هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲و۳ بهمن ۱۳۹۶
7th Annual Conference
on Electronic Banking
and Payment Systems

آسیب شناسی بلاک‌چین

سید جواد کاظمی‌تبار، شرکت داده‌کاوان هوشمند توسن، jkazemitabar@tosanidm.com
استادیار دانشگاه صنعتی نوشیروانی بابل ، j.kazemitabar@nit.ac.ir

چکیده (فارسی)

بلاک چین یا زنجیره بلوکی، یک فهرست گسترش یابنده از اقلام است که آن را بلاک یا زنجیره می‌نامیم. این زنجیره‌ها توسط روشهای رمزنگاری تامین امنیت می‌شوند. بلاک چین‌ها را می‌توان به صورت دفتر کّل غیر متمرکز و در برخی موارد باز در نظر گرفت که می‌توانند تراکنش‌های بین دو نفر را به صورت کارا و قابل راست آزمایی و دائمی ثبت کنند. بلاک چین‌ها معمولا امن هستند و مقاومت خوبی نسبت به خطا از خود نشان می‌دهند. خاصیت غیر متمرکز بلاک چین‌ها آنها را علاوه بر تراکنش‌های مالی برای ثبت انواع وقایع همچون سوابق پزشکی نیز مناسب می‌کند. ولی از آنجایی که در سامانه همتا به همتا نظر اکثریت تعیین کننده خواهد بود با وجود همه فواید بلاک چین، به دلیل طبیعت این سامانه، امکان تخلف وجود دارد. در این مقاله به برخی از آسیب‌های ممکن و راه‌های مقاوم سازی آن در بلاک چین‌ها می‌پردازیم .

واژگان کلیدی : بلاک چین، تبانی اکثریت، شبکه همتا به همتا، دفترکل، بیت کوین

Blockchain is a continually growing list of items. The security of blocks is provided using cryptographic methods, such as hashes. Blockchain can be described as a non-centralized ledger that records transactions between two parties. These transactions can be verified and are permanently recorded. If designed correctly, blockchains are secure and resilient to errors. The peer-to-peer nature of blockchains makes them suitable not only for financial transactions, but also recording many different types of events, such as medical records. However, since the majority vote is a deciding factor in non-centralized systems, blockchains are vulnerable to some attacks if not designed or used without due care and attention

Blockchain, majority collusion, peer-to-peer network, general ledger, bitcoin

امروزه در دنیا بانکها و تامین کنندگان تکنولوژی در بخش خصوصی در سطوح تجاری بلاک چین سرمایه گذاری می‌کنند. این مساله که بانکها در سطح دنیا به چنین کاری مشغول هستند نشانه بارزی از وجود نتایج امیدوارکننده در این صنعت است. سوال، دیگر این نیست که این تلاشها آیا به تولید انبوه خواهند رسید یا خیر. بلکه سوال در مورد زمان وقوع این پیشامد است.

به همین دلیل الان زمان خوبی برای در نظر گرفتن این مساله است که بلاک چین و ارز رمز پایه (cryptocurrency) از نظر فساد مالی چگونه خواهد بود. چه مخاطراتی از سوی نقدینگی دیجیتالی ما را تهدید می‌کند و چگونه می‌توان آن را مهار کرد؟ ابزارها و تکنیکهایی که به مدیریت جلوگیری در فساد و جرایم مالی در دنیای جدید کمک می‌کند چه چیزهایی هستند؟

این نوشته با ارزیابی نرخ پذیرش بلاک چین و ارزهای رمز پایه توسط بانکها و بنگاههای تجاری شروع می‌شود. سپس تاثیرات فناوری دفاتر کل غیر متمرکز برروی فساد و جرایم مالی بررسی می‌شوند. این مقاله با بحث در مورد اهمیت ابزارهای مدرن مبارزه با فساد مالی همچون یادگیری ماشین و تحلیل رفتاری به پایان می‌رسد.

فناوری دفتر کل نامتمرکز

دورنمای دفتر کل نامتمرکز از زمانی که بلاک‌چین بیت‌کوین در سال ۲۰۰۹ پا به عرصه گذاشت بسیار تغییر کرده است. از آن زمان تا کنون، هیجان ناشی از ارزهای رمزپایه و بلاک‌چینهای عمومی کمی کمتر شده است، همچنانکه سروصدای بلاک‌چینهای سازمانی و خصوصی بیشتر شده. برخلاف بلاک‌چینهای عمومی، امور بانکی و تجاری نیاز به بلاک‌چینهای خصوصی دارد که مشارکت‌کننده‌های آن باید به طور انتخابی دست‌چین و یا دعوت شوند.

دفاتر کل به اشتراک گذاشته شده

ویژگیهای دفتر کل به اشتراک گذاشته شده (که اغلب آن را دفتر کل غیر متمرکز می‌نامند) به یک سامانه بسیار امن منتهی می‌شود که آن را منبع طلایی می‌نامند. این سامانه هیچ واسط یا نقطه تکی شکست(single point of failure) ندارد. برای خدمت رسانی به بانکها و بنگاهها، بلاک‌چین عمومی نیاز به تغییراتی دارد. اولا، نمی‌تواند عمومی و بدون مجوز باشد. بلکه آنها باید دست‌چین شده باشند. دوم این است که مشارکت‌کنندگان باید بر روی یک ساختار مدیریتی که مشتمل بر مسولیت کاربران است توافق کنند. سوم آنکه دفاتر مختلف باید با یکدیگر سازگاری داشته باشند و از مدلهای دیگر کم هزینه تر باشند.

امنیت و راست آزمایی داده ها

ساتوشی ناکاموتو (Satoshi Nakamoto)، یک برنامه نویس ناشناس، مفهوم بلاک چین را در سال ۲۰۰۸ معرفی کرد. در این سامانه تراکنش ها، و دارائی‌های افراد در بلاک‌های به هم پیوسته‌ای با ترتیب زمانی ذخیره می‌شوند. بلاک‌ها بوسیله یک فرایند اجماع که در بیت‌کوین به آن "اثباتِ انجام کار" (proof of work) می‌گویند راست آزمایی می‌شوند. امنیت در این روش با استفاده از یک کلید عمومی و خصوصی تامین می‌شود. فایده این کار این است که یکپارچگی داده حفظ می‌شود، هزینه نگهداری دفاتر پایین می‌آید و به علاوه داده‌ها قابل رهگیری هستند. با وجود اینکه فرایند "اثبات انجام کار" بسیار ساز و کار ظریفی است، انرژی و توان محاسباتی گرانی می‌طلبد. به عنوان مثل برای بلاک چین بیت‌کوین تا ۱۰ دقیقه ممکن است

طول بکشد. بدیهی است بلاک چین‌های سازمانی نیازمند سرعت و مقیاس پذیری بالا هستند. بنابرین سعی می‌شود بلاک چین‌های سازمانی با ساز و کار اجماع متفاوتی برای اثبات انجام کار ساخته شوند. به علاوه اشتراک گذاری داده به شکل محدودتری انجام می‌شود تا سرعت پردازش را بالا ببرد و در مقیاس‌های بزرگتری قابل استفاده باشد. به علاوه سازمانها نیازمند گزینه‌ای برای تامین محرمانگی تراکنش‌ها هستند (مثلا بانکها یا سازمانهای رقیب نباید بتوانند برخی جزئیات تراکنش‌ها را ببینند). ضمنا خاصیت تغییر ناپذیری رکوردها در بلاک چین برای برخی موارد استفاده، مشکلاتی به وجود آورده است. مثلا اینکه گاهی نیاز است یک رکورد اشتباه تصحیح شود. البته راه حلی که پیشنهاد می‌شود ایجاد یک ترکنش جدید با مقدار صحیح است.

دارائی‌های دیجیتال

بلاک چین می‌تواند با انواع اقلام ترکیب شود. مثلا نقدینگی رمز پایه، دارائی، هویت، و یا قرارداد. نقدینگی‌های رمز پایه مهمترین دارائی‌های دیجیتال هستند ولی قراردادهای هوشمند به سرعت در حال گسترش می‌باشند. به عنوان مثل اتریوم (Etherium از انواع نقدینگی‌های رمز پایه) دارای چنین قابلیتی است. معمولا به اتریوم عنوان بلاک چین نسخه دو و به بیت کوین بلاک چین نسخه یک اطلاق می‌شود .

بلاکچین برای بانکها و موسسات تجاری

سوال اساسی ۱: بانکها و موسسات تجاری چگونه با دفتر کّل غیر متمرکز برخورد می‌کنند؟ بانکها در سه ناحیه پیشقدم شده‌اند:

الف) پرداخت‌های فرامرزی

ب) مبادلات تجاری

ج) شناخت مشتری و مبارزه با پول شویی

تقریبا یک دهه از زمانی که مقاله ساتوشی منتشر شده می‌گذارد. این مفهوم انقلابی برای نفوذ به مصارف تجاری نیازمند زمان است. اگرچه ما در مرحله تجاری سازی بلاک چین در بانکداری و تجارت نرسیده ایم، ولی قطعاً در مرحله کارهای سخت آن هستیم. احتمالا در یک دهه شاهد استفاده از بانکهای مرکزی کشورها از بلاک چین و نسخه دیجیتال پول خواهیم بود.

پذیرش بلاک چین‌های تجاری

اثبات انجام کار. پس از هیجان اوایل دهه ۲۰۱۰، برخی از افراد آینده نگر در حوزه فناوری پتانسیل‌های این مساله که بلاک چین را از بیت‌کوین جدا کنند دریافتند و تصمیم به ساخت بلاک چین‌های تجاری گرفتند. اولین کسانی که در این راه قدم نهادند از بلاک چین‌ها برای بهبود گردش کار (workflow) و انتقال مالکیّت یا مبلغ استفاده کردند. در سال ۲۰۱۵ بیش از ۸۰ بانک در سراسر جهان چندین شرکت نوپا و کنسرسیوم، در حال کاوش درباره کاربردهای بلاک چین بودند و یا روی

استانداردهای لازم برای بلاک چین‌های تجاری کار می‌کردند. نیازهای خاص بانکها باعث شد بسترهای آماده‌ای مخصوص به آنها ساخته شود از قبیل کنسرسیوم بانکی Ripple, Chain, R3 و Quorum که توسط JPMorgan ساخته شده است.

در سه سال اخیر ۱۵۰ بلاک چین توسط بانکها و شرکایشان تست و ارزیابی شده است. چند شرکت با همکاری پیمانکاران بانکی در حال ساخت نرم افزارهای مبتنی بر بلاک چین هستند. کنسرسیوم‌های بانکی تشکیل شده اند تا استانداردهای متن باز (open source) را ترویج کنند. ورود شرکتهایی همچون، مایکروسافت، آی بی ام، سپ، و اوراکل به حوزه "بلاک چین به عنوان سرویس"(blockchain as a service)، سیگنال قدرتمندی ارسال می‌کند که بلاک چین کم کم به محصول نهایی تبدیل خواهد شد.

نرم افزارها هنوز در حال بالغ شدن هستند و به پایداری بالاتری می‌رسند. بانک‌ها هنوز در حال متصل کردن بلاک چین‌ها به سامانه‌های سنتی هستند که البته به این زودی‌ها جای خود را به بلاک چین نخواهند داد.

به گفته سرشماری اقتصادی آکسفورد (ژوئن ۲۰۱۷) بلاک چین در رتبه دهم فناوریهای بسیار مهم در نظر مدیران مالی قرار می‌گیرد (رتبه اول و دوم به ترتیب از آن برنامه ریزی منابع سازمانی و رایانش ابری است). از میان شرکت‌های پیش قراول در زمینه مالی ۲۰ درصد بلاک چین را در رده بسیار مهم قرار دادند.

پیش بینی برای دو سال آینده. در دو سال آینده شاهد آن خواهیم بود که موارد مصرف خاصی همچون پرداختها برای بلاک چین ظهور خواهند کرد و برخی شرکتها برای دفتر حساب داخلی خود این فناوری را به کار خواهند برد. احتمالا شرکتهایی به این کار دست خواهند زد که مبتنی بر پیمانکاران مستقل و فریلنسرها هستند و پرداخت‌های پیچیده‌ای به پیمانکاران خود را باید مدیریت کنند. ولی تعداد آن دسته از شرکتهایی که محصول مبتنی بر بلاک چین خواهند داشت محدود خواهد بود. در واقع مانع اصلی بلاک چین‌های تجاری وجود استاندارد پیاده سازی، تعامل، ساختار کارامد مدیریت و دستیابی به شبکه‌ای موثر می‌باشد. در دو سال آینده، جزایر بلاک چین فراوانی تولید خواهد شد که تعداد زیادی از آنها شرکای مشترکی دارند و گسترش نمی‌یابند. معدود مسیرهای موفق به سوی تعامل در زمینه بلاک چین شامل بانکها و موسسات شخص ثالثی خواهد بود که به دنبال توسعه پروتکل‌هایی (همچون Interledger Protocol) وای پی آی‌ها(API) هستند که بلاک چین را یا با همدیگر و یا با سیستمهای سنتی فعلی متصل می‌کنند (همچونCitiConnect for Blockchain)

مورد استفاده از بلاک چین

موارد استفاده از بلاک چین شامل انتقال املاک، تسویه وجوه(clearing)، حّل و فصل‌های مالی(settlement)، ثبت اطلاعات و قراردادها هستند. این سوال ممکن است پیش بیاید که چگونه این موارد استفاده به صنعت بانکی مربوط خواهند شد. برای پاسخ به این سوال می‌توان دو طبقه بندی کلی ارزش و پیچیدگی را در نظر گرفت. در طبقه بندی ارزش(سود) هرچه یک فرایند کندتر، گران تر و پر خطا تر و مبهم تر باشد و با چالشهای اعتماد و امنیت مواجه باشد، احتمال آنکه بلاک چین بتواند راه حال بهتری برای آن باشد بیشتر است. در طبقه بندی پیچیدگی، عواملی که باید در نظر بگیریم شامل تعداد مشارکت کنندگان، فرایندها و سامانه‌های آی تی است؛ هر چه این تعداد بیشتر باشد، چالش اجرایی بیشتری پیدا می‌شود، و هزینه استفاده از آن افزایش می‌یابد .
وقتی این چارچوب را بر روی بانکداری و تجارت عمل کنیم، موارد استفاده زیر به ذهن متبادر خواهند شد: پرداخت‌های

بین‌المللی، زنجیره تامین، شناسایی مشتری و مبارزه با پولشویی. برای تراکنش‌های مالی یک بنگاه یک مورد مصرف متمایز می‌شود: دفاتر حساب داخلی برای مدیریت کردن پرداخت‌های پیچیده . بانکها بیشتر تلاش و انرژی خود را بر روی پرداختهای بین‌المللی قرار داده اند. تعدادی از آنها نیز در مورد استفاده از نقدینگی‌های رمز پایه کاوش می‌کنند .

دورنمای نقدینگی‌های رمز پایه

پایه‌های اصلی پرداخت امروزه سامانه‌های حساب محور هستند. درخواست‌ها توسط واسطه‌هایی به حسابها منتقل می‌شوند و در دفاتر حساب جداگانه‌ای در بانک‌های مبدا و مقصد ثبت می‌شوند. پیغام‌ها و مبالغ در دو کانال مختلف مدیریت می‌شوند. حسابهای جداگانه نسترو (Nostro) و وسترو(Vostro) از قبل شارژ شده‌ای نیاز است که کار تسویه حساب وجوح را ترتیب دهند. استفاده از نقدینگی‌های رمز پایه (مثلا در پرداخت‌های بین‌المللی از دلار به نقدینگی رمز پایه و بعد به یورو) به ترکیبی از فرایندهای پیغام رسانی، تسویه وجوح و حل و فصل نیازمند است. به گفته یکی از تامین کننده‌گان بسترهای بلاک چین اگر بانکها برای پرداخت‌های کم مبلغ بین‌المللی خود در کنار بلاک چین از نقدینگی‌های رمز پایه نیز استفاده کند میزان صرفه جویی خود را دو برابر خواهند کرد .

تا امروز تجربیات اندکی در استفاده از نقدینگی‌های رمز پای توسط بانکها و بنگاه‌های تجاری گزارش شده است. در واقع استفاده غیر موجّه از بیت کوین تابویی ساخته است که به دیگر نقدینگی‌ها نیز سرایت کرده. به علاوه شناورترین نقدینگی رمزپایه یعنی بیت‌کوین هنوز نسبت به نقدینگی‌های معمولی (پول کاغذی) شناوری لازم را ندارد. قوانین نامشخص را هم به این مشکلات اضافه کنید .

صرفه اقتصادی و کارایی بالقوه نقدینگی‌های رمز پایه آن قدر هستند که نمی‌توان آنها را ندیده گرفت .استفاده از نقدینگی‌های رمز پایه نیاز به واسطه‌های سنتی را از بین می‌برند (مثلا حساب‌های نیابتی، شرکت‌های انتقال پول، و سامانه‌های انتقال پیغام مانند سوئیفت). اندکی از بانکهای آینده نگر، در تلاشند تا به مشتریان خود این قابلیت را بدهند تا به نقدینگی‌های رمز پایه دسترسی پیدا کنند. به عنوان مثال، بانک سانتاندر(Santander) با مجموعه اتر کمپ(ether.camp) در زمینه سرویسی که به مشتریان این بانک قابلیت تبدیل پول واقعی به اتریوم را بدهد کار می‌کند. در یک دهه آینده، انتظار می‌رود که بانکهای مرکزی قابلیت توکن کردن(tokenization) پول واقعی را داشته باشند. (یعنی یک روش برای نمایش مبتنی بر بلاک چین از پول واقعی)

با گسترش بلاک چین بانکهای جهانی تنها ذی نفعان این فناوری نخواهند بود.

پسایندهای تقلب و مدیریت جرائم مالی

پسایندهای تقلب و جرائم مالی ناشی از دفاتر غیر متمرکز چه چیزهایی هستند؟

نقدینگی‌های رمز پایه و شبکه‌های باز مخاطرات زیادی را برای کاربران و تامین کنندگان بستر چنین شبکه‌هایی را به بار می‌آوردند. در مقابل محصولات تجاری (خصوصی) مبتنی بر بلاک چین می‌توانند به بانکها و بنگاه‌های تجاری فایده برسانند و ریسک تقلب را کاهش دهند.

هیچ بحثی در مورد اینکه گسترش بلاک چین‌های عمومی و پذیرش آنها توسط بانک‌ها و بنگاه‌های تجاری در تقلب و جرائم مالی موثر خواهند بود وجود ندارد. با اینکه در این مرحله هنوز پیش بینی دقیق این تاثیرات آسان نیست، ولی اتفاقاتی که تا حالا افتاده نشانه‌هایی از نوع تقلبها و جرایمی که ممکن است به وجود بیایند را به دست می‌دهد.

اول اینکه باید بین نقدینگی‌های رمز پایه و بلاک چین‌های عمومی با پیشقدمان صنعتی و بلاک چین‌های (خصوصی) تجاری تمایز قائل شد. مخاطراتی که از نقدینگی‌های رمز پایه ناشی می‌شوند تا اندازه خوبی قابل فهم هستند. کما اینکه در تقلب‌ها و نفوذهای امنیتی که منجر به از دست رفتن بیت کوین و نقدینگی‌های رمز پایه دیگر شده است این امر بر همگان هویدا شده است.

باید توجه داشت که تعداد کمی از پیاده سازی‌های تجاری بلاک چین از فاز امکان سنجی فراتر رفته اند. در نتیجه سخت خواهند بود تا قابلیت امکان کاهش تقلب و مخاطرات تقلب‌های جدید یا نفوذهای امنیتی را اندازه گیری کرد. اگرچه تاثیر اصلی بلاک چین تجاری در کارایی خواهند بود، ولی باور بر این است که بلاک چین باعث کاهش تقلب در بانکداری و تجارت نیز خواهند شد. البته میزان تاثیر به مورد مصرف بستگی خواهند داشت. ولی ما انتظار نداریم بلاک چین تقلب و جرائم مالی بالکل از بین ببرد.

نقدینگی‌های رمز پایه و بلاک چین‌های عمومی: استعداد مخاطره

نقدینگی‌های رمز پایه پتانسیل بالایی برای کاهش هزینه‌های پرداخت خواهند داشت. با این حال، در حال حاضر این نقدینگی‌ها در معرض استفاده‌های نامناسب ، تقلب و نفوذهای امنیتی هستند. تا زمانی که این مشکلات امنیتی برطرف نشوند، بانک‌ها و بنگاه‌های قانونی تجاری در استفاده از آنها مردّد خواهند بود.

در سال ۲۰۱۴ رگولاتوری بانکی اروپا (European Banking Authority) نوشته‌ای را با عنوان نقدینگی مجازی منتشر کرد که شامل تحلیل دقیقی از مخاطرات ناشی از نقدینگی‌های رمز پایه بود. مقاله مزبور حدود ۷۰ مخاطره را شناسایی کرد که بر اساس اینکه چه کسی در معرض ریسک قرار دارد، طبقه بندی کرد (از قبیل کاربران، دیگر مشارکت کنندگان بازار، یکپارچگی مالی، سامانه پول کاغذی، و رگولاتور ها). مخاطرات شناسایی شده شامل کاربرانی است که وقتی تراکنش هک شده یا متقلبانه انجام می‌گیرد متضرّر می‌شوند. یا کاربرانی که هویت آنها در حین تراکنش دزدیده می‌شود، و نیز مجرمانی که می‌توانند درآمدهای ناشی از کارهای مجرمانه خود را به دلیل بی نام بودن این تراکنش‌ها به سرعت و در مقیاس بین‌المللی پولشویی کنند.

می توان یک جور دیگر هم به مخاطرات نقدینگی‌های رمز پایه نگاه کرد؛ اینکه منشأ آسیب پذیری کجاست. یعنی تقلب و نفوذهای امنیتی از کجا نشأت می‌گیرند. آیا در سطح کاربر است؟ یا مثلا کیف پولهای دیجیتال و مشکل صرافی‌های آنلاین هستند؟ اگر بفهمیم که چه کسی در معرض آسیب پذیری قرار دارد می‌توان نسبت به آن مقاوم شد.

متاسفانه مخاطرات بسیار زیادی به تحقق پیوسته اند. باعث تعجّب نیست اگر بیشترین آسیب پذیری‌ها در سطح کاربر و نیز بستر فعالیت هستند. در مقابل شبکه بیت کوین ثابت کرده که به خودی خود امن و مقاوم است. و در نتیجه بیشتر مخاطرات در سطح شبکه هنوز مجال بروز نداشته اند. جدول ۱، مخاطرات و تقلب‌های جرائم مالی را که از طرف نقدینگی‌های رمز پایه ایجاد می‌شوند را با جزئیات بیشتری توضیح می‌دهد.

جدول ۱: مثالهای تقلب و جرائم مالی مربوط به نقدینگی‌های رمز پایه

منشأ آسیب پذیری	تقلب/جرم مالی	توضیحات و شواهد
کاربران	فیشینگ و لو رفتن ایمیل‌های شرکتی	فیشینگ معمولان یک ایمیل است که از کاربران می‌خواهد به کیف پول بیت کوین خود لاگین کنند. این ایمیل‌ها از کاربر می‌خواهند عملیات لاگین طریق آدرسی که مدعی برنده شدن یا ارایه تخفیف است انجام شود. و این نقطه‌ای است که هکرها کنترل حساب را به دست می‌گیرند یک راه مشابه زمانی است که ایمیل شرکتی لو می‌رود. در این گونه موارد مشتری امیلی دریافت می‌کند که شبیه شرکتی است که او با آن تعامل داشته است و اددعا می‌کند اگر از طریق بیت‌کوین پرداخت را انجام دهد مشمول تخفیف خواهد شد. با این کار مشتری فریب می‌خورد و پول را به حساب شخص متقلب می‌ریزد. در ژوئن ۲۰۱۷ مردی در دادگاه به دزدیدن تعدادی بیت‌کوین به مبلغ معادل ۳۶۵،۰۰۰ دلار اعتراف کرد. او این کار را با عملیات فیشینگ انجام و با ساختن وبسایت‌هایی که شبیه بازارهای سیاه معروف بودند انجام داد[۱]
	اخاذی	یک حمله سایبری بزرگ بر روی سازمانهای سراسر دنیا در ۲۰۱۷ انجام شد. باج افزاری به نام واناکرای کامپیوترهای آلوده را با رمز کردن فایل‌ها قفل کرد و تقاضای مبلغی معادل ۳۰۰ دلار به صورت بیت‌کوین نمود تا کامپیوتر را از قفل درآورد. [۲]
	تقلب در لوای عرضه اولیه سکّه	برخی شرکت‌های نوپا در زمینه نقدینگی‌های رمز پایه، با پیش فروش نقدینگی‌هایی که می‌خواهند به بازار عرضه کنند کار خود را آغاز می‌نمایند. به این فرایند عرضه اولیه سکّه می‌گویند. پلتفرم کوین دش به تازگی به وسیله یک متقلب هک شد که آدرس یک کیف پول اتریوم را در جریان عرضه اولیه سکّه شرکت تغییر داده بود. [۳]
	پول شویی	یک مرد روسی که در آمریکا به ظن طراحی یک عملیات پولشویی به مبلغ حداقل ۴ میلیارد دلار از طریق بیت کوین تحت تعقیب است، در جولای ۲۰۱۷ در یونان دستگیر شد [۴]
	فروش غیر قانونی/کالاهای تقلبی	بیت کوین تبدیل به یک سازو کار پرداخت پر طرفدار در بازارهای سیاه شده است که اغلب شامل کالاهای غیر قانونی می‌شود. در سال ۲۰۱۵، اف بی آی، یک کلاه بردار را تفهیم اتهام کرد که برگه تخفیف‌های تقلبی را در سیلک رود می‌فروخت. در نتیجه کارهای این کلاهبردار، برخی شرکت‌ها تا ۱ میلیون دلار متضرّر شدند [۵]

	عملیات نابهنجار	یک مامور مخفی سابق آمریکا به دزدیدن بیت‌کوین به مبلغ ۸۰۰،۰۰۰ دلار در جریان بازرسی پرونده داروخانه آنلاین سیلک رود اعتراف کرد [۶] باترفلای لبز، که یک شرکت استخراج بیت کوین بود توسط کمیسیون تجارت فدرال آمریکا تعطیل شد. چون ده‌ها هزار کامپیوتر سفارش داده شده را تحویل مشتریان نداد و یا برخی دیگر از ادوات سفارش داده شده را وقتی تحویل داد که دیگر مصرف نداشتند. (سخت افزارهای سریعتر به بازار آمده بودند)[۷]
بستر	هک بازار مبادلات	یکی از بزرگترین بازارهای مبادلات بیت‌کوین با نام مونت گاکس که در توکیو قرار داشت در سال ۲۰۱۵ بسته شد. آنها اعتراف کردند که ۸۵۰،۰۰۰ بیت‌کوین معادل ۴۸۰ میلیون دلار در آن زمان از کیف پول‌های دیجیتال آنها ناپدید شدند[۸]
	واسطه‌های تقلبی	برخی شرکت‌ها تظاهر می‌کنند که بازار مبادلات موجهی هستند. ولی در عوض فقط پول مشتریان را بالا می‌کشند و یا بد افزار منتشر می‌کنند. مقامات آمریکا یک تاجر انگلیسی را به جرم تقلب در اوراق بهادار محکوم کردند. اتهام او این بود که سرمایه گذاران را با جذب به یک بستر تقلبی مبادلات بیت‌کوین می‌فریفت. [۹]
شبکه	مجموعه‌های استخراج نابهنجار	در شبکه بیت‌کوین، اگر کسی بیشتر از ٪۵۰ قدرت استخراج را به دست آورد می‌تواند تراکنش‌های متقلبنه انجام دهد. اگرچه زمانهایی بوده که یک مجموعه خاص از استخراج کنندگان بیشتر از ٪۵۰ کّل شبکه را در اختیار داشته ولی اطلاعی از اینکه این طور تقلبی صورت گرفته باشد در دست نیست.
	بد افزار استخراج و فلج دیجیتال	فلج دیجیتال مخاطره‌ای است که توسط بد افزار صورت می‌گیرد. به این ترتیب که وقتی بد افزار وارد شبکه بیت‌کوین می‌شود بخش کوچکی از بیت‌کوین‌های استخراج کننده را بدون آنکه صاحب آن بفهمد می‌دزدد. یکی دیگر از انواع بد افزارها نوعی است که رایانه را آلوده می‌کند و از توان محاسباتی آن برای استخراج استفاده می‌نماید بدون آنکه صاحب آن متوجه شود. در سال ۲۰۱۳، مقامات آلمانی دو نفر را که با تولید بد افزار و آلوده کردن رایانه دیگران به استخراج پول مجازی می‌پرداختند دستگیر کردند. ولی در سالهای اخیر و با افزایش قدرت محاسباتی لازم برای استخراج بیت‌کوین، خیلی بعید است که چنین بدفزارهایی قابلیت فعالیت داشته باشند.

بسیاری از انواع تقلب‌ها و نفوذهای امنیتی مخاطرات سنتی و به اصطلاح "از قبل موجود" (pre-existing) می‌باشند. بلاک چین عمومی برخی از مخاطرات را تشدید می‌کند (مثلا هک کردن حساب ها) و انجام برخی جرائم مالی مخصوصاً پول شویی را تسهیل می‌نماید. به علاوه، نقدینگی‌های رمز پایه مخاطرات جدیدی را به همراه دارد همچون از دست دادن کلید خصوصی. وقتی کلید خصوصی از دست برود دیگر قابل بازیافت نیست. اگرچه این مثالی برای تقلب نیست ولی مخاطره آن کاملا جدی است. روزنامه تلگراف گزارش می‌دهد که یک فرد اهل ولز ۷۵۰۰ بیت‌کوین را در سال ۲۰۱۳ به دلیل دور انداختن یک هارد درایو قدیمی از دست داد.[۱۰]

تا به امروز بانکها دخالت اندکی در حوزه نقدینگی‌های رمز پایه داشته اند چون توسط این گونه نقدینگی‌ها کاربران بدون واسطه می‌توانند پول به هم ارسال نمایند. ولی بانکها از طریق مشتریانشان که از این نقدینگی‌ها استفاده می‌کنند در معرض ریسک پول شویی و دیگر فعالیت‌های غیر قانونی قرار می‌گیرند. مگر در حالتی که کاربران، بیت‌کوین خودشان را خودشان استخراج کنند یا به عنوان پرداخت از دیگران دریافت کنند، باید آن را با پول سنتی بخرند. انتقال چنین مبالغی از حسابهای بانکی به کیف پولهای دیجیتال مختص نقدینگی‌های رمز پایه می‌تواند نشانه پولشویی باشد و ریسک از دست رفتن شهرت برای بانکها داشته باشد. به علاوه بسیاری از بانکها سعی کرده اند میزان آسیب پذیری خود را با امتناع از ارائه دادن خدمات به شرکتهای فعال در زمینه نقدینگی‌های رمز پایه کاهش دهند. ولی با افزایش مشتریانی که به دلیل قانونی و موجه نیاز به تراکنشهای مبتنی بر نقدینگی‌های دیجیتال دارند بانکها مجبور خواهند شد تا به فکر چاره باشند.

بلاک چین‌های تجاری: احتمالا تقلب کم می‌شود ولی بی آسیب هم نیست.

بر خلاف نقدینگی‌های رمز پایه که با غنی سازی و استفاده‌شان در پرداخت‌ها تجربه سطوح بالای رفتار بدخیم را داشته اند، بلاک چین‌های تجاری (خصوصی) هنوز پا را از مرحله امکان سنجی فراتر نگذشته اند که بتوان در مورد آسیب پذیری آنها سخن گفت. یا مشابهاً در مورد توانایی آنها در زمینه کم کردن تقلب‌های سنتی و نفوذهای امنیت سخنی به میان آورد. باور بر این است که بسته به نوع فناوری که بلاک چین خصوصی در آن استفاده می‌شود، این قابلیت وجود دارد که بتواند مخاطره را کاهش دهد.

پرداخت. همچنان که پیشتر آمد پیشرفته‌ترین مورد مصرف این است که بلاک چین را به عنوان بستر بین بانکی جهت تسهیل پرداخت‌ها پیاده سازی نمود. مخصوصاً وقتی دو بانک در دو کشور مختلف هستند. بلاک چین فرصتی به دست می‌دهد که سرعت پرداخت‌های بین‌المللی را افزایش و مخاطرات تسویه وجوه را کاهش دهیم.

به علاوه بلاک چین به همراه محصولات مدرن پرداختی دیگر یک ابزار پیشرفته پیغام رسانی بین مشارکت کنندگان است که جزئیاتی همچون شناخت مشتری و مخاطرات مربوطه، کارمزدها، نرخ تبدیل عرض، جزئیات پرداخت و زمان مورد انتظار وصول پول در مقصد را قبل از انجام تراکنش به دست می‌دهد. این مساله نرخ هشدارهای غلط هنگام ارزیابی ریسک تقلب تراکنش‌ها را کاهش می‌دهد.

ولی باید توجه داشت که اگرچه بلاک چین ریسک تسویه وجوه را کاهش می‌دهد و اطلاعات پرداخت را بهبود می‌بخشد، ولی در مقابل عوامل بدکار محافظتی ایجاد نمی‌کند. اگر یک مجرم تراکنشی تقلبی به بانک بفرستد، این تراکنش هنوز ممکن است اجرا شود. در این حالت بلاک چین فقط کمک کرده عمل کلاه برداری سریعتر انجام شود!

دانش مالی تجارت و زنجیره تامین

بلاک چین‌های تجاری می‌توانند به حوزه دانش مالی تجاری و زنجیره تامین فایده بسیاری برسانند. پروژه‌های فراوانی وجود دارند که مواردی همچون فاکتورهای تقلبی، فاکتورهای دوبله را هدف قرار داده اند.

تعدادی از شرکتها در حال سخت پاسپورت‌های دیجیتالی هستند که اصل بودن کالا را به اثبات می‌رساند. محصولات تضمین کیفیت مبتنی بر بلاک چین کمک می‌کند تا شرکت‌های دخیل در یک مبادله تجاری را از نظر قواعد پولشویی و شناسایی مشتری ارزیابی کنند. به علاوه این اطمینان خاطر را به دست می‌دهد که کالاهای دخیل در معامله تقلبی، غیر قانونی و یا شامل مواد سمّی نبوده باشند. (جزئیات همه مراحل تهیه و توزیع کالا در یک بلاک چین ذخیره می‌شود)

همانطور که بلاک چین به اثبات اصل بودن کالا کمک می‌کند، از ریسک صورت حساب‌های تقلبی یا گران فروشی و کم فروشی نیز می‌کاهد. به عنوان مثال در مارس ۲۰۱۷ گزارش شده بود که کشور انگلیس مجبور به پرداخت احتمالی ۲ میلیارد یورو به اتّحادیه اروپا شد. این از آنجا ناشی می‌شد که مقامات این کشور نسبت به یک شبکه بزرگ واردات کالاهای ارزان چینی به اروپا چشم پوشی کردند. [۱۱]. این شبکه به طور مصنوعی قیمت کالاها را پایین اعلام می‌کرد تا از مالیات ارزش افزوده و حق گمرک در انگلیس فرار کند. این در حالی است که صورت حسابهایی که در یک دفتر حساب به اشتراک گذشته شده به آسانی قابل دستکاری نخواهند بود.

در نهایت بلاک چین می‌تواند از صورتحساب دوباره زدن جلوگیری کند. در حال حاضر تراکنش‌ها فقط نزد وام گیرنده و بانک معلوم هسند. این فرصتی است برای کلاه بردارن تا از یک صورت حساب چندین وام درخواست دهند. مرکز خبری کریپتوکوینز (Cryptocoins) گزارش داد [۱۲] که موسسه اعتباری استاندارد چارتر(Standard Charter) قربانی چنین حقه‌ای شد. در نتیجه این شرکت به این فکر افتاد تا با همکاری بانک سنگاپوری دی بی اس(DBS bank) یک محصول مبتنی بر بلاک چین جهت افزایش شفافیت صورت حساب‌ها تولید کند. این پایگاه داده بین چندین بانک به اشتراک گذشته می‌شود تا در عین رعایت محرمانگی بتوان درخواست‌های وام مبتنی بر صورت حساب را ارزیابی نمود.

هویت دیجیتالی

هویت دیجیتال یک موضوع داغ این روزهاست. مدل سنتی تشخیص هویت مشتریان با نام کاربری و رمز عبور در دراز مدت پاسخگو نخواهد بود. روش‌های جایگزینی برای مدیریت هویت مشتری در جهان دیجیتال نیاز است. هویت دیجیتال می‌تواند عملیات باز کردن و راست آزمایی کاربران را تسریع بخشد. با توجه به اینکه هویت‌های دزدیده شده یکی از ابزارهای مهم تقلب هستند این مهم می‌تواند ابزار قدرتمندی برای مبارزه با جرائم مالی باشد.

ضدّ گلوله وجود ندارد

باید تاکید کنیم که اگرچه ما انتظار داریم بلاک چین تاثیر مثبتی بر تقلب بگذرد ولی اکثر این فواید حداقل ۳ تا ۵ سال طول می‌کشد تا پیاده سازی شوند. همینطور که محصولات مبتنی بر بلاک چین ساخته می‌شوند صنعت بهتر می‌تواند آن را ارزیابی کند و دریابد تا چه حدی قابلیت مقابله با تقلب و جرائم مالی را واجد هستند.

به علاوه، با در نظر گرفتن این مساله که فناوری از ارزیابی تاثیر خود بر تقلب عاجز است، ما تعجّب نخواهیم کرد اگر مولفه‌های ریسک دیگری سر برورند. وزارت خزانه داری آمریکا با این نظر موافق است. کمیته نظارت بر پایداری بازار در سال ۲۰۱۶ در گزارش سالیانه خود چنین می‌گوید:

"مشارکت کنندگان بازار تجربه کمی با سامانه‌های دفاتر غیر متمرکز دارند و ممکن است آسیب پذیری‌های عملیاتی دخیل در این سامانه‌ها هنوز تا در مقیاس بالا پیاده سازی نشده اند معلوم نگردد. به علاوه با وجود اینکه دفاتر غیر متمرکز برای جلوگیری از خطا یا تقلب طراحی شده اند، برخی سامانه‌ها ممکن است در اثر تبانی تعدادی مشارکت کنندگان در سامانه در معرض تقلب قرار گیرند."

مبارزه با جرائم مالی: امروز و فردا

چه ابزارهایی برای کاهش تقلب در آینده نیاز است؟

ابزارهای جدید برای مخاطرات تولید شده توسط نقدینگی هایا رمز پایه. ابزارهایی به بازار آمده که اختصاصا برای مدیریت ریسک نقدینگی‌های رمز پایه طراحی شده اند. مثلا شرکت چین آنالیز(Chainalysis) و الیپتیک(Elliptic)، کارشان این است که بر شبکه بیت‌کوین نظارت می‌کنند و حساب‌های افراد کلاه بردار یا آنهایی که به بازار سیاه مرتبط می‌شوند را شناسایی می‌کنند. اگر این محصولات با محصولات کشف تقلب شرکت‌های سنتی ادغام شوند، نتیجه این خواهد بود که قواعد پولشویی و تطبیق را برای بانکها پیاده سازی کنند. به علاوه بازارهای مبدل بیت‌کوین با رعایت قواعد پولشیی می‌توانند بانکها را از سلامت مالی خود مطمئن کنند. تا کنون چنین اطمینان خاطری به بانکها داده نشده است .
بسیاری از محصولات کشف تقلب امروزی مبتنی بر روش‌های یادگیری ماشین و تحلیل رفتاری هستند. این روش‌ها به کشف ناهنجاری در تراکنش‌ها می‌پردازند. بسیاری از تکنیک‌های مورد استفاده در کشف تقلب بانکداری سنتی برای بانکداری مبتنی بر بلاک چین نیز هستند. مثلا این نکته که اگر یک کاربر از آی پی غیر معمولی به سیستم لاگین کرد در مورد کیف پول دیجیتال هم صادق خواهد بود. فهمیدن اینکه آیا کلید خصوصی یک کاربر لو رفته یا خیر به طور مستقیم کار آسانی نیست. ولی وقتی رفتار مالی شخص در سامانه تغییر می‌کند می‌توان حدس زد که احتمال لو رفتن کلید خصوصی وجود درد.

نتیجه: بانکها نقش غالبی در جلو بردن بلاک چین‌های تجاری و نیز استفده از نقدینگی‌های رمز پایه خواهند داشت. قطعاً ارسال پول بین‌المللی با کارمزد کم بازاری بسیار جذاب برای بانکها خواهد بود. بنابرین بانکها باید به طور اساسی خدمات و فرایندهایی که امکان بهبود یا انقضای آنها پس از رواج بلاک چین می‌رود را ارزیابی کنند. برای آنکه بانکها در آشوبی که بلاک چین به پا خواهد کرد آماده باشند مدیریت بانک لازم است در جریان تغییرات این فناوری روز قرار بگیرد. به علاوه به موازات تولید محصولات مبتنی بر بلاک چین لازم است ابزارهای کشف تقلب و ارزیابی شبکه‌های بلاک چین پایه ریزی شوند.

فهرست منابع

[1] https://www.coindesk.com/Bitcoin-phishing-scheme-perpetrator-pleads-guilty-in-connecticut-court/

[2] http://www.bbc.co.uk/news/technology-39901382

[3] https://www.thepaypers.com/digital-identity-security-online-fraud/hacker-breaches-coindash-and-stealsusd-7-mln-worth-of-ethereum/769554-26
[4] https://www.bloomberg.com/news/articles/2017-07-26/russian-wanted-in-us-caught-in-greece-for-moneylaundering

[5] https://www.wired.com/2015/05/inside-a-million-dollar-dark-web-coupon-counterfeiting-scheme/

[6] https://www.theguardian.com/technology/2015/sep/01/us-federal-agent-investigating-silk-road-admits-800000-Bitcoin-theft

[7] https://www.theverge.com/2014/9/23/6833047/Bitcoin-conspiracy-theorists-vindicated-as-ftc-shuts-downbutterfly-labs

[8] https://www.theguardian.com/technology/2016/jan/20/Bitcoin-netherlands-arrests-cars-cash-ecstasy

[9] https://www.theguardian.com/technology/2017/jul/01/Bitcoin-fake-site-uk-dealer-charged-us-multimilliondollar-scam

[10] http://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-ofdisappearing-Bitcoins.html

[11] http://www.politico.eu/article/uk-faces-e2-billion-eu-payment-for-china-fraud-trade/

[12] https://www.cryptocoinsnews.com/standard-chartered-dbs-work-on-blockchain-tech-for-trade-finance/