قراردادهای هوشمند و نقش آن‌ها در خلق ارزش از منظر بانک‌ها

زهرا ابراهیمی غفار
کارشناس مدیریت برنامه‌ریزی و پروژه‌های راهبردی، شرکت خدمات انفورماتیک
z_ebrahimi@isc.co.ir

چکیده

بلاک چین از زمان پیدایش خود تا کنون به واسطه مزیتِ قابلیتِ بکارگیری در تعداد بیشماری از سناریوهای دنیای واقعی، توجه بسیاری از محققانِ این زمینه را به خود جلب نموده است. در حال حاضر بلاک‌چین بعد از اینترنت، اختراعی مهم و فنی به شمار می‌آید چرا که قادر است بسیاری از تکنولوژی‌ها و کسب وکارهای فعلی را دگرگون سازد. ویژگی‌های بارز بلاک‌چین همچون غیر قابل تغییر بودن، ارائه محیطی بدون نیاز به اعتماد متقابل طرفین تجارت، قابلیت بازگشت به حالت تعادل در صورت ایجاد تغییرات غیر قانونی، استفاده از الگوریتم رمزنگاری هش و فرایند اجماع موجب شده این تکنولوژی به یکی از بهترین پیشرفت‌های دنیای تکنولوژی تبدیل شود و بسیاری از الزامات محاسباتیِ مسائل دنیای واقعی را حل نماید. انقلاب بلاک‌چین با ارائه قراردادهای هوشمند و بلاک‌چین‌های قابل برنامه‌نویسی به نام اتریوم دستاوردهای عظیمی داشته است.

قرارداد هوشمند پروتکلی کامپیوتری جهت تسهیل، تأیید و اجرای شرایط یک توافق‌نامه تجاری است. در این مقاله در راستای اهمیت بحثِ پیرامون پیاده‌سازی قراردادهای هوشمند بر بستر اتریوم، ابتدا به معرفی برخی از مفاهیم تئوری و بنیادی بلاک-چین اتریوم پرداخته شده است و سپس سعی شده پاسخ‌های دقیق و مناسبی برای پرسش‌های مورد توجه آن مطرح گردد برخی از این پرسش‌ها در ادامه بیان می‌گردد. قراردادهای هوشمند برای بانک‌ها و مشتریان آن‌ها چه مزایایی به همراه خواهد داشت و چالش‌های فنی، قانونی و سازمانی که پیش از استقرار این قراردادها باید مرتفع گردند کدامند، بانک‌ها در جهت بکارگیری و استقرار قراردادهای هوشمند و استفاده از مزایای آن‌ها چه اقداماتی باید انجام دهند. علاوه بر پاسخ دادن به این پرسش‌ها، نمونه‌هایی از کاربرد این قراردادها جهت خدمات بانکی بیان می‌گردد و در پایان با توجه به شرایط تحریم در ایران، فرایند گشایش اعتبار اسنادی به عنوان نمونه‌ای از کاربرد این قراردادها در صنعت واردات و صادرات کالا پیشنهاد می‌شود.

واژگان کلیدی:

بلاک‌چین، اتریوم، قراردادهای هوشمند، دفتر کل

Smart Contracts and their contribution on creating value from banks point of view

Zahra Ebrahimi Ghaffar, Planning and Strategic Projects Management Expert, Informatics Services Corporation

z_ebrahimi@isc.co.ir

Abstract

From the time of inception, Blockchain technology has gained considerable attention among researchers due to its mind-blowing application potential in a variety of real world scenarios. Presently, most of them consider blockchain as an important technical invention after ا The Internetب which could disrupt most of the existing technologies and business domains. The compelling features of blockchains, such as immutability, trust-free nature, resilience to illegal modifications, cryptographic hashing, consensus based decision making etc., makes this technology one of the most promising technical breakthrough capable of addressing many avenues of computational requirement in real world problem solving. The blockchain revolution is now reaching new heights with the release of Smart contracts and programmable blockchains such as Ethereum.

A smart contract is often defined as بcomputer protocols that facilitate, verify, execute and enforce the terms of a commercial agreementپ We discuss what are the benefits of smart contracts for banks and their customers and, what technical, legal and organizational challenges are required to address before smart contracts can become mainstream and, how banks can realize the full potential of smart contracts and also explain smart contracts application areas in banking services. Finally, considering the sanctions conditions in Iran, Letter of Credit process is offered as a use case for export and import industry.

Key Words:

Blockchain, Ethereum, Smart Contracts, Ledger

۱-مقدمه

بلاک‌چین یک پایگاه داده توزیع شده است که پیوسته لیستی از رکوردهای حاوی داده رمزنگاری شده را در قالب بلاک، نگهداری نموده و از دستکاری و تجدیدنظر محافظت می‌کند. بلاک‌چین پارادایم جدیدی از تکنولوژی است که درهای جدیدی را به روی معاملات و تراکنش‌ها می‌گشاید. این تکنولوژی از طریق رمزنگاری، امنیتی بی نظیر در تراکنش‌ها و معاملات به وجود آورده و نیاز به مراکز داده و مین‌فریم‌های هزینه‌بر را از بین می‌برد و به طور کلی مدل هزینه پردازش تراکنش‌ها را تغییر می‌دهد.

اتریوم پلتفرمی جدید است که مفهوم بلاک‌چین را چندین گام به جلو می‌راند. تکنولوژی بلاک‌چین پردازش تراکنش‌های مالی

به طور توزیع شده را میسر ساخت و اتریوم این مفهوم را به مدلی قابل برنامه‌ریزی جهت پردازش مفهومی به نام قراردادهای هوشمند تعمیم داده است. قرارداد هوشمند پروتکلی کامپیوتری جهت تسهیل، تأیید و اجرای شرایط یک توافق‌نامه تجاری است. با استفاده از فناوری بلاک‌چین در قراردادهای هوشمند، ساختار این قراردادها، غیر متمرکز و به طور یکسان در اختیار تمامی طرف‌های درگیر در فرایند انتقال ارزش مورد نظر قرار می‌گیرد. شرکت سرمایه‌گذاری Santander Innoventures در طی گزارش بیان کرد تکنولوژی‌های بلاک‌چین تا سال ۲۰۲۰، هزینه‌های زیرساختی بانک‌ها را سالانه به مقدار ۱۵ تا ۲۰ بیلیون دلار کاهش خواهد داد. لذا شرکت‌های مالی ناچار به برنامه‌ریزی در خصوص پیاده‌سازی و بکارگیری قابلیت‌های این تکنولوژی باشند[1].

قراردادهای هوشمند بر بستر بلاک‌چین و یا دفترهای همگانی توزیع‌شده، درمانی برای بسیاری از مشکلات قراردادهای مالی سنتی است، از جمله این مشکلات، تکیه کردن بر اسناد کاغذی، تأخیر، عدم کارایی،احتمال خطا و تقلب می‌باشد. واسطه‌های مالی با کاهش دادن ریسک به یاری سیستم‌های مالی می‌آیند اما هزینه‌های سربار و الزامات مورد نیاز را افزایش می‌دهند.

با توجه به اهمیت موضوع پیاده‌سازی قراردادهای هوشمند بر بستر بلاک‌چین، در این مقاله سعی شده است بلاک‌چین اتریوم مورد بررسی قرار گرفته و بر اساس آن پیشنهادی در خصوص شرایط تحریم فعلی ایران مطرح گردد. همچنین تلاش شده است تا سؤالات زیر که مجریان باید به منظور تحقق منافع، خلق استراتژی و رویکرد قراردادهای هوشمند، در نظر گیرند پاسخ داده شود.

- قراردادهای هوشمند برای بانک‌ها و مشتریان آن‌ها چه مزایایی به همراه خواهد داشت؟
- چالش‌های فنی، قانونی و سازمانی که پیش از استقرار این قراردادها باید مرتفع گردند کدامند؟
- بانک‌ها در جهت بکارگیری و استقرار قراردادهای هوشمند و استفاده از مزایای آن‌ها چه اقداماتی باید انجام دهند؟

در ادامه‌ی این مقاله و در بخش بعد، مروری بر ادبیاتِ موضوع می‌شود و پس از اشاره به روش تحقیق، در بخش چهارم به تفصیل به ذکر مفاهیم بنیادی فناوری اتریوم پرداخته شده است. در بخش پنجم، محدودیت‌های قراردادهای فیزیکی، منافع قراردادهای هوشمند برای بانک‌ها و مشتریان آن‌ها و نیز چالش‌های پیش‌رو و راهکارها ارائه می‌گردد. در آخر، به ذکر نمونه‌ای کاربردی از این قراردادها در شرایط فعلی تحریم ایران پرداخته و پس از آن جمع‌بندی مطالب ارائه می‌گردد.

۲-ادبیات موضوع

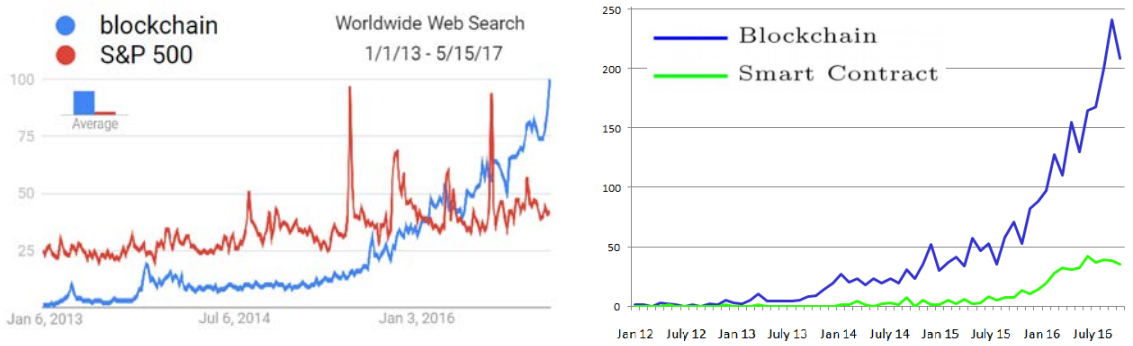
زیربنای علمی قراردادهای هوشمند به نظریه بازی‌ها برمی‌گردد. نظریه بازی‌ها به نحوه تعامل طرف‌های درگیر تحت شرایط و قواعد خاص می‌پردازد. بر اساس نظریه‌های مطرح در این زمینه، هر بازی‌گر در یک گروه که استراتژی‌های سایر طرف‌های درگیر در بازی را بداند، می‌تواند به گونه‌ای بازی کند، که دیگران تمایلی به تغییر استراتژی خود نداشته باشند. همین اصل، مبنای قراردادهای هوشمند است. تمام بازی‌گرها با توجه به یک سری قانون و قاعده‌های شفاف که به طور اتوماتیک اجرا می‌شوند، به نقش خود در بازی پای‌بند می‌مانند و نیازی به یک مراقب ناظر وجود ندارد؛ به این دلیل که هر کس با ایفای نقش خودش، بیشترین بهره را از بازی می‌برد. با این توضیح، اولین تعریف رسمی قرارداد هوشمند ارائه شده توسط زابو[1] در ۱۹۹۴ به شرح زیر است:

[1] Szabo

قرارداد هوشمند یک پروتکل تراکنش کامپیوتری[۲] جهت اجرای مفاد قراردادها است. اهداف کلی طراحی قراردادهای هوشمند ارضای شروط معمول قرارداد مانند شرایط و ضوابط پرداخت، حفظ محرمانگی و اتمام قراداد و نیز حداقل نمودن استثنائات تصادفی و عمدی و نیاز به وجود واسطه‌های مورد اعتماد می‌باشد.

با این تعریف، ماشین فروش خودکار[۳] در واقع یک قرارداد فروش هوشمند را اجرا می‌کند. پول‌های دیجیتال نیز، همین کار را در فضای آنلاین انجام می‌دهند. سیستم «مدیریت کپی‌رایت دیجیتال» (DRM)[۴] به خوبی می‌تواند کاربرد قرارداد هوشمند را نشان دهد. این سیستم برنامه‌ای است که همراه با بیشتر رسانه‌های دیجیتال (از جمله DVD

پلتفرم‌های مختلف بلاک‌چین ارائه نموده‌اند. پیترز [10] و پانایی [11] در سال ۲۰۱۶ به ذکر جنبه‌های کلیدی بلاک‌چین و قراردادهای هوشمند پرداخته و چالش‌های اساسی پیاده‌سازی این قراردادها در حوزه بانکداری بیان نمودند. در شکل ۱، تعداد جستجوی تکنولوژی بلاک‌چین در گوگل نشان داده شده است که این آمار حاکی از محبوبیت فزاینده‌ی این تکنولوژی در ۵ سال گذشته است. همچنین روند اخیر پروژه‌های متن‌بازِ جدید مرتبط با قراردادهای هوشمند و بلاک‌چین ارائه گردیده است[3].



شکل ۱-روند گرایش به بلاک‌چین و قراردادهای هوشمند(شکل سمت چپ آمار جستجو در گوگل، شکل سمت راست تعداد پروژه‌های متن‌بازِ جدید گزارش شده در سایت GitHub)

۳-روش تحقیق

با توجه به اهمیت مفهوم قراردادهای هوشمند بر بستر بلاک‌چین و اقبال زیاد صنعت خدمات مالی و به خصوص بانکداری به آن، در این مقاله سعی شده است مطالبی که در سطح جهانی بصورت پراکنده و در قالب کاربردها، چالش‌های پیش روی به همراه راهکارها و نیز مقالات فنی در این باره منتشر شده‌اند جمع‌آوری و تجمیع شده و براساس آن یک تعریف جامع از قراردادهای هوشمند بر بستر بلاک‌چین ، کاربردها و ملزومات پیاده‌سازی این قراردادها ارائه گردد بطوری که عاری از تناقض بوده و شفافیت لازم را جهت استفاده بانک‌ها و شرکت‌های فعال در حوزه فناوری‌های پرداخت کشور دارا باشد.
برای ارائه پیشنهاد مناسب جهت بکارگیری این قراردادها در شرایط فعلی تحریم در ایران، خدمات بانکی در ارتباط با بانک-های خارج از کشور مورد بررسی قرار گرفته است تا در حد امکان پیشنهادی راهگشا ارائه گردد.

۴-بلاک چین اتریوم

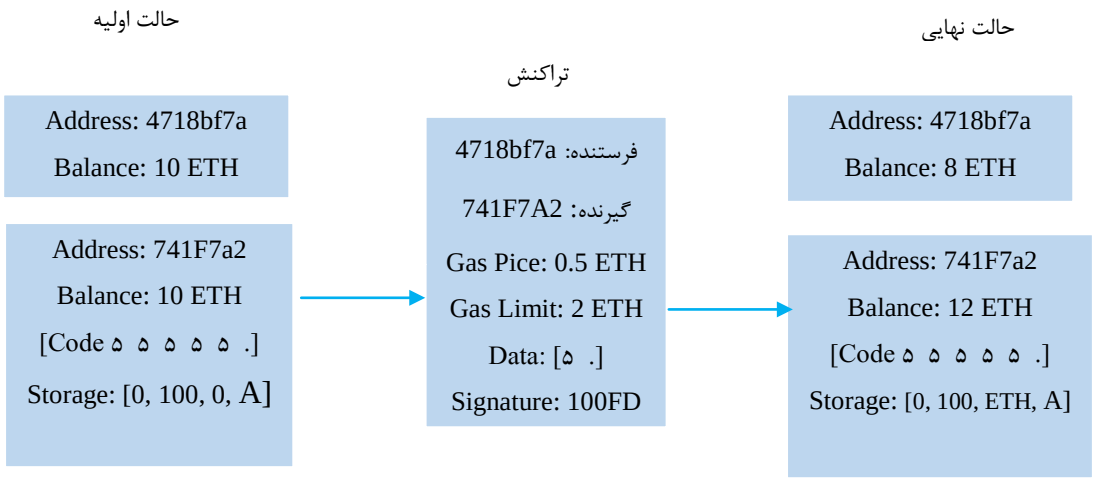
شاید از شایع‌ترین پلتفرم‌های قرارداد هوشمند که در جولای ۲۰۱۵، راه‌اندازی شده اتریوم [12] است. اتریوم نیز مانند سایر بلاک‌چین‌ها، یک ماشین حالتِ مبتنی بر تراکنش [13] است، روش کار آن بدین صورت که حالت اولیه با اجرای تراکنش‌ها و به

[9] Bartoletti and Pompianu
[10] Peters
[11] Panayi
[12] Ethereum
[13] Transaction-based state machine

صورت افزایشی به حالت نهایی می‌رسد و آخرین تبدیل به عنوان نسخه قطعی حالت، پذیرش می‌گردد. در دیاگرام شکل ۲، تابع گذر حالت[14] اتریوم نشان داده شده است، طوری که اجرای تراکنش به یک گذر حالت منتهی می‌گردد. در مثال ارائه شده، ۲ اتر از آدرس 4718bf7a به آدرس 741f7a2 منتقل گردیده است[4].

۴-۱-ارز (ETH و ETC)

اتریوم جهت انگیزش، ارز مبادله خود را با نام اختصاری ETH به عنوان جایزه به معدن کاوان[15] ارائه می‌دهد. از آنجا که بعد از هک DAO، یک هارد فورک[16] جهت حل این مسئله ارائه شد بنابراین در حال حاضر دو بلاک‌چین اتریوم وجود دارد: اولی



شکل ۲-تابع گذر حالت اتریوم

کلاسیک اتریوم با ارز ETC و دیگری نسخه هارد فورک با ارز ETH که هر در حال توسعه و رشد می‌باشد. در این بخش بر روی ETH تمرکز شده است که فعال‌ترین و رسمی‌ترین نسخه بلاک‌چین اتریوم است[4].

۴-۲-فورک

با انتشار نسخه فورک homestead، به جهت ارتقای اساسی پروتکل، نتیجه به یک هارد فورک منجر شد. پروتکل در بلاک شماره ۱۱۵۰۰۰۰ ارتقا یافت و نسخه اولیه اتریوم با نام Frontier به روزرسانی شده و به عنوان نسخه دوم تحت نام homestead ارایه گردید.

اخیراً در تاریخ ۲۴ نوامبر ۲۰۱۶ در ساعت ۱۴:۱۲:۰۷، به دلیل باگ در مکانیسم ژورنالینگ[17] کلاینت Gas، یک فورک ناخواسته اتفاق افتاده است؛ فورک شبکه در بلاک شماره ۲۶۸۳۵۱ اتفاق افتاد. این بدین معناست که از بلاک شماره

[14] State transition
[15] Miners
[16] Hard-forked
[17] Journaling mechanism

۲۶۸۳۵۱، بلاک‌چین اتریوم به دو بخش تقسیم می‌شود، یکی روی کلاینت‌های parity و دیگر روی Gas و این مسئله موجب انتشار نسخه Gas 1.5.3 گردیده است[4].

Gas-۳-۴

یکی دیگر از مفاهیم کلیدی دیگر اتریوم Gas است. تمامی تراکنش‌های اتریوم باید هزینه‌های محاسباتی خود را بپردازند که این هزینه توسط Gas پوشش داده می‌شود. مفهوم Gas به عنوان مبلغ اجرای تراکنش از طریق بنیانگذار یا مؤسس تراکنش[18] به صورت بیعانه یا پیشاپیش پرداخت شده و با انجام هر عملیات هزینه می‌شود. به هر عملیاتی یک مقدار از پیش تعیین شده Gas، اختصاص داده می‌شود. هر تراکنش مشخص می‌کند که چه مقدار Gasای می‌بایست جهت اجرای تراکنش پرداخت و مصرف شود. اگر مقدار Gas قبل از اجرای تراکنش تمام شود، تمامی عملیات انجام شده تا این مرحله در طی تراکنش انجام شده، بازگشت داده می‌شود و در صورت با موفقیت انجام شدن تراکنش، مقدار باقیمانده Gas به بنیانگذار تراکنش باز خواهد گشت[4].

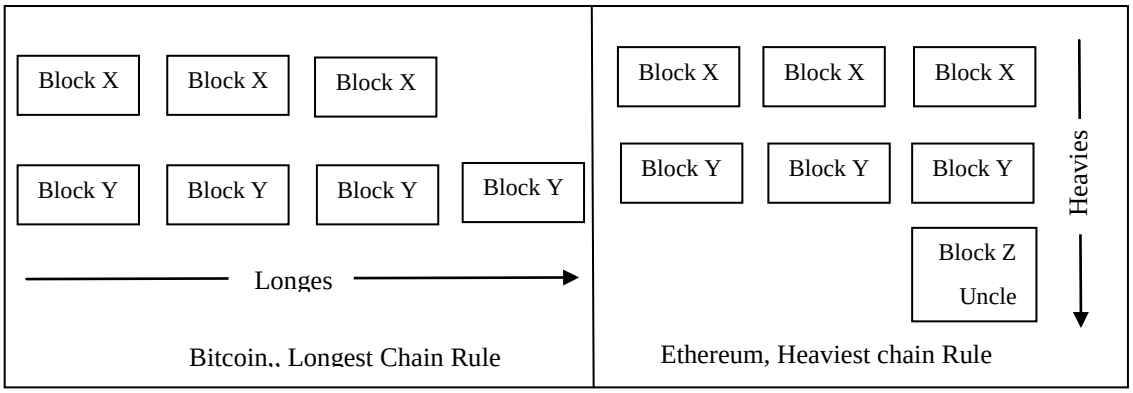
۴-۴-مکانیسم اجماع

مکانیسم اجماع در اتریوم بر اساس پروتکل GHOST است و ابتدا توسط زهر[19] و سومپولینسکی[20] در دسامبر ۲۰۱۳ مطرح شد. اتریوم از نسخه ساده‌تری از این پروتکل استفاده می‌کند، بدین صورت که، زنجیره‌ای که بیشترین تلاش محاسباتی جهت ایجاد آن صرف شده به عنوان نسخه قطعی شناخته می‌شود و می‌توان گفت، این زنجیره طولانی‌ترین زنجیره است چرا که بیشترین تلاش محاسباتی را به خود اختصاص می‌دهد[4]. پروتکل GHOST برای اولین بار به عنوان مکانیسمی جهت حل این مسئله که تولید بلاک‌ها در زمان خیلی کوتاه منجر به ایجاد تعداد بسیاری بلاک یتیم[21] می‌شود، معرفی گردید[5]. این بلاک‌ها در شبکه منتشر شده و درستی آنان توسط تعدادی از نودها تأیید می‌شود اما نهایتا به دلیل تسلط یک زنجیره طولانی‌تر، کنار گذاشته خواهند شد. در پروتکل GHOST ، همانطور که در شکل ۳ نشان داده شده بلاک‌های یتیم جهت تعیین طولانی‌ترین و سنگین‌ترین زنجیره در محاسبات شرکت داده می‌شوند. بلاک‌های یتیم uncles یا Ummers نامیده می‌شوند[4].

۴-۵-حالت کلی[22]

حالت کلی، حالت سراسری بلاک‌چین اتریوم را نشان می‌دهد که اساساً نگاشتی با طول ۲۰ بایت بین آدرس‌ها و حالت‌های حساب است. این نگاشت، ساختار داده‌ای است که توسط RLP[23] سریال سازی می‌شود. RLP یک تابع رمزگذاری است که در اتریوم جهت سریال‌سازی داده باینری به منظور ذخیره‌سازی و انتقال داده به شبکه مورد استفاده قرار می‌گیرد و همچنین ذخیره حالت در درخت پاتریسیا انجام می‌گردد. این تابع یک رشته یا یک آیتم را به عنوان ورودی دریافت نموده و بایت‌های سریال را جهت ذخیره یا انتقال بر روی شبکه ایجاد می‌نماید.

[18] Transaction Originators
[19] Zohr
[20] Sompolinsky
[21] Orphan blocks
[22] The World state
[23] Recursive Length Prefix



شکل ۳-طولانی‌ترین زنجیره در مقابل سنگین‌ترین زنجیره

۴-۵-۱-حالت حساب[۲۴]

حالت حساب شامل ۴ فیلد nonce، balance، storageroot و codehash می‌باشد.

Nonce: متغیر Nonce بدین صورت عمل می‌کند؛ با ارسال هر تراکنش توسط آدرس، یک عدد اضافه می‌شود. در مورد حساب‌های قراردادی، این متغیر نشاندهنده تعداد قراردادهایی است که توسط حساب، ساخته شده است.

Balance: Balance نشاندهنده تعداد wies (کوچکترین واحد پولی در اتریوم) است که توسط آدرس جابجا می‌گردد.

Storageroot: Storageroot فیلد نود ریشه درخت پاتریسیای مرکل است که محتوای ذخیره شده حساب را رمزنگاری می‌کند.

Codehash: Codehash فیلدی غیر قابل تغییر است که دربردارنده هش کد قرارداد هوشمند است و به حساب اختصاص داده می‌شود. در حساب‌های نرمال، این فیلد هش ۲۵۶ بیتی keccak از رشته‌ای خالی است. این کد توسط یک تماس پیامی فراخوانی می‌شود.

حالت کلی و ارتباط آن با ترای حساب‌ها، حساب‌ها و هدر بلاک‌ها در شکل ۴ نشان داده شده است. هش Storageroot حساب از درخت ترای در سمت چپ حاصل می‌شود. ساختار داده حساب که نگاشتی بین حساب‌ها و آدرس‌ها می‌باشد، سپس در ترای حالت کلی استفاده می‌گردد. در نهایت نود ریشه درخت ترای با استفاده از الگوریتم ۲۵۶ بیتی keccak هش شده و قسمتی از هدر بلاک را تشکیل می‌دهد[4].

۴-۶-تراکنش‌ها

یک تراکنش در اتریوم یک بسته داده امضای دیجیتال است که از کلید خصوصی استفاده نموده و شامل دستوراتی است که در زمان تکمیل منجر به ایجاد یک تماس پیامی یا خلق قرارداد می‌شوند. تراکنش‌ها بر اساس خروجی که ایجاد می‌کنند به دو دسته تقسیم می‌شوند:

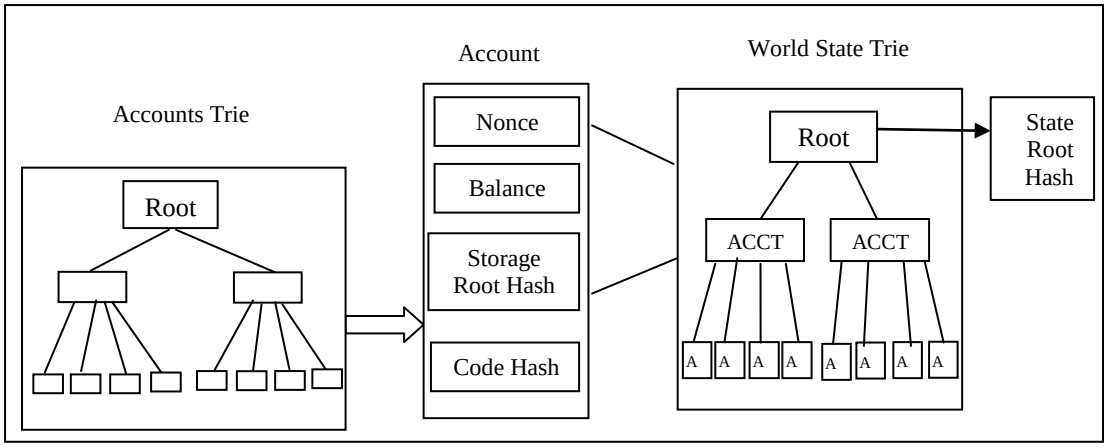
۱-تراکنش‌های تماس پیامی: این تراکنش به سادگی یک تماس پیامی را برای انتقال پیام بین یک حساب به حساب دیگر،

[24] The account state

ایجاد می‌نماید.

۲-تراکنش‌های ایجاد قرارداد: این تراکنش‌ها موجب ایجاد یک قرارداد جدید می‌شوند. این بدان معنی است که موقع با موفقیت اجرا شدن این قراردادها، حسابی با کد اختصاص داده شده ایجاد می‌شود.

هر دو تراکنش نامبرده یکسری فیلدهای مشترک دارند که در ادامه شرح داده می‌شود:



شکل ۴-ارتباط حالت کلی و ارتباط آن با تراي حساب‌ها، حساب‌ها و هدر بلاک‌ها

Nonce: عددی است که در زمانی که یک تراکنش توسط فرستنده ارسال می‌شود یک عدد به آن اضافه می‌گردد و باید برابر تعداد تراکنش‌های ارسال شده باشد و به عنوان شاخص واحد برای تراکنش استفاده شود. مقدار nonce فقط یک بار قابل استفاده است.

GasPrice: مقدار wie مورد نیاز جهت اجرای تراکنش را نشان می‌دهد.

Gas Limit: مقدار ماکزیمم Gasای را نشان می‌دهد که جهت اجرای تراکنش قابل مصرف است.

To: آدرس گیرنده تراکنش را مشخص می‌کند.

Value: مقدار نهایی wieای را نمایش می‌دهد که به گیرنده ارسال می‌گردد و در مورد قرارداد، بالانسی است که قرارداد حمل خواهد نمود.

امضا: امضا شامل سه فیلد به نام‌های r،s ، v می‌باشد. متغیرهای s و r نشاندهنده امضای دیجیتال و متغیر s شامل اطلاعاتی است که با آن بتوان کلید خصوصی را بازیابی نمود. جهت امضای یک تراکنش از تابع ECDSASIGN استفاده می‌شود و پیامی که باید امضا شود به همراه کلید خصوصی به عنوان ورودی گرفته و سه متغیر یک بایتی v، ۳۲ بایتی r و ۳۲ بایتی S را ایجاد می‌نماید.

ECDSASIGN(کلید خصوصی ،پیام)= (V,R,S)

INIT: فیلد INIT فقط برای تراکنش‌هایی است که قصد ایجاد قرارداد را دارند. این فیلد آرایه‌ای از جنس بایت با طول نامحدود است و کد EVMای را که در فرایند مقداردهی اولیه‌ی حساب استفاده شده است مشخص می‌کند و این کد تنها یک بار اجرا می‌گردد؛ موقعی که حساب برای اولین بار ایجاد می‌شود و بعد از آن بلافاصله از بین می‌رود.

Data: اگر تراکنش از نوع تماس پیامی باشد فیلد Data که شامل داده ورودی تماس پیامی است به جای INIT استفاده می‌شود. این فیلد نیز سایز نامحدود داشته و آرایه‌ای از جنس بایت است.

مطابق شکل ۵، هر تراکنش حاوی فیلدهای ذکر شده در ترای تراکنش قرار گرفته و نود ریشه ترای تراکنش با الگوریتم ۲۵۶ بیتی keccak هش شده و در هدر بلاک در کنار لیستی از تراکنش‌ها قرار می‌گیرد. تراکنش‌ها در بلاک‌ها و یا استخرهای تراکنش یافت می‌شوند. زمانی که یک نود miner شروع به انجام عملیات در راستای تأیید بلاک‌ها می‌کند، او کار خود را با تراکنش‌هایی که بالاترین پرداختی را در استخر تراکنش‌ها داشته آغاز و آن‌ها را به نوبت اجرا می‌کند. معدن‌کاوی موقعی شروع می‌گردد که Gas Limit تمام شود یا هیچ تراکنشی جهت پردازش در استخر تراکنش باقی نماند. در این فرایند، بلاک تا موقع یافت شدن یک nonce معتبر با مقداری کمتر از هدف سختی[۲۵]، مرتباً هش می‌شود. زمانی که بلاک با موفقیت معدن‌کاوی شد، به سرعت به شبکه اطلاع داده می‌شود و اعلام موفقیت می‌گردد و توسط شبکه تأیید و مورد قبول واقع می‌شود[4].

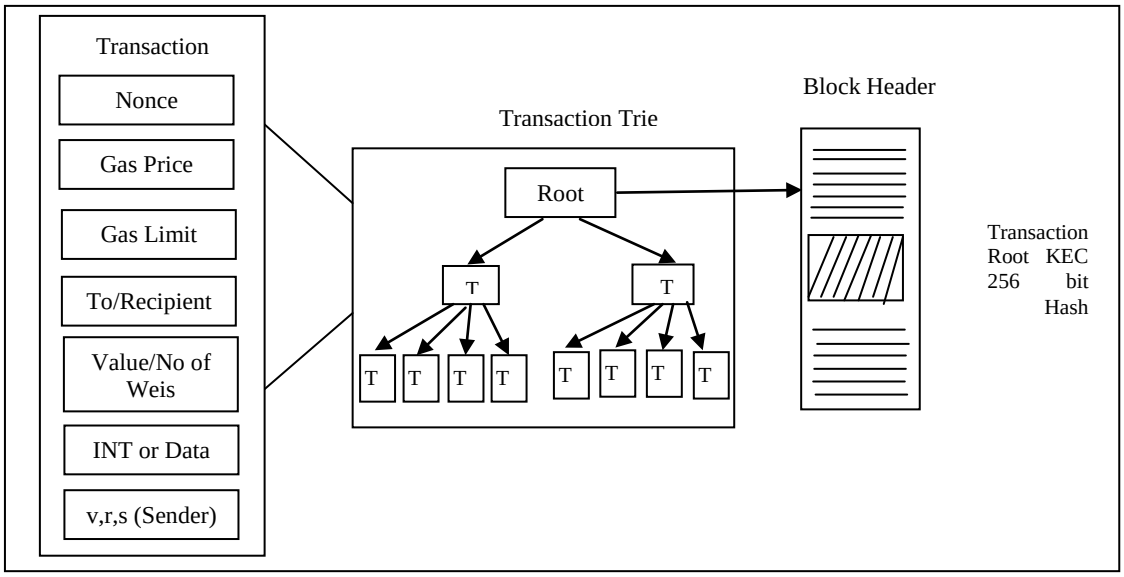
۴-۶-۱-تراکنش ایجاد قرارداد

به تعدادی پارامتر ضروری جهت ایجاد یک حساب نیاز است این پارامترها عباتند از: فرستنده، مؤسس اولیه، Gas در دسترس، Gas price، سرمایه‌گذاری (مقدار اتر که در ابتدا اختصاص داده شده است)، آرایه‌ای از جنس بایت با طول دلخواه، مقدار اولیه کد EVM، عمق فعلی(تعداد اقلام موجود فعلی) پشته تماس پیامی[۲۶]/ پشته خلق قرارداد.

طول آدرس‌هایی که به عنوان نتیجه تراکنش خلق قرارداد ایجاد می‌شود ۱۶۰ بیت است. دقیقا این آدرس‌ها ۱۶۰ بیت سمت راست هش keccak از رمزگذاری RLP که شامل فقط فرستنده و nonce است، می‌باشد. در ابتدا، nonce در حساب مقدار صفر را دارا می‌باشد. بالانس حساب، مقدار تصویب شده در قرارداد است. Storage خالی است. Codehash یک هش ۲۵۶ بیتی از رشته‌ای خالی است.

حساب، با اجرای کد EVM مقدار دهی اولیه می‌شود. اگر هیچ استثنایی همانند تمام شدن Gas (نداشتن Gas به اندازه مورد نیاز)، در طول اجرای کد رخ ندهد حالت تغییر نمی‌کند. اگر اجرا موفقیت‌آمیز باشد سپس حساب بعد از پرداخت هزینه Gas کافی، ایجاد می‌شود. نسخه فعلی اتریوم (homestead) مشخص می‌کند که نتیجه اجرای تراکنش یا یک قرارداد جدید با بالانس آن است، یا اینکه هیچ قرارداد جدیدی با هیچ مقداری یا انتقالی ساخته نشده است. این موضوع با نسخه قبلی متفاوت است، در نسخه قبلی ایجاد قرارداد بدون توجه به موفقیت آمیز بودن استقرار کد انجام می‌شد یا اینکه استثنا تمام شدن Gas در نظر گرفته نمی‌شد

[25] Difficulty target
[26] Message call stack



شکل ۵-ارتباط بین تراکنش، ترای تراکنش و هدر بلاک

۴-۶-۲-تراکنش تماس پیامی

یک تماس پیامی به چندین پارامتر برای اجرا نیاز دارد که عبارتند از: فرستنده، مؤسس تراکنش، گیرنده، حسابی که آن را اجرا می‌کند، مقدار Gas در دسترس، value، Gas price، آرایه از جنس بایت با طول دلخواه داده وروی call، عمق فعلی(تعداد اقلام موجود فعلی) پشته تماس پیامی/خلق قرارداد. تماس‌های پیامی منجر به گذر حالت و نیز ایجاد داده خروجیِ مورد استفاده می‌گردد. اگر تراکنش‌ها در مواردی اجرا گردد که تماس‌های پیامی توسط کد VM راه‌اندازی شده است، از خروجی برای اجرای تراکنش استفاده می‌شود[4].

۴-۷-بلاک

بلاک‌های اتریوم از سه جزء اصلی هدر بلاک، لیست تراکنش‌ها و لیستی از هدرهای Ommers و یا Uncles تشکیل شده است(شکل ۶). هدر بلاک، ضروری‌ترین جزء بلاک اتریوم است و شامل اطلاعات ارزشمندی است که در ادامه توضیح داده می‌شود:

Parent Hash: هشی ۲۵۶ بیتی keccak از هدر بلاک قبلی است.

Ommers Hash: هشی ۲۵۶ بیتی keccak از بلاک‌های Ommers موجود در بلاک است.

Beneficiary: این فیلد دربردارنده آدرسی ۱۶۰ بیتی از دریافت‌کننده جایزه معدن‌کاوی است و به محض اینکه بلاک به طور موفقیت‌آمیز کشف شد، دریافت می‌شود.

State Root: این فیلد شامل هشی ۲۵۶ بیتی از نود ریشه‌ی ترای حالت است و پس از پردازش و نهایی شدن تمامی تراکنش‌ها محاسبه می‌شود.

Transaction Root: این فیلد شامل هشی ۲۵۶ بیتی از نود ریشه‌ی ترای تراکنش است و این نود حاوی لیست تراکنش‌های

موجود در بلاک است.

Receipts Root: این فیلد هشی ۲۵۶ بیتی از نود ریشه ترای گیرنده تراکنش است. این ترای، ترکیبی از گیرنده‌های تمامی تراکنش‌های موجود در بلاک است. گیرنده تراکنش پس از پردازش هر تراکنش ایجاد می‌گردد.

Difficulty: درجه سختی بلاک فعلی است.

Number: نشاندهنده تعداد بلاک‌های قبلی است.

Gas Limit: این فیلد، محدودیت مصرف Gas در هر بلاک را نشان می‌دهد.

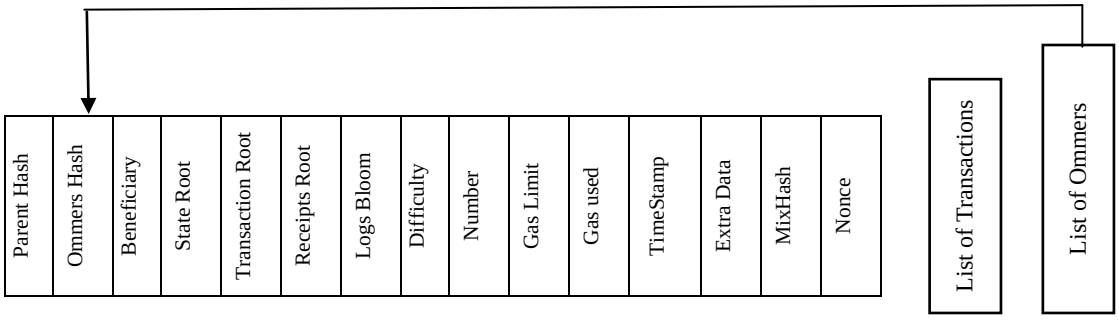
Gas used: مقدار کلی Gas مصرف شده جهت تراکنش‌های بلاک را نشان می‌دهد.

TimeStamp: فیلد برچسب زمانی، نشاندهنده زمان آغاز بلاک است.

Extra Data: جهت ذخیره داده دلخواه در هر بلاک است.

MixHash: این فیلد شامل هشی ۲۵۶ بیتی که با Nonce ترکیب شده و جهت اثبات انجام تلاش کافی برای ساخت بلاک به کار می‌رود.

Nonce : هشی ۶۴ بیتی است که در ترکیب با MixHash برای اثبات این مطلب که محاسبات کافی برای ایجاد بلاک انجام شده است به کار می‌رود[4].



شکل ۶-ساختار بلاک

۵- سیر تحول خدمات مالی با پیاده سازی قراردادهای هوشمند

وقتی بانک رویال اسکاتلند[۲۷] در سال ۲۰۰۹، تصمیم گرفت با ویلیامز[۲۸] معامله کند، دوره اختتام به صورت سنتی چند ماهه پیش‌بینی شد اما هفت سال بعد از فروش هنوز این معامله به سرانجام نرسیده بود. سیستم‌های ناکارآمد تا حدودی علل علاقه به بلاک‌چین و قراردادهای هوشمند را نمایان می‌سازند. قراردادهای هوشمند، قراردادهایی هستند که می‌توانند بخشی از توابع قرارداد را اجرایی سازند و وقتی این قراردادها بر روی بلاک‌چین و یا دفتر همگانی توزیع‌شده قرار می‌گیرند عناصر به شدت تأثیرگذاری همچون دوام و تغییرناپذیری نیز به آن اضافه می‌گردد.

[27] Royal Bank of Scotland
[28] Williams

در ماه‌های اخیر، اتحادی برای قرارداد هوشمند تشکیل شده، بانک‌ها و کنسرسیوم‌های صنعتی نمونه‌های اولیه‌ای را معرفی کرده‌اند و شرکت‌های فناوری کارگروه‌هایی جهت تقویت فناوری راه‌اندازی نموده‌اند و مجریان بانک‌ها به طور جدی پیگیر این امر هستند. رابرت منکون[۲۹] با خوشبین بودن نسبت به قراردادهای هوشمند می‌گوید "فناوری قراردادهای هوشمند پتانسیل فوق‌العاده‌ای دارد و مدل کسب وکار بسیاری از بخش‌های بانک‌ها را دگرگون خواهد ساخت و آن همچنین بسیاری از مشکلاتی را که بانک‌ها و قانونگذاران با آن مواجه‌اند حل خواهد نمود". او همچنین اذعان می‌دارد که "این صنعت هنوز باید آزمون کند و همانطور که تعهد داده است این اطمینان را حاصل نمایند که عوامل آن پایدار، خودکار و امن بوده و از جهات جغرافیایی، چارچوب‌های قانونگذاری و پیچیدگیِ دارایی مدیریت شده، تطابق داشته باشند[6].

۵-۱-محدودیت‌های قراردادهای فیزیکی

۵-۱-۱-افزایش هزینه‌های عملیاتی

در بازار وام سندیکایی[۳۰] تریلیون دلاری، هنوز هم بین شرکت‌کنندگان معمول است که از طریق فکس با همدیگر ارتباط برقرار کنند، و در سال ۲۰۱۲ باعث ارسال حدود ۴ میلیون فکس شده‌اند و این مقدار ارسال فکس از نظر سرپرست بازارهای اوراق بهادار، فابیان واندنریت[۳۱] نقص مهمی به شمار می‌آید. هنوز هم بخش‌های عظیمی از صنعت اوراق بهادار مانند وام‌های سندیکایی، دیجیتالی نشده‌اند و از طریق فکس و اسناد کاغذی فعالیت می‌نمایند. دیگر زمان آن فرارسیده است که گردانندگان صنعت این عدم کارایی را کنار گذارند و فناوری‌های جدید همچون قراردادهای هوشمند را به عنوان فرصتی برای دیجیتالی شدن در کوتاه مدت و کاهش هزینه‌های عملیاتی همراه با مدل‌های کسب و کار جدید در بلند مدت، به کار گیرند.

فرایندهای نامناسب اذهان شرکای بازار را به خود مشغول کرده و سرمایه آنان را مسدود ساخته است. به همین دلیل و به منظور به تصویر کشیدن مشکلات افزایش قراردادهای مالی سنتی، می‌توان به مثالی که در ادامه مطرح می‌شود اشاره نمود، در اکتبر سال ۲۰۱۳ سرمایه‌گذاران ۱,۲ میلیارد دلار به یک شرکت وام دادند و به مدت ۱۰ ماه بعد از این تاریخ هیچ بهره‌ای بابت آن دریافت نکردند.

۵-۱-۲- تأخیر و ریسک متمرکزِ مراجع مرکزی مانند اتاق پایاپای[۳۲]

به دنبال بحران مالی بین سال‌های ۲۰۰۷ تا ۲۰۰۹، طرفین معاملات مرکزی جهت کاهش دادن ریسک و اثر دومینو[۳۳] شکست‌های مؤسسات، به طور فزاینده‌ای درصدد تثبیت جایگاه خود در بین گردانندگان بازار درآمدند. اگر چه این موضوع ریسک سیستم مالی و تعامل آن را کاهش خواهد داد اما موجب تأخیر در فرایند تسویه و پایاپای قراردادهای مالی و رشد الزامات انطباقی می‌گردد. به طور مثال، تسویه قراردادها به غیر از ارز خارجی، با وقفه همراه است به علاوه، در بازار، هزینه‌های مرتبط نیز برای فعالیت‌های اداری و خدمات مؤسسات مرکزی وجود دارد. ASX، نماینده بورس اوراق بهادار در استرالیا، تخمین زده است که بازارهای سهام استرالیا در حدود ۴ الی ۵ میلیارد دلار هزینه AUD[۳۴] پرداخت می‌کنند و این مبلغ در نهایت به صادرکنندگان و سرمایه‌گذاران نهایی پرداخت می‌گردد.

با توجه به موارد ذکر شده، مشکلات فزاینده قراردادهای مالی سنتی را می‌توان در ۴ مورد زیر دسته‌بندی نمود:

[29] Roberto mancone
[30] syndicated loan market
[31] Fabian Vandenreydt
[32] Clearinghouses
[33] domino effect

[۳۴] دلار استرالیا (در انگلیسی Australian Dollar) نام واحد پول کشور استرالیا است.

- فرایندهای نامناسب و منسوخ شده: در سال ۲۰۱۲، بیش از ۴ میلیون فکس دریافتی منسوخ شده در خصوص وام سندیکایی وجود داشت.
- تأخیر در تسویه: میانگین زمان تسویه برای وام سندیکایی در امریکا بیش از ۲۰ روز و در اروپا بیش از ۴۸ روز است.
- تقلب: به عنوان مثال FBI هزینه کلی تقلب بیمه غیر سلامت[۳۵] را بیش از ۴۰ میلیارد دلار در سال تخمین زده است. همچنین ۲ میلیارد دلار هزینه تقلب در صنعت الماس[۳۶] در لندن.
- هزینه سربار: ASX هزینه‌های پرداختی بازار سهام استرالیا را که نهایتا به صادرکننده‌ها و سرمایه‌گذران نهایی پرداخت می‌گردد، ۴ الی ۵ میلیارد دلار تخمین می‌زند.
- ریسک‌های متمرکز: حجم پول مسدود شده در سیستم تسویه ناخالص آنی بریتانیا که به مدت ۱۰ ساعت آفلاین شد، بیلیون‌ها دلار ارزش داشت. ۲۷۷ میلیارد یورو در روز [6].

۵-۲-منافع استفاده از قراردادهای هوشمند برای بانک‌ها و مشتریان

قراردادهای هوشمند احتمالا برای حداقل هفت مورد خاص در بخش‌های مختلف خدمات مالی به کار گرفته خواهد شد.
موارد کلیدی کاربرد قراردادهای هوشمند در صنعت خدمات مالی عبارتند از:

۱)بازارهای سرمایه و بانکداری سرمایه‌گذاری[۳۷]

تامین مالی شرکتی:عرضه اولیه سهام، سرمایه‌گذاری خصوصی

تامین مالی ساختاریافته: وام‌های سندیکا و وام‌های اهرمی[۳۸]

زیرساخت بازار بورس اوراق بهادار

۲)بانکداری خرد و بانکداری تجاری[۳۹]:

تجارت بین‌الملل[۴۰]: مستندسازی زنجیره تامین، صورتحساب و پرداخت‌ها

قرض وام رهن[۴۱]

وام‌ها یا تأمین مالی جمعی برای استارتاپ‌ها و شرکت‌های کوچک و بزرگ

تأمین مالی جمعی برای سهام خصوصی در استارتاپ‌ها، یکی از موارد کلیدی بلاک‌چین به شمار می‌آید که اولویت روش‌های دیگر نیز می‌باشد. فیلیپ دنیس[۴۲] به بررسی دو مثال از این موارد می‌پردازد که بیشترین تأثیر را دارا است، تخمین تحلیل این نوع کسب‌وکارها حاکی از این است که اتوماسیون از طریق منطبق شدن با قراردادهای هوشمند، فرایندهای مرتبط و تغییرات سازمانی منافع اساسی را ایجاد خواهد کرد. این تخمین‌ها بر مبنای تحلیل تکنولوژی، تحلیل فرایندها و عناصر هزینه مقرراتی است که در محیط امروزی وجود دارد و با تکامل سیستم، این تخمین‌ها نیز تغییر خواهد یافت.

35 non-health insurance
36 diamond industry
37 Investment Banking
38 leveraged loans
39 Commercial and Retail Banking
40 Trade Finance
41 Mortgage Lending
42 Philippe Denis

مثال ۱: صرفه‌جویی با کاهش زمان تسویه وام سندیکا:

بازار وام اهرمی با مشکلات حادی روبرو است. درحالیکه معاملات اوراق قرضه با نرخ بازده بالا[۴۳] در T+3 روز تسویه می‌شود، دوره تسویه برای وام‌های اهرمی با هر مبلغی تقریبا ۲۰ روز طول میکشد. این مسئله ریسک بالا و چالش های نقدینگی در بازار وام اهرمی به دنبال خواهد داشت و به جذابیت و رشد آن صدمه می‌زند. از سال ۲۰۰۸، بازار جهانی وام اهرمی، شاهد رشد منفی بوده در حالیکه بازار اوراق قرضه با نرخ بازده بالا ، بالای ۱۱٪ رشد را تجربه کرده است. چنین سازمان‌هایی بر این باورند که قراردادهای هوشمند می‌تواند باعث کاهش دادن تأخیر در فرایندهای مستندسازی، تأیید فروشنده و خریدار، چک کردن قوانین Fatca، قوانین ضدپول‌شویی[۴۴] و شناسایی اولیه مشتری[۴۵] با کمک دفتر همگانی دارای مجوز شود.

دوره تسویه وام‌های اهرمی می‌تواند تا طیف T+10 و T+6 کاهش یابد و منجر به افزایش نقدینگی وام‌های اهرمی شود. تخمین‌زده می‌شود که با کاهش زمان‌های تسویه، اگر وام‌های اهرمی نصف وام‌های اوراق قرضه با بازده بالا یعنی در حدود (۵٪ تا ۶٪) میزان رشد داشته باشند، تقاضای بازار وام را با پیشرفت ۱۴۹میلیارد دلاری مواجه خواهند ساخت. این وام‌ها معمولا ۱٪ الی ۵٪ کارمزد سازمانی دارند که درآمدی در حدود ۱,۵ الی ۷,۴ میلیارد دلار برای بانک‌های سرمایه‌گذار به ارمغان خواهد آورد. به علاوه، هزینه‌های عملیاتی، سرمایه مورد نیاز جهت نظارت و هزینه‌های مربوط به خسارت تأخیر تأدیه در طول تسویه وام‌های اهرمی را با کوتاه شدن دوره تسویه، کاهش خواهند داد.

مثال ۲: افزایش سود صنعت رهن

فرایند وام اهرمی به اکوسیستمی پیچیده برای ایجاد، تامین و سرویس‌دهی رهن‌ها تکیه می‌کند که با خود هزینه و تأخیر به همراه دارد. روبرتو[۴۶] می‌گوید "حال حاضر، بهترین زمان برای حل مشکلات سیستماتیکِ پردازش وام‌های رهنی است. وام‌ها یکی از بهترین عوامل برای رشد به حساب می‌آیند اما در عین حال، پیچیدگی صنعت بانکداری خرد را نیز افزایش خواهند داد. این مسئله نیاز به بهبود کارایی فرایندها و خدمات داخلی دارد. قراردادهای هوشمند هزنیه و زمان مورد نیاز فرایند را از طریق اتوماسیون، بازطراحی فرایند و دسترسی تمامی طرفین قرارداد به اسناد فیزیکی حقوقی، کاهش خواهد داد و این امر را از طریق به اشتراک گذاشتن این اسناد و دسترسی به اطلاعات بیرونی انجام می‌دهد.

تحقیقات صورت گرفته اخیر در مورد اتوماسیون پشت باجه بانکی[۴۷] پیش بینی می‌کند که وام دهندگان رهنی می‌توانند از طریق سیستم‌های مدیریت فرایند کسب و کار، پلتفرم‌های بانکداری متمرکز الکترونیکی[۴۸] و نیز سیستم‌های مدیریت اسناد[۴۹] هزینه‌های خود را بین ۶٪ الی ۱۵٪ کاهش دهند. این اعداد در کنار تجربه و بحث‌های صورت گرفته با مجربان صنعت، موجب کاهش دادن هزینه‌های فرآیندهای وام‌دهی می‌شود. برای مثال در بازار مسکن آمریکا، تقریبا ۶,۱ میلیون خانه در سال ۲۰۱۵ به فروش رسید. بر اساس میانگین‌های آماری، ۶۴٪ از صاحب خانه‌ها با وام رهنی این خانه‌ها را خریده بودند و تخمین زده شد که وام دهندگان حداقل ۱,۵ میلیارد دلار از طریق اتوماسیون فعالیت‌ها برای سازمان‌های خود صرفه‌جویی به همراه خواهند داشت. بر طبق شکل ۵. به علاوه، در صورتی که شرکای خارجی از قبیل سازمان‌های ارایه‌دهنده امتیاز اعتباری[۵۰]، ادارات ثبت

[43] High-Yield Bond trades
[44] Anti-money laundering
[45] Know your customer
[46] Roberto Mancone
[47] banking back-office automation
[48] core banking platforms
[49] document management systems
[50] credit scoring companies

املاک[51] و مراجع مالیاتی[52] از طریق بلاک‌چین قابل دسترسی باشند با تسهیل فرایندهای سریعتر و کاهش هزینه‌ها در حدود ۶ میلیارد دلار صرفه‌جویی خواهد شد.

همچنین تخمین زده می‌شود که با انطباق قراردادهای هوشمند، هزینه‌های پردازش وام رهنی مشتریان حدود ۱۱٪ الی ۲۲٪ کاهش خواهد یافت. در واقع، به ازای هر وام مبلغ ۴۸۰ تا ۹۶۰ دلار صرفه‌جویی خواهد شد؛ میانگین هزینه پردازش ۴۳۵۰ دلار است. میزان وام‌های معلق[53] در سال ۲۰۱۴ در کشورهای ایالات متحده و اروپا ۲۰,۹۸ میلیارد دلار بوده است. در مورد بازار رهن آمریکا و اروپا، قراردادهای هوشمند می‌تواند در فرایند جدید ایجاد وام رهنی به طور بالقوه بین ۳ الی ۱۱ میلیارد دلار کاهش هزینه داشته باشند.

در ادامه می‌توان به تأثیر مثبت بر سود خالص از طریق کاهش هزینه های خدمات و اداری نیز اشاره نمود. قراردادهای هوشمند با خودکار نمودن فرایندهای کسب‌وکار در کوتاه مدت و احتمالا کلیه فرایندها در بلند مدت، به طور قابل توجهی هزینه‌های مربوط به انطباق، نگهداری سوابق و مداخله دستی را کاهش می‌دهد. قدرت و منفعت این تکنولوژی بیشتر از کاهش هزینه‌ها، ریسک‌ها، نرخ‌های خطا و فرایندهای مغایرت‌گیری است چرا که امکان داشتن زیرساختی مشترک را برای اعضاء فراهم می‌کند و منجر به آزاد نمودن سرمایه و گزارش‌دهی قانونی می‌گردد[6].

۵-۳-ملزومات پیاده‌سازی قراردادهای هوشمند در صنعت خدمات مالی

تکنولوژی که لازمه‌ی قراردادهای هوشمند است به سرعت در حال تکامل است. قابلیت‌هایی از قبیل پرداخت‌های چند امضایی[54]، خدمات escrow و غیره قبلاً برای قراردادهای هوشمند انجام شده‌اند اما هنوز شکاف‌هایی برای حل شدن وجود دارد. چالش‌های کلیدی‌ای که مانع از منطبق شدن قراردادهای هوشمند هستند به چهار دسته ذیل تقسیم می‌شود.

- چالش‌های سازمانی: حکمرانی بلاک‌چین‌ها[55]، کمبود هوش در قراردادهای هوشمند
- چالش‌های قانونی: چالش‌های قانونی در قانون‌های قابل دسترسی
- چالش‌های تکنولوژیکی: مقیاس‌پذیری[56] در سرعت اجرا، قابلیت همکاری با سیستم‌های قانونی
- چالش‌های مشترک: عدم انعطاف قراردادهای هوشمند، خصوصی بودن و امنیت کاربران و تراکنش‌ها

۵-۳-۱-قابلیت همکاری با سیستم‌های قانونی و داده خارجی

صنعت خدمات مالی به شدت نظام‌مند است، مجوزها و تأییدیه‌ها به سازمان‌ها جهت شرکت در یک بازار مبتنی بر دفتر همگانی توزیع‌شده، ارسال گردیده است. به عنوان مثال، کمیسیون بورس و اوراق بهادار ایالات متحده[57] اخیراً سایت خرده-فروشی اینترنتی Overstock.com را جهت صدور سهام شرکت بر روی پلتفرم مبتنی بر بلاک‌چین بیت کوین تأیید نموده است. با این حال، قانونی بودن قراردادهای هوشمند تاکنون منتشر نشده است. مراحل اولیه این امر در ایالت ورمونت آمریکا[58] به منظور به رسمیت شناختن دفاتر همگانی تویع شده در دادگاه‌های ایالتی، در حال انجام است. همچنین ترجمه دقیق مفاد و شرایط قانونی کدهای نرم‌افزاری، جنبه کلیدی دیگری است که باید در نظر گرفته شود. استارتاپ‌هایی مانند

[51] land registry offices
[52] tax authorities
[53] outstanding mortgage loans
[54] multi-signature payments
[55] Governance of blockchains
[56] Scalability
[57] US Securities and Exchange Commission
[58] State of Vermont

CommonAccord در حال خلق سیستمی هستند که بتواند مستندات قانونی را به طور خودکار برای قراردادهای هوشمند ترجمه کنند و باعث تسهیل نمودن تفسیر این قراردادها برای وکلا و توسعه‌دهنگان می‌شود. قانونگذاران، تنظیم‌کنندگان و دولت‌ها به دنبال محقق نمودن پتانسیل دفاتر همگانی توزیع‌شده، جهت افزایش دادن شفافیت و سهولت در انطباق و گزارش-دهی هستند.

همچنین سؤالات قابل توجهی در خصوص اقدامات پیش‌نیاز و سرمایه لازم جهت پیاده‌سازی قراردادهای هوشمند مطرح می-شود. توماس هاردجونو معتقد است "موقعی که یک شرکت یا یک بانک بزرگ در تلاش برای تعریف و استقرار یک تکنولوژی جدید است، می‌بایست برای این امر هزینه کند و مدیران در این خصوص ROI[59] را محاسبه می‌کنند. اما در مورد بلاک‌چین مسئله، نحوه محاسبه شدن ROI است؟ چه میزان سرمایه لازم است؟ و آیا این اقدام مقرون‌به‌صرفه است یا خیر؟

قراردادهای هوشمند همچنین باید قادر به کارکردن با پایگاه داده‌های مورد اعتماد دنیای بیرون باشند. این قراردادها با کمک اوراکل‌ها به این داده‌ها دسترسی پیدا می‌کنند اوراکل‌ها برنامه‌هایی هستند که داده‌های مورد نیاز قراردادهای هوشمند دنیای بیرون را فراهم می‌کنند. سرجی نازارو[60]، استارتاپی که به ساخت اوراکل‌ها می‌پردازد در خصوص کلیدی بودن داده‌های بیرونی می‌گوید: "ما در حال خلق قرادادهایی هوشمندی هستیم که قادر به برقراری ارتباط با دنیای بیرون باشد. اکثر قراردادها به داده‌هایی همچون آب و هوا، دما، حمل و نقل و مشتریان نیاز دارد و اوراکل‌ها توانسته‌اند این نیاز را با فراهم نمودن داده‌های امن و قابل اطمینان بودن، مرتفع سازند."

۵-۳-۲-قراردادهای منعطف‌تر

قراردادهای هوشمند برنامه‌های نرم افزاری هستند که بر روی دفاتر همگانی توزیع‌شده، نوشته می‌شوند و این بدان معنی است که اگر قراردادی نوشته شود دیگر قابل تغییر نخواهد بود و همین ویژگی باعث به وجود آمدن مشکل در بسیاری از سناریوهای دنیای واقعی می‌شود. پروفسور دانشگاه کرنل[61]، آری جونز[62]، چگونگی تغییر دادن مفاد قرارداد را بعد از نوشته شدن مورد بررسی قرار می‌دهد. حقوق قراردادها، قوانینی را جهت اعمال تغییر یا لغو قراردادها در نظر می‌گیرد. مکانیسم‌های فنی در قراردادهای هوشمند می‌تواند نتایج مشابهی را دربرداشته باشد. یک رویکرد می‌تواند در نظر گرفتن یک "راه فرار[63]" و در واقع یک "راه برنامه ریزی" شده برای ایجاد تغییر در مفاد قرارداد باشد. در این راستا، ارائه مجوز و نیز پیاده‌سازی صحیح باعث پیچیدگی فرآیند می‌شود. لذا نیاز به استخراج تکنیک‌هایی جهت ارتقاء یا تغییر قراردادها بر حسب ضرورت در طول اجرای قرارداد است.

۵-۳-۳-مقیاس‌پذیری تراکنش‌ها

در تراکنش‌هایی مانند وام‌های سندیکا و وام‌های رهنی که سرعت بالا مطرح نیست، در حال حاضر، دفاتر همگانی دارای مجوز از محبوبیت بیشتری برخوردارند و این بدین دلیل است که برای اجماع به اعضای کمتری نیاز است و لذا زمان لازم جهت اجماع و اجرای تراکنش‌ها کاهش می‌یابد. پروفسور آری جونز می‌گوید: "گردانندگان صنعت احتمالاً به دلایلی که در ادامه ذکر خواهد شد از بلاک‌چین‌های دارای مجوز استفاده خواهند کرد. اولین دلیل؛ اینکه بلاک‌چین‌های دارای مجوز در مقایسه با بلاک‌چین‌های بدون مجوز، به طور راحت‌تری با الزامات قانونی تطابق پیدا می‌کنند. دومین دلیل؛ بلاک‌چین‌های دارای مجوز،

[59] Return on investment
[60] Sergey Nazarov
[61] Cornell University
[62] Ari Juels
[63] escape hatch

مکانیزم‌های حکمرانی و اجماع قوی‌تری را ارائه می‌دهند. سومین دلیل؛ بلاک‌چین‌های دارای مجوز از مزایای عملکردی قابل توجهی برخوردارند.

علاوه بر این، آزمایشاتی در خصوص مکانیزم‌های اجماع در حال انجام است که امکان پردازش موازی تراکنش‌ها را فراهم می‌کند. توماس می‌گوید: "یکی از زمینه‌های تحقیقاتی مورد علاقه در دانشگاه ام‌آی‌تی[64]، یافتن الگوریتم‌های اجماع برای تکنولوژی بلاک‌چین و قراردادهای هوشمند است."

۵-۳-۴-سبد استعدادها[65]

کمبود استعداد و قابلیت در زمینه بلاک‌چین و قراردادهای هوشمند در شرکت‌های خدمات مالی وجود دارد. به طور مثال، شرکت‌ها ممکن است نیاز به استخدام وکلای برنامه‌نویس-ترکیبی نادر از مهارت‌ها(قانون و برنامه‌نویسی)- داشته باشند. سازمان‌ها نیاز به برنامه‌هایی جهت توسعه مهارت‌های نیروی انسانی خود دارند. تعدادی از استارتاپ‌ها اقدام به پشتیبانی آموزشی از پلتفرم‌های خود کرده‌اند. همانطورکه برین اشاره می‌کند: "کسب دانش و مهارت در این مرحله ضروری است. ما آموزش‌هایی برای توسعه‌دهندگان جهت فهم بلاک‌چین و قراردادهای هوشمند برگزار نموده‌ایم تا نحوه ایجاد کردن برنامه‌های قراردادهای هوشمند در سطح کلان سازمانی را فرابگیرند. یک راه‌حل بالقوه دیگر، می‌تواند همکاری با دانشگاه‌ها برای تحقیقات بیشتر و نیز پرورش استعدادها باشد. دانشگاه‌های برتر همچون ام‌آی‌تی، استنفورد[66]، کرنل و آکسفورد[67] گروه‌های تحقیقاتی به بلاک‌چین و قراردادهای هوشمند تخصیص داده‌اند و تعدادی از آن‌ها شروع به پیشنهاد دوره‌هایی در این خصوص نموده‌اند.

۵-۳-۵-نیازهای امنیتی و محرمانگی قرارداد

محرمانگی قراردادهای هوشمند ممکن است بر پایه بلاک‌چین برای سازمان‌ها بسته به داشتن یا نداشتن مجوز چالش‌برانگیز باشد. به دلیل اینکه رکوردهای تراکنش‌ها برای تمامی اعضا قابل رؤیت است قاعدتاً بانک‌ها تمایلی به حضور در پلتفرم‌های اجرایی مشترکی که امنیت و خصوصی بودن داده‌ها را حفظ نمی‌کند، ندارند و به همین دلیل ضروری است که کلید رمزنگاری، جهت پنهان کردن جزئیات تراکنش از سوی طرفین ناشناس، مدیریت شود. لذا باید به سؤالاتی از قبیل اینکه چه داده‌هایی باید بین تمامی اعضا به اشتراک گذاشته شود؟، چگونه می‌توان از امنیت و اعتبار داده‌های تأمین شده توسط اوراکل‌ها اطمینان یافت؟، پاسخ داده شود.

از پروژه‌های در حال انجام در خصوص محرمانگی قرارداد، می‌توان به پروژه MIT Enigma که در تلاش است با استفاده از ساختارهای رمزنگاری پیشرفته به حل مشکل حفظ حریم خصوصی در شرایط به اشتراک گذاری داده‌ها بپردازد اشاره نمود. به طور مشابه، مفهوم آشنایی به نام "اثبات دانایی صفر[68]" به دنبال راهی برای تأیید تراکنش، بدون رؤیت محتوای آن است[6].

۶- ارائه پیشنهاد برای استفاده از قراردادهای هوشمند بر بستر بلاک‌چین در شرایط تحریم ایران

یکی از کاربردهای این قراردادها که در شرایط تحریم به صنعت واردات و صادرات کشور یاری خواهد رساند، اعتبار اسنادی[69] است. که به اختصار شرح داده می‌شود. اعتبار اسنادی، یک وسیله پرداخت در مبادلات بین‌المللی و یکی از خدماتی است که

[64] MIT
[65] Talent Pool
[66] Stanford
[67] Oxford
[68] zero knowledge proofs
[69] Letter of Credit

به موجب آن (بانک گشایش کننده) بنا به درخواست مشتری (متقاضی اعتبار/خریدار) و یا از طرف خود موظف می شود به منظور خرید یا سفارش کالا یا خدمات در مقابل اسناد مقرر و مطابق با شرائط اعتبار، پرداختی را به شخص ثالث (ذینفع/فروشنده) یا به حواله کرد او انجام دهد یا به بانک دیگر اجازه پرداخت یا معامله دهد. این فرایند همانطور که در شکل ۷ قابل مشاهده است، شامل چهار عضو (شکل ۴) می‌باشد:

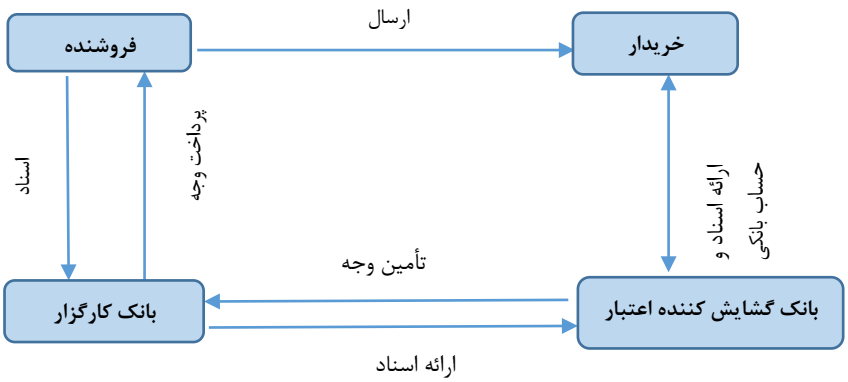
گشایش کننده اعتبار (خریدار): شخصی است که قصد واردات کالا از کشور دیگری دارد و برای گشایش اعتبار اسنادی به بانک مراجعه می کند.

بانک گشایش کننده اعتبار: بانکی است که به درخواست خریدار کالا اقدام به گشایش اعتبار اسنادی می‌کند.

بانک کارگزار: بانکی است که با بانک گشایش کننده اعتبار، در ارتباط بوده و از طرف خریدار و بانک گشایش کننده اعتبار ،پرداخت وجه کالا به فروشنده را تعهد می‌کند.

ذینفع اعتبار اسنادی(فروشنده کالا): شخصی است که پس از ارسال کالا و ارائه مدارک مورد توافق طبق شرایط اعتبار اسنادی وجه اعتبار را از بانک کارگزار دریافت می‌کند.

با استفاده از قراردادهای هوشمند، خریدار و فروشنده مستقیماً بدون نیاز به هیچ واسطی قادر به انجام معامله هستند. فروشنده بر حسب معیارهای تعیین شده، تأییدیه‌ای در خصوص پرداخت وجه توسط خریدار در زمان مناسب، دریافت می‌کند. کالا از طریق QR-code به قرارداد هوشمند لینک شده و در صورتی که کالا در زمان و مکان مورد توافق به دست خریدار برسد، قرارداد هوشمند به طور خودکار اجرا و وجه از حساب خریدار کسر شده و به حساب فروشنده انتقال می‌یابد[7].



شکل ۷-فرایند کلی اعتبار اسنادی(منبع:Scotiabank)

۷-جمع بندی

با توجه به تحقیقات صورت گرفته در مورد جزئیات بحث با متخصصان صنعت خدمات مالی، استارتاپ‌های برجسته‌ی قراردادهای هوشمند و آکادمی‌های مورد بررسی می‌توان نتیجه گرفت که پیاده‌سازی قراردادهای هوشمند موجب کاهش ریسک، کاهش هزینه‌های اداری و خدماتی و نیز باعث افزایش کارایی فرایندهای کسب و کار در تمامی بخش‌های صنعت خدمات مالی می‌گردد. چنین منافعی از تکنولوژی، با طراحی فرایندها و اعمال تغییرات بنیادی در مدل‌های عملیاتی میسر می‌گردد چرا که نیاز است طرفین تجارت، به درک مشترکی نسبت به قراردادها برسند. در این صورت، مصرف‌کنندگان علاوه

بر بهره‌مندی از فرایندهای ساده‌تر که عاری از هرگونه نگرانی است، منافعی نیز در رابطه با محصولات رقابتی مانند وام‌های رهنی عایدشان خواهد شد. همچنین باید توجه داشت که تبلیغات وسوسه‌انگیز در حوزه تکنولوژی قراردادهای هوشمند نباید مانع بررسی وجود نیاز و یا عدم نیاز به این تکنولوژی گردد. مؤسسات مالی با شکل‌دهی شراکت‌های استراتژیک [۷۰] قادر خواهند بود بر چالش‌های مرتبط با استعداد و نوآوری که در این حوزه وجود دارد فائق آیند. لذا همکاری بین آزمایشگاه‌های نوآوری [۷۱]، مراکز رشد [۷۲] و استارتاپ‌ها در راستای تلاش برای ایجاد نوآوری ضروری است.

منابع

[1] Cant, B. Vergn, C. Evan, C. Weime, M. (2015), بBlockchain: A Fundamental Shift for Financial Services Institutionsپ Capgemini Consulting, Available at https://www.capgemini.com/wp-content/uploads /2017/07/blockchain_pov_2015.pdf

[2] Frantz, C. and Nowostawski[73], M. (2016), بFrom institutions to code: towards automated generation of smart contractsپ In: Workshop on Engineering Collective Adaptive Systems (eCAS), Available at http://ieeexplore.ieee.org/abstract/document/7789470/.

[3] Cong, L. He, Z. (2017), بBlockchain Disruption and Smart Contractsپ SSRN, Available at https://ssrn.com/abstract=2985764.

[4] Bashir, I. (2017), بMastering Blockchainپ Packt Publishing, Available at https://www.safaribooksonline.com/library/view/mastering-blockchain/9781787125445/

[5] Madeira, A. (2017), بWhat is the GHOST protocol for Ethereum?پ Crypto Compare, Available at https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/

[6] Cant, B. Khadikar, A. Ruiter, A. Bronebakk, J. Coumaros, J. Buvat, J. Gupta, A. (2016), بSmart Contracts in Financial Services: Getting from Hype to Realityپ Capgemini Consulting, Available at https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/smart-contracts.pdf

[7] Reilich, L. (2016), بWhy Ethereum Is a Better Letter Of Creditپ Market Mogul, Available at https://themarketmogul.com/why-ethereum-is-a-better-letter-of-credit/.

[70] strategic partnerships
[71] innovation labs
[72] Incubators