پاییز ۱۴۰۰، دوره ۶، شماره ۳، پیاپی ۲۲
DOR :20.1001.1.2538161.1400.6.3.5.7

دریافت مقاله: ۱۳۹۹/۰۹/۳۰
پذیرش مقاله: ۱۴۰۰/۰۵/۲۳

نوع مقاله: پژوهشی

اعمال ضوابط قانونی در قراردادهای هوشمند مبتنی بر بلاک‌چین*

علیرضا علیخانی
گروه مهندسی کامپیوتر، دانشگاه بین‌المللی امام خمینی(ره)،
a.alikhani@edu.ikiu.ac.ir

حمیدرضا حمیدی**
گروه مهندسی کامپیوتر، دانشگاه بین‌المللی امام خمینی(ره)،
hamidreza.hamidi@eng.ikiu.ac.ir

چکیده

قرارداد هوشمند پروتکلی دیجیتالی (کُد نرم‌افزاری) است که امکان انجام خودکار نظارت‌ها و اجرای مفاد قراردادها بدون نیاز به واسطه‌ها را فراهم می‌آورد. فناوری بلاک‌چین حذف مجری و یا ناظر در قراردادها را از طریق یک دفتر کل توزیع شده فراهم می‌کند امّا شیوه‌ای مطمئن برای اعمال ضوابط قانونی ندارد. به‌عنوان نمونه در شبکه‌ای مانند بیت‌کوین امکان انجام فعالیت‌های غیرقانونی مانند پول‌شویی و خرید و فروش اسلحه وجود دارد و همچنین هزینه‌های قانونی مانند مالیات و عوارض قابل حسابرسی و اعمال نیست. در این پژوهش طرحی ابداع شده است که به مجریان و ناظران قانونی اجازه اعمال ضوابط و حسابرسی را می‌دهد در حالی که فرآیند اجرایی قراردادِ هوشمند، خودکاری مناسب را حفظ می‌کند. در این مقاله پنج چالش مهم در اعمال ضوابط قانونی بر روی بلاک‌چین مطرح شده است: اعتبارسنجی طرفین قرارداد، اعتبارسنجی ماهیت کالا، وصول هزینه‌های قانونی، اعمال قوانین سرزمینی و حسابرسی. در پژوهش‌های جدید تلاش‌هایی برای پاسخگویی بعضی از آن‌ها انجام شده است. ایده پیشنهادی این مقاله راهکاری جهت پاسخگویی همه نیازها برای اعمال ضوابط قانونی است. طرح پیشنهادی بر روی شبکه اتریوم پیاده‌سازی شده است. نسل فعلی قراردادهای هوشمند برای تضمین اجرای صحیح طرح پیشنهادی دو محدودیت دارد؛ فراخوانی خدماتِ بیرونی از داخل قرارداد هوشمند ممکن نیست و برقراری اتصال بین قراردادهای هوشمند خودکار نیست.

واژه‌های کلیدی: قرارداد هوشمند، بلاک‌چین، اعمال ضوابط قانونی، اتریوم، رمز ارز.

۱- مقدمه

فناوری اطلاعات در حوزه کسب‌وکارها عموما مبتنی بر ساختارهای متمرکز نظیر کارخواه-کارساز[1] بنا می‌شود [۱]. که در آن هر سازمان از طریق یک سامانه نرم‌افزاری به‌صورت مستقل به ثبت تراکنش‌های خود می‌پردازد و در صورت نیاز به اطلاعات بین سازمانی، اطلاعات بین سامانه‌ها قابل انتقال است. به‌عنوان مثال بین دو شرکت، فاکتورها و معین حساب به‌صورت جداگانه نگهداری می‌شود. این شیوهٔ سنتی می‌تواند گران باشد

1-Client server

* این مقاله مستخرج از رساله کارشناسی ارشد نویسنده اول در دانشگاه بین‌المللی امام خمینی(ره) است.
** نویسندهٔ مسئول

زیرا واسطه‌هایی نیاز است که برای خدمات هزینه دریافت می‌کننـد [۲]. این کار بـه دلیل بروز تاخیرهـا در اجرای توافقنامه‌هـا و دوباره‌کاری‌های لازم برای نگهداری تعداد زیـادی دفترکل، ناکارآمد اسـت. این کار آسـیب‌پذیر هم هست، چرا که اگر سـامانهٔ مرکزی (برای مثال، یک بانک) به دلیل کلاهبرداری، حملهٔ سـایبری یا اشـتباهی کوچک به خطر بیفتد، کل شـبکهٔ کسـب وکار از آن متاثر خواهد شد [۱].

بلاک‌چین یک دفترکل توزیع شـده و مشترک است که کار فرآیند ثبت تراکنش‌ها و ردگیـری یا پیگیری دارایی‌ها را در یک شـبکهٔ کسب وکار خودکار می‌کند [۳]. یک دارایی می‌تواند به‌طور ملموس خانه، خودرو، پول نقد و زمین باشد یا به‌صورت ناملوس مانند مالکیت معنوی نظیر حق اختراع، حق چاپ یا نشـان تجاری باشد. تقریباً هر چیز ارزشمندی را می‌توان در یک شبکهٔ بلاک‌چین ردگیری و معامله کرد و مخاطرات و هزینه‌ها را برای طرف‌های درگیر در این شبکه، کاهش داد [٤]. منظور از دفتر کل توزیع شـده این است که پایگاه‌داده‌ای وجود دارد که به ثبت تراکنش‌های موجود در شـبکه پرداخته و نکته حائز اهمیت آن عدم تمرکز اسـت و منظور از مشترک بودن این است که نسخه‌ای از این اطلاعات (دفتر کل) در اختیار تمام کاربران موجود در شبکه است که شفافیت را در بستر شبکه افزایش می‌دهد [٥]. یکی از اولین کاربردهای بلاک‌چیـن، ارز دیجیتال (رمز ارز)[۲] بیت کوین[۳] است که در سال ۲۰۰۹ ارائه شده است [٦].

امـروزه به‌کارگیری فنـاوری بلاک‌چیـن از محدوده تعاملات مالی مسـتقیم (نظیر رمز ارزها) فراتر رفته است و هرگونـه تعاملات و یـا قراردادها را می‌تواند پوشـش دهـد. اصطلاح قرارداد هوشـمند[٤] به مدلـی از قراردادها گفته می‌شـود که در آن مراحل مختلـف تعاملات طرفین به‌صورت نرم‌افزاری و خودکار انجام می‌شـود و نیاز به حضور عامل واسـط برای نظارت و کنترل ندارد. فناوری بلاک‌چین توانسته است پیاده‌سازی قراردادهای هوشمند را حتی از نظر سـاختار نرم‌افزاری به‌صورت غیرمتمرکز درآورد. شـبکه اختصاصی اتریوم[٥] بستری مناسب برای اجرای قراردادهای هوشـمند به‌وجود آورده است. مزیت ایـن فناوری برای پیاده‌سـازی قراردادهای هوشـمند را می‌توان به شرح زیر طرح نمود [۷، ۸، ۹]:

- صرفه‌جویی در زمان: سرعت انجام تراکنش‌های پیچیده به حداقل رسـیده زیرا دیگر نیاز به یک سامانه متمرکز برای تایید نیست.
- صرفـه جویی در هزینـه: از آنجاکه نظـارت و کنترل نرم‌افزاری اسـت، نیـاز به حضور واسـطه را کاهش می‌دهد.
- امنیت بالا: اسـتفاده از روش‌هـای رمزنگاری اطلاعات و توزیع شـدن دفتر کل موجب شده احتمال دستکاری اطلاعات بسیار کاهش یابد.
- بهبود حسابرسـی: به دلیل وجود یک دفتر کل مشترک صرفنظـر از تعدد عامل‌هـای موثر در قـرارداد، عمل حسابرسی آسان‌تر و کامل‌تر خواهد بود.
- بهبود حریم شخصی: حذف واسطه‌ها می‌تواند موجب حفاظت بیشتر از حریم شخصی شود.
- انعطاف‌پذیـری: خـودکار شـدن فرآیندهـای کنترلی و نظارتـی موجب می‌شـود بروزرسـانی و تغییر در فرآیندهای قرارداد با سهولت بیشتری قابل اعمال باشد.

به‌عنوان مثال بیت‌کوین یک دفترکل عمومی و شفاف را که امن و قابل‌اعتماد است برای تعامل ارز دیجیتالی ایجاد کرده اسـت. مالکیت افراد بر بیت‌کویـن از طریق قرارداد هوشمند متناظر کنترل می‌شود [٦].

قرارداد هوشـمند مبتنی بر بلاک‌چین امکان اعمال همه کنترل و نظارت‌ها را ندارد. به‌عنوان مثال یک دستگاه فروش خودکار را درنظر بگیریم. اگر دسـتگاه بخواهد نوشابه را توزیع کند مشکلی ایجاد نمی‌شود، مشتری هزینه را تامین می‌کند و دسـتگاه کالا را تحویل می‌دهد. امّا اگر دسـتگاه برای توزیع مواد مخدر اسـتفاده شود، چالش‌های حقوقی ایجاد می‌شـود. اعتبارسـنجی طرفین قـرارداد و ماهیت

2- Cryptocurrency.
3- Bitcoin: www.bitcoin.org
4- Smart contract.
5- Ethereum: www.ethereum.org

کالا، پرداخت هزینه‌های قانونی، اِعمال قوانین سرزمینی و حسابرسی تراکنش‌ها از چالش‌هایی است که در این پژوهش مورد توجه قرار گرفته است.

در بخش بعد پژوهش‌هایی که تلاش کردند چالش‌های حقوقی تراکنش‌های بلاک‌چین را مورد توجه قرار دهند و بسته به کاربرد به آن بپردازند، مرور می‌کنیم. سپس در بخش ۳ ایده اَبَرقرارداد هوشمند را از طریق یک کاربردِ عملی پیاده‌سازی شده معرفی می‌کنیم و توانایی آن در برخورد با چالش‌های مطرح شده را ارزیابی می‌کنیمن در برخورد با چالش‌های قانونی می‌پردازیم.. این مقاله با جمع‌بندی و شرح کمبودهای نسل فعلی فناوری قرارداد هوشمند، به پایان می‌رسد.

۲- پژوهش‌های مرتبط

اولین چالش برای اعمال ضوابط این است که روش «اعتبارسنجی طرفین قرارداد» در شبکه‌ای مبتنی بر بلاک‌چین به چه صورت امکان دارد؟ زیرا در یک نمونه شناخته‌شده بلاک‌چین، مانند بیت‌کوین، همه اشخاص اجازه ورود دارند و از طریق یک نشانی به تبادل پول و ایجاد تراکنش می‌پردازند [٦]. از همین رو شناسایی این افراد دشوار بوده و در بیشتر مواقع مشخص نیست چه شخص حقیقی/حقوقی از آن نشانی برای انتقال دارایی یا پول استفاده می‌کند. در نتیجه اعمال ضوابط قانونی مانند کسر مالیات از طرف‌های معامله پیچیده و گاه غیر ممکن می‌شود. در بیشتر پروژه‌ها مانند هایپرلجرفبریک[6] [٥] یا اینشورچین[7] [١٠] تلاش می‌کنند تا کاربران در شبکه شناخته شده باشند. به‌عنوان مثال در پروژه اینشورچین کاربران باید با اطلاعات واقعی خود در شبکه شرکت کنند و با آگاهی به معاملات بپردازند. ولی در اتریوم کاربران نیازی به شناخته شدن ندارند و هرکسی می‌تواند در شبکه شرکت کند.

چالش دوم این است که اگر از بلاک‌چین برای معامله کالایی استفاده شود، آنگاه «ماهیت کالا» ممکن است به کنترل قانونی نیاز داشته باشد. به‌عنوان مثال در یک مغازه لوازم تحریر فروشی، صاحب امتیاز این مغازه مجاز به فروش محصولات خوراکی نیست و تنها مجاز به فروش لوازم تحریر است. چگونه می‌توان ماهیت کالای مورد معامله را کنترل قانونی کرد؟ چگونه می‌توان از فروش غیر قانونی محصولات قاچاق مانند مواد مخدر و اسلحه جلوگیری کرد؟ تنها پروژه‌ای که برای این سوال طرحی را ارائه کرده است، پروژه زنجیره تامین محصولات (پرووِننس)[8] است [١١]. در این پروژه به کمک برنامه استانداردی که طراحی شده اجازه داده می‌شود نمونه یا دسته‌ای از کالاها در بلاکچین اضافه یا پردازش شوند. تولیدکننده برای استفاده و تولید یک محصول خاص باید استاندارد آن را دریافت نماید. تولید کننده درخواست خود را برای تولید محصولی ارائه می‌دهد و در صورت تایید توسط حسابرسان یا بازرسان، استاندارد مورد نظر به تولیدکننده داده می‌شود. این حسابرسان با بازدید حضوری از شرکت تولید کننده، مجوز مربوطه را صادر می‌کند و تمام این موارد درشبکه ثبت می‌شود.

چالش سوم این است که چگونه می‌توانیم «هزینه‌های قانونی» مانند عوارض، جریمه‌های مالی و مالیات در یک تراکنش را محاسبه کرده و آن را از طرفین قرارداد وصول کنیم و به حساب‌های قانونی واریز کنیم؟ برای حل این مشکل چند سوال دیگر هم رخ می‌دهد. به‌عنوان مثال به چه حسابی واریز شود یا چه کسی کنترل این حساب را دارد؟ با بررسی صورت گرفته در پروژه‌های مختلف، تاکنون طرحی برای این چالش ارائه نشده است.

چالش چهارم پیش روی اعمال ضوابط در تراکنش‌های بلاک‌چین، «اعمال قوانین سرزمینی» است که در هر کشور و ایالتی متفاوت است. اگر از یک دفتر کل عمومی برای یک شبکه جهانی استفاده کنیم، نیاز به روشی انعطاف‌پذیر نسبت به قوانین سرزمینی وجود دارد. در بیشتر پروژه‌ها ساختاری ثابت برای انجام هدف مورد نظر طراحی شده

6- Hyperledger Fabric.
7- InsurChain.
8- https://www.provenance.org/

است. به‌عنوان مثال پروژه پروونِنس می‌گوید تمام قوانین خاص در برنامه استاندارد انجام می‌شود. در صورتی که این امکان وجود داشته باشد که برنامه استاندارد قابل تغییر باشد می‌توانیم بگوییم که با توجه به نیاز هر کشور طراحی شـــود. ولی اگر این طور نباشد فقط توانایی استانداردهای مختلـف در زمینـــه زنجیـــره تامین را خواهد داشـــت. در پروژه اینشـــورچِین سیاست‌های بیمه‌ای توسط بیمه‌گران یا افراد متخصص در این زمینه به‌عنوان یک سیاســـت در ســـامانه ثبت می‌شـــود. در نتیجه با توجه به قوانین محلی هر کشور متخصصان آن منطقه بر اساس قوانین موجود، سیاســـت‌های بیمه‌ای متفاوتی را می‌توانند در سامانه ثبت نماینـــد. کاربران هم در خرید محصولات آزاد می‌باشـــند و محصول بیمه‌ای را خریداری می‌کنند که مناســـب آن‌ها باشـــد. لذا این امکان وجود دارد که سیاست‌های مختلف با توجه به قوانین هر کشوری انجام شود.

آخرین چالشـــی که در این مقاله مورد بررســـی قرار می‌گیرد، «حسابرســـی» اســـت که برای بررسی تخلف و جرایـــم، عموما با ارزیابی اطلاعـــات ریز تراکنش‌ها ممکن می‌شود. با حفظ حریم خصوصی، چگونه امکان استخراج ریـــز معاملات اشـــخاص حقیقـــی و یا حقوقـــی به‌وجود می‌آید؟ به‌عنوان مثـــال در هایپرلجرفِبریک یکی از اهداف کسب‌وکار می‌باشد، در نتیجه بر اساس کسب‌وکار خاص می‌توان گره‌های حسابرســـی برای امور خاصی در شبکه تعریـــف نمود و از طرفی امکان ایجاد ســـطح دسترســـی برای گره‌های مختلف در شـــبکه وجود دارد. در پروونِنس حسابرســـان یا بازرسانی در این ســـامانه وجود دارد، که توســـط مدیر شبکه ثبت تایید شده‌اند و دارای مجوز برای بررسی اطلاعات موجود در بلاک‌چین می‌باشند. همچنین اینشورچِین شـــخص ثالثی را برای رسیدگی به ادعاهای پیچیده‌تر معرفی می‌کند. کاربران قادر خواهند بود اطلاعات مرتبـــط را برای ادعاهای خود بارگـــذاری کنند و اطلاعات توسط یک شـــخص متخصص (حسابرس) مورد بررسی قرار گرفته و بر روی بلاک‌چین ثبت شود. در مِدیکال‌چِین[9]

9- Medicalchain.

اطلاعات در اختیار کاربران است و در صورتی که نیاز به حسابرسی مانند بیمه سلامت باشد، کاربران می‌توانند به بیمه ســـلامت اجازه دسترسی به ســـوابق سلامت خود را بدهند. شرکت‌های بیمه می‌توانند مطمئن باشند که اطلاعات مورد اعتماد، قابل تایید و قابل رسیدگی است [۱۲].

در این بخش، پنج چالش مهم در اعمال ضوابط قانونی بـــر روی بلاک‌چین مطرح شـــد و مشـــاهده کردیم که در پژوهش‌هـــای مختلف تلاش‌هایی برای پاســـخگویی آن‌ها مدنظر قـــرار گرفته اســـت. جدول ۱ ارزیابـــی پروژه‌های مختلف را بر پایه خدمات ادعایی این پروژه‌ها، ارائه می‌کند. بیت‌کوین با فرض ایجاد فضـــای بدون ناظر و کاملا همتا محـــور[10] هیچگونه ضوابط قانونی بیـــش از توافق طرفین تراکنش را مدنظر قرار نداده است. پروژه هایپرلجرفبریک بستر عمومی ایجاد کسب‌وکارها را با امکان اعتبارسنجی طرفین تراکنش و حسابرســـی مورد نیاز هر کســـب‌وکار فراهم می‌کنـــد و درخصوص دیگـــر چالش‌ها هیچ خدمت خـــودکاری عرضه نمی‌کند [۵]. بســـتر ایجاد شـــده برای زنجیره تامین در پروژه پروونِنس علاوه بر اعتبارســـنجی طرفیـــن تراکنـــش و حسابرســـی، خدمت اعتبارســـنجی محصول را نیز عرضه کرده است ولی درخصوص اِعمال قوانین به رعایت اســـتانداردها قناعت می‌کند [۱۱]. پروژه اینشـــورچِین در زمینه بیمه علاوه بر این‌که اعتبارسنجی بیمه‌گزارها و خدمات حسابرســـی را ممکن می‌کند، اِعمال سیاســـت‌های بیمه‌ای دلخواه را به‌صورت خودکار انجام می‌دهد [۱۰]. پروژه مِدیکال‌چِین نیز برای پرونده ســـلامت و زنجیره خدمات سلامت اعتبارسنجی اشخاص و خدمات حسابرسی را عرضه می‌کند امّا در خصوص اعتبارسنجی دارو به‌عنوان کالا و اِعمال قوانین را به‌عهده نمی‌گیرد [۱۲]. همان‌طور که در جدول ۱ دیده می‌شود، هیچ یک از کارهای مشـــابه درخصوص کســـر هزینه‌های قانونـــی راهکاری خودکار ارائه نمی‌کنند.

طرحی که در این مقاله پیشنهاد می‌دهیم یک نمونه اولیه از ایده‌ای است که بتواند پاسخگوی همه چالش‌های مطرح

10- Peer-to-Peer.

جدول ۱: ارزیابی پژوهش‌های مرتبط برای پاسخدهی به چالش‌های قانونی

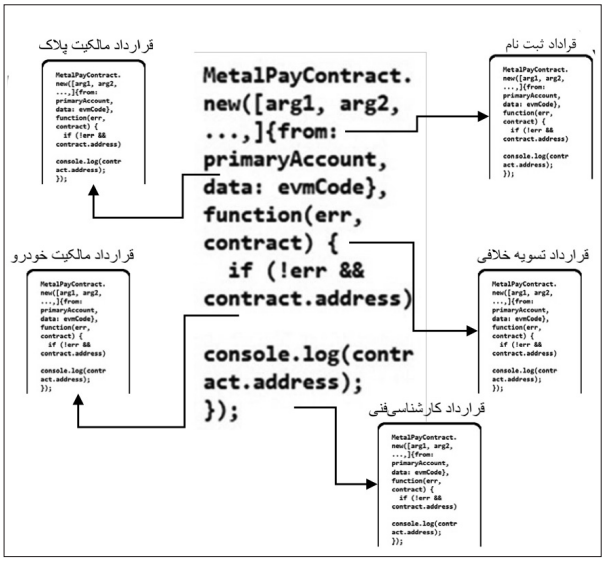
پروژه بلاک‌چین	اعتبارسنجی شرکت‌کنندگان	اعتبار سنجی محصول	کسر هزینه قانونی	اعمال قوانین	حسابرسی
بیت‌کوین	–	–	–	–	–
هایپرلجرفبریک	✔	–	–	–	✔
پروونِنس	✔	✔	–	؟	✔
اینشورچین	✔	–	–	✔	✔
مِدیکال‌چین	✔	–	–	–	✔

شـــده باشد و با ایجاد بستر لازم بر روی همه قراردادهای هوشمند قابل اعمال باشد.

۳- اَبَرقرارداد هوشمند

طرح پیشـــنهادی این پژوهش مبتنی بر این ایده اســـت که یک ســـازمان بـــا جایگاه قانونی بـــرای اعمال ضوابط، نیاز نیســـت در یک قرارداد نهایی مستقیما وارد شود. بلکه به‌صورت مجزا و از طریق یک قرارداد هوشـــمند ساده‌تر می‌توانـــد اعمال ضوابط قانونی نماید. عنـــوان «اَبَرقرارداد هوشـــمند[11]» را برای طرح پیشـــنهادی درنظـــر گرفته‌ایم. ایده اصلی در ســـاخت قرارداد نهایی با مجموعه‌ای از چند ریزقرارداد مجزا اســـت. به‌عنوان مثال، برای این‌که نیروی انتظامی حسابرسی تخلف یک خودرو را انجام دهد، کافی است با مالک فعلی خودرو در یک قرارداد مجزا این تسویه انجام شود. اگر تاییدیه این ریزقرارداد انجام شود، قرارداد فروش خودرو از یکی از مراحل نظارت نهایی عبور می‌کند. اَبَرقـــرارداد هوشـــمند از به هم پیوســـتن ریزقراردادهای هوشـــمند ایجاد می‌شـــود که با یکدیگر در ارتباط هستند. هر ریزقرارداد هوشـــمند در اَبَرقرارداد هوشمند، می‌تواند به‌صورت مستقل عمل کرده و مسئولیت قانونی خاصی را بر عهده خواهد گرفت. تمام این ریزقراردادها بر اساس نیاز می‌تواند اضافه یا کم بشـــوند در نتیجه تعداد و مسئولیت هر ریزقرارداد به نوع اســـتفاده و هدفی که اَبَرقرارداد آن را دنبال می‌کند، بســـتگی خواهد داشـــت. برای درک بهتر

11-Hyper Smart Contract



شکل ۱: نمایی کلی از اَبَرقرارداد هوشمند فروش خودرو

اَبَرقرارداد هوشمند، آن را روی مثال فروش خودرو مطرح می‌کنیم. اَبَرقرارداد هوشمند فروش خودرو می‌تواند شامل ۵ ریزقرارداد هوشمند باشد (شکل ۱).

۳-۱- اَبَرقرارداد هوشمند فروش خودرو

فروش خـــودرو دســـت دوم در ایران نیـــاز به اعمال ضوابط قانونی متعددی دارد. هویت فروشـــنده، خریدار و همچنین خود خودرو باید احراز شود. در ایران برای هویت خودرو دو شناسه لحاظ می‌شود: شناسه انحصاری بدنه/موتور خودرو و پلاک خودرو. اخذ نظر کارشناس فنی که معمولا به‌عهده بنگاه معاملات است و یا با مسئولیت خود خریدار انجام می‌شود. خلافی رانندگی خودرو باید تسویه شـــود و در نهایت باید هزینه های مختلف نظیر عوارض، مالیات، تعویض پلاک، ثبت ســـند و حق الزحمه‌ها پرداخت شود. برای قرارداد فروش خودرو، ایده اَبَرقرارداد هوشمند شامل قراردادهای مستقل زیر پیشنهاد می‌کنیم:

- قرارداد «ثبت نام»: فروشـــنده و خریدار می‌بایست ثبت نـــام کنند. ثبت نام همراه با احراز هویت شـــخص حقیقی/حقوقی انجام می‌شود. با فرض اشخاص حقیقی، سازمان قانونی ناظر، سازمان ثبت احوال است.
- قـــرارداد «مالکیت پـــلاک»: مالکیت فروشـــنده بر پلاک خودرو می‌بایست احراز شود. فروشنده‌ای که در قرارداد

«ثبت نام» احراز هویت شـــده است، وارد قرارداد «مالکیت پلاک» می‌شود. سازمان قانونی ناظر، نیروی انتظامی است.

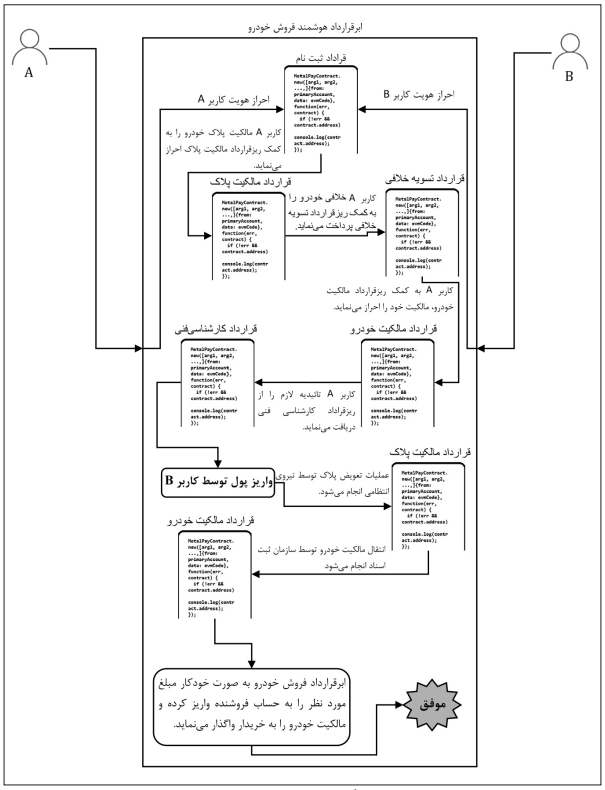
● قرارداد «تســـویه خلافی»: فروشـــنده‌ای که در قرارداد «مالکیـــت پلاک» احراز هویت شـــده اســـت، وارد قرارداد «تســـویه خلافی» می‌شود. ســـازمان قانونی ناظر، نیروی انتظامی است.

● قرارداد «مالکیت خودرو»: مالکیت فروشـــنده بر خودرو می‌بایست احراز شود. فروشنده‌ای که در قرارداد «ثبت نام» احراز هویت شـــده و توسط قرارداد «مالکیت پلاک» احراز مالکیت پلاک شـــده اســـت، وارد قرارداد «مالکیت خودرو» می‌شود. ســـازمان قانونی ناظر، سازمان ثبت اسناد (و یا دفترخانه‌های رسمی) است.

● قرارداد «کارشناسی‌فنی»: فروشنده برای فروش خودرو نیاز به تایید مشـــخصات فنی ادعا شـــده خـــودرو با نظر کارشناس فنی خواهد داشت. در نتیجه فروشنده‌ای که در قرارداد «ثبت نام» احراز هویت شـــده اســـت، وارد قرارداد «کارشناسی‌فنی» می‌شود. سازمان قانونی ناظر، بنگاه‌های رســـمی ماشین (و یا اشخاص حقیقی که مجوز مربوطه را دارند) است.

یک اَبَرقرارداد هوشـــمند «فروش خودرو» برای حالت ساده شده‌ای که توافق بر سر مبلغ معامله خارج از قرارداد فروش باشـــد و همچنین پرداخت مبلـــغ در پایان موفقیت آمیز قرارداد به‌صورت خودکار به فروشـــنده انجام شود، به شرح زیر است (مطابق شکل ۲):

● اَبَرقـــرارداد هوشـــمند «فـــروش خـــودرو»: کاربـــران (خریدار و فروشـــنده) وارد اَبَرقرارداد هوشـــمند «فروش خودرو» شـــده و ابتدا از طریق قـــرارداد «ثبت نام» احراز هویت می‌شـــوند. مراحل تاییدیه «مالکیت پلاک»، «مالکیت خودرو»، «کارشناســـی‌فنی» و « تســـویه خلافی» توســـط ریزقراردادهای مربوطه برای فروشـــنده انجام می‌شـــود. سپس فروشـــنده مبلغ پیشـــنهادی را اعلام می‌کند. بعد از آن خریـــدار درخواســـت خرید می‌دهد و مبلـــغ مورد نیاز را نـــزد اَبَرقرارداد «فروش خودرو» به امانت می‌ســـپارد.

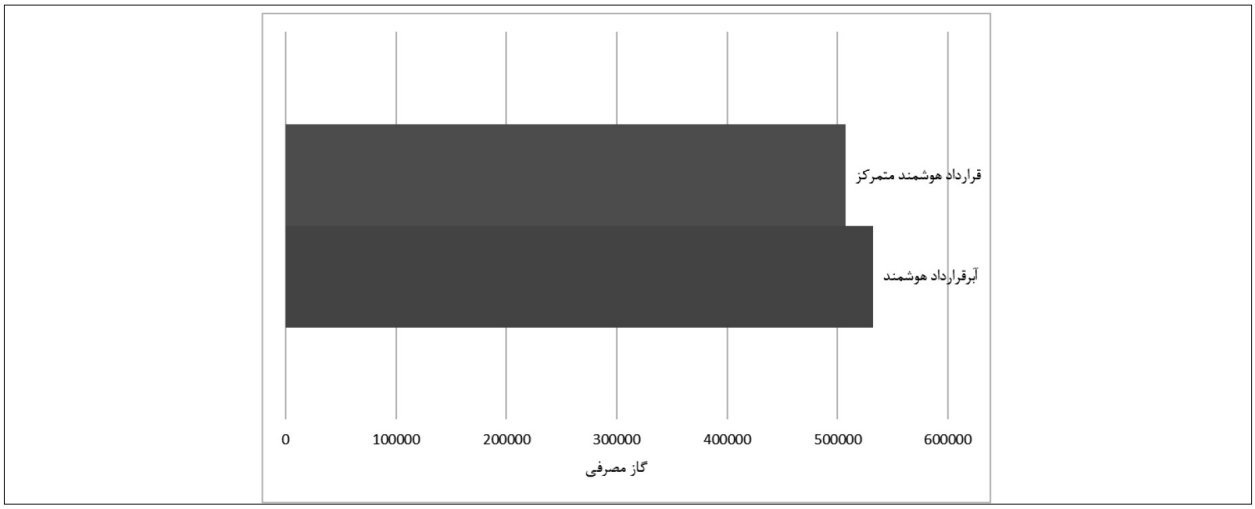


شکل ۲: مراحل کلی اَبَرقرارداد هوشمند فروش خودرو.

ســـپس ابتدا عملیات تعویض پلاک و بعد از آن ثبت ســـند توســـط قراردادهای مربوطه برای خریدار انجام می‌شود. در نهایت انتقال مبلغ به فروشـــنده انجام می‌شـــود. بدیهی است که پرداخت هزینه‌های قانونی فرآیندها در طی اجرای قراردادهای مربوطه انجام می‌گیرد.

همان طور که مشاهده شد، به کمک اَبَرقرارداد هوشمند فروش خودرو امکان اعمال ضوابط بر روی تراکنش‌های بلاک‌چین فراهم می‌شـــود. و این در حالی است که عوامل نظارتی و اجرایی، صرفـــا در محدوده وظایف و در زمان ضروری وارد می‌شوند.

پیاده‌سازی اَبَرقرارداد هوشمند فروش خودرو در یک پایان نامه کارشناســـی ارشـــد به انجام رسیده است [۱۴]. شـــیوه فنی پیاده‌سازی نرم‌افزاری و الزامات اجرای آن بر روی بســـتر بلاک‌چینِ اتریوم مـــورد ارزیابی قرار گرفته است. آنچه در این مقاله بر آن تاکید داریم، ارزیابی توانایی ایده اَبَرقرارداد هوشـــمند در اعمال ضوابط قانونی اســـت به‌گونه‌ای که محاسن هوشمند سازی قراردادها حفظ شود.



نمودار ۱: مقایسه هزینه مصرفی دو نمونه پیاده‌سازی قرارداد فروش خودرو.

۴-ارزیابی اَبَرقرارداد هوشمند

قرارداد هوشمند مبتنی بر بلاک‌چین علاوه بر خودکارسازی فرآیندهای کنترلی و اجرایی قراردادها، امکان حذف واسطه‌ها را فراهم می‌آورد. امّا اعمال ضوابط قانونی بدون دخالت عوامل اجرایی و نظارتی قانونی ممکن نیست. ایده اَبَرقرارداد هوشمند تلاش دارد با حضور عوامل اجرایی وکنترلی قانونی، محاسن خودکارسازی قرارداد هوشمند را نیز حفظ نماید.

طرح اَبَرقرارداد هوشمند را می‌توان برپایه عملکرد و یا تاثیر بر هزینه پردازشی ارزیابی کرد.

٤-١- ارزیابی عملکردی

در بخش ۲ تعدادی از چالش‌های پیش رو برای اعمال ضوابط قانونی را مطرح کردیم. ابتدا در یک ارزیابی عملکردی، شرح می‌دهیم که چگونه اَبَرقرارداد هوشمند می‌تواند این چالش‌ها را پاسخ بدهد.

- «اعتبارسنجی طرفین قرارداد»: نشان دادیم که در اَبَرقرارداد فروش خودرو امکان اعتبارسنجی شرکت کنندگان به کمک ریزقرارداد ثبت نام انجام می‌شود. در این ریزقرارداد کاربری که به کمک کلید عمومی در سامانه ثبت نام کرده است، به کمک فراخوانی یک خدمت بیرونی متعلق به سازمان ثبت احوال بررسی می‌شود و در صورت صحت اطلاعات، نشانی مورد نظر با اطلاعات وارد شده تایید می‌شود. در نتیجه این اطمینان به‌وجود می‌آید که با شخص حقیقی معتبر در حال انجام معاملات هستیم.
- «ماهیت کالا»: در اَبَرقرارداد فروش خودرو به کمک دو ریزقرارداد، مالکیت فروشنده بر پلاک و خودرو اعتبارسنجی می‌شود. این ریزقراردادها زیر نظر نیروی انتظامی و سازمان ثبت اسناد، اطلاعات وارد شده توسط فروشنده را مورد بررسی قرار می‌دهند و در صورت تایید در بلاک‌چین ثبت می‌شود. در نتیجه اَبَرقرارداد هوشمند توانایی بررسی ماهیت محصول و مجوز فروش آن محصول را دارد. این مورد می‌تواند در بسیاری از کسب‌وکارهای پیچیده امروزه مورد استفاده قرار بگیرد.
- «پرداخت هزینه‌های قانونی»: در اَبَرقرارداد فروش خودرو از طریق ریزقراردادهای مربوطه و در هر مرحله اجرایی هزینه‌های قانونی مانند عوارض، مالیات، خلافی، ثبت سند و تعویض پلاک از طرف مربوطه دریافت می‌شود. البته قابل ذکر است که هزینه های قانونی باید به‌صورت ارز دیجیتال از کاربران دریافت شود. در نتیجه اَبَرقرارداد هوشمند فروش خودرو اگر بخواهد با سازمان های مختلف کار کند، باید آن سازمان ها دارای حساب ارز دیجیتالی در بلاک‌چین باشند.
- «اعمال ضوابط قانونی سرزمینی»: یکی از نقاط قوت اَبَرقرارداد هوشمند توانایی تطبیق با هر نوع قوانین سرزمینی می‌باشد. اَبَرقرارداد هوشمند از ریزقراردهای

مختلف با اهداف متفاوتی طراحی شده است. در نتیجه این ریزقراردادها در سازوکار اَبَرقرارداد هوشمند می‌توانند با توجه به قوانین سرزمینی هر منطقه طراحی شده و مورد استفاده قرار بگیرند.

- «حسابرسی»: اَبَرقرارداد فروش خودرو دارای چند نهاد ناظر برای حسابرسی و اعمال ضوابط است. هر نهاد از طریق قرارداد مربوطه و به‌صورت خودکار حسابرسی بخش مربوط به خود را انجام می‌هد.

٤-٢- هزینه پردازشی

گاز اتریوم[12]، منبع حیات زیست‌بوم اتریوم است. گاز واحدی است که میزان محاسبات مورد نیاز برای انجام عملیات خاص را اندازه‌گیری می‌کند. هر عملی که در اتریوم انجام شود، یک معامله ساده یا یک قرارداد هوشمند و یا حتی ارائه ارز اولیه مقداری گاز مصرف می‌کند. گاز چیزی است که برای محاسبه میزان هزینه‌هایی که باید برای انجام عملیات به شبکه پرداخت شود، مورد استفاده قرار می‌گیرد [۱۳].

در این بخش بالاسری هزینه ایده پیشنهادی سنجیده می‌شود. ایده اَبَرقرارداد هوشمند، یک قرارداد را به چندین قرارداد مجزا تجزیه می‌کند و سپس آن‌ها را در یک قرارداد جدید به‌کار می‌گیرد. از نظر پردازش‌های اصلی هیچ تفاوتی بین یک قرارداد متمرکز و نمونه اَبَرقرارداد آن وجود ندارد امّا تجزیه و سپس ترکیب ریز قراردادها هزینه پردازشی بیشتری نیاز دارد. برای سنجش این بالاسری در یک نمونه پیاده‌سازی شده، اَبَرقرارداد هوشمند فروش خودرو، هزینه‌ها را به‌صورت عملی می‌سنجیم.

هزینه گاز اتریم قراردادها را با استفاده از کنسول ترافل[13] اندازه‌گیری کردیم. هنگام اجرای یک عملکرد، این کنسول هزینه گاز را ثبت می کند. نمودار ۱ میزان گاز مصرفی دو پیاده‌سازی متفاوت از قرارداد فروش خودرو را در زمانی که همه شرایط برای موفق شدن قرارداد آماده است نمایش می‌دهد. همان‌طور که پیش‌بینی کرده بودیم هزینه اَبَرقرارداد هوشمند بیشتر است امّا میزان بالاسری کمتر از یک درصد (حدود ۰.٤۹٪) است که قابل قبول است.

12-Ethereum Gas.
13- www.trufflesuite.com

نتیجه‌گیری

برای استفاده از فناوری بلاک‌چین در کسب‌وکارها و معاملات واقعی و گسترده در سطح جامعه، نیاز به شیوه‌هایی برای اعمال ضوابط قانونی است. اَبَرقرارداد هوشمند رویکردی برای پیاده‌سازی کسب‌وکارهای قانونی مبتنی بر بلاک‌چین است. در جدول ۱ توان پاسخگویی پژوهش‌های مرتبط با اَبَرقرارداد هوشمند را ارزیابی کرده‌ایم. همان‌طور که مشاهده می‌شود، ایده اَبَرقرارداد هوشمند تنها پژوهشی است که به همه نیازها برای اعمال ضوابط قانونی پرداخته است.

در این پژوهش برای پیاده‌سازی اَبَرقرارداد هوشمند از شبکه اتریوم استفاده شد ولی با توجه به بررسی‌های انجام شده در این شبکه برای پیاده‌سازی اَبَرقرارداد هوشمند، دو محدودیت وجود دارد:

- در شبکه اتریم امکان فراخوانی راه‌دور خدمات بیرونی[14] وجود ندارد. به‌عنوان مثال امکان آن که بخواهیم اطلاعات هویتی کاربران را از خدمتی خارج از بلاک‌چین (مثلا از سامانه ثبت احوال) دریافت کنیم، وجود ندارد. راه‌حل نرم‌افزاری می‌تواند بروزرسانی دوره‌ای وضعیت‌ها در بلاک‌چین از طریق سامانه خارجی باشد. می‌شود انتظار داشت که در نسل بعدی قراردادهای هوشمند، امکان فراخوانی راه‌دور خدمات بیرونی ایجاد شود.
- در شبکه اتریم ارتباط بین قراردادهای مختلف می‌بایست به‌صورت دستی توسط برنامه‌ساز و از طریق به‌کارگیری شناسه عمومی قراردادها انجام شود که امکان خطای برنامه‌سازی را بالا می‌برد. مناسب است که در نسل بعدی اتریوم، امکان تعریف وابستگی قراردادها در هنگام تعریف آن‌ها، بدون نیاز به برنامه‌سازی، ممکن شود.

14- External Service based on service oriented architecture.

منابع

1. Boroń, Michał, Jerzy Brzeziński, and Anna Kobusińska. “P2P matchmaking solution for online games.” Peer-to-peer networking and applications, vol 13, no. 1, pp. 137-150, 2020.
2. Arteaga, Carlos Hernan Tobar, Armando Ordoñez, and Oscar Mauricio Caicedo Rendon. “Scalability and performance analysis in 5G core network slicing.” IEEE Access 8, 2020.
3. Xiaoqi Lia, Peng Jianga, Ting Chenb, Xiapu Luoa and Qiaoyan Wenc, ”A Survey on the Security of Blockchain Systems”, Future Generation Computer Systems, vol 107, pp. 841-853, 2020.
4. W. Fan, H. -J. Hong, S. Wuthier, X. Zhou, Y. Bai and S. -Y. Chang, “Security Analyses of Misbehavior Tracking in Bitcoin Network,” 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-3, 2021.
5. Ma, C., Kong, X., Lan, Q. et al. “The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. “ Cybersecur 2, 5 , 2019.
6. Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system”, 2008. Available online: https://bitcoin.org/bitcoin.pdf. (Accessed 2 June 2020).
7. Benjamin Collette, Francois-Kim Hugé, Simon Ramos, Maxime Heckel, Patrick Laurent, Thibault Chollet, Laurent Collet, “Impacts of the Blockchain on fund distribution”, Deloitte Tax & Consulting Designed and produced by MarCom at Deloitte Luxembourg, 2018.
8. Dziuba, Dariusz, “The Blockchain Crowdfunding Technology: Usage, Benefits, and Expectations”, Annales Universitatis Mariae Curie-Skłodowska, sectio H, Oeconomia. Vol. 52, No 2, p 61-69, 2018.
9. Christopher Mann and Daniel Loebenberger, “Two-Factor Authentication for the Bitcoin Protocol”, International Journal of Information Security, Vol 16, pages213–226, 2017.
10. Francesco Corea, “An Introduction to Data”, eBook ISBN 978-3-030-04468-8, DOI 10.1007/978-3-030-04468-8, Springer International Publishing, 2019.
11. Steiner, J. and J. Baker, “Blockchain: The Solution for Transparency in Product Supply Chains”, https://www.provenance.org/. (Accessed 2 June 2020).
12. Cleverence Kombe, Mussa Ally and Anael Sam, “A review on healthcare information systems and consensus protocols in blockchain technology.” International Journal of Advanced Technology and Engineering Exploration 5 (49): 473-483, 2018.
13. Ellis Solaiman, Todd Wike, Ioannis Sfyrakis, “Implementation and evaluation of smart contracts using a hybrid on- and off- blockchain architecture” Concurrency and Computation: Practice and Experience, 2020.

۱۴. علیخانی، علیرضا (۱۳۹۸) «قانونمندکردن تراکنش‌های بلاک‌چین: چالش‌ها و روش‌ها»، پایان‌نامه کارشناسی ارشد، دانشگاه بین‌المللی امام خمینی(ره)، بهمن ۱۳۹۸، قزوین، ایران.