین را ارائه می‌کند. برای شهود بیشتر می‌توان بلاک‌چین را به‌عنوان سیستم‌عامل و بیت‌کوین را یکی از هزاران نرم‌افزاری که روی این سیستم‌عامل اجرا می‌شود، در نظر گرفت. بلاک‌چین یک دفتر کل توزیع‌شده و مشترک است که کار فرایند ثبت تراکنش‌ها و ردگیری دارایی‌ها را در یک شبکه کسب‌وکار ساده می‌کند. تقریباً هر چیز ارزشمندی می‌تواند در یک شبکه بلاک‌چین ردگیری و معامله شود و مخاطرات و هزینه‌ها را برای همه طرف‌های درگیر کاهش دهد [۷-۸]. برهمین اساس حملات متعددی به بیت‌کوین ارائه شده است که بعضا از ضعف‌های نحوه استفاده و یا مشکلات شبکه بهره می‌برند [۹-۱۲].

همان‌طور که در شکل (۱) مشاهده می‌شود، استفاده از بیت‌کوین به‌صورت نمایی در حال افزایش است. در شکل (۱) افزایش اعتبار بیت‌کوین برحسب دلار در بازه زمانی ۲۰۱۳ الی ۲۰۱۷ نشان داده شده است.

۲. بیت‌کوین

۲-۱. ویژگی‌ها

غیرمتمرکز (Decentralized)**:** شبکه بر اساس ارتباط همتا به همتا[1] عمل می‌کند و برای انجام تراکنش به شخص ثالث مورد اعتماد نیازی نیست تا امنیت تراکنش را تضمین کند.

امنیت: در این روش ردگیری روند تراکنش‌ها آسان‌تر است؛ زیرا تاریخچه تمامی تراکنش‌ها در زنجیره وجود دارد و تغییر آن‌ها تقریباً غیرممکن است.

کنترل: اگر بانک مشاهده کند که حساب شما بیش از حد کاهش‌یافته یا چند هفته اوضاع مالی نامساعدی داشته‌اید، حساب شما را مسدود می‌کند. با استفاده از بیت‌کوین هیچ‌کس جز شما نمی‌تواند پولتان را کنترل کند. شما تنها کسی هستید که کلیدهای حسابتان را در دست دارید، این یعنی مسئولیت خیلی زیادی بر عهده خود شماست، اما در عوض آزادی زیادی هم دارید.

بدون محدودیت: هرکسی که به اینترنت متصل باشد می‌تواند در یک شبکه بلاک‌چین مانند بیت‌کوین شرکت کند؛ یعنی هیچ مرز فیزیکی، ملیتی یا جغرافیایی وجود ندارد. نرخ مبادلات محدودیتی ندارد و هزینه مبادلات و احتمال عدم پاسخگویی سیستم بسیار پایین است.

شفافیت (Transparent): ثبت و به‌روزرسانی داده‌ها توسط سیستم بلاک‌چین برای هر نود قابل مشاهده است. به همین دلیل است که بیت‌کوین می‌تواند مورد اعتماد قرار گیرد.

حفظ حریم شخصی: بیت‌کوین برای حفظ حریم شخصی از اصل گمنامی استفاده می‌نماید.

حذف واسطه‌گری: به دلیل اساس توافق، هر نود در سیستم بلاک‌چین می‌تواند داده‌ها را به‌طور امن انتقال دهد و یا به‌روزرسانی کند و هیچ‌کس نمی‌تواند در آن مداخله کند.

[1] Peer to Peer

متن‌باز (Open Source): بیشتر دستگاه‌های بلاک‌چین متن‌باز هستند. ثبت اطلاعات می‌تواند به‌صورت عمومی بررسی گردد.

رایگان: برای انتقال پول در زنجیره بیت‌کوین هزینه بالایی پرداخت نمی‌شود. در مقایسه با سامانه‌های کنونی که برای انتقال و خدمات دیگر هزینه دریافت می‌کنند، بیت‌کوین رایگان است.

۲-۲. کارهای مرتبط

همان‌طور که پیش از این بیان شد، بیت‌کوین اولین ارز دیجیتال است که از فناوری زنجیره قالبی استفاده کرده است. پس از ارائه بیت‌کوین شاهد یک مسیر جدی در تحقیقات مرتبط بوده‌ایم مبنی بر ارائه رمزارزهای جدید که ویژگی‌های خاصی دارند که بیت‌کوین ندارد.

مهمترین نقاط ضعف بیت‌کوین به شرح ذیل است:

- مصرف انرژی زیاد برای کاری که سودی برای جامعه ندارد!
- در عمل تنها افرادی که سخت افزار خاص دارند می‌توانند در فرآیند گسترش زنجیره شرکت کنند.
- نمی‌توان بیت کوین را با ماشین تورینگ آن را شبیه‌سازی کرد.
- در عمل ممکن است با تجزیه و تحلیل داد و ستدها، گمنامی بیت کوین زیر سوال برود.

برهمین اساس سوالات مهمی که در این حوزه به‌وجود آمد به شرح ذیل است:

۱. آیا می‌شود یک رمزارز ارائه کرد که عملیات استخراج را نتوان براساس سخت افزارهای خاص انجام داد؟
۲. آیا می‌شود یک رمزارز ارائه کرد که انرژی کمتری مصرف کند؟
۳. آیا می‌شود یک رمزارز ارائه کرد که یک مسئله مفید را حل کند؟
۴. آیا می‌شود یک رمزارز ارائه کرد که که قابلیت ائتلاف برای استخراج وجود نداشته باشد.
۵. آیا می‌شود یک رمزارز ارائه کرد که در آن گمنامی را به صورت کامل و واقعی فراهم کند؟
۶. آیا می‌شود یک رمزارز ارائه کرد که بتوان با زبان ماشین تورینگ آن را شبیه‌سازی کرد؟

برهمین اساس رمزهای جدیدی ارائه شد که برخی از مهمترین آنها به همراه مهمتری ویژگی رزمارز، به شرح ذیل می‌باشند:

- Litecoin: استفاده از سخت‌افزار کار ساده‌ای نیست.
- Spacecoin: مسئله براساس Proofs of Space
- Primecoin و Permacoin: حل مسائل مفید
- Zerocash: گمنامی واقعی
- Ehereum: براساس اسکریپت تورینگ

۳. نحوه عملکرد بیت‌کوین

۳-۱. نحوه ارسال بیت‌کوین

در بیت‌کوین به‌جای طرف سوم مورد اعتماد، در اجرای تراکنش‌های برخط بین دو طرف از امضای دیجیتال، توابع چکیده‌سازی، زنجیره قالب و رمزنگاری کلید عمومی استفاده می‌شود. رمزنگاری کلید عمومی خود شامل دو بخش می‌شود:

کلید امضا خصوصی (Secret Key): که برای انجام تراکنش نیاز است و تنها در دسترس خود دارنده ID قرار دارد.

$$Sig = sign(sk, message)$$

کلید امضا عمومی (Public Key): که هم به‌عنوان آدرس ID کاربرد دارد و هم صحت هویت طرف مقابل در انجام تراکنش بررسی می‌نماید.

$$Valid = Verify(pk, message, sig)$$

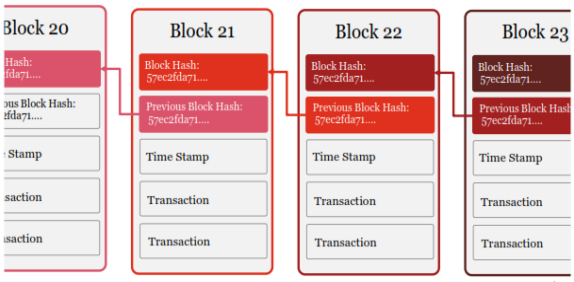
برای ارسال بیت‌کوین، به دو چیز نیاز است: آدرس بیت‌کوین (کلید عمومی) و یک کلید خصوصی.

آدرس بیت‌کوین به‌صورت تصادفی تولید می‌شود و یک دنباله ساده از حروف و اعداد است و می‌توان آن را به اشتراک گذاشت. کلید خصوصی توالی دیگری از حروف و اعداد است که درواقع، قلب کیف پول شماست و می‌توان از آن برای بازیابی کیف پول در نرم‌افزارهای دیگر استفاده کرد [۱۳]. اگر کسی کلید خصوصی شما را داشته باشد، دسترسی به کیف پولتان برایش آسان می‌شود.

آدرس بیت‌کوین را می‌توان یک جعبه شیشه‌ای محکم در نظر گرفت که همه می‌توانند محتویات آن را ببینند اما فقط با کلید خصوصی می‌توانند آن را باز کرد و به محتویات دسترسی داشته باشند. این ساختار به‌نحوی است که در مقابل حملات فرد در میانی امن است [۱۴].

۳-۲. ساختار زنجیره قالبی

ساختار زنجیره قالب به این‌صورت است که یک قالب شامل اطلاعات تراکنش‌ها و مقدار چکیده قالب قبلی است. همان‌طور که در شکل (۲) نشان داده شده است مقدار چکیده قالب قبلی، باعث می‌شود قالب‌ها به شکل زنجیره‌ای باهم ارتباط پیدا کنند.



شکل (۲): ساختار قالب در بیت‌کوین

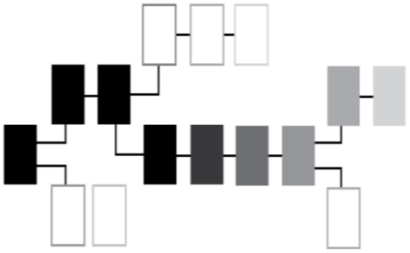
با توجه به این ساختار تغییر کوچکی در بخشی از اطلاعات قالب، باعث تغییر چکیده آن می‌شود. در واقع برای تغییر اطلاعاتی به شکلی که دیگران متوجه آن نشوند بایستی در ادامه آن تمامی مقادیر چکیده قالب‌های موجود در زنجیره را تغییر داد که در عمل این کار غیرممکن است.

قالب‌های جدید در ادامه زنجیره طولانی‌تر ساخته می‌شوند. در واقع زنجیره طولانی، زنجیره اصلی است که دارای اعتبار است و تراکنش‌های موجود در زنجیره‌های فرعی بی‌اعتبار هستند. در شکل (۳) زنجیره اصلی که دارای اعتبار است رنگی است و سایر زنجیره‌ها که اعتباری ندارند بدون رنگ هستند.

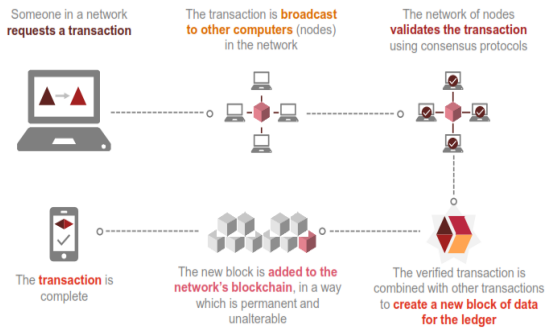
۳-۳. نحوه انجام تراکنش

روند آنجا تراکنش در بیت‌کوین بدین شکل مطرح شد که فردی که می‌خواهد تراکنشی انجام دهد بایستی تراکنش را به تمام نودهای موجود در زنجیره ارسال می‌کرد و نودها، تراکنش را بررسی می‌کردند. در صورت تائید صحت تراکنش توسط اکثر نودها، تراکنش در قالب جدید قرار می‌گرفت و به زنجیره اضافه می‌شد. در صورت متصل شدن به زنجیره تراکنش صورت می‌گرفت. این روند در شکل (۴) به‌صورت تصویری نشان داده شده است.

در بخش ۴- خواهیم دید که روش ارسال تراکنش به‌تمامی نودها امکان‌پذیر نیست و روش‌های دیگری کاربرد دارند. همچنین در این بخش بیان خواهد شد که استخراج‌کنندگان بیت‌کوین، تراکنش را بررسی می‌کنند و در یک قالب از تراکنش‌ها قرار می‌دهند و درنهایت تراکنش تائید می‌شود.



شکل (۳): زنجیره قالبی در بیت‌کوین



شکل (۴): نحوه انجام تراکنش در بیت‌کوین

۳-۴. نحوه ذخیره تراکنش

اولین مدلی که برای ثبت اطلاعات در قالب به ذهن می‌رسد به این شکل است که صرفاً مقدار بیت‌کوین‌های جابه‌جاشده بانام افراد در تراکنش نوشته شود. این مدل به نام مدل Account-based دارای این مشکل است که برای دانستن مقدار باقی‌مانده حساب یک فرد بایستی کل تراکنش‌های انجام‌شده را موردبررسی قرار دهیم. روند ذخیره تراکنش بر اساس این مدل در شکل (۵) نشان داده شده است.

Create 25 coins and credit to Alice$_{\text{ASSERTED BY MINERS}}$
Transfer 17 coins from Alice to Bob$_{\text{SIGNED(Alice)}}$
Transfer 8 coins from Bob to Carol$_{\text{SIGNED(Bob)}}$
Transfer 5 coins from Carol to Alice$_{\text{SIGNED(Carol)}}$
Transfer 15 coins from Alice to David$_{\text{SIGNED(Alice)}}$

شکل (۵): مدل Account-based [۱۵].

روش دیگر مدل Transaction-based است که در این روش بعد از انجام تراکنش مقدار بیت‌کوینی که از شخصی مثل آلیس باقی می‌ماند را هم به‌روز می‌کند. درواقع در اطلاعات ثبت‌شده هم مقدار پول واریزی نوشته می‌شود و هم مقدار باقی‌مانده حساب شخص ارسال‌کننده. در نتیجه برای بررسی اطلاعات حساب کاربر، فقط نیاز به بررسی آخرین تراکنش است. روند ذخیره تراکنش در شکل (۶) نمایش داده شده است.

شکل (۶): مدل Transaction-based [۱۵].

۳-۵. نحوه مدیریت کلید

در دنیا واقعی نگهداری از کلید چالش‌برانگیز است. درواقع کلید بایستی به‌گونه‌ای باشد که هم در دسترس باشد و بتوان از آن به‌راحتی استفاده کرد و هم امنیت داشته باشد.

برای این منظور دو نوع ذخیره‌سازی کلید مطرح است:

Hot: برخط است و استفاده از آن راحت‌تر است.

Cold: آفلاین است و به اینترنت متصل نمی‌شود. درنتیجه دارای امنیت بالایی است.

به‌طور مثال برای ذخیره مقدار زیاد پول از مدل Cold استفاده می‌شود و برای پرداخت که به‌صورت مکرر از کلید استفاده می‌شود، مدل Hot مورد استفاده قرار می‌گیرد.

۴. نحوه استخراج بیت‌کوین

یکی از ویژگی‌های بیت‌کوین غیرمتمرکز بودن آن است؛ یعنی این فناوری برای تائید تراکنش‌ها یک مجری مرکزی ندارد. حال این سؤال به وجود می‌آید که با نبود یک مرکز، تراکنش‌ها چگونه تائید یا رد می‌شوند؟ بیت‌کوین چگونه تولید می‌شود؟ چه سازمانی تعیین می‌کند که قوانین سیستم چگونه تغییر کند؟

پاسخ این است که چون شبکه مبتنی بر شبکه P2P است، تائید تراکنش‌ها توسط خود افراد انجام می‌گیرد و نیازی به وجود شخص ثالث نیست. بیت‌کوین توسط استخراج‌کنندگان تولید می‌شود که در ادامه در مورد عملکرد استخراج بیشتر توضیح خواهیم داد. قوانین توسط گسترش‌دهنده‌های اولیه نوشته شده‌اند و غیرقابل تغییر است. برنامه به شکلی نوشته شده است که در طول زمان به‌طور خودکار به‌روزرسانی می‌شود.

چالش کلیدی بیت‌کوین در ویژگی غیرمتمرکز بودن آن است که ابتدا به شکل اجماع توزیع‌شده، در نظر گرفته شده بود. به این مفهوم که برای تائید تراکنش‌ها تمام نودهای صحیح موجود در شبکه، شرکت کنند؛ یعنی زمانی که آلیس می‌خواهد تراکنشی را انجام بدهد باید این تراکنش را به‌تمامی نودها ارسال کند تا صحت آن را بررسی کنند.

پیشبرد این روند به دلیل وجود نودهای خرابکار در شبکه (به این مفهوم که بدون دلیل تراکنش‌ها را تائید نکنند)، برخط نبودن همه نودها در زمان ارسال تراکنش، تأخیر بالای انجام تراکنش (زیرا نودها به‌طور مستقیم باهم در ارتباط نیستند و در طول زنجیره به هم مربوط می‌شوند و ارسال تراکنش به همه نودها زمان‌گیر است.) دشوار بود.

در ادامه روش‌های متفاوت تخصیص پاداش را بررسی می‌کنیم [۱۶]:

۴-۱. روش Proof of work

روش پیشنهادی دیگر انتخاب نود تصادفی بود که نودها درازای داشتن رفتار صادقانه، پاداش (Incentives) دریافت کنند [۱۷]. به این شکل که نود به‌طور تصادفی انتخاب شود و تراکنش‌ها را بررسی کند و تراکنش‌های تائید شده را در قالب جدید قرار دهد و با ایجاد قالب جدید پاداش دریافت کند اما مشکلی که وجود دارد این است که همه برای دریافت پاداش، تعداد IDهای زیادی تولید می‌کنند تا احتمال انتخاب شدن آن‌ها به‌عنوان نود منتخب بالا رود.

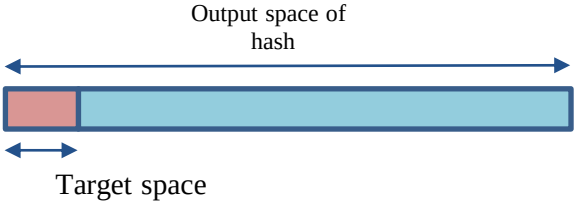
برای رفع این مشکل نود را بر اساس معیاری انتخاب می‌کنند. مثلاً بر اساس توان محاسباتی بالا (Proof of work) یا سرمایه بیشتر (Proof of stake) انتخاب شوند.

POW: نود با توان محاسباتی بالا بایستی یک مسئله سخت از قبل طراحی‌شده را حل کند و نودی که توان محاسباتی بالایی داشته باشد می‌تواند مسئله را زودتر از دیگران حل و قالب جدید را ایجاد کند و پاداش را دریافت کند.

مسئله به این شکل است که باید برای اطلاعات داخل قالب یک nonce بیابد که با گرفتن چکیده آن عبارت مقدار خیلی کمی‌شود. مدل ریاضی آن در فرمول زیر بیان شده است:

$$H(nonce \parallel prev\_hash \parallel tx \parallel tx \parallel tx \parallel \dots \parallel tx) < target$$

شکل (۱)، کاهش حجم اطلاعات را نشان می‌دهد. این الگوریتم به شکلی است که دیگران بتوانند با قراردادن مقدار nonce در الگوریتم صحت آن را به‌سادگی بررسی نمایند. در حال حاضر پیچیدگی محاسباتی آن 10^{20} است و در هر ۱۰ دقیقه یک قالب جدید به زنجیره اضافه می‌شود.



شکل (۷): کاهش حجم اطلاعات با قرار دادن مقدار nonce

به کسی که مقدار nonce را می‌یابد استخراج‌کننده و به این عمل استخراج می‌گویند [۱۸]. در عمل از تجهیزات گران‌قیمت به‌منظور پردازش موازی برای یافتن مقدار نانس استفاده می‌شود [۱۹].

قابل‌توجه است که با روش POW تعداد IDهای جعلی که به دلیل پاداش می‌توانست ایجاد شود، کنترل می‌شود. ولی در عوض فقط نودهایی که توان محاسباتی بالا دارند در بررسی تراکنش‌ها و ایجاد قالب نقش دارند، نه همه نودهای موجود در زنجیره.

شکل (۸): ارتباط فرایند استخراج با امنیت و اعتبار ارز

در این زنجیره امنیت، ارزش بیت‌کوین، سلامت استخراج‌کنندگان به هم وابسته‌اند. در شکل (۸) این ارتباط نشان داده شده است. در واقع با کاهش امنیت، اعتبار و ارزش بیت‌کوین نیز کاهش می‌یابد و برای استخراج‌کنندگان صرفه اقتصادی ندارد که به دنبال استخراج بیت‌کوین باشند.

۴-۲. انواع پاداش

Block reward: که به‌ازای ساخت هر قالب جدید به استخراج‌کننده تعلق می‌گیرد و مقدار آن ثابت است و هرچند سال یک‌بار با به‌روزرسانی شبکه مقدارش کاهش می‌یابد.

Transaction Fees: به‌ازای تائید هر تراکنش، به استخراج‌کننده تعلق می‌گیرد. مقدار آن توسط نودی که درخواست تراکنش را داده، تعیین می‌شود.

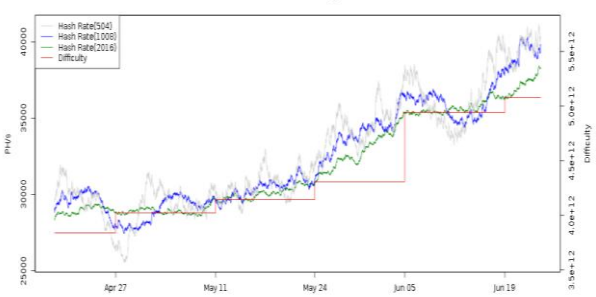
استخراج‌کننده‌ها زمانی عمل استخراج را انجام می‌دهند که مقدار BR و TF بیشتر از هزینه‌های تجهیزات و مصرف انرژی باشد.

کارمزد تراکنش‌ها با استفاده از عوامل مختلف محاسبه می‌شود. برخی از کیف پول‌های برخط اجازه می‌دهند کارمزد تراکنش را خودتان مشخص کنید. هر چه مقدار کارمزدی که مشخص می‌کنید بیشتر باشد، تراکنش شما زودتر تائید می‌شود؛ اما حتی بیشترین کارمزد برای انتقال بیت‌کوین، از کارمزد دستگاه‌هایی مثل پی پال و ... کمتر است.

۴-۳. مدت‌زمان استخراج

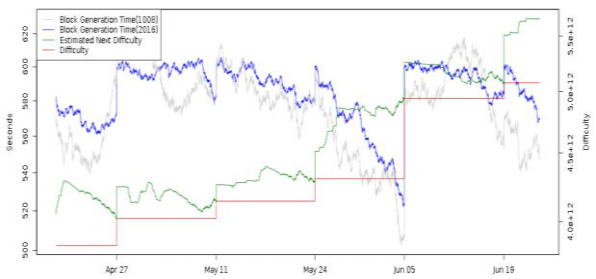
با استفاده از یک CPU مقدار زمان موردنیاز که یک قالب جدید ایجاد شود، حدود ۱۳۹۴۶۱ سال است. با یک FPGA این زمان به ۲۵ سال کاهش می‌یابد. ASIC این عمل را در ۱۴ ماه انجام می‌دهد. به دلیل مقدار زمان زیادی که لازم بود برای ایجاد قالب، مراکز حرفه‌ای استخراج شکل گرفتند. این مراکز با گردهمایی استخراج‌کننده‌ها سعی بر کاهش زمان تولید قالب دارند. البته این مراکز باعث متمرکز شدن بیت‌کوین می‌شوند.

در شکل (۹) تابع پله‌ای (به رنگ قرمز)، نشان‌دهنده سختی استخراج است که با نرخ چکیده، نمودار با شیب ملایمی افزایش پیدا می‌کند. تغییر گام در تابع پله‌ای از این حقیقت ناشی می‌شود که سختی فقط با هر ۲۰۱۶ قالب تنظیم می‌شود [۲۱-۲۲].



شکل (۹): سختی استخراج در طول زمان (۲۰۱۸) [۲۰].

در شکل (۱۰) بیانگر این مفهوم است که زمان یافتن قالب جدید در دوره‌های مختلف در حال تغییر است. درواقع در هر ۲۰۱۶ قالب، سختی تغییر می‌کند و در طول این مدت میانگین زمان ایجاد قالب به ۱۰ دقیقه برمی‌گردد. در یک دور سختی تغییری نمی‌کند، اما تعداد استخراج‌کنندگان بیشتری برخط می‌شوند. درنتیجه قالب‌ها در این مدت زودتر پیدا می‌شوند (حدود دو هفته) تا اینکه سختی بعد از ۲۰۱۶ قالب، افزایش پیدا کند.



شکل (۱۰): زمان یافتن قالب جدید (۲۰۱۸) [۲۰].

۴-۴. چالش اجماع استخراج‌کنندگان

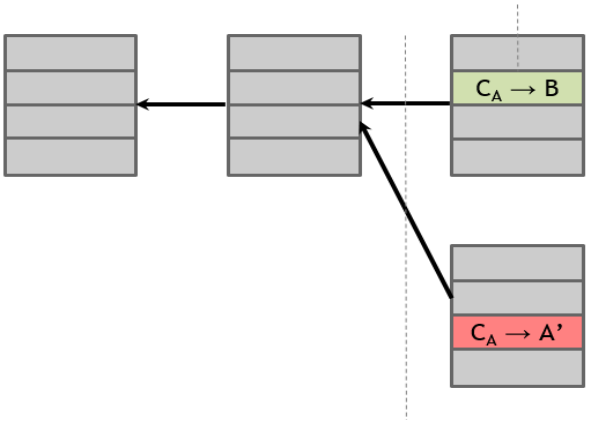
اگر ۵۱٪ توان محاسباتی متعلق به یک نفر شود این سؤال ایجاد می‌شود که چه چالش‌هایی در زنجیره می‌تواند ایجاد کند؟ موارد ذیل را می‌توان برشمرد [۲۳]:

- عدم دزدی بیت‌کوین از IDهای موجود: به دلیل نداشتن کلید خصوصی نمی‌تواند بیت‌کوین برداشت کند و فقط شخصی که کلید خصوصی دارد، می‌تواند از ID بیت‌کوین منتقل کند.
- اخلال در زنجیره: شخص می‌تواند با ایجاد قالب انحرافی و قالب‌سازی در ادامه‌ی آن، باعث شود زنجیره از شاخه انحرافی ادامه پیدا کند و مسیر اصلی از دور خارج شود.
- عدم اخلال در شبکه P2P: زیرا ۴۹٪ توان محاسباتی دیگر این تراکنش را بررسی می‌کنند، فقط تراکنش با تأخیر بیشتری انجام می‌شود.
- عدم تغییر مقدار BR: زیرا قوانین ثابت‌اند و کسی نمی‌تواند آن را تغییر دهد بلکه شبکه به‌صورت خودکار طبق قوانین اولیه‌ای که نوشته شده است به‌روزرسانی می‌شود.
- صدمه به اعتبار بیت‌کوین: با ایجاد شاخه انحرافی و حمله‌هایی که با قدرت محاسباتی بالا می‌تواند انجام دهد، امنیت بیت‌کوین را کاهش می‌دهد و درنتیجه آن، اعتبار بیت‌کوین کاهش می‌یابد.

۵. معرفی انواع حمله‌های ممکن به بیت‌کوین

۵-۱. حمله Double spending

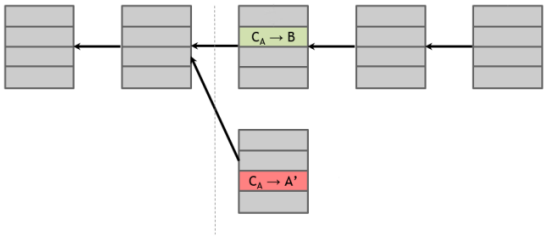
به این شکل است که آلیس هم‌زمان دو تراکنش ایجاد می‌کند که یکی از این تراکنش‌ها صحت ندارد. به‌طور مثال آلیس دو بیت‌کوین دارد و یک‌بار این دو بیت‌کوین را برای باب می‌فرستد و هم‌زمان در تراکنشی دیگر دو بیت‌کوین را به شخصی دیگر (که می‌تواند خودش باشد) ارسال کند.



شکل (۱۱): حمله Double spending ارسال هم‌زمان بیت‌کوین به دو حساب متفاوت [۱۵].

در این صورت اگر زنجیره دوم ادامه پیدا کند، درواقع تراکنش برای باب صورت نمی‌گیرد و باب دو بیت‌کوین را دریافت نمی‌کند. درواقع ارز دو بار خرج شده است. در شکل (۱۱) ارسال هم‌زمان بیت‌کوین را به دو شخص نشان می‌دهد.

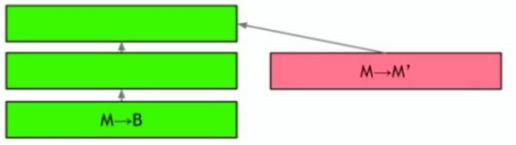
برای جلوگیری از این حمله باب بایستی صبر کند تا چند قالب به زنجیره تراکنشش اضافه شود تا مطمئن شود تراکنش به‌طور حتمی انجام گرفته است. مانند شکل (۱۲) که زنجیره تراکنش باب ادامه پیدا کرده است.



شکل (۱۲): حمله Double spending، جلوگیری از حمله spending Double با صبر کردن برای ادامه پیدا یافتن زنجیره اصلی [۱۵].

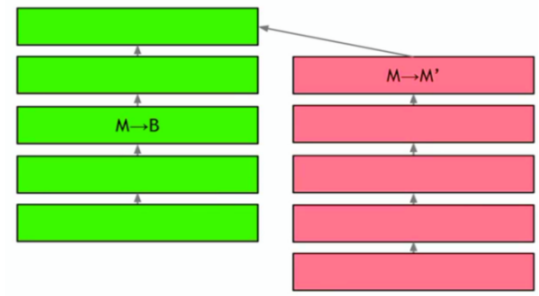
۵-۲. حمله Fork

مهاجم با انجام یک تراکنش جدید یک قالب جدید ایجاد می‌کند. شکل (۱۳)، نحوه ایجاد شاخه انحرافی را نشان می‌دهد.



شکل (۱۳): حمله **Fork** ایجاد شاخه انحرافی توسط مهاجم [۱۵].

همانند شکل (۱۴) طول این زنجیره را با توان محاسباتی بالایی که دارد افزایش می‌دهد تا جایی که طول آن از زنجیره اصلی بیشتر شود. در این صورت تراکنش‌های موجود در مسیر اصلی بی‌اعتبار می‌شوند و زنجیره از شاخه انحرافی ادامه پیدا می‌کند.



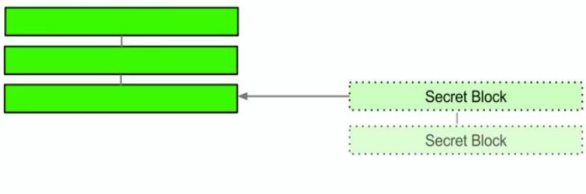
شکل (۱۴): حمله Fork، ادامه یافتن زنجیره انحرافی توسط مهاجم و بی‌اعتبار شدن تراکنش‌های زنجیره اصلی [۱۵].

این نوع حمله برای مهاجم به‌صورت مستقیم سود مالی ندارد ولی می‌تواند باعث کاهش اعتبار بیت‌کوین شود. همچنین حمله در زنجیره قابل تشخیص است.

این حمله با داشتن توان محاسباتی بالای ۵۰٪ امکان‌پذیر است. مهاجم در صورت نداشتن این مقدار از توان محاسباتی می‌تواند با رشوه دادن به‌طور مستقیم و یا غیرمستقیم به استخراج‌کنندگان، توان محاسباتی خود را به بالای ۵۰٪ برساند.

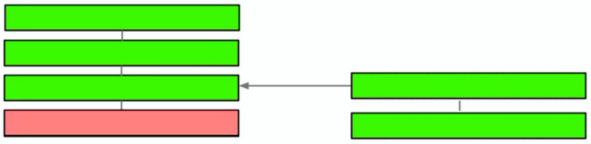
۵-۳. حمله Block with holding

این حمله بانام Selfish mining هم شناخته می‌شود. مهاجم ابتدا برای ساخت قالب جدید، مقدار nonce را می‌یابد ولی آن را اعلام نمی‌کند. سپس با فرض مقدار nonce ای که به‌دست آورده است، nonce قالب بعدی را به‌دست می‌آورد. این روند در شکل (۱۵) نشان داده شده است.



شکل (۱۵): حمله Block with holding. یافتن دو nonce بدون اعلام کردن آن [۱۵].

زمانی که استخراج‌کنندگان nonce یافته شده برای قالب جدید را اعلام می‌کنند، مهاجم دو مقدار nonce یافته‌اش را اعلام می‌کند و دو قالب ساخته می‌شود. همان‌طور که در شکل (۱۶) نشان داده شده، طول زنجیره مهاجم طولانی‌تر است و این زنجیره در سیستم ادامه پیدا می‌کند.



شکل (۱۶): حمله Block with holding. اعلام دو nonce که باعث ایجاد زنجیره طولانی‌تر می‌شود [۱۵].

درنتیجه این حمله وقت و انرژی استخراج‌کنندگان به هدر می‌رود. با این نوع حمله سازمان‌های بزرگ می‌توانند رقیب‌های کوچک و نوپا خود را از دور خارج کنند. البته در عمل، این حمله تاکنون رخ نداده است.

۶- بررسی گمنامی در بیت‌کوین (Anonymity)

در این بخش می‌خواهیم بدانیم که گمنامی دقیقاً به چه معناست و رابطه گمنامی با مباحثی مانند امنیت چیست.

۶-۱. تعریف گمنامی

گمنامی در لغت به معنای «بدون اسم» است. زمانی که این مفهوم را برای بیت‌کوین به کار می‌بریم، به دو معنا می‌توان آن را تفسیر نمود: تعامل بدون استفاده از اسم حقیقی، یا تعامل بدون استفاده از هیچ اسم حقیقی. در تفسیر دوم آدرس مورد استفاده، در علم کامپیوتر شناسه مستعار (Pseudonymity) نامیده می‌شود. به این طریق آدرس به‌عنوان ID را به هر مقدار می‌توان تولید کرد؛ اما همان‌طور که در ادامه بیان خواهد شد، شناسه مستعار باعث گمنامی بیت‌کوین نمی‌شود.

بیت‌کوین دارای ویژگی شناسه مستعار است، اما این ویژگی برای داشتن امنیت کافی نیست. همان‌طور که می‌دانیم هر فردی می‌تواند تراکنش‌های بیت‌کوین را مشاهده کند. حال اگر شخصی بتواند ارتباطی بین آدرس بیت‌کوین شما و هویت واقعیتان بیابد، تمام تراکنش‌های شما درگذشته، حال و آینده را مشاهده خواهد کرد. یافتن این ارتباط گاهی بسیار آسان است. به‌طور مثال شما از یک فروشگاه خرید می‌نمایید درحالی‌که در آن محل حضور فیزیکی دارید. درنتیجه مهاجم ارتباطی بین هویت شما با یکی از تراکنش‌هایی که همان زمان انجام شده است، می‌یابد.

در علم کامپیوتر گمنامی تواما شامل شناسه مستعار و توانایی عدم اتصال (Unlinkability) است. توانایی عدم اتصال بدین معناست که اگر کاربر با دستگاهی به‌طور مکرر در تعامل باشد، در بین این تعاملات متفاوت، مهاجم نتواند ارتباطی پیدا کند.

ویژگی‌های کلیدی توانایی عدم اتصال بیت‌کوین عبارت‌اند از:

- سخت بودن برقراری ارتباط بین آدرس‌های مختلف یک کاربر
- سخت بودن برقراری ارتباط بین تراکنش‌های مختلفی که یک کاربر انجام داده
- سخت بودن برقراری ارتباط بین فرستنده و گیرنده تراکنش

عملی ساختن دو ویژگی اول آسان است، ولی عملیاتی کردن ویژگی سوم سخت است. هر تراکنشی ورودی و خروجی دارد و این ورودی‌ها و خروجی‌ها در یک زنجیره قالبی قرار می‌گیرند و باهم در ارتباط‌اند. موضوعی که دارای اهمیت است این است که مطمئن شویم با مشاهده زنجیره قالبی که ورودی و خروجی‌های آن واضح‌اند، نتوان ارتباطی بین فرستنده و گیرنده یافت.

این سؤال وجود دارد که چرا به گمنامی نیاز داریم؟ می‌توان دو انگیزه مختلف برای رمزنگاری گمنامی تعریف نمود. انگیزه اول که رسیدن به سطح امنیتی در آن ساده است، هم‌اکنون در بانکداری سنتی در حال استفاده است. این روش خطر شناسایی

شدنی که بلاک‌چین به همراه می‌آورد را کاهش می‌دهد. در انگیزه دوم به سطح امنیتی بالاتری روی می‌آوریم و ارزها را گسترش می‌دهیم که ازنظر فناوری عضویت در آن برای هرکسی امکان‌پذیر باشد [۱۵].

دلایل زیادی برای استفاده از گمنامی وجود دارد. بیشتر مردم تمایلی ندارند که مقدار حقوق دریافتی‌شان را دوستان و همکارانشان بدانند. اگر در بلاک‌چین گمنامی وجود نداشته باشد و فرد حقوق خود را در بیت‌کوین دریافت کند، به‌راحتی دیگران می‌توانند مقدار حقوقش را بفهمند. اعم از مردم، سازمان‌ها هم نگرانی‌های امنیتی خود را دارند. برای مثال، تولیدکننده وسیله‌ای برای تهیه محصول جدیدش خریداری می‌نماید و رقبایش در زنجیره مشاهده می‌کنند که چه کسی چه کالایی خریداری کرده است. درواقع نوع محصول جدید را حدس می‌زنند که درنتیجه آن ایده تولیدکننده آشکار می‌شود.

بااین‌حال، نگرانی قابل قبولی در رمزنگاری گمنامی وجود دارد زیرا در آن پول‌شویی یا سایر فعالیت‌های غیرقانونی می‌تواند اتفاق بیافتد. البته درست است که در انجام تراکنش، گمنامی وجود دارد ولی در تبدیل ارز دیجیتال به ارز فیات این گمنامی وجود ندارد. در حقیقت این جریان قابل‌کنترل است؛ بنابراین، رمزنگاری برای پول‌شویی یا سایر جرائم مالی مزایایی ندارد.

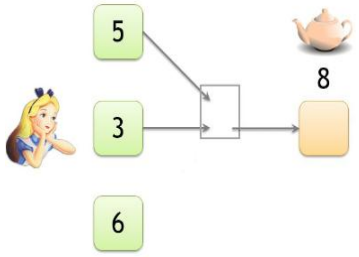
بااین‌وجود، ممکن است این سؤال مطرح شود که آیا نمی‌توان فناوری را به‌گونه‌ای طراحی کرد که به کاربردهای قانونی گمنامی مجوز دهد و در مقابل، کاربردهای غیرقانونی را ممنوع کند؟ متأسفانه عملیاتی کردن این موضوع غیرممکن است؛ زیرا مواردی را که ما به‌عنوان خوب و بد طبقه‌بندی می‌کنیم، ازنظر فناوری یکسان است. درواقع چگونگی به‌کارگیری استخراج‌کنندگان برای اتخاذ این نوع تصمیم‌ها روشن نیست.

از طرف دیگر معیار گمنامی و غیرمتمرکز بودن اغلب در تعارض با یکدیگرند. مثلاً اگر شبکه را غیرمتمرکز نماییم، باید نوعی سازوکار را برای ردیابی تراکنش‌ها و جلوگیری از Double Spending بیابیم. این ردیابی درواقع تهدیدی برای گمنامی به شمار می‌آید.

۶-۲. روش‌های نامعتبر کردن گمنامی

در این بخش مواردی که گمنامی بیت‌کوین را زیر سؤال می‌برد، بررسی می‌نماییم. درواقع مشاهده می‌نماییم که بیت‌کوین با داشتن ویژگی شناسه مستعار، دارای گمنامی نیست و می‌توان با یافتن رابطه تراکنش‌ها و آدرس‌ها، هویت‌های واقعی را شناسایی کرد.

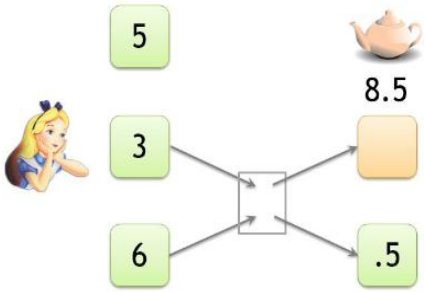
برای واضح‌تر شدن موضوع فرض کنید آلیس می‌خواهد ظرفی به قیمت ۸ بیت‌کوین خریداری کند. همچنین او دارای سه حساب با مقادیر ۳ و ۵ و ۶ بیت‌کوین که در شکل (۱۷) نشان داده شده است؛ یعنی در هیچ‌یک از حساب‌های خود ۸ بیت‌کوین ندارد و برای خرید ظرف بایستی از دو حساب برداشت کند. در این صورت دو خروجی از دو نود به یک نود وارد می‌شود. حال می‌بینیم که با این روند بعضی نکات آشکار می‌شود. به دلیل هم‌زمان بودن برداشت از دو حساب و ورود به یک نود، احتمال این‌که این دو حساب برای یک کاربر باشد، زیاد است. درواقع خرید مشترک نشان‌دهنده کنترل‌کننده مشترک آدرس‌های متفاوت است. هرچند امکان‌پذیر است که آلیس و هم‌اتاقی‌اش برای خرید قوری به‌طور هم‌زمان اقدام کنند؛ اما در کل احتمال رخداد این حالت کم است.



شکل (۱۷): پرداخت هزینه با آدرس‌های متفاوت که کنترل مشترک دارد [۱۵].

مهاجم می‌تواند این فرایند را بارها و بارها تکرار کند و کل تراکنش‌ها و آدرس‌های متعلق به یک نفر را بیابد.

حال فرض کنید قیمت قوری ۸/۵ بیت‌کوین باشد. در این صورت دارایی آلیس به‌گونه‌ای است که پس از خرید بایستی مقدار باقی‌مانده پول بازگرداننده شود. در این حالت باقی پول در حسابی جدید ذخیره می‌شود. شکل (۱۸) بیانگر همین موضوع است.



شکل (۱۸): پرداخت هزینه با ایجاد دو خروجی، یکی برای فروشنده و دیگری برای دریافت باقی‌مانده پول [۱۵].

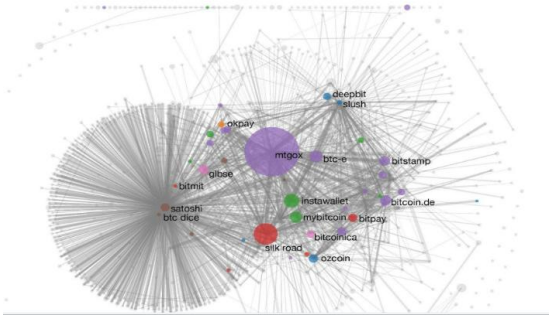
در این صورت دو خروجی داریم که مهاجم نمی‌داند کدام‌یک به آلیس تعلق دارد. با ایده این روش که مقدار پول باقی‌مانده (حتی مقدار صفر) در آدرس جدید ذخیره شود، می‌توان مشکل

مثال قبل را برطرف نمود. محققان برای استفاده از این ایده، نرم‌افزارهای کیف پولی را تولید کردند که هنگام نیاز به تغییر آدرس بتواند آدرس جدیدی تولید نماید. البته این روش هم مستعد خطا است که در ادامه این مشکل را بیشتر مورد بررسی قرار می‌دهیم.

۶-۲-۱. ارتباط دادن هویت‌های واقعی به خوشه‌ها

در شکل (۱۹) آدرس‌های بیت‌کوین به‌صورت خوشه‌ای دیده می‌شوند؛ اما این گراف دارای برچسب نیست، یعنی هنوز نمی‌دانیم خوشه‌ها چه هویت‌هایی دارند. شاید بر اساس آنچه در مورد اقتصاد بیت‌کوین می‌دانیم، بتوان حدس‌های حساب‌شده‌ای در مورد این خوشه‌ها زد.

در سال ۲۰۱۳، Mt. Gox بزرگ‌ترین تبدیلگر بیت‌کوین بود. درنتیجه می‌توان حدس زد که در شکل (۱۹) دایره بزرگ نشان‌دهنده آدرس Mt. Gox است. همچنین می‌توان فهمید دایره کوچک در سمت چپ باوجود حجم کم در بیت‌کوین، بیشترین تعداد تراکنش‌ها را دارد. این الگو نشان‌دهنده سرویس قمار Satoshi Dice است که یک بازی پرطرفدار است. به‌طورکلی این روش، روش عالی برای شناسایی خوشه‌ها نیست. این روش به آگاهی از اقتصاد بیت‌کوین و حدس زدن نیاز دارد و فقط برای سرویس‌های برجسته می‌توان از آن استفاده کرد.



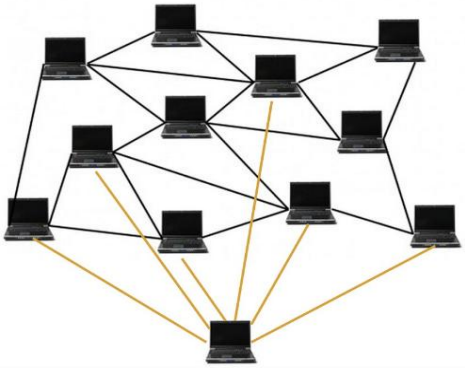
شکل (۱۹): شناسایی هویت واقعی نودها و برچسب خوشه‌ها [۱۵].

۶-۲-۲. شناسایی لایه شبکه

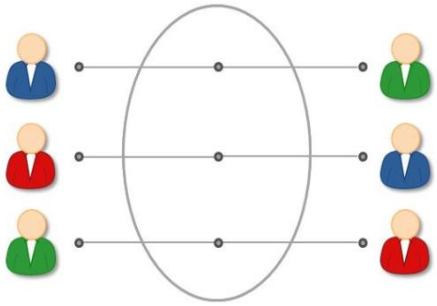
یک‌راه کاملاً متفاوت وجود دارد که کاربران می‌توانند بدون تکیه‌بر روش گراف تراکنش‌ها را شناسایی کنند. در اصطلاحات شبکه، بلاک‌چین، لایه کاربردی و شبکه P2P، لایه شبکه نامیده می‌شود. زمانی که نود یک تراکنش انجام می‌دهد، در وهله اول به تعداد زیادی نود متصل می‌شود و تراکنش به این شکل منتشر می‌شود (شکل ۲۰). از طریق تأخیر زمانی ارسال تراکنش به نودها، می‌توان اولین نود منتشرکننده تراکنش را یافت؛ زیرا اولین نود با کمترین تأخیر تراکنش را دریافته است و احتمالاً نودهای اطراف آن، نود ایجادکننده تراکنش است. در واقع مهاجم با به اجرا درآوردن مجموعه‌ای از نودها، نود اولیه را تشخیص می‌دهد. درنتیجه مهاجم می‌تواند تراکنش را به آدرس IP نود ارتباط دهد. درعین‌حال آدرس IP به هویت واقعی کاربر نزدیک است. روش‌های زیادی وجود دارد که از آدرس IP، هویت شخص آشکار می‌شود؛ بنابراین، شناسایی لایه شبکه از مشکلات جدی برای امنیت است.

۶-۳. مخلوط‌سازی (Mixing)

سازوکارهای متفاوتی وجود دارد که باعث می‌شود تحلیل گراف تراکنش، کمتر مؤثر واقع شود. یکی از این سازوکارها، مخلوط‌سازی است که به‌صورت گسترده در مقالات مورد بررسی قرار گرفته است [۲۶-۲۴]. این اصل متعلق به بیت‌کوین نیست و در موقعیت‌های دیگر که هدف گمنامی است، کاربرد دارد. مخلوط‌سازی با یک واسطه صورت می‌گیرد. در شکل (۲۱) گمنامی با کیف پول برخط، مشابه آنچه توسط سیستم بانکداری سنتی ارائه شده است. ماهیت بلاک‌چین به این‌گونه است که اگر چیزی در آن نادرست باشد (مثلاً کیف پول هک شود و یا سوابق در معرض عموم قرار گیرد) خطر امنیتی آن بدتر از دستگاه‌های سنتی است. علاوه‌بر این، بیشتر افرادی که به گمنامی بیت‌کوین روی می‌آورند، می‌خواهند که گمنامی به‌خوبی عمل کند؛ زیرا از ویژگی گمنامی در دستگاه‌های سنتی راضی نبودند و ضمانت بهتری در گمنامی می‌خواهند. همین موضوع، انگیزه روی‌آوری به سرویس‌های مخلوط‌سازی را بیان می‌کند.



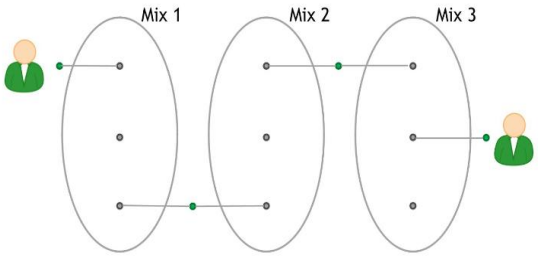
شکل (۲۰): شناسایی توسط Ip در سطح شبکه



شکل (۲۱): مخلوط‌سازی با ارسال سکه به‌واسطه [۱۵].

۶-۴. استفاده از مجموعه مخلوط‌سازی

به‌جای استفاده از یک مخلوط‌سازی تنها، از یک مجموعه مخلوط‌سازی، یکی پس از دیگری استفاده می‌شود. این‌یک اصل شناخته‌شده و معتبر است. به‌عنوان مثال در شکل (۲۲)، Tor از یک مجموعه متشکل از ۳ مسیریاب برای ارتباط گمنامی استفاده می‌کند. این روش حالت وابستگی اعتماد به هر مخلوط‌سازی را کاهش می‌دهد. انتظار می‌رود که در این روش هیچ‌کس قادر نباشد اولین ورودی‌تان را به خروجی نهایی دریافتی، مرتبط کند. این اتفاق تا زمانی رخ می‌دهد که مخلوط‌سازی‌ها در مجموعه به وعده‌های خود پایبند باشند.



شکل (۲۲): مجموعه مخلوط‌سازی‌ها [۱۵].

۶-۴-۱. مخلوط‌سازی در عمل

سرویس‌های مخلوط‌سازی زیادی وجود دارند، اما به دلیل مجموعه کوچکشان مخلوط‌سازی کمی انجام می‌دهند و درنتیجه گمنامی به حد کافی ایجاد نمی‌شود. بدتر از همه این است که گزارش سرقت بیت‌کوین از بسیاری از مخلوط‌سازی‌ها داده شده است. علاوه‌بر این، در صورت عدم وجود هزینه کافی برای ارائه بهتر خدمات تبلیغاتی، ممکن است اپراتورهای مخلوط‌سازی دچار وسوسه سرقت بیت‌کوین شوند و چرخه مخلوط‌سازی‌های غیرقابل اعتماد را ادامه دهند. با توجه به این رویکرد مخلوط‌سازی‌ها، بسیاری از مردم نمی‌خواهند از آن‌ها استفاده نمایند.

امروزه مخلوط‌سازی‌ها هیچ‌یک از اصول قراردادی را دنبال نمی‌کنند و هر مخلوط‌سازی به‌طور مستقل عمل می‌کند.

برای مخلوط‌سازی (نرم‌افزار کیف پول) نیاز است به مدلی روی آورد که به سمت دست‌یابی گمنامی قوی و مقاومت در برابر حملات هوشمندانه حرکت کند.

۶-۴-۲. مخلوط‌سازی غیرمتمرکز

مخلوط‌سازی غیرمتمرکز ایده‌ای است که از خدمات مخلوط‌سازی و از جاگذاری آن به‌جای پروتکل P2P رها می‌شود. به این شکل که توسط گروهی از کاربران سکه‌ها مخلوط می‌شوند. همان‌طور که می‌توان تصور کرد، این رویکرد بهتر با فلسفه بیت‌کوین هماهنگ می‌شود. زیرا دیگر نیاز به شخص سومی نیست.

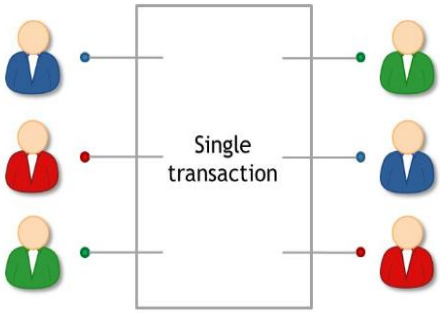
غیرمتمرکز کردن مزایای عملی زیادی دارد. مشکل bootstrapping را ندارد؛ کاربران مجبور نیستند منتظر به وجود آمدن مخلوط‌سازی‌های مرکزی قابل‌اعتماد باشند. مزیت دوم این است که سرقت از مخلوط‌سازی غیرمتمرکز غیرممکن است. درواقع پروتکل دریافت همان مقدار بیت‌کوین واردشده را تضمین می‌کند. درنهایت، در بعضی موارد مخلوط‌سازی غیرمتمرکز می‌تواند گمنامی را بهبود بخشد.

Coinjoin: پیشنهاد اصلی برای مخلوط‌سازی غیرمتمرکز، Coinjoin نامیده می‌شود. در این پروتکل کاربران متفاوت به‌طور مشترک تراکنش ایجاد می‌کنند که تمام ورودی‌های آن‌ها را ترکیب کند. این فرایند در شکل (۲۳) نشان داده شده است.

اصل کلیدی این روش برای گمنامی این‌گونه است: زمانی که تراکنش چندین ورودی از آدرس‌های مختلف دارد، همبستگی امضاهای آن‌ها با هر ورودی، جدا از هم و مستقل از یکدیگرند؛ بنابراین این آدرس‌های متفاوت را می‌توان توسط افراد مختلف کنترل کرد. در این حالت به یک بخش برای جمع‌آوری کلیدهای خصوصی نیازی نیست. به این طریق گروهی از کاربران اجازه دارند تا سکه‌های خود را با یک تراکنش مخلوط کنند. هر کاربر یک آدرس ورودی و خروجی ایجاد می‌کند و این دو باهم، یک تراکنش با این آدرس‌ها تشکیل می‌دهند. آدرس‌های ورودی و خروجی به‌صورت تصادفی است. درنتیجه مهاجم قادر به تشخیص ورودی و خروجی نیست.

کاربران آدرس خروجی‌شان را در تراکنش بررسی می‌کنند تا درج‌شده باشد و همان مقدار بیت‌کوین ارسالی در ورودی را دریافت کرده باشند (با کسر هزینه تراکنش T.F). پس از تائید، تراکنش امضا می‌شود.

کسی که به این تراکنش در زنجیره قالبی نگاه می‌کند (حتی اگر بداند این تراکنش Coinjoin است) قادر به تشخیص بین ورودی و خروجی نخواهد بود. از دیدگاه یک بیگانه سکه‌ها مخلوط شده‌اند که در واقع اصل Coinjoin همین است.



شکل (۲۳): تراکنش Coinjoin [۱۵].

مطلبی که تاکنون بیان کردیم، تنها برای یک دور از مخلوط‌سازی بود؛ اما اصولی که قبل از آن بحث کردیم، هنوز اعمال می‌شود. نیاز است که این فرایند با گروه‌های متفاوتی از کاربران تکرار شود. همچنین بایستی از تعداد و اندازه گروه در نظر گرفته شده، برای استانداردسازی اطمینان حاصل کرد.

جزئیات مراحل Coinjoin را می‌توان به ۵ مرحله تقسیم نمود:

۱) یافتن یک جفت کاربر که تقاضا مخلوط‌سازی دارد.
۲) تبادل آدرس ورودی/ خروجی
۳) ساخت تراکنش
۴) ارسال تراکنش به سایرین. هر طرف پس از تائید خروجی‌شان، امضا می‌نمایند.
۵) انتشار تراکنش

این روند باعث ساختارمند شدن مخلوط‌سازی می‌شود.

۷. نتیجه‌گیری

در این مقاله به معرفی اجمالی بیت‌کوین و ساختار آن پرداخته شد. سپس نحوه تولید قالب و استخراج که بر اساس معیار توان محاسباتی بالا عمل می‌کرد، توضیح داده شد. بعضی از حمله‌های ممکن به بیت‌کوین از لحاظ توان محاسباتی مهاجم و درصد عملیاتی شدن آن بررسی شد. چالش مهم دیگری که در این مقاله بررسی شد، گمنامی آدرس‌ها بود که برای عملیاتی شدن آن ایده‌ای مثل مخلوط‌سازی بیان شد. هرچند این ایده به‌تنهایی موجب متمرکز شدن بیت‌کوین می‌شد که درنتیجه آن ویژگی مهم بیت‌کوین، یعنی غیرمتمرکز بودنش زیر سؤال می‌رفت. برای حل این مشکل از مخلوط‌سازی غیرمتمرکز استفاده شد که با فلسفه بیت‌کوین بیشتر هماهنگ بود.

۸. مراجع

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Oct. 2008.

[2] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” in IEEE Symposium on Security and Privacy, 2013.

[3] E. B. Sasson , A. Chiesa , C. Garman, M. Green, I. Miers , E. Tromer, and M. Virza, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” in Symposium on Security and Privacy, 2014.

[4] N. Van Saberhagen, “CryptoNote v. 2.0,” [Online]. Available: https://cryptonote.org/whitepaper.pdf.

[5] “CNBC Analysis of Coindesk Data,” [Online]. https://www.cnbc.com/2017/10/13/these-charts-show-how-quickly-bitcoin-is-growing.html

[6] A. Antonopoulos, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies,” O'Reilly, 2015.

[7] J. Bonneau, A. Miller , J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” in IEEE Symposium on Security and Privacy, 2015.

[8] M. Moser and R. Bohme, “Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees,” in International Workshops Financial Cryptography and Data Security, 2015.

[9] T. Moore and N. Christin, “Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk,” in 17th International Conference Financial Cryptography and Data Security, 2013.

[10] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder,“Bitcoin and Cryptocurrency Technologies,” Princeton University Press, Feb. 2016.

[11] M. Rosenfeld, “Analysis of Bitcoin Pooled Mining Reward Systems,” arXiv, 2011.

[12] A. Back, “Hashcash - A Denial of Service Counter-Measure,” 2002. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf.

[13] M. B. Taylor, “Bitcoin and the Age of Bespoke Silicon,” in International Conference on Compilers, Architectures and Synthesis for Embedded Systems, 2013.

[14] A. Kampl, “Analysis of Large-Scale Bitcoin Mining Operations,” White paper, 2014.

[15] “bitcoin wisdom,” [Online]. https://bitcoinwisdom.com/

[16] J. Kroll, I. C. Davey, and E. W. Felten, “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,” in Workshop on the Economics of Information Security 2013, 2013.

[17] I. Eyal, “The Miner’s Dilemma,” in Symposium on Security and Privacy, 2015.

[18] I. Eyal and M. G. Esirer, “Majority Is Not Enough: Bitcoin Mining Is Vulnerable,” in 18th International Conference Financial Cryptography and Data Security, 2014.

[19] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of Bitcoins: characterizing payments among men with no names,” Commun. {ACM}, vol. 59, no. 4, pp. 86-93, 2016.

[20] J. Bonneau, A. Narayanan, A. Miller, J. Clark , J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for Bitcoin with Accountable Mixes,” in 18th International Conference Financial Cryptography and Data Security, 2014.

[21] M. Malte, R. Böhme, and D. Breuker, “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem,” in eCrime Researchers Summit, 2013.

Introducing Bitcoin and its Security Challenges

F. Azizi, H. Soleimany*

Abstract

The growing trend in data and transactions in the world implies the need for fast high-security systems. For this reason, digital exchange has attracted the attention of researchers over the past few years. The Bitcoin is the first digital currency to be offered and operates on the block chain. The demand for using Bitcoin is now high due to the special features of digital currencies. Specifically, the most important feature of these currencies, and in particular the Bitcoin is decentralization, which does not require a trustworthy intermediary for security matters. In this paper, while introducing Bitcoins and the mechanisms for producing this digital currency, we will examine its security against attacks. Specifically, this article examines challenges such as attack and anonymity in Bitcoin. Understanding the challenges and characteristics of digital currencies especially Bitcoin, can help us understand the challenges and opportunities ahead in this area. Using Bitcoin is surprisingly increasing in our country, and because in case of any threats or attacks, this could potentially cause severe weakness in some parts of country's economy, studies such as the present research appear indispensable in the field of passive defense.

Key Words: *Bitcoin, Cryptocurrency, Block Chain,Anonymity*

* Shahid Beheshti University (h_soleimany@sbu.ac.ir)- Writer-in-Charge