بسم الله الرحمن الرحیم

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دانشگاه خوارزمی

دانشکده اقتصاد

گروه اقتصاد و بانکداری اسلامی

پایان نامه کارشناسی ارشد رشته علوم اقتصادی

گرایش: بانکداری اسلامی

عنوان:

طراحی مدلی از قرارداد های هوشمند در نظام بانکداری بدون ربا: کاربردی از مدل های هوش مصنوعی

استاد راهنما:

دکتر حسین امیری

استاد مشاور:

دکتر احمد جعفری صمیمی

پژوهشگر:

سمانه اصفهانی

زمستان ۱۳۹۸

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تعهدنامه اصالت پایان‌نامه

اینجانب سمانه اصفهانی دانش‌آموخته مقطع کارشناسی ارشد ناپیوسته در رشته علوم اقتصادی و گرایش بانکداری اسلامی که در تاریخ۹۸/۱۰/۱۷ از پایان‌نامه خود تحت عنوان «طراحی مدلی از قراردادهای هوشمند در نظام بانکداری بدون ربا: کاربردی از مدل‌های هوش مصنوعی » با کسب نمره ۱۷دفاع نموده‌ام، بدین‌وسیله متعهد می‌شوم :

۱) این پایان‌نامه حا صل تحقیق و پژوهش انجام شده تو سط اینجانب بوده و در مواردی که از د ستاوردهای علمی و پژوهشی دیگران (اعم از پایان‌نامه، کتاب، مقاله و...) استفاده کرده‌ام، مطابق ضوابط و رویه معمول موجود،نام منبع مورداستفاده و سایر مشخصات آن را در فهرست مربوط درج نموده‌ام.درصورتی‌که اثبات شود که این پایان‌نامه به شخص دیگری تعلق دا شته ا ست، دانشگاه می‌تواند مدرک تحصیلی این‌جانب را ابطال نماید.در آن صورت این‌جانب اقدام دانشگاه رامی پذیرم و حق هرگونه اعتراضی را از خود سلب می‌کنم.

۲) این پایان‌نامه قبلاً برای دریافت هیچ مدرک تحصیلی (هم‌سطح، پایین‌تر، یا بالاتر) در سایر دانشگاه‌ها و مؤسسات آموزش عالی ارائه نشده است.

۳) چنانچه پس از فراغت از تحصیل، قصد استفاده و هرگونه بهره‌برداری اعم از چاپ مقاله، چاپ کتاب، ثبت اختراع و...از مفادو نتایج این پایان‌نامه داشته باشم، از حوزه معاونت پژوهشی دانشگاه مجوز لازم را و در کلیه انتشارات خود نام دانشگاه و استاد راهنمایم را درج کنم.

۴) چنانچه در هر مقطع زمانی خلاف موارد فوق ثابت شود عواقب ناشی از آن رامی پذیرم و دانشگاه خوارزمی مجازاست با این‌جانب مطابق ضوابط و مقررات رفتار نماید.

نام و نام خانوادگی : امضاء

سمانه اصفهانی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بسمه تعالی

دانشگاه خوارزمی

تاریخ: ۱۳۹۸/۱۰/۲۳
شماره: ۲۴۱۳۱۲
پیوست:
واحد:

صورتجلسه دفاع پایان نامه مقطع کارشناسی ارشد دانشکده اقتصاد

به استحضار میرساند جلسه دفاع از **پایان نامه کارشناسی ارشد خانم سمانه اصفهانی** به شماره دانشجویی **۹۶۵۱۷۶۶۰۲**

رشته : **بانکداری اسلامی**

تحت عنوان:**طراحی مدلی از قراردادهای هوشمند در نظام بانکداری بدون ربا کاربردی از مدل های هوش مصنوعی**

در تاریخ **۱۳۹۸/۱۰/۲۳** ساعت **۱۴:۰۰** در محل **دانشکده اقتصاد، شامل** ۱۷ **نمره پایان نامه و** ---- **نمره مقاله** با حضور هیات محترم داوران در دانشگاه خوارزمی برگزار گردید و رای نهایی به شرح زیر است:

الف: نمره ---۱۷--- با درجه ---خوب--- مورد تصویب اعضای کمیته قرار گرفت.مقرر گردید دانشجو اشکالات ذکر شده توسط هیات داوران را در اسرع وقت برطرف نموده و به تایید برساند.

ب: پایان نامه از نظر هیات داوران دارای اشکالات اساسی به شرح پیوست می باشد و بنابراین مورد تصویب قرار نگرفت و دانشجو باید پس از رفع آن ها مجددا دفاع نماید.

۱-عالی(۱۹ - ۲۰)۲-خیلی خوب(۱۸ - ۱۸/۹۹)۳-خوب(۱۶ - ۱۷/۹۹)۴-متوسط(۱۴ - ۱۵/۹۹)۵-مردود(کمتر از ۱۴)

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
راهنما	حسین امیری	استادیار	
مشاور	احمد جعفری صمیمی		
داور داخلی	وحید شقاقی شهری	استادیار	

رئیس دانشکده اقتصاد
وحید شقاقی شهری

مدیر گروه اقتصاد

تهران: خیابان شهید مفتح نرسیده به خیابان انقلاب ـ شماره ۴۳ ـ دانشگاه خوارزمی، کد پستی ۱۵۷۱۹-۱۴۹۱۱، تلفن: ۳-۸۸۳۲۹۲۲۰
کرج: خیابان شهید بهشتی ـ میدان دانشگاه ـ دانشگاه خوارزمی، کد پستی: ۳۱۹۷۹-۳۷۵۵۱، تلفن: ۰۲۶-۳۴۵۷۹۶۰۰
Kharazmi University, No. 43, Shahid Mofateh Ave.- Tehran, Iran
Tel: +98 21 88329220-3 www.khu.ac.ir

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کلیه حقوق مادی و معنوی مترتب بر نتایج مطالعات، ابتکارات و نوآوری‌های ناشی از تحقیق، همچنین چاپ و تکثیر، نسخه‌برداری، ترجمه و اقتباس از این پایان‌نامه کارشناسی ارشد، برای دانشگاه خوارزمی محفوظ است. نقل مطلب با ذکر منبع بلامانع است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تشکر و قدردانی:

وظیفه خود می‌دانم سپاس گزار تمام آنهایی باشم که در این دوره ارزشمند بودنشان و امیدشان راهگشای من بود؛

اساتید عزیز و گرانقدر، بخصوص **جناب آقای دکتر حسین امیری و همچنین همسر عزیزم،**

که در انجام این پایان نامه مرا یاری نمودند و به هنگام نیاز برای حل مشکلات اینجانب از هیچ کمکی دریغ نورزیدند.

برای ایشان آرزوی سلامتی، موفقیت و سربلندی را دارم.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تقدیم به:

این پایان نامه را ضمن تشکر و سپاس بیکران و در کمال افتخار و امتنان تقدیم می نمایم به:

محضر عظیم و ارزشمند **پدر و مادر عزیزم** به پاس عاطفه سرشار و گرمای وجودشان که همواره امیدبخش لحظه هایم بوده اند

به آنان که در راه کسب دانش راهنمایم بودند و نفس خیرشان و دعای روح پرورشان بدرقه ی راهم بوده و یادشان

خاطرنشان زیباترین آموزه های زندگی است. باشد که توفیق زدودن غبار خستگی هایشان را داشته باشم.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

چکیده

با توجه به اهمیت بانک در توسعه و رشد اقتصادی کشورها، بهبود عملکرد بانک‌ها از نظر شاخص‌های مختلف عملکردی می‌تواند زمینه ساز دستیابی به اهداف تعیین شده باشد. با توجه به ظهور تکنولوژی‌های جدید مانند هوش مصنوعی، بلاکچین، تکنولوژی مالی و ...، در سال‌های اخیر بانک‌ها برای بهبود عملکرد خود در حوزه‌های مطرح شده از این تکنولوژی‌ها استفاده می‌کنند تا هزینه‌ها خود را کاهش داده و میزان سود خالص خود را افزایش دهند. یکی ازاین تکنولوژی‌ها قراردادهای هوشمند می‌باشد که تحت عنوان قراردادهوشمند معمول یا مبتنی بر بلاک‌چین شناخته می‌شود. از آنجا که قراردادهوشمند معمول بر بستر بلاک‌چین هستند علاوه برمزیت‌هایی که دارند، دارای یک سری عدم مزیت‌هایی مانند نیاز به توان پردازشی بالا و مقیاس‌پذیری، عدم سازگاری با سیستم‌های سنتی، نیاز به ارزیابی‌های تکنولوژیک رگولاتوری، مشکل بودن توسعه پروتکل‌های اجماع و رمزنگاری و ... هستند. لذا مفهوم جدیدی با ماهیت مشابه ولی با انعطاف پذیری بیشتری به نام قراردادهای هوشمند مبتنی بر هوش مصنوعی مطرح شد که بیشتر متکی بر هوش مصنوعی و الگوریتم‌های آن بوده است تا ساختاری کاملا نامتمرکزمانند بلاک‌چین. اما از آنجا که این مفهوم کاملا جدید بوده، لذا در این تحقیق به بررسی ساختار و ماهیت هر کدام از این قراردادها پرداخته ایم. با بررسی کامل نحوه عملکرد قراردادهای‌هوشمند معمول به اصولی مطابق با مبانی نظری، جهت توسعه قراردادهای هوشمند هوش مصنوعی رسیدیم. که این اصول شامل بستر و شبکه قرارداد، حفاظت پیشگیرانه، تایید در حال انجام فرآیند، تایید پویا گره‌ها و قضاوت عقلانی و ارزیابی و چک‌های ترکیبی براساس کتابخانه قانون می‌باشد. و بر اساس همین اصول، در فصل چهارم یک پروتکل پیشنهادی را جهت توسعه این نوع از قراردادها ارائه کردیم. و در نهایت با توجه به پروتکل پیشنهادی، به بیان نحوه عملکرد این نوع قراردادها بر اساس پروتکل پیشنهادی در زمینه پرداخت و وام نفر به نفر در سیستم بانکی پرداختیم. استفاده از چنین قراردادهایی با توجه به شرایط کنونی در بانکداری ایران معقول‌تر به نظر می‌رسد و یکی از دلایل اصلی این امر انعطاف‌پذیری این قراردادها و سازگاری این قراردادها با سیستم‌های سنتی بانک‌ها است.

کلمات کلیدی: هوش مصنوعی، قرارداد هوشمند، قرارداد هوشمند(مبتنی بر الگوریتم های هوش مصنوعی)، الگوریتم هش، سیستم غیر متمرکز، قراردادهای فیزیکی (قرار دادهای سنتی)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فهرست مطالب

عنوان **صفحه**

فصل اول : کلیات تحقیق

۱-۱- مقدمه ۱

۱-۲- بیان مساله ۲

۱-۳- ضرورت و اهمیت تحقیق ٤

۱-۳-۱- محدودیت های قرارداد سنتی ٤

۱-۳-۲- منافع استفاده از قراردادهای هوشمند برای مشتریان و بانکها ٤

۱-٤- اهداف پژوهش ٥

۱-٥- سوالات پژوهش ٥

۱-٦- روش تحقیق ٥

۱-۷- خلاصه فصل ۷

فصل دوم: مبانی نظری و ادبیات پژوهش

۲-۱- مقدمه ۹

۲-۲- انواع قراردادها از منظر پیادهسازی ۱۰

۲-۲-۱- قراردادهای سنتی ۱۱

۲-۲-۲- قراردادهای الکترونیکی ۱۱

۲-۲-۲-۱- ماهیت واشکال قراردادهای الکترونیکی ۱۲

۲-۲-۳- قراردادهای هوشمند ۱۳

۲-۲-٤- مقایسه قراردادهای هوشمند با قراردادهای سنتی و الکترونیکی ۱٥

۲-۳- مقایسه ماهیت قراردادهای هوشمند ۱٦

۲-۳-۱- قراردادهای هوشمند مبتنی بر بستر بلاک چین ۱٦

۲-۳-۱-۱- عناصر قرارداد هوشمند ۱۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۲-۱-۳-۲- محیط قرارداد هوشمند ۱۷
۲-۳-۲- قرارداد های هوشمند مبتنی بر هوش مصنوعی ۱۸
٤-۲- ساختار و چگونگی پیادهسازی قراردادهای هوشمندمبتنی بربلاکچین ۱۹
۱-٤-۲- بلاکچین ۱۹
۲-٤-۲- چگونگی عملکرد قراداد هوشمند مبتنی بر بلاکچین ۲۱
٥-۲- محدودیتها و عدم مزیتهای بلاکچین و قراددادهای هوشمند مبتنی بر بلاکچین ۲۳
۱-٥-۲- محدودیت های قرارداد هوشمند مبتنی بر بستر بلاکچین ۲۳
۱-۱-٥-۲- ارتباط با جهان فیزیکی ۲٤
۲-۱-٥-۲- قرارداد هوشمند به عنوان یک قرارداد کامل؟ ۲٤
۳-۱-٥-۲- قرارداد قانونی و قرارداد هوشمند ` ۲٥
۲-٥-۲-عدم مزیتهای بلاکچین ۲٦
۱-۲-٥-۲- حملات و مشکلات دیگر بلاکچین ۲۸
۲-۲-٥-۲- سایر چالشهای بلاکچین: ۲۹
٦-۲- هوش مصنوعی ۳۰
۱-٦-۲- مفهوم هوش مصنوعی ۳۰
۲-٦-۲- کاربردهای هوش مصنوعی در اقتصاد وبانکداری ۳۲
۱-۲-٦-۲- کشف کلاهبرداری مالی ۳۲
۲-۲-٦-۲- هوش مصنوعی وبازارهای سهام ۳۲
۳-۲-٦-۲- تشخیص کلاهبرداری در بیمه ۳۲
۷-۲- مزیت ها و عدم مزیتهای قراردادهای هوشمند مبتنی بر هوش مصنوعی ۳٤
۸-۲- کاربردها و فواید قراردادهای هوشمند و تاثیر آن بر بانکداری ۳٦
۱-۸-۲- کاربردها ۳۷
۱-۱-۸-۲- کاربرد دولتی قرارداد هوشمند ۳۷
۲-۱-۸-۲- کاربرد مدیریتی قرارداد هوشمند ۳۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۳-۱-۸-۲- کاربرد قرارداد هوشمند در زنجیره تأمین ۳۷
٤-۱-۸-۲- بانکداری و خدمات مالی ۳۸
۲-۸-۲- منافع استفاده از قراردادهای هوشمند برای بانکها و مشتریان ٤۱
۹-۲- بررسی قرارداد های اتوماتیک و هوشمند از نظر منظر مبانی قرارداد های اسلامی ٤۳
۱-۹-۲- الحاقی بودن ٤٤
۲-۹-۲- رضایی بودن ٤٤
۳-۹-۲- آنی بودن ٤٤
۱۰-۲- زیر ساختهای ضروری پیادهسازی قراردادهای هوشمند ٤٤
۱۱-۲- پیشینه تحقیق ٤٥

فصل سوم: روش تحقیق

۱-۳- مقدمه ٥۱
۲-۳- بستر و شبکه ٥٤
۳-۳- حفاظت پیشگیرانه ٥٤
۱-۳-۳- زبانهای برنامه نویسی مورد نیاز برای نوشتن قرارداد هوشمند ٥٤
۲-۳-۳- استانداردسازی کدها ٥٥
۳-۳-۳- شناسایی باگها ٥٥
٤-۳- تایید در حال انجام فرآیند ٥٦
۱-٤-۳- اجرای کدها و ارزیابی امنیتی پویا ٥٦
٥-۳- تایید پویا گرهها در هنگام اجرای قراردادها ٥٦
٦-۳- قضاوت عقلانی بعد از اجرای قرارداد ٥۷
۷-۳- مکانیزمی برای فرآیند شکایات و روش هایی برای قضاوت اتوماتیک ٥۷
۱-۷-۳- ارزیابی و چک های ترکیبی بر اساس کتابخانه قانون ٥۷
۲-۷-۳- تعیین مدل تراکنش ها و تبادلات و ارزیابی امنیتی بر اساس تجزیه و تحلیل معنایی ٥۸
۳-۷-۳- بررسی امنیت قرارداد های هوشمند بر اساس الگوریتمهایAI ٥۸

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

٤-٧-٣- بهینه سازی پویا و بهینه سازی امنیت بر اساس مدل شبکه تخاصمی مولد ٥٩
٨-٣- خلاصه روش تحقیق ٥٩
٩-٣- خلاصه فصل ٦٠

فصل چهارم: پروتکل پیشنهادی

١-٤- مقدمه ٦٣
٢-٤- فریمورک ٦٣
٣-٤- حفاظت پیشگیرانه ٦٥
١-٣-٤- زبان برنامه نویسی ٦٥
٢-٣-٤- استاندارد سازی کدها و شناسایی باگها ٦٥
٤-٤- تایید قرارداد و قضاوت عقلانی بعد از تایید قرارداد ٦٦
١-٤-٤- ماشین مجازی VM AI و تایید و ارزیابی قرارداد ٦٦
٢-٤-٤- تایید و ارزیابی براساس کتابخانه قانون ٦٨
٥-٤- تعیین مدل تراکنش ها و تبادلات و ارزیابی امنیتی بر اساس تجزیه و تحلیل معنایی ٦٨
٦-٤- استفاده از الگوریتمها جهت افزایش امنیت و ارزیابی قراردادها و تایید انجام مبادلات و تراکنشها ٦٨
١-٦-٤- الگوریتم SHA512 ..... ٦٨
٢-٦-٤- الگوریتم جستجوی اول عمق(DFS) ٦٩
٣-٦-٤- شبکههای مولد تخاصمیGAN ٦٩
٧-٤- نحوه عملکرد بر اساس پروتکل پیشنهادی ٧٠
١-٧-٤- شکلگیری شبکه و نحوه و شرایط ورود یک نود به شبکه ٧٠
٢-٧-٤- کتابخانهها و ارزیابی قرارداد ٧٣
٣-٧-٤- پرداخت حقوق کارکنان بانک توسط بانک در پروتکل مورد نظر ٧٣
٤-٧-٤- وام دهی نفر به نفر ٧٦

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامهها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل پنجم: پیشنهادات و تحقیقات آتی

۱-۵- مقدمه ۸۰

۲-۵- تجزیه و تحلیل ۸۰

۳-۵- پیشنهادات و تحقیقات آتی ۸٤

منابع و مآخذ :..... ۸٦

Abstract: ۱۱۱

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فهرست اشکال

عنوان

صفحه

شکل (۲-۱) دلایل استفاده از هوش مصنوعی در بانکداری ۳۳

شکل (٤-۱) تایید رسمی قراردادهای هوشمند ٦۷

شکل (٤-۲) نوع ارتباط شبکه ای نودها (کاربران) در بستر شبکه شبه نامتمرکز بر اساس پروتکل پیشنهادی..... ۷۰

شکل (٤-۳) نحوه ورود یک کاربر جدید به شبکه ۷۱

شکل (٤-٤) مسیر جریان اطلاعات وتایید در شبکه ۷۲

شکل (٤-۵) نمونه شبکه مورد نظر برای پرداخت حقوق کارکنان..... ۷٤

شکل (٤-٦) جریان کلی پرداخت به کارکنان در پروتکل مورد نظر ۷۵

شکل (٤-۷) نحوه اجرای قرارداد وام نفر به نفر در پروتکل پیشنهادی ۷۷

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل اول :

کلیات تحقیق

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقدمه

بخش واقعی اقتصـــاد، ظرفیت محدود و مشـــخصـــی برای تولید دارد و برای گســـترش فعالیت‌های آن به سرمایه‌گذاری جدید نیاز است. بخش مالی اقصاد، منابع مالی لازم برای سرمایه گذاری و به تبع آن توسعه بخش واقعی را فراهم می کند(طاهرپور و دیگران، ۱۳۹۷). ارتباط درســـت بین نظام های مالی و تولیدی از مهمترین عوامل رشد و توسعه اقتصادی در هر کشوری می‌باشد. بانک‌ها به عنوان بخش اصلی نظام مالی، اصلی ترین نقش را در تأمین مالی بخش‌های تجاری، تولیدی و مصرفی دارند. در ایران نیز با توجه به ساختار اقتصادی کشور و به دلایلی همچون عدم توســعه بازارهای ســرمایه و ســایر شــبکه‌های غیربانکی و قراردادی، شــبکه بانکی کشــور بخش‌های واقعی اقتصـــاد را تأمین مالی می کند(رحمانی و دیگران، ۱۳۹۶). از آنجا که بخش عمده بازار مالی ایران بانک محور اســت و برای دســتیابی به رشــد و توســعه اقتصــادی کشــورها در جهت تجهیز منابع و تامین مالی برای اجرای پروژه‌ها، تامین ســرمایه در گردش واحدهای تولیدی، اعطای وام‌های رهنی و رفع نیازهای اســـاســـی جمعیت وجلوگیری از تعمیق روند کاهنده فعالیت‌های اقتصــادی ، ســرمایه‌گذاری و اشــتغال نیاز به توجه دارد، لذا تمرکز بر عوامل موثر بر گسترش عملکرد بانک‌ها را می‌طلبد(شاه‌آبادی، داوری‌کیش، ۱۳۹۶).

با توجه به اهمیت بانک در توســعه و رشــد اقتصــادی کشــورها، افزایش اشــتغال، افزایش ســرمایه‌گذاری و غیره...، بهبود عملکرد بانک‌ها از نظر شـــاخص‌های مختلف عملکردی در حوزه‌های مدیریت، مالی، مدیریت هزینه‌ها و سرمایه‌گذاری می‌تواند زمینه ساز دستیابی به اهداف تعیین شده باشد. با توجه به ظهور تکنولوژی‌های جدید مانند هوش مصـــنوعی[1]، بلاکچین[2]، تکنولوژی مالی[3] و ...، در ســـال‌های اخیر بانک‌ها برای بهبود عملکرد خود در حوزه‌های مطرح شــده از این تکنولوژی‌ها اســتفاده می‌کنند تا هزینه‌ها خود را کاهش داده و میزان ســود خالص خود را افزایش دهند. به طور کلی اســتفاده از هوش مصــنوعی و ســیســتم‌های هوشــمند، تکنولوژی مالی، شـــبکه های عصـــبی[4] و الگوریتم‌های ژنتیک در حل مســـائل پیچیده کاربردی این روزها بیش از بیش رواج یافته اســـت. هوش مصـــنوعی از زمان پیدایش خود تاکنون به واســـطه مزیت قابلیت بکارگیری در تعداد بیشـــماری از ســناریوهای دنیای واقعی، توجه بســیاری از محققان این زمینه را به خود جلب نموده اســت. در حال حاضــر هوش مصنوعی و 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.

اهمیت هوش مصــنوعی در صــنعت بانکداری در حال حاضــر آنقدر قابل توجه اســت که رایان نورث[5] در مقاله‌ای در ســال ۲۰۱۸، اســاســی‌ترین بخش این صــنعت را کاربرد هوش مصــنوعی در بانکداری می‌داند و بیان می‌کند این مســـاله تاثیر عمیقی دارد، زمانی که یادگیری ماشـــین در صـــنعت بانکداری می‌تواند از طریق

[1]Artificial intelligence
[2]Block chain
[3]Financial technology(fintech)
[4]Neural network
[5]Ryan North

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تصمیم‌گیری و تشویق و ترغیب مشتریان، با انسان ارتباط برقرار کند و در تعامل با شد. هدف اصلی از وجود و کاربرد هوش مصنوعی در صنعت بانکداری، به دست آوردن یک بینش نسبت به ترجیحات مشتریان، اطمینان از رضایت مشتریان از خدمات ارائه شده توسط بانک‌ها و کمک به مشتریان در درک انتظارات خود از بانک‌ها است.

یکی از این تکنولوژی‌های جدیدی که در حوزه مالی و بانکداری مطرح شده است، قراردادهای هوشمند است. قرارداد هوشمند واژه‌ای است که از سال ۱۹۹۴ توسط نیک زابو[1] مطرح شد و از پروتکلی مخصوص تشکیل‌شده که برای مشارکت و تأییدیا اجرای یک قرارداد یایک شرط یا شروط خاص، به مرحله اجرا درمی‌آید.

قراردادهای هوشمند معاملات و فرایندها را به صورت کاملا تضمینی و بدون دخالت اشخاص ثالث[2] انجام می‌دهند. فعالیت و ثبت‌های قرارداد هوشمند قابل‌پیگیری و غیر قابل برگشت‌اند. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف‌گذاریشده به‌صورت اتوماتیک است.به طور کلی قراردادهای هوشمند به واسطه ویژگی‌هایی که دارد باعث شفافیت و کاهش هزینه ها شده و موجب بهبود شاخص‌های عملکردی می شود. این قراردادها که در بستر بلاکچین مطرح شده‌اند در بستر هوش مصنوعی نیز قابل پیاده سازی می‌باشند به این مفهوم که از ابزارها و الگوریتم‌های مرتبط با هوش مصنوعی جهت پیاده‌سازی قراردادهای هوشمند استفاده شود که در حقیقت یکی از قسمت‌های نوآورانه تحقیق می‌باشد. به طورکلی در این تحقیق ابتدا با بررسی دقیق قرارداد های هوشمند، ساختار آن بررسی شده است . همچنین بستر ایجاد قرارداد هوشمند را علاوه بر بلاکچین، هوش مصنوعی را نیز در نظر گرفته است و به بررسی نقاط ضعف بلاکچین نیز پرداخته ایم و ضمن بررسی این مطلب که در حال حاضر با توجه به شرایط کنونی، بانکداری ایران قادر به استفاده از بستر بلاکچین برای طراحی قراردادهای هوشمند نیست به طراحی مدلی برای قراردادهای هوشمند با استفاده از الگوریتم‌های هوش مصنوعی و ابزارهای آن پرداخته‌ایم.

بیان مساله

در چند سال اخیر گسترش روز افزون سیستم‌های معاملاتی خودکار و الگوریتمی را در بازارهای جهانی مالی شاهد هستیم. در حال حاضر بخش عمده‌ای از معاملات بازارهای مالی توسط الگوریتم‌های خودکار اجرا می شود. همراه با این رشد حضور سیستم‌های معاملات هوشمند، تقاضا برای امکان سنجی، طراحی و توسعه این نوع سیستم‌ها در داخل کشور رو به افزایش است. ویژگی اصلی این نوع سیستم‌ها افزایش سرعت و دقت برای تحلیل اطلاعات و تصمیم‌گیری نهایی، کاهش هزینه‌ها و حذف واسطه به اطلاع شخص ثالث است که باید مورد توجه قرار گیرد.

[1]Nick Szabo
[2]Thirty party

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

امروزه وارد شدن به یک قرار داد، نیازمند یک شخص ثالث است که مورد اعتماد طرفین باشد و بتواند قرار داد را اجرا کند و بر آن نظارت داشته باشد. به دلیل وجود چنین نیازی، چند مساله مطرح می شود :

اول، اینکه ممکن است این شخص ثالث خودش مخرب و زیان آور باشد.

دوم، ممکن است اطلاعات کافی به منظور حل ایجاد اختلاف احتمالی را نداشته باشد.

سوم، مشکل رایجی که وجود دارد این است که اگر در هنگام خرید آنلاین وقتی مشکلی پیش آید، زمانی که مدرکی دال بر صادق بودن وجود ندارد، ممکن است این قضاوت جانبدارانه باشد.

چهارم، یک مساله جالب‌تر این است که چگونه می‌توان این قرارداد را با امنیت کامل اجرا کرد بدون اینکه به آن شخص ثالث نیاز داشته باشیم.

همچنین قراردادهای هوشمند، 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. واسطه های مالی با کاهش دادن ریسک به یاری سیستم‌های مالی می‌آیند اما هزینه‌های سربار و الزامات مورد نیاز را افزایش می دهند. لذا با توجه به محدودیت‌های قراردادهای سنتی و منافع قراردادهای هوشمند در نظام بانکداری، استفاده از چنین قراردادهایی ممکن است بسیار قابل توجه باشد. بنابراین استفاده از چنین قراردادهایی در نظام بانکداری و مالی قابل توجیه است. ولی از آنجا که بستر این قراردادها بلاکچین می‌باشد و همچنین اکثر مقالات و تحقیقات به این نوع قراردادهای هوشمند پرداخته‌اند، در این تحقیق به دلایل زیر به مفهوم جدیدی به نام قرارداد هوشمند مبتنی بر هوش مصنوعی پرداخته شده است:

- ✓ قراردادهای هوشمند مبتنی بر بلاکچین هستند. اگرچه بلاکچین دارای ویژگی‌ها و منافع مهمی است با این حال دارای عدم مزیت‌های نیز می‌باشد که باید موردتوجه قرار بگیرد.
- ✓ قراردادهای هوشمند مبتنی بر هوش مصنوعی که در ماهیت شبیه قراردادهای هوشمند مبتنی بر بلاکچین است، برخلاف قراردادهای هوشمند معمول که مبتنی بر بلاکچین به واسطه بکارگیری الگوریتم های مختلف واستفاده از هوش مصنوعی قابلیت کاربردی و انعطاف‌پذیری بیشتری دارد.

حال با توجه به مطالب بالا، مساله اصلی ما دراین تحقیق این است که چگونه می‌توان با استفاده از الگوریتم‌ها و هوش مصنوعی با توجه به مبانی نظری در حوزه‌ی پیاده‌سازی قراردادهای هوشمند و الگوریتم‌ها، پروتکلی جهت توسعه این قراردادها در بستر هوش مصنوعی برای استفاده در نظام بانکی طراحی کرد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ضرورت و اهمیت تحقیق

در این قسمت با توجه به اینکه مساله اصلی تحقیق طراحی مدلی از قراردادهای هوشمند است جهت بیان ضرورت و اهمیت تحقیق به منافع قراردادهای هوشمند و محدودیت‌های قراردادهای سنتی اشاره می کنیم.

محدودیت های قرارداد سنتی

مشکلات فزاینده قراردادهای مالی سنتی را می توان در ۴ مورد زیر دسته بندی نمود(کانت و دیگران، ۲۰۱۵):

- ✓ فرایندهای نامناسب و منسوخ شده: در سال ۲۰۱۲، بیش از ۴ میلیون فکس دریافتی منسوخ شده در خصوص وام سندیکایی[1] وجود داشت.
- ✓ تأخیر در تسویه: میانگین زمان تسویه برخی از وام های اتحادیه ای در امریکا بیش از ۲۰ روز و در اروپا بیش ۴۸ روز است.
- ✓ تقلب: به عنوان مثال اداره تحقیقات فدرال هزینه کلی تقلب در بیمه‌ای غیر از سلامت را بیش از ۴۰ میلیارد دلار در سال تخمین زده است. همچنین ۲ میلیارد دلار تقلب در هزینه صنعت الماس در لندن اتفاق افتاده است.
- ✓ هزینه سربار: بازار سهام استرالیا هزینه های پرداختی بازار سهام استرالیا را که نهایتا به صادرکننده‌ها و سرمایه گذران نهایی پرداخت می گردد، ۴ الی ۵ میلیارد دلار تخمین میزند.
- ✓ ریسک های متمرکز: حجم پول مسدود شده در سیستم تسویه ناخالص آنی بریتانیا که به مدت ۱۰ ساعت آفلاین شد، بیلیون‌ها دلار ارزش داشت. این ضرر معادل با ۲۷۷ میلیارد یورو در روز بوده است.

منافع استفاده از قراردادهای هوشمند برای مشتریان و بانک‌ها

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

- ✓ بازارهای سرمایه و بانکداری سرمایه گذاری
- ✓ تامین مالی شرکتی:عرضه اولیه سهام، سرمایه گذاری خصوصی
- ✓ تامین مالی ساختار یافته: وام های سندیکا و وام های اهرمی
- ✓ زیرساخت بازار بورس اوراق بهادار
- ✓ بانکداری خرد و بانکداری تجاری

[1]Syndicated Loans

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

- ✓ تجارت بین الملل : مستندسازی زنجیره تامین، صورتحساب و پرداخت‌ها
- ✓ قرض وام رهن
- ✓ وام‌ها یا تأمین مالی جمعی برای استارتاپ‌ها و شرکت‌های کوچک و بزرگ

تأمین مالی جمعی برای سهام خصوصی در استارتاپ‌ها، یکی از موارد کلیدی هوش مصنوعی به شمار می‌آید که اولویت روش‌های دیگر نیز می‌با شد. فیلیپ دنیس به برر سی دو مثال از این موارد می‌پردازد که بیشترین تأثیر را دارا ا ست، تخمین تحلیل این نوع کسب وکارها حاکی از این ا ست که اتوما سیون از طریق منطبق شدن با قراردادهای هوشمند، فرایندهای مرتبط و تغییرات سازمانی منافع اساسی را ایجاد خواهد کرد. این تخمین ها بر مبنای تحلیل تکنولوژی، تحلیل فرایندها و عناصر هزینه مقرراتی است که در محیط امروزی وجود دارد و با تکامل سیستم، این تخمین ها نیز تغییر خواهد یافت(بشیر، ۲۰۱۷[1]).

اهداف پژوهش

در این تحقیق اهداف به شرح زیر می باشد:

- ✓ بررسی شکل و ساختار قرارداد های هوشمند
- ✓ طراحی مدلی از قراردادهای هوشمند در نظام بانکداری ایران

سوالات پژوهش

لذا با توجه به مساله اصلی تحقیق، در این تحقیق به سوالات زیر پاسخ داده می‌شود.

مزیت‌ها و عدم‌مزیت‌های قراردادهای هوشمند بر بستر بلاک‌چین و هوش مصنوعی چیست؟

بستر و الگوریتم‌های مناسب برای طراحی مدلی از قراردادهای هوشمند در نظام بانکداری چیست؟

روش تحقیق

پایه هر علمی در حقیقت، روش شنا سی آن علم ا ست. د ست یابی به اهداف علم و یا شناخت علمی در هر رشته ای میسر نخواهد بود، مگر زمانی که با روش شناسی درستی همراه شود. به عبارت دیگر هر تحقیق علمی از باب روش انجام است که اعتبار می یابد و نه موضوع تحقیق(خاکی، ۱۳۸۷).

در این تحقیق برای پاسخ به سوال اول تحقیق از روش بررسی اسنادی، ادبیات پیشینه، مقالات و نتایج تجربی(روش کتابخانه‌ای) استفاده کرده‌ایم.

نکته مهم در این تحقیق این ا ست که این تحقیق به دنبال طراحی مدلی برای قرارداد های هو شمندا ست که

[1]Bashir. I, 2017

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بتواند در بانکداری با توجه به قرارداد های اسلامی، با توجه به شرایط و امکانات موجود قابل پیاده سازی با کارکرد های قرارداد هوشمند مورد استفاده در حال حاضر باشد که جهت طراحی چنین قرارداد هایی میخواهیم از روش های هوش مصنوعی و ابزار ها و الگوریتم های هوش مصنوعی استفاده کنیم. که برای پاسخ به این مساله از ترکیب روش مقایسه تطبیقی و تحلیل محتوایی استفاده کرده ایم.

از آنجایی که ما می‌خواهیم در تحقیق خود به جای استفاده از بلاک چین، از هوش مصنوعی و ابزار های و الگوریتم های آن برای ایجاد قرارداد های هوشمند استفاده کنیم باید یک سیستم محافظ کامل و جامع طراحی کرده که شامل جزئیات زیر باشد:

- حافظت پیشگیرانه : استاندارد سازی در فرآیند نوشتن کدها و شناسایی باگ ها و نقاط خلا در خروجی کد نهایی .
- تایید در حال انجام فرآیند : اجرای کد ها و ارزیابی امنیتی پویا در یک ماشین مجازی برای قرارداد های هوشمند انجام می شود.
- جبران خسارت بعد از حادثه : نتایج و خروجی های قرارداد های هوشمند برای اطمینان از اینکه در جریان فرآیند اجرا هیچ اشتباهی رخ نداده است به طور کامل رسیدگی شوند، به اینمعنی که نتایج قرارداد در یک دامنه قابل اطمینان قرار داشته باشد. صاحبان مشاغل می توانند در هر زمانی که با شرایط سازگار باشند با توجه به آن مورد رسیدگی قرار گیرند.
- تایید و بررسی، زمانی که کد ها به طور کامل نوشته شده اند و منتشر می شوند: مسلما برنامه نویس تمایل دارد که تایید و بررسی قرارداد ها به طور اتوماتیک و منظم انجام بگیرد تا اطمینان حاصل شود که کدهای استاتیک فرآیند بررسی را انتقال دهند، و اینکه تمام باگ‌ها و نقاط خلا را پیدا کنند.
- تایید پویا گره‌ها در هنگام اجرای قراردادها : فرآیند تایید پویا تایید قرارداد و مسائل مربوط به قراردادها را پوشش می‌دهد و وضعیت فرآیند اجرا مورد بررسی قرار خوهد گرفت تا هر باگی که در جریان اجرا پیش آمده را درست کند. حتی اگر یک هکر یک خطا و خلا ای ایجاد کند اجرا کننده های قرارداد برسی های سخت گیرانه ای انجام می دهند و فرایند را متوقف می کنند.
- قضاوت عقلانی بعد از اجرای قرارداد: نتایج پس از اجرای قرارداد از طریق قوانین خاصی قضاوت می شوند و در عین حال، هوش مصنوعی باید برای تجزیه و تحلیل محدوده معقول اجرای قراردادها، به منظور تصمیم گیری در مورد خروجی نتایج نهایی و اینکه آیا هدف برآورده شده است فرآیندی را تعریف کند. برای مثال بررسی حساب ها برای مساله عدم پرداخت دوبار یا چند باره.
- یک مکانیزمی برای فرآیند شکایات و روش هایی برای قضاوت اتوماتیک: در میان گره‌ها برای توسعه قرارداد های هوشمند، هر کدام دارای مکانیسم قضایی و مکانیزم هوش مصنوعی، مبتنی بر رای دادن جهت تصمیم گیری است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

از آنجایی که هر پژوهش علمی با ظهور مساله و یا مجهولی در ذهن محقق شروع می شود، هدف اصلی تحقیق علمی را باید معلوم نمودن مجهول و عبارتی حل مساله و یافتن پاسخ مناسبی برای آن دانست، اما یک پژوهش علمی یک هدف اولیه و یک هدف نهایی دراد. هدف اولیه محقق روشن نمودن مساله خاصی است که با آن روبرو شده استو لی هدف نهایی او دستیابی به معلوم کلی و به عبارتی قضایای علمی کلی است.

این پژوهش از نظر اهداف، اکتشافی است زیرا منابع زیادی برای آن وجود ندارد. روش شناسی این پژوهش از نوع مطالعات اکتشافی و رویکرد تحقیق نیز کیفی است.

خلاصه فصل

در این فصل به معرفی و کلیات طرح پژوهش پرداخته شد، تا برای خواننده روشن گردد که هدف و خروجی پژوهش پیشرو چه خواهد بود. در همین راستا ابتدا به بیان مسئله مورد نظر پژوهش پرداخته شد و مشخص گردید که سیستم موردنظر چه ویژگی‌های کلی خواهد داشت.

در ادامه ضرورت و کاربرد پژوهش تشریح شد و سپس به بررسی اهداف اجرای پژوهش پرداخته شد. بر اساس اهداف، سوالات مورد نظر پژوهش عنوان گردید. همچنین روش تحقیق با توجه به مرور ادبیات تشریح شد. در فصل بعدی مبانی نظری پژوهش مورد بررسی قرار می‌گیرد و مروری بر پیشینه پژوهش نیز انجام خواهد شد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل دوم:

مبانی نظری و ادبیات پژوهش

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقدمه

در سراسر جهان، صنعت بانکداری یکی از ارکان مهم اقتصاد هر کشور به شمار می‌رود و به دلیل ارائه خدمات متنوع مالی و اعتباری، نقش تعیین‌کننده‌ای در تو سعه و ر شد اقتصادی کشورها ایفا می‌کند و می‌توان از آن به عنوان نیروی محرکه، شتاب‌دهنده، متعادل‌کننده و سامان بخش اقتصاد یاد کرد. نگاهی به تاریخچه بانک موید این است که این نهادها علاوه نقش پول، در دادو ستدهای درونی و برونی مسئولیت مبادلات مالی و پولی را در اقتصاد داشته‌اند؛ بنابراین توسعه و بهبود فعالیت‌های بانکی به همراه نظامی کارآمد، نقش عمده‌ای در توسعه و پیشرفت اقتصاد و صنعت بانکداری کشور خواهد داشت(گلمیمی، ۱۳۹۶). لذا هر چه عملکرد بانک‌ها در راستای اهداف اصلی آن‌ها دقیق‌تر و بهتر باشد، بانک‌ها نقش مثبت و سازنده‌تری در توسعه و پیشرفت اقتصاد کشور ایجاد خواهند کرد.

درمباحث نظری مربوط به ارزیابی عملکرد بانک‌ها، مفهوم عملکرد، با کارایی[1] و اثربخشی[2] تعریف شده است. چون اثربخشی بیانگر میزان دستیابی به اهداف است و کارایی به این موضوع اشاره دارد که منابع از نظر اقتصادی، چگونه برای کسب هدف بکار رفته‌اند و می توان آن‌ها را دو بعد مهم عملکرد دانست، یعنی هم علل داخلی(کارایی) و هم دلایل خارجی(اثربخشی) برای بخش های خاص عملکرد، می‌توانند وجود داشته باشند. از اینرو، عملکرد تابعی از کارایی و اثربخشی فعالیت‌های صورت گرفته است.این افزایش کارایی و اثربخشی می‌تواند در حوزه‌هایی مانند تجهیز منابع پولی در بانکداری نوین، فناوری اطلاعات و ارتباطات، مهارت‌های نیروی انسانی، تنوع و کیفیت خدمات بانکی، رضایت مشتریان و مدیریت جهت بهبود مدیریت نقدینگی، مدیریت ریسک، افزایش درآمد، مدیریت ساختار سپرده‌ها، کنترل هزینه‌ها و .....انجام گیرد. هر چند شناخت و فهم درست از حوزه‌هایی که در بانک می‌تواند تغییرات آن‌ها باعث افزایش بهبود و عملکرد بانک‌ها شود، اهمیت دارد ولی مهمتر از این مساله شناخت ابزارها و چگونگی ایجاد تغییرات است. استفاده از هوش مصنوعی و تکنولوژی‌ها مختلف نیزدر همین راستا است که منجر به شکل‌گیری مفاهیم جدیدی در حوزه مالی و بانکی مانند فین‌تک(تکنولوژی مالی)[3]، بانکداری باز[4]، قراردادهای هوشمند و.... شده است. همچنین امروزه در اقتصاد هوشمند، بانک‌ها نقش مؤثری در هموارسازی مسیر رشد و توسعه اقتصادی دارند. با توجه به تغییراتسریع فناوری های نوین، نقش بانک‌ها در بازتعریف و جایگزین نمودن روش‌های سنتی و متعارف ارایه خدمات باروش‌های نوین با اتکا به فناوری‌های جدید، بسیار حایز اهمیت است. در اقتصاد دیجیتالی یا هوشمند، نه تنها بانکداری به سمت صنعت کوچکتری پیش می‌رود بلکه ناچار است تحول بسیاری یابد تا بتواند تامین کننده نیازها و انتظارات فعالان اقتصادی و مشتریان باشد. در اقتصاد هوشمند، نیازی به حضور بانک‌های بزرگی به لحاظ ابعاد فیزیکی نیست و بانک ها از طریق در دسترس قرار دادن خدمات در هر جایی و در هر زمانی به اقتصاد وجامعه کمک

[1]Efficiency
[2] Effectiveness
[3] Financial Technology
[4] Open Banking

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

می‌نمایند. البته این مهم، مستلزم تحول بانکداری متناسب با رشد فناوری است تا زمینه تحقق وتوسعه اقتصاد هوشمند را فراهم سازد. لذا یکی از مهمترین ابزارهای نوین جهت تحقق بانکداری دیجیتال و هوشمند، قراردادهای هوشمند است.

یکی از دلایلی که قراردادهای هوشمند طی دو سال اخیر گسترش یافته است، امکان استفاده از تکنولوژی‌های جدیدی مانند فناوری بلاکچین ا ست. در چند سال اخیر با ظهور انواع شبکه‌های بلاکچین، امکان ثبت قرارداد های هو شمند در بعضی از آن‌ها فراهم شده ا ست. وقتی یک قرارداد هو شمند در یک شبکه بلاک چین ثبت می‌شود، این قرارداد زندگی جاوید پیدا می کند. یعنی تازمانی که آن شبکه بلاکچین کار می کند، اصل قرارداد هوشمند و کلیه تبادلات و تراکنش ها با جزئیات کامل، مستمرا و برای همیشه در شبکه بلاکچین ثبت و نگهداری می شوند. اصولا مزیت و قابلیت فناوری بلاک چین دقیقا این است که پس از ثبت اطلاعات و یا ثبت قرارداد هو شمند، دیگر هیچ انسانی حتی طراح و نویسنده قرارداد هو شمند، نمی‌تواند کوچکترین تغییری در مفاد اولیه قرارداد ایجاد کند و همچنین به هیچ عنوان امکان تغییر تراکنش‌ها و دست‌کاری در آن‌ها وجود ندارد به همین دلیل، شاید بتوان گفت که بزرگترین مزیت قراردادهای هو شمند، عدم فسادپذیری آن‌ها ست(کاظمی نیا و غلامی، ۱۳۹۷).

با وجود مزایایی که این نوع از قراردادهای هوشمند دارند، ولی به دلیل نبود بسترهای لازم و کافی و همچنین وجود یک سری عدم‌مزیت‌ها در ارتباط با بلاکچین، باعث شده مفهوم دیگری از قراردادهای هو شند از منظر ساختار و بستر شکل‌گیری و آناتومی این قراردادها شکل بگیرد که تحت عنوان قرارداد هو شمند مبتنی بر هوش مصنوعی شناخته می‌شوند. لذا در این فصل ابتدا به بررسی انواع قرارادادها از نظر نوع آناتومی و پیاده‌سازی آن‌ها می‌پردازیم. سپس به بیان ویژگی‌های این قراردادها پرداخته و سپس به طور مفصل ویژگی‌های قرارداد هوشمند و انواع آن‌ها را توضیح خواهیم داد و مبانی نظری مربوط به ساختار این قراردادها را بیان می‌کنیم.

انواع قراردادها از منظر پیاده‌سازی

در دنیای امروز توافق و قرارداد شاکله اصلی زندگی اجتماعی را تشکیل می‌دهد و جز لاینفک آن به حساب می‌آید. تمامی انسان‌ها در هر جایگاهی که قرار بگیرند هم تعهداتی را می‌پذیرند و هم تعهداتی را می‌دهند. در این میان قراردادهای، حقوقی و تجاری و غیر تجاری هم در واقع تعهداتی هستند که میان دو طرف قرارداد منتقل می‌شوند با این تفاوت که هر کدام از این قراردادها در قالب خاص و ویژه‌ای در می‌آیند و این امر آن‌ها را از سایر توافقات روزمره متمایز می‌کند. به طور کلی قرارداد توافق دو یا چند نفر برای برقراری رابطه تجاری یا غیر تجاری است. قرارداد معادل فارسی واژه عقد که یک واژه عربی است می‌باشد. در یک طرف قرارداد شخصی قرار دارد که قصد به وجود آوردن قرارداد را دارد که به عمل او ایجاب می‌گویند و در طرف دیگر قرارداد شخصی قرار دارد که ایجاب طرف مقابل را قبول می‌کند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

در این راستا ماده ۱۸۳ قانون مدنی بیان می‌دارد:

" عقد عبارت است از این که یک یا چند فرد در مقابل یکیا چند فرد دیگر تعهد بر امری نمایند و مورد قبول آن‌ها باشد. نکته قابل توجه این است که کسی به تنهایی نمی‌تواند قرارداد منعقد کند و قانون تحقق توافق یا قرارداد را از دو فرد به بالا مقدور دانسته است(شهیدی، ۱۳۸۱).

با توجه به این مفهوم از قرارداد، نوع پیاده سازی آن‌ها از گذشته تاکنون بویژه در سال‌های اخیر با پیشرفت تکنولوژی و هوش مصنوعی تغییرات چشم‌گیری داشته است. این تغییرات شامل قراردادهای سنتی، قراردادهای الکترونیکی، قراردادهای هوشمند می‌باشد.

قراردادهای سنتی

قرارداد سنتی به طور کلی شامل یک یا چند شرکت، گروهی از وکلا، چندین دور مذاکرات، مراحل پیش نویس و بازنویسی و در نهایت پس از مدت طولانی توافق نهایی بر روی قرارداد است. خروجی و نتیجه مذاکرات و طراحی فرآیند همیشه با ذکر جزئیاتی که مربوط به طرفین قرارداد باشد به امضا و توافق نهایی می رسد که اغلب شامل، پیوست ها و بند های اضافی و اصلاحات مختلف است. البته قبل از عصر دیجیتال، نسخه های چنین موافقت نامه‌ها و قرارداد هایی(قرارداد های فیزیکی و سنتی) در فایل نامه‌هایی نگهداری می شد اما امروزه اکثر نسخه‌های قراردادها به صورت دیجیتالی و الکترونیکی در کامپیوتر ذخیره می‌شوند.

البته تعریف اصلی ما از قراردادهای سنتی یا فیزیکی، متمم تعریف قراردادهای هوشمند و الکترونیکی از منظر آناتومی قراردادهاست. به این معنی که قرارداد سنتی و فیزیکی و قراردادهای الکترونیکی و هوشمند از منظر حقوقی و از لحاظ شرایط اساسی قرارداد و تنظیم آثار مترتب بر آن، تابع احکام و قواعد عمومی حقوق قراردادها و تعهدات می‌باشد. ولی از لحاظ ویژگی‌های فنی و روش‌های انعقاد این قراردادها دارای تفاوت هستند. این تفاوت ها در محیط شکل‌گیری وانعقاد قرارداد، نحوه تعیین مفاد قرارداد و مذاکره در مورد مفاد قرارداد، ثبت قرارداد و تبادل داده‌ها واطلاعات و پیاده‌سازی مفاد قرارداد می‌باشد.

در قراردادهای سنتی و فیزیکی طرفین قراراداد بر اساس ماهیت قرارداد در باره مفاد قرارداد به مذاکره می‌پرداختند و در نهایت قرارداد در تجارت ممکن بود به صورت کالا یا بصورت دستی و کاغذی انجام گیرید و در قراردادهای غیر تجاری، اسناد مربوط به قرارداد و خود قرار داد در بایگانی قراردادها ذخیره می‌شده است.

قراردادهای الکترونیکی

تجارت الکترونیکی عبارت از مبادلهٔ اطلاعات تجاری بدون استفاده از کاغذ است که در آن نوآوری‌هایی مانند مبادلهٔ الکترونیکی داده‌ها، پست الکترونیک، انتقال وجه و سایرفن آوری‌های مبتنی بر شبکه بکار برده می شود (عربی، ۱۳۸۹). .قراردادهای الکترونیکی از حیث ماهیت همانند قراردادهای سنتی بوده و برای

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

انعقـــادصحیح آن‌ها باید همان احکام عمومی قراردادها در قانون مدنی را مورد توجه قـــرار داد. تنهـــااز رهگذر شـــکلی با نوع ســـنتی متفاوت بوده و در یک مجرای مجازی و الکترونیکی صـــورت می پذیرند. البته خاصـــیت الکترونیکی قرارداد گاهی سبب می‌شود مسائلی مطرح شـــوند کـــه قواعد عمومی و سنتی قادر به پاسخگویی آنها نبوده و نیاز به وضـع احکام جدید می‌باشـد. باید متذکر شـد که اصـطلاح قرارداد الکترونیکی، برای اولین بار در آیین‌نامه‌ی تجارت الکترونیکی (178, 17, 7, 2000, OJL) اتحادیه‌ی اروپا به‌کار برده شده است که در شمول این آیین نامه در قسمت معاملات تجاری، به و ضع حقوقی یکسان قراراداد الکترونیکی، همانند دیگر قراردادهای مبتنی بر برگه و ابزار سنتی، اشاره شده است و تعریف خاصی از قراردادهای الکترونیکی تصریح نگردیده است.

ماهیت واشکال قراردادهای الکترونیکی

در فضای الکترونیکی در ماهیت قرارداد هیچ تغییری ایجاد نمـــی‌شـــود و تنهـــا بـــه گونـــه ایست که " ابراز اراده" بـرای شـکل گیـری ماهیـت حقـوقی مزبـور از طریـق واسـطه هـای الکترونیکی صورت می‌پذیرد(شکوری مقدم، ۱۳۸۴). بنابراین قرارداد الکترونیکی در مفهـوم مصـدری: «فرآینـد شـکل گیـرییـک ماهیـت حقوقی از طریق واسطه‌های الکترونیکی» مـی‌باشـد، کـه پـس از شـکل گیـری در فضـای الکترونیکی، اوصاف و آثار آن با قراردادهای سنتی تفاوتی ندارد. قانون تجارت الکترونیکی اینگونه قراردادها را با عنوان "عقد از راه دور" تعریـف و بـــه رسمیت شناخته است و در بند «ص» مـــاده ۲ مقرر مـــی دارد: «عقـــد از راه دور عبارتســـت ازایجاب و قبول راجع به کالاها و خدمات بـین تـأمین کننـده و مصـرف کننـده بـا اسـتفاده از وسایل از راه دور».

همانگونه که ملاحظه شد، تغییر در لوازم تبعی و برخی جنبه‌های آیـــین صـــوری انعقـــاد قرارداد از قبیل جایگزین شدن روش‌های کاغذی ارتباط با تسهیلات جدیـــد الکترونیکـــی، در ماهیت قرارداد هیچ تغییریا تبدیلی ایجـاد نمـی‌کنـد و احکـام و آثـار قراردادهـا در هـر دو حالتیکسان می باشد. تنها شیوۀ ظهور آن‌ها متفاوت بـوده و در برخـــی مـــوارد نیـــز مصـــادیق جدیدی مطرح می شـــوند کـــه تحقـــق آن‌هـــا در فضـــای واقعـــی متصـــور نمـــی‌باشـــد و مخـــتص قراردادهای الکترونیکی است که نیازمند تدوین مقررات و قوانین مستقل است. قرارداد الکترونیکی نوع خا صی از قراردادها نیست و بلکه و صف الکترونیکی، فقط بیانگر نحوه تشکیل آن ا ست؛ یعنی شکل این نوع قراردادها به صورت الکترونیکی است و استفاده از اصطلاح قراردادهای سنتی شاید درست به نظر نرسد و تقسیم قراردادها به سنتی، الکترونیکی (و هوشمند) درست نباشد(وصالی، ۱۳۸۵).

به طور کلی، ایجاد رابطه حقوقی در محیط اینترنت بویژه انعقاد قراردادها، در راســـتای حاکمیت اراده و آزادی قراردادها، مادام که بر خلاف آن در قانون و اراده طرفین تصریحی نباشد، تابع شکل و یا تشریفات خاصی نمی‌با شد(صفایی، ۱۳۸۶). یعنی انعقاد قراردادها در ا صل ر ضایی ا ست و ا شخاص می‌توانند با اراده‌های خود در چارچوب قانون هر قراردادی را انعقاد کنند[1]. با توجه به روش‌های فناوری ارتباطات الکترونیکی، شـــکل انعقاد

[1] در حقوق ایران بر حسب قانون و رویه قضایی، شکلی بودن قرارداد، متضمن نوشته بیان اراده و امضای آن از طرف صاحب بیان است.

دسترسی به این مدرک بر پایۀ آیین‌نامۀ ثبت و اشاعۀ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارۀ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایۀ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قراردادهای الکترونیکی یکنواخت نمی‌باشدولی به طور عمده شکل انعقاد قراردادهای الکترونیکی در محیط رایانه در سه شکل متفاوت انجام می گیرد:

- ✓ انعقاد قرارداد بواسطه صفحه وب
- ✓ انعقاد قرارداد بواسطه پست الکترونیکی
- ✓ انعقاد قرارداد بواسطه تبادل داده‌ها

قراردادهای هوشمند[1]

یکی از راه های دستیابی به امنیت، استفاده از کلیدهای خصوصی است. با استفادهاز کلید های خصوصی بر روی بلاکچین کاربران می‌توانند انتخاب کنند که تنها شبکه‌هایانتخابی خودشان اجازه‌ی دستیابی به داده‌ی شخصی آن‌ها را داشته باشند. یکی دیگر از راه های حفظ امنیت و حریم خصوصی مشتری استفاده از قراردادهای هو شمند می‌با شد. قراردادهای هو شمند پروتکل های کامپیوتری می با شند که می توانند شرایط خا صی از یک قرارداد را با د سترسی به تغذیه داده‌ی اضافی آسان کرده، بررسی نموده و یا اجرا کنند. این تکنولوژی نقش یک واسط را بازی می کند و این اطمینان را ایجاد می کند که اشخاص شریک به قوانین تراکنش از طریق استفاده از قراردادهای هو شمند وفادار هستند. قراردادهای هو شمند این اطمینان را می‌دهند که هر کس که قوانینیک سانی را اجرا می کند، از امکان عمل بد جلوگیری می کند(هیلبوم و تیلستروم[2]، ۲۰۱۷).

یکی از سطوح هیجان انگیز توسعه، قراردادهای هوشمند هستند که توسط ابزارهای هوش مصنوعی(بلاکچین و الگوریتم و ابزارهای هوش مصنوعی و یادگیری ماشین) ساخته می‌شوند. یک قرارداد هوشمند یک کد کامپیوتری است که شرایط یک قرارداد را خودش اجرا می کند. اکنون بلاکچین و پایگاه داده‌های دیگری به عنوان پایگاهی که می‌تواند از تراکنش‌های قرارداد هوشمند بی شماری حمایت کند سرویس می‌دهد، و این توانایی را دارد که برای انجام دادن وظایف خاصی بدون نیاز به ورود یا مداخله انسانی برنامه‌نویسی شود. قرارداد هوشمند به ما کمک می کند که پول، دارایی، اشتراکات و یا هر چیز با ارزشی را در یکروش شفاف و بدون ناسازگاری که سرویس‌ها از واسطه اجتناب دارند، تبادل کنیم. بهترین راه برای تشریح قراردادهای هوشمند مقایسه‌ی این تکنولوژی با یک ماشین داد و ستداست. در معاملات معمول، ما به یک وکیل دادگستری یا سردفتر اسناد رسمی مراجعه کرده، هزینه را پرداخت و صبر می کنیم تا سند را به ما بدهند. با قرارداد هوشمند، به سادگییک پول الکترونیکی مثل بیت‌کوین[3] یا هر پول دیگری را برای ما شین دادو ستد قرار داده، و سند ر سمی، گواهی راننده، و یا هرچیز دیگر در حساب کاربری ما قرار می گیرد. قرارداد هوشمند نه تنها قوانین و مجازات مربوط بهیک توافق را به روش یک قرارداد سنتی تعریف می کند، بلکه به صورت اتوماتیک آن‌ها را اجباریمی

[1]نکته مهم در این قسمت این است که مباحث مطرح شده در این قسمت هم شامل smart contract و هم شامل intelligent contract ها می‌باشد.

[2]Erik Hillbom, Tobias Tillstrom, 2017

[3]Bitcoin

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

سازد.

دریک قرارداد هوشـــمند، یک دارایی یا پول رایج به یک برنامه انتقال یافته و برنامه این کد را در چندین نقطه اجرا می کند، سپس به صورت اتوماتیک یک شرط را اعتبار سنجی کرده وتشخیص می‌دهد که آیا دارایی باید به یک شخص داده شده، یا به شخص دیگری بازگردانده شود، ویا اینکه بلافاصله به شخصی که آن را ارسال کرده ا ست پس داده شده یا برخی اعمال ترکیبی انجام شود. در ضمن، لبه‌ی غیر متمرکز سندی که به آن یک امنیت قطعی داده شده است راذخیره و کپی می کند(سمنانی، ۱۳۹۶).

اگرچه برنامه نویسـی قرارداد هوشـمند در خیلی از روش‌ها مشـابه برنامه نویسـی سـنتی اسـت، اماچالش‌های امنیتی جدید و مهمی را به وجود آورده است. قراردادها "play – for – keeps" هستند، زیرا پول های مجازی ارزش واقعی دارند و اگر پول را دریک قرارداد هوشـمند که اشـکال دارد بارگیری کنیم، احتمالا آن را از دسـت خواهیم داد. به علاوه، برنامه نویسی قرارداد هوشمند به دیدگاهی با "فکر اقتصادی" نیاز دارد که برنامه نویس‌های سنتی ممکن ا ست بد ست نیاورده با شند. قراردادها باید به گونه ای نو شته شوند که حتی زمانی که شرکاء برای تقلب در روش‌های مسـتبدانه تلاش می کنند تا سـودهای اقتصـادی‌شـان حداکثر شـود، از بی طرفی آن مطمئن باشیم(آپوو و دیگران[1]، ۲۰۱۶).

به طور کلی قراردادهای هوشمند برنامه‌های کامپیوتری هستند که می‌توانند به طور خودکار می‌توانند شرایط قرارداد را اجرا کنند. بر اسـاس گفته نیک سـازبو[2]، قراردادهای هوشـمند مجموعه‌ای از وعده‌ها، ازجمله پروتکل هایی که در آن‌ها طرفین مطالبات یکدیگر را انجام می‌دهند(انجام وعده‌ها). پروتکل‌ها از طریق برنامه‌هایی در شـبکه کامپیوتر،یا به شـکل های دیگر الکترونیک دیجیتالی انجام می‌شـود بنابراین این قراردادها، نسـبت به قراردادهای کاغذی و قدیمی، هوشمندتر و دقیق‌ترهستند. هیچ استفاده ای از هوش مصنوعی نمی‌شود. این برنامه‌ها مسـاله اجرا و پاسـخگویی را در یک سـیسـتم قابل اعتماد که خارج از محدوده مرزی عمل می کند به انجام می‌ر ساند. با حذف نیاز به دخالت م ستقیم ا نسان، زمانی که یک قرارداد هو شمند در لی ست توزیع شده[3]ا ستفاده شود، برنامه کامپیوتر می‌تواند رابطه قراردادی را کارآمدتر و ارزان ترکند که می‌توانست(در صورت وجود نیاز به دخالت مستقیم انسان) با چند اشتباه، سوءتفاهم، تاخیر یا اختلاف نظر همراه باشد.به طور خلاصه درخواست برای قرارداد های هوشـمند، منجر به دیجیتالی کردن اعتماد از طریق مطمئن شـدناجراوایجاد کارآمدی و بهره‌وری از طریق حذف واسـطه‌ها وهزینه‌های که آن‌ها در هنگام اجرای قرارداد به ارمغان می‌آورند، می‌شـود(لیم و شـائو، ۲۰۱۶[4]).

[1]Paramasiven Appavoo, Mun Choon Chan, Anand Bhojan, Ee-Chien Chang, 2016
[2]Nick Szabo
[3]distributed ledger
[4] Cheng Lim & T. J. Shaw, 2016

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقایسه قراردادهای هوشمند با قراردادهای سنتی و الکترونیکی

قرارداد های هوشمند اساسا یک قرارداد مبتنی بر داده[1] است و قراردادی که طرفین در آن یکیا تعدادی بیشتر شرایطیا مفاد در قراردادشان تعیین می‌کنند به شیوه‌ای که بر اساس سیستم کامپیوتری طراحی شده است. به عبارت دیگر، به جای استفاده از زبان طبیعی، قراردادهای هوشمند از داده های مربوط به امکانات تجزیهو تحلیل کامپیوتری ، اتوماسیون یا ارتباطات مربوط به تعهدات قراردادی شان استفاده می کنند این در واقع اولین تفاوت بین قرارداد هوشمند و قرارداد سنتی است. با این حال با گفتن این مساله که قرارداد هوشمند، یک قرارداد مبتنی بر داده است به این معنی نیست که تمام جنبه های قرارداد در یک فرآیند سیستم کامپیوتری[2]مانند قراردادهای الکترونیکی صورت می‌گیرد.

دومین تفاوت مربوط به مخاطبان تفسیر قرارداد است. قرارداد های سنتی طوری طرحی شدند که افراد قرارداد ها را می خوانند ولی در قرارداد های هوشمند علاوه بر طرفین قرارداد، طرفی دیگری نیز وجود دارد که قرار داد را می خواند و آن هم سیستم کامپیوتری است.

سومین تفاوت بر می‌گردد به رو شی که آن‌ها معنای واقعی و ماهیت واقعی آن را درک می‌کنند و به د ست می‌آورند در یک قرارداد سنتی ماهیت ومعنی اصلی قرارداد از به اشتراک‌گذاری زبانی که طرفین قرارداد استفاده می‌کنند به دست می‌آید ولی در قرارداد هوشمند طرفین، روند صریح ومشخص در فریم‌ورک مربوط به قراردادهای هوشمند را به کار می‌گیرند تا اطلاعات لازم و مربوطه را طبق روند مشخص شده به‌دست آورند.

بنابراین، قراردادهای هوشمند هنگامی که با کد برنامه ریزی می‌شوند، به صورت خودکار ۲ کار را می‌توانند انجام دهند: (۱) درک آنچه بر طبق شرایط وعده داده شده است؛ و (۲) مقایسه آنچه که وعده داده شده در قرارداد با آنچه اتفاق افتاده است. اتوماتیک سازی[3]این امر را ممکن ساخته است که در قرارداد های هوشمند اگر این امکان وجود داشته باشد که بعضی از شرایط و مفاد قرارداد، به یک مجموعه ثابتی از دستوالعمل‌های کامپیوتری تبدیل شوند و همچنین اگر داده‌های مربوط به تایید و قبول برای تطابق با مفاد قرارداد در سیستم کامپیوتری و فرآیند آن قابل دسترس باشد، طرفین قرارداد بتوانند شرایط را برای تایید کامپیوتری به صورت خودکارآماده کنند.

[1]data oriented
[2]computer processable form
[3]Automation

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقایسه ماهیت قراردادهای هوشمند

برای تبیین تفاوت بین قرارداد های هو شمند مبتنی بر هوش مصنوعی و بلاکچین باید به برر سی آناتومی این دو نوع قرارداد پرداخت . اما قبل از آن به طور خلاصـــه به بیان مفهومی از این دو قرارداد می‌پردازیم. نکته ای وجود دارد این اســت که باید توجه داشــت که ماهیت و کاراییعملیاتی این قرارداد ها با وجود تفاوت‌هایی، تقریبا یکسان هستند ولی هرکدام مزیت ها و عدم مزیت‌های خود را دارند.

قراردادهای هوشمند مبتنی بر بستر بلاک چین

در بیـان مفهـوم و تعریف قراردادهای هوشمندنظرات مختلفی ارائه شده است. بـه نظـر برخـی، قراردادهـای هوشـمند، قراردادهایی خود اجرا می‌باشند که به صورت کدهایی در بستر گسترده و نامتمرکز بلاکچین ذخیره می‌گردند. به نظر برخی دیگر قراردادهای هوشمند پروتکل های کامپیوتر می باشند کـه امکان انتقال دارایی های دیجیتالی را تحت شروطی که میان طرفین مورد توافق واقع شده اســـت فراهم می نمایند. برخی دیگر از آن به عنوان یک قرارداد رمزنگاری شده که بـه طـور مسـتقیم انتقال ارزهای دیجیتالی و دارایی های افراد را کنترل می نماید یاد نموده اند و نهایتاً برخی دیگـــر از آن به عنوان د ستورالعمل های الکترونیکی خود اجرا که به صورت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پیش نویش در کدهای کامپیوتری ذخیره شده و به کامپیوتر امکان بازخوانی قرارداد، تقـدیم دسـتور کـار و افزایش هوشمندی قرارداد را می دهد تعبیر نموده انـد(ساموئل و دیگران،۲۰۱۴). با جمع بنـدی اقـوال فـوق مـی تـوان قراردادهای هوشمند را به عنوان قراردادهای الکترونیکی که در بسترهای عمومی منعقد گردیده و عوض قراردادی در آن‌ها دارایی های هوشمند یا ارزهای رمزنگـاری شـده دیجیتـالی می باشد تعریف نمود. در حال حاضـر امکان انعقاد این نوع قراردادها در معاملاتی که یکی از طرفین معامله تعهد بر انجام یا عدم انجام عملی را می نماید وجود ندا شته و تنها در معاملاتی که انتقال عین یـا منفعت مورد معامله به طرفین مقصود طرفین با شد کاربرد دارد. این قراردادها از زمـان انعقـاد تـا امضا و تأیید نهایی توسط متعاملین تحت نظارت قوه حاکم و هوش مصنوعی انجام مـی شـوند.

مفهوم قراردادهای هوشمند در ابتدا توسط فردی به نام نیک سازبو با اختراع ماشین های پرداخت خودکار به صـورت کاملا پیش پا افتاده در سـال ۱۹۹۰ مطرح گردید(الن و برامرتز، ۲۰۱۶) . به گونه ای که در ابتدا قراردادهای انجام یافته توسط سیستم های رایانه ای که محاسبه‌گر دریافت‌ها و پرداخت های مـالی روزانه بودند برای چند دهه در امریکا و برخی کشورهای توسعه یافته پا به عرصه نهادند بعدها بـا گسترش قراردادهای هوشمند در بستر تکنولوژی بلاک چین و اختراع بیت کوین و استفاده آن در معاملات انجام یافته حیطه انجام این معاملات گسترش هر چهبیشتر یافـت (الکس و دان، ۲۰۱۶). این قراردادها پس از تأیید نهایی، توسـط هـوش مصـنوعی بـازخوانی و بـا توجـه بـه دارا بـودن خصیصه خوداجرایی و شفافیت، در صورت عدم مغایرت مفاد قرارداد با دستورالعمل داده‌شـده بـه هوش مصنوعی، در بستر بلاک‌چین ثبت و جهت مشاهده عموم عرضه شده و توسط هر فردی بدون امکان تغییر مفاد آن یا دستکـاری در قـرارداد بـدون وجـود هرگونـه ابهـام در مفـاد آن قابل مشاهده هستند.

عناصر قرارداد هوشمند

قراردادهای هوشمند سه جزء اساسی دارند که به‌عنوان اجزای قرارداد هوشمند شناخته می‌شوند. اول امضای دیجیتال که طرفین قرارداد با آن بر مفاد و قوانین قرارداد توافق می‌کنند. جزء بعدی موضـوع قرارداد اسـت. این جزء باید در محیط قرارداد باشـد یا قرارداد هوشـمند به آن دسـترسـی مسـتقیم داشـته باشـد. اگرچه مفهوم قرارداد هوشمند اولین بار در سال ۱۹۹۶ مطرح شد اما نبود این بخش، پیاده‌سازی آن را تا سال ۲۰۰۹ و ظهور رمزارزها به تاخیر انداخت. هر قرارداد هوشـمند باید شـروطی نیز داشـته باشـد. باید بتوان این شـروط را به‌صـورت ریاضـی و منطقی و به‌وسـیله زبان برنامه‌نویسـی در محیط قرارداد هوشـمند پیاده‌سـازی کرد. همچنین این شـروط باید خواسته‌های طرفین را تأمین و در صورت بروز اختلاف میان طرفین خسارات وارده را پوشش دهد.

محیط قرارداد هوشمند

قراردادهای هوشـمند باید در محیط مناسـب کار کنند تا عملکرد درسـتی داشـته باشـند. این محیط باید با

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

استفاده از کلید عمومی رمزنگاری شده باشد و به کاربران اجازه دهد با کدهای رمزنگاری شده منحصربه‌فرد خود وارد آن شوند. این دقیقاً همان سیستمی است که بیشتر رمزارزهای موجود، از آن استفاده می‌کنند.همچنین وجود یک پایگاه داده غیرمتمرکز و خودکار که تمام ذینفعان قرارداد بتوانند به آن اعتماد کنند ضروری است. علاوه بر این خود محیط نیز باید غیرمتمرکز باشد. زنجیره‌بلوک و به‌خصوص زنجیره‌بلوک اتریوم محیط ایده‌ال برای پیاده سازی قراردادهای هوشمند است. درنهایت منابع و داده‌های دیجیتال مورد استفاده در قراردادهای هوشمند باید قابل‌اعتماد باشند. به این منظور از پروتکل‌های ارتباط امن که در بیشتر نرم‌افزارهای مدرن امروزی به‌طور خودکار وجود دارند استفاده می‌شود(استارک، ۲۰۱۶[1]).

قرارداد های هوشمند مبتنی بر هوش مصنوعی

این نوع قراردادهای هوشمند شامل جزئیات و ویژگی های حفاظت پیشگیرانه، تایید در حال انجام فرایند، جبران خسارت بعد از حادثه، بررسی و شناسایی باگ‌ها، تایید گره‌های فعال در انجام قراردادها، قضاوت مبتنی برمفاد قرارداد و ... می‌باشد که این جزئیات با استفاده از الگوریتم‌ها و ابزارهای هوش مصنوعی انجام می گیرد. برای هر قسمت از این ویژگی‌ها و اجرای آن می توان از الگوریتم‌های مختلف استفاده کرد. یکی از مباحث مهم بستر ایجاد این قراردادها و امکانات آن است که این قراردادها در چه بستری انجام گیرد که می‌توان از رادیکس[2] که اولین پلتفرم غیر بلاکچینی با سیستم غیر متمرکز است، استفاده کرد. یا می توان از شبکه های غیرمتمرکز به این معنی که ذخیره داده‌ها از ابتدای تایید هویت تا تایید تراکنش در چند مرکز مستقل از هم صورت بگیرد استفاده کرد. یا از شبکه‌های نیمه متمرکز جهت پیاده‌سازی پلتفرم‌های قراردادهای هوشمند مبتنی بر هوش مصنوعی ستفاده کرد.

در مرحله حفاظت پیشگیرانه که مربوط به استاندارد سازی کدها و تشخیص باگ ها می باشد می توان از ابزارهای استاندارد سازی کدها مانند CSSO برای برای بهینه سازی ساختاری فایل های سی اس اس یا سایر ها ابزارها با توجه به نوع زبان استفاده شده برای نوشتن کد قرارداد هوشمند استفاده کرد.

تایید فرایند قرارداد های هوشمند در ماشین مجازی انجام می گیرد. فرآیند ماشین مجازی[3] که به ماشین مجازی اپلیکیشن نیز مشهور است گونه دیگری از ماشین‌های مجازی‌هاست که مشابه یک اپلیکیشن معمولی در سیستم عامل رایانه میزبان اجرا می‌شود. هدف از طراحی این ماشین‌ها ایجاد محیطی مستقل از پلتفرم است که امکان اجراییک برنامه روی هر پلتفرمی را فراهم می‌آورد. این ماشین‌های مجازی بر اساس یک مفسر ساخته می‌شوند و از مشهورترین آن‌ها می‌توان به ماشین مجازی جاوا[4] Common Language Runtime اشاره نمود که به ترتیب برای اجرای برنامه‌های جاوا و برنامه‌های مبتنی بر ساختار شبکه[5] طراحی شده‌اند(Oliphant,

[1] Stark, 2016
[2] Radix
[3] Process Virtual Machine
[4] Java Virtual Machine
[5] Net Framework

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

.(2016

ساختار و چگونگی پیاده‌سازی قراردادهای هوشمندمبتنی بربلاکچین

قرارداد هوشمند بر روی یک پایگاه ارز دیجیتال[1] ساخته می شوند. یک ارز دیجیتال یک سیستم غیرمتمرکز برای فعل و انفعال دا شتن با پول مجازی در یک دفترکل سرا سری ا شتراکی می با شد.کاربران با انت شار پیام‌های امضاء شده به نام تراکنش‌ها به شبکه‌ی ارز دیجیتال پول را مبادله کرده و با قراردادها تقابل می کنند. شبکه شامل گره هایی هســت(miners)که اطلاعات را منتشــر، داده را ذخیره، و داده‌ها را با به کار بردن تراکنش‌ها آپدیت می‌کنند. واسط اصلی فراهم شده توسط شبکه‌ی ارز دیجیتال زیرین یک فایل ثبت وقایع پیوست شده است که یک بلاکچین نامیده می‌شــود، که یک مرتب ســازی جزئی یا کلی را بر روی تراکنش‌های ارائه شــده توســط کاربران تحمیل می‌کند(ســمنانی، ۱۳۹۶). لذا ابتدا باید به توضــیح بلاکچین و چگونگی عملکرد آن بپردازیم تا با نحوه عملکرد قراردادهای هوشمند آشنا شویم.

بلاکچین

ظهور و پیدایش تکنولوژی بلاکچین به طور کامل به پیدایش بیت کوین[2]، ارز دیجیتالی غیر متمرکز در اینترنت، مربوط می شــود . ناکاموتو در ســال ۲۰۰۸ توضــیح داد که چطور یک شــبکه از کاربران می توانند در امنیت تراکنش های مالی خود را با کاهش هزینه و کاهش واسطه های مالی و کاهش هزینه های مربوط به پرداخت مالی را انجام دهند. در طی انجام این کار، بااین حال، ناکاموتو یک ساختاری به نام بلاکچین را توصیف کرد، همراه با یک پروتکل ارتباطی، که به طور کلی و اساسی مساله ژنرال‌های بیزانس[3] را حل کرد، بنابراین شبکه قادر است قراردادی در آن به توافق برســد بدون اینکه به آگاهی و دانشــی در مورد هویت کاربران و اعتماد به طرف مقابل نیاز باشد.

بلاکچین در فرم خام خود، بیشتر به یک دفترچه یادداشت یا دفتر کل[4] یا بطور ساده تر می توان آن را یک پایگاه داده[5]دارای ترتیب زمانی وقوع[6] از معاملات ثبت شــده در یک شــبکه کاپیوتری اســت. اصــطلاح بلاکچین به این معاملاتی که در این بلاک‌ها گروه بندی می شــوداشــاره دارد و زنجیره ای از این بلاک‌ها که تاریخ تراکنش‌ها از آغاز بلاکچین درآن پذیرفته شده است شکل می گیرد. در چنین بلاکچینی، هر کسی سعی می کند با یک رکورد

[1]cryptocurrency
[2]Bitcoin
[3]in the Byzantine Generals' problem, introduced by Lamport *et al.* [1982], a group of ByzantineGeneralsarecamped around an enemy city in different locations. If they all attack simultaneously, then they have superiorfirepower to their enemy. The problem is that they need to agree a common battleplan, so that they attack at thesame time, with the additional complication that there may be a traitor amongst their ranks.
[4]ledger
[5]Data base
[6]chronological

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

و مدیریت جدید یک بروزرســـانی جدید برای دفتر کل بلاک چین آماده کند، که آن ها با کلید رمزنگاری خصوصی آن‌ها امضا شده‌اند.(پانایی و پیتر[1]، ۲۰۱۵).

ویژگی های بارز بلاکچین همچون غیر قابل تغییر بودن، ارائه محیطی بدون نیاز به اعتماد متقابل طرفین تجارت، قابلیت بازگشت به حالت تعادل درصورت ایجاد تغییرات غیر قانونی، استفاده از الگوریتم رمزنگاری هش و فرایند اجماع موجب شده این تکنولوژی به یکی ازبهترین پیشرفت‌های دنیای تکنولوژی تبدیل شود و بسیاری از الزامات محاســـباتیِ مســـائل دنیای واقعی را حل نماید. انقلابلاکچین با ارائه قراردادهای هوشـــمند و بلاکچین‌های قابل برنامه‌نویسی به نام اتریوم دستاوردهای عظیمی داشته است(مادریا[2]، ۲۰۱۷).

برای اطمینان از اینکه تنها تراکنش های قانونی در بلاکچین ثبت شـده اند، شـبکه تراکنش های جدیدی که معتبر هسـتند را تصـدیق می کند، با توجه به تاریخ تراکنش های ثبت شـده در بلاک های قبلی. یک بلاک جدیدی از داده ها به پایان زنجیره ا ضافه خواهد شد تنها بعد از اینکه کامپوتر های مربوط به شبکه در مورد اعتبار و در ست بودن تمام تراکنش هایی که تا آن لحظه انجام شده به توافق برسند. بنابراین تنها تراکنشی که معتبر است (در بلاک تصدیق شده ا ست[3]) در یک بلوک قرار می گیردو در شبکه منتشر می شود. به این ترتیب پروتکل های بلاک چین قادرند مطمئن شوند که تراکنش‌های مربط به بلاک چین همگی معتبر هستند و هرگز رکوردی بیش از یکبار ثبت نمی شود و افراد را قادر می سازد مختصات تراکنش‌های افراد را بدون اینکه نیازی به تایید هویت و اعتماد به آن‌ها باشـــد به روش غیر متمرکز تایید کنند و تمام معاملات را به صـــورت واضـــحی درک کنند(بوئیتن‌هک[4]، ۲۰۱۶).

درســـت مانند تعداد زیادی از تکنولوژی های دیگر در اینترنت، بلاکچین به کلید عمومی رمزنگاری شـــده[5] برای حفاظت کاربران از اینکه شـخص غیر مجازی بر حسـاب های آن ها کنترل داشـته باشـد بسـتگی دارد.هر دو کلید خصوصی و عمومی افراد را قادر می سازد تا اطلاعات را برای اینکه به یک فرد دیگر انتقال دهند،پنهان کنند. آن طرفی که آن پیام را دریافت می کند قادراسـت مشـخص کند که آیا این پیغام واقعا یک پیام اصـلی اسـت یا این پیغام دستکاری شده است.این یک مساله کاربردی و حیاتی است، زمانی که یک شخص با شبکه ارتباط برقرار می کند و یک تراکنش بین دو طرف مورد موافقت قرار گرفته باشد.

در این زمینه، یک مفهوم کلیدی به نام توابع هش[6]وجود دارد. ایده اصـــلی در اســـتفاده از توابع هش ، امکانات و کاربرد این توابع در جستجوی اطلاعات در یک مجموعه از رکوردها است.در تعریف کاملا کلاسیک تابع هش، به هر تابعی که اســـتفاده شـــود برای مطابقت دادن و مپ کردن هر داده با اندازه‌های مختلف به داده‌های با اندازه ثابت که خروجی آن یک نوع داده رشته‌ای با اندازه مشخصی از بیت باشد به عنوان مقدار هش، گفته می‌شود. این

[1]Gareth W. Peter&Efstathios Panayi،
[2]Madeira, A
[3]Confirm
[4]Mark Buitenhek
[5]Key Cryptography
[6]Hash

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقادیر هش در یک فرم جدولی شناخته شده به عنوان جدول هش ذخیره می شود و در هنگام انجام جستجو به عنوان یک مکانیزم نمایه‌سازی کارآمد استفاده می‌شود(هاسیو[1]، ۲۰۱۷).
به نظر می‌رسد زمانی که توابع هش و جدول‌های هش با تکنیک‌های رمزنگاری ترکیب می‌شوند، نتایج رمزنگاری توابع هش مستقیما و کاملا برای سازماندهی و ایجاد پروتکل‌های امنیتی و خصوصی که مورد نیاز تکنولوژی دفتر کل بلاک چین است،می‌تواند مورد استفاده قرار بگیرد. در این زمینه می‌توان یک هش رمزنگاری را به عنوان یک امضا برایک متن یایک فایل داده مورد استفاده قرار داد. این مساله امن است چرا که توابع هش رمزنگاری شده اجازه می‌دهد هر کسی به آسانی بتواند داده‌های ورودی مربوط از کاربر دیگر را با مطابقت دادن با مقدار هش داده شده و تعیین شده، تایید کند، اما اگر داده ورودی ناشناخته باشد، دوباره ساختن آن، با شناختن مقدارهش ذخیره شده، کار بسیار مشکلی است(اشفاق[2]، ۲۰۱۹). در نتیجه تقریبا غیر ممکن است که دو بار، در وسط معامله، خرج شود[3].

تکنولوژی بلاکچین نشان دهنده گام بعدی در اقتصاد مربوط به نفر به نفر است. و این گام بعدی با ترکیب شبکه‌های نفر به نفر می باشد، الگوریتم های رمزنگاری ، توزیع داده ذخیره شده و مکانیسم های اجماع غیر متمرکز، زمینه ای را ایجاد می کند برای افراد، تا یک توافق خاص از منظر ثبت، با شیوه‌ای امن و قابل تایید ایجاد کنند.

بلاکچین رمز نگاری شده و سازمان دهی شده به دیتا بیس[4]های کوچکتر بنام بلاک[5] است. هر بلاکی شامل اطلاعاتی در مورد تعداد خاصی از تبادلات ویک مرجع برای بلاک پیشین در زنجیره بلاک است. همچنین یک پاسخ به معمای ریاضی پیچیده است که برای اعتبار سنجی داده مرتبط با آن بلاکاستفاده می شود.از آنجایی که بلاکچین همیشه در وضعیت همزمانی[6]قرار دارد، تنها یک رکورد واقعی برای مالکیت اصلی[7]وجود دارد تا از هر کسی که سعی می کند دارایی‌هایش را در یک زمان به چند نفر بفروشد جلوگیری کند.

چگونگی عملکرد قرارداد هوشمند مبتنی بر بلاکچین

قرارداد هوشمند، اسکریپت‌هایی هستند که در بلاکچین ذخیره شده‌اند و به دلیل اینکه روی زنجیره قرار گرفته‌اند، یک آدرس یکتا دارند. ما یک قرارداد هوشمند را با آدرس دهی یک تراکنش به آن نشانه می رویم، سپس به صورت مستقل و اتوماتیک در یک روش تعیین‌شده روی هر گره در شبکه براساس داده‌ای که در تراکنش مدنظر است، اجرا می کنیم. قرارداد هوشمند به ما اجازه می دهد که محاسبات کلی مورد نظر را در d

[1]Jerry I-H Hsiao
[2]Muhammad Ashfaq
[3]Satoshi Nakamoto
[4]Database
[5]Block
[6]Synchronization
[7]ownership-essential

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

زنجیره انجام دهیم(کریستیدیس و دیگران[1]، ۲۰۱۶).

یک مثال، یک بلاکچین با مشـــارکت باب، آلیس و کارل رادر نظر بگیرید، دارایی های دیجیتال از نوع Xو Yمبادله می شوند. باب یک قرارداد هو شمند روی شبکه ایجاد می کند که این گونه تعریف میشود. (a)تابع سپرده یا حساب[2] او اجازه می دهد که واحدهایXرا برای قراردادذخیره کند. (b) تابع مبادله[3]که در ازای دریافت هر ۵ واحد از Y،۱ واحد از X(از ذخیره خود قرارداد برمی گرداند. و (C) تابع برگرداندن[4] به باب اجازه می‌دهد که کل دارایی‌هایی که قرارداد نگهداری می کند را برگرداند. توجه کنید که توابع سپرده و برگرداندن به گونه ای نوشته شده اند که فقط باب به کلیدخودش می‌تواند آن‌ها را بخواند، زیرا این چیزی است که باب خواسته است، هم چنین آن چیزیکه برای این مثال مهم است:

آن‌ها می‌توانند نوشته شوند بنابراین می‌توانند توسط هر کاربر روی شبکه فراخوانی شوند.

باب یک تراکنش به آدرس قرارداد هوشمند ارسال می کند، تابع سپرده را فراخوانی کرده و ۳ واحد ازXرا به قرارداد می‌فرستد. این تراکنش روی بلاکچین ذخیره شـده اسـت. آلیس که مالک ۱۲ واحد Y اسـت، یک تراکنش می فرســتد که۱۰ واحد از Yرا به تابع مبادله قرارداد حرکت داده، و ۲ واحد Xرا پس می گیرد. این تراکنش نیز بر روی بلاکچین ذخیره می شود. باب سپس یک تراکنش امضاء شده به تابع برگرداندن قرارداد می فرستد. قرارداد امضاء را چک می کندتا مطمئن شود که برگرداندن توسط مالک قرارداد ایجاد شده است، و تمام دارای اش ۱واحد Xو ۱۰واحد Yرا به باب برمی گرداند. موارد زیر را مشاهده می کنیم:

۱- قرارداد حالت خودش را دارد و می‌تواند از دارایی‌هایش روی بلاکچین محافظت کند. بدین صورت که انگار قرارداد حسـاب خود را روی بلاکچین داشـته و بلاکچین یک مدل براسـاس حسـاب کاربری را پشـتیبانی می کند. در مثال بالا می‌تواند دارایی های Xو Yرانگهداری کند.

۲- قرارداد به ما اجازه می‌دهد که منطق کاری را بیان کنیم(در کد): تجارت ۱واحد X برای هر ۵ واحد Yدریافتی.

۳- یک قرارداد هوشـمند به درسـتی نوشـته شـده باید تمام خروجی‌های ممکن قرارداد را شـرح دهد. برای مثال، تابع مبادله ممکن است نوشته شده باشد بنابراین برای نپذیرفتن پیشنهادهایی که موجب کمیت هایی از Yمی شود که ۵ واحد نیستند، مثلا ۱۲ واحد از Yپذیرفته نشده و رد می‌شود. یا تابعی نوشته شود که ورودی را به عنوان بزرگترین مضـرب۵ (که بدون مواردی مبادله خواهد شـد) و یک باقی مانده (که برگردانده خواهد شـد) تجزیه می کند. یک پیشنهاد ۱۲ واحدی از Y ،۲ واحد ازX و ۲ واحد ازYرا به فرستنده برمی گرداند.

[1]Christidis & Devetsikiotis
[2]deposit
[3]trade
[4]withdraw

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۴- ارتباطی که باب می‌خواهد با شـرکایش ایجاد کند با داده کنترل می‌شـود. یک تراکنش یک سـاختار داده‌ی امضـاء شـده می‌باشـد که یک انتقال ارزش نشـان می‌دهد. باب قرارداد هوشـمند ایجاد می کند که به طور کارا می گوید: "اگر تواین قرارداد را برای این داده(۵واحد Y)، چگونه پاسخ داده خواهد (۱ واحد X).

۵- یک قرارداد هوشمند توسط پیام ها/تراکنش هایی که به آدرس آن ارسال می شوند نشان داده می شود.

۶- یک قرارداد هوشـمند قطعی اسـت: ورودی یکسـان همواره خروجی یکسـانی تولید می کند.اگر کسـی قرارداد غیرقطعی بنویسـد، وقتی که راه اندازی می‌شـود بر روی هر گره‌ی شـبکه اجرا خواهد شـد و ممکن اسـت نتایج رندم مختلفی را برگرداند، بنابراین شـبکه را از بدسـت آوردن اتفاق آرا روی نتایج اجرایی منع می کند. یک قرارداد هوشمند روی بلاکچین و کد آن می‌تواند توسط هر عضو شبکه بررسی وکنترل شود.

۸- به این دلیل که تمام تقابل‌ها با قرارداد از طریق پیام‌های امضـاء شـده بر روی بلاکچیناتفاق می‌افتد، تمام اعضای شبکه یک پیگیری تایید رمزگذاری از اعمال قرارداد بدست میآورند.

قراردادهای هو شمند به عنوان عامل های خودمختار عمل می کنند، که رفتار شان کاملا قابل پیشبینی ا ست. آن‌ها می توانند برای اجرای هر منطق روی زنجیره که می‌تواند به عنوان یک تابع ورودی های داده روی زنجیره قابل اعتماد باشـد، داده‌هایی که آن‌ها برای مدیریت نیاز دارند فراهمکنند. قراردادهای هوشـمند همچنین مفهوم DAOs7را دارا می باشـند، اگر یک پروسـه‌ی حتمی درقرارداد دنبال شـود، موجودیت‌های روی بلاکچین رفتار شان ممکن ا ست ا صلاح شوند. ساده‌ترینمثالیک قرارداد هو شمند این ا ست که قرارداد دیگری را با آدرس برای اجرای تابع اصـلی‌اشـفراخوانی می کند. این آدرس در قسـمت ناپایدار پایگاه داده داخلی قرارداد، قرار دارد. قراردادهمچنینیک لیست از اعضاء و آدرس ها (کلیدهای عمومی) را نگهداری می کند که برای رفتارشرای گیری می کند. یک قانون در قرارداد می‌تواند شامل این باشد که اگر اکثریت رای دهندگانرای دهند، قرارداد رفتارش را با فراخوانی آدرسـی که اکثریت آراء برای اجرای تابع اصـلی دریافتشـده اسـت، اصـلاح می کند(کریسـتیدیس و دوستسیکوتیس، ۲۰۱۶؛ کاچین و دیگران، ۲۰۱۶؛ بونه و دیگران، [1]۲۰۱۲).

محدودیت‌ها و عدم مزیت‌های بلاکچین و قراددادهای هوشمند مبتنی بر بلاکچین

محدودیت های قرارداد هوشمند مبتنی بر بستر بلاکچین

با این حال تردید هایی در مورد استفاده از قراردادهای هو شمند باقی مانده است. به عنوان مثال برخیمفسرین در مورد مطلوبیت قراردادهای هو شمند سوال مطرح می کنند، بخصوص در مورد استفاده قراردادهای هو شمند در ارتباط با قراردادهایی که ارزش پایینی دارند یا تبادلات ساده مالی مانند خرید و فروش یک ماشین[2]حتی در مورد

[1] Christidis & Devetsikiotis, 2016 ;[1]Cachin & et.al, 2016 ; [1]Boneh & et.al, 2012

[2]Andy Robinson and Tom Hingley, Smart Contracts: The Next Frontier?, OXFORD LAW FACULTYBUSINESS LAW BLOG, https://www.law.ox.ac.uk/business-law-blog/blog/2016/05/smart-contractsnext-frontier (May 23, 2016).

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قرارداد های خرید و فروش ساده، فقط بخشی از مفاد این قراردادها مانند پرداخت وجوه، انتقال مالکیت و انتقال عناوین برای ا شترک گذاری تبدیل به قراردادهای هو شمند خواهد شد. با این وجود، اقدامات دیگر مانند نظارت بر نقض های گارانتی[1] ممکن است هنوز به صورت دستی و توسط انسان انجام شود.

علاوه بر این،از آنجایی که طرفین قرارداد می توانند از برنامه نویس بخواهند قرارداد هوشمند را متناسب با نیاز های آن‌ها طراحی کند، اگرچه این امر قدرت و مساله مذاکره، توسط مشتریان را به مبادلات و تبادلات آنلاین بر می گرداند، اما با این وجود هزینه های معاملات قرارداد های هوشمند نسبت به قرارداد های استاندارد سنتی افزایش پیدا می‌کند. مواردی نیز وجود دارد از حمله‌ی اخیر به سازمان خودمختار توزیع شده[2](DAO)، که در آن یک مجموعه از قراردادهای هوشمند توسط یکی از مشارکت کننده‌ها به میزان ۵۳ میلیون دلار که نقطه ضعف این قراردادها را در کد فهمیده بود قبل از بازگردانده شدن آن به سیستم کامپیوتری با مصرف و خرج کرد.

ارتباط با جهان فیزیکی

این شک و تردید ها به این دلیل که تبادلات تجاری اغلب پیچیده هستند و جود دارد. قرارداد های هوشمند می تواند به میزان زیادی غیر قابل انعطاف پذیر باشد، و شرایط و مفاد و منابع طرفین آن غیر قابل تغییر باشد. گاهی اوقات ممکن است زمانی که قابل پیشبینی نبود توسط طرفین مبادله مفاد و شرایط قرارداد تغییر پیدا کند مانند زمانی که وارد قرارداد شده اند.یا طرفین ممکن ا ست به دلیل غیر قابل پیشبینی مساله و مشکلی برای آن‌ها در زمانی که وارد قرارداد شده اند پیش آید اما عمدا از بیان آن ها درطول مذاکره خودداری کرده‌اند به دلیل ترس یا به دلیل اینکه شکست بخورد یا طرف قرارداد راضی به انجام مبادله نشود. طرفین ممکن است همچنین در شرایطی باشند که نخواهند مفاد قرار داد به طور کامل و دقیقا اجرا شود. از این رو، تهیه پیش نویس قرارداد با استفاده از زبان طبیعی به این سطح ابهام اجازه می دهد. برای مثال، راه اندازی سیستم ثبت نام زمین مبتنی بر بلاک چین بر روی یک سرور یا کد کردن قرارداد هوشمند مبتنی بر بلاک چین ممکن است بخش آسان این کار باشد. تایید اینکه یک شخص ادعا می کند که او یک تیکه از زمین دارد یا تایید اینکه نگه دارنده کلید عمومی، اغلب کار غیر ممکنی خواهد بود. به طور کلی، تمام قوانین و تعهدات و وظایف برنامه های کاربردی مبتنی بر بلاک چین باید مبتنی بر قانون قابل اجرا باشد و اغلب تصدیق توسط دولت یا شخص ثالث، و سازماندهی لینک فیزیکی اغلب پرزحمت ترین و گرانترین بخش‌هایی است که باید برطرف شوند(گئو و لیانگ[3]، ۲۰۱۶).

قرارداد هوشمند به عنوان یک قرارداد کامل؟

اگر قرارداد های هو شمند کد های کامپیوتری غیر قابل تغییر، غیر قابل توقف و غیر قابل انکار هستند، کدها به طور ضمنی یا به طورصریح بیان می کنند که جه اتفاق ها و وقایع قابل ممکنی در طول زندگی اتفاق خواهد

[1]monitoring warranty breaches
[2]Distributed Autonomous Organization
[3]

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

افتاد.با این حال اکثر قرارداد های سنتی کامل نیستند به این معنی که دقیقا مشخص نیست در موقعیت های جدید و آینده چه اتفاقی خواهد افتاد اما ترجیح می دهد که در آینده مشخص شود.دلایلی وجود دارد که چرا قرارداد ها ناقص ، اینقدر رایج هستند، واضح ترین دلیل این است که هزینه های زیادی برای پیش بینی و پذیرش شرایط قرارداد غیرمستقیم برای هر مجموعه ای از شرایط وجود دارد. قراردادهای ناقص همچنین بازنگری در مذاکرات را ارزان تر یا کارآمدتر می کنند.

قرارداد های هو شمند این گونه طراحی می شوند که یک قرارداد کامل با شند با تمرکز بر روی قرارداد های ex ante تا قرارداد های ex post. با این حال مورد سازمان خودمختار غیرمتمرکز(DAO) نشان داد که قرارداد هوشمند غیر کامل بود و نشان داد که اشتباهات کد نویسی می تواند منجر به جابه جایی ثروت به صورت غیر منتظره شود.علاوه بر این قرارداد هوشمند ممکن است منجر به قرارداد های پیچیده تجاری و غیر قابل پیش بینی شود که در کد کردن پاسخ های احتمال به سوالات احتمالی شکست بخورد. همچنین این قرارداد دارای مسائل دیگری نیز مانند تقلب، فشار، فقدان ظرفیت قانونی، و عدم اطمینان ا ست. به صورت سنتی اگر این مسائل اتفاق بیفتد دادگاه این مشکلات را حل خواهد کرد. یک قرارداد هوشمند هدف آن حذف واسطه ها مانند دادگاه ا ست احتمالا عواقب جدی دارد. برای قرارداد های هو شمند تا جایگزین قرارداد های سنتی شوند، آن نیاز دارد که نشان دهد فواید مورد انتظار این نوع قراردادها برای طرفین قرارداد بیشتر از هزینه های مربط به این نوع قرارداد ها باشد نه اینکه چنین قرارداد های تمام مشکلات مربوط به قرارداد های سنتی را حل می کند.

قرارداد قانونی و قرارداد هوشمند[1] `

از آنجا که قرارداد هو شمند یک برنامه کامپیوتری ا ست، مو ضوعات خا صی مطرح می شود که تعهدات قراردادی پیچیده هستند. برای مثال اول، طرفین قرارداد در مورد مفادی از قرارداد که قابلیت ارزیابی به طور قطعی توسط برنامه کامپیوتری را ندارند مذاکره کنند، دوم، ممکن است طرفین قرارداد مفاهیم غیر منطقی یا ، غیر مناسب که برای تعیین الگوریتم مناسب نیستند وارد کنند ، سوم، بیانیک تعهد در کد ممکن است دقیقا توافق طرفین را منعکس نکند؛ و چهارم، قرارداد ممکن ا ست شامل توافق بیشتری برای توافق یا مکانیسم برای ا صلاح قرارداد باشد.

مسئله مربوط به قرارداد هوشمند حتی زمانی برجسته است که بخواهد به طور مستقل از چارچوب قانونی اطراف اتفاق بیفتد. بنابراین چه اتفاق هایی می افتد اگر کدهیی که زده می شود با فهم طرفین قرارداد مطابقت نداشته باشد؟؟

چه اتفاقی می افتد اگر اثر کد نشان داده شود، توسط یک بخش متفاوتی که اطلاعات درستی در آن وجود نداشته باشد؟؟

[1]Contract Law and Smart Contract

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کد نمی تواند همه چیز را در نظر بگیرد، مانند بحث های فوق، قرارداد هوشمند در موارد محدود به کار برده می شود، زیرا نمی تواند انعطاف پذیری کامل در همه قراردادهای هوشمند را تضمین کند.

با این حال، کدها زبان طبیعی نیستند، ممکن است مبهم باشند، و تفسیر قرارداد توسط طرفین با هم همخوانی نداشته باشد لذا اگر سوء تفاهم در رابطه با قرارداد وجود داشته باشد، آیا طرفین می‌توانند از قانون قرارداد یا دادگاه برای کمک استفاده کنند؟

عدم مزیت‌های بلاکچین

بلاکچین اگرچه برتری‌هایی دارد ولی عدم مزیت هایی هم دارد:

ضرر اصلی بلاک چین مصرف انرژی بالاست. هر بار که گره جدید ایجاد می شود و در همان زمان با گره‌های دیگر ارتباط برقرار می کند که به این ترتیب شفافیت ایجاد می شود. آن‌ها از مقادیر قابل توجهی از قدرت کامپیوتر ا ستفاده می کنند. اینکه هر گروه یا بلاکی که ا ضافه می شود و بلاک جدید هش جدیدی ا ضافه می شود و تمام زنجیره باید باید تغییر کند، نیاز به زمان و مصرف انرژی دارد(فائوول[1]، ۲۰۱۷). تایید امضاء[2] یکی دیگر از چالش‌های بلاکچین است. چون هر تراکنشی باید با یک طرح رمزنگاری تایید شود.بنابراین قدرت محاسباتی بزرگی برای پردازش محاسبات لازم است. که این خود یکی از دلایل مصرف انرژی بالاست.

مشکل بعدی بلاکچین، مربوط به مفهومی به نام فورک است. که در واقع فرصتی برای تقسیم زنجیره[3] است.گره هایی که با نرم افزار قدیمی کار می کنند،تراکنشات رادر زنجیره جدید قبول نمی کنند(همان).

گاهی اوقات ممکن است باگ اساسی در شبکه یافت شود که وضعیت ارز دیجیتال را به خطر بیاندازد و یا ممکن است برای بهتر شدن عملکرد کوین فورک زده شود و نحوه تصمیم گیری اینکه شبکه بلاک چینی به فورک نیاز دارد یا خیر بر عهده جامعه آن ارز دیجیتال خاص است. وقتی برنامه نویسان و توسعه دهندگان یک شبکه بعد از خطا و آزمون به این نتیجه برسند که شبکه نیازمندیک سری تغییرات است و با اعمال اصلاحات کارکرد شبکه بهبود پیدا خواهد کرد، مو ضوع را در شبکه مطرح می‌کنند و با به اجماع ر سیدن تو سط اع ضای شبکه، فورک اتفاق می‌افتد. این فضای دموکراتیک که همه بتوانند نظر خود را اعلام کنند و بهترین تصمیم برای بهبود شبکه گرفته شود، از ویژگی های مهم اکو سیستم ارزهای دیجیتال ا ست. که شامل دو نوع هارد فورک و سافت فورک می‌باشد.

اگر تغییراتی در پروتکل ارز دیجیتال ایجاد شود که با نسخه قبلی متفاوت است و یا کوینی با بلاک چین جدیدی ایجاد شود هارد فورک رخ داده است. البته هارد فورک همیشه به این معنی نیست که کوین و توکن

[1]Fauvel
[2]signature verification
[3]opportunity to split the chain

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

جدید تولید شـود اما هارد فورک زمانی اسـت که نسـخه جدیدیا فورک شـده با نسـخه قبلی مطابقت یا هماهنگی ندارد و تغییرات زیادی در آن رخ داده اســت. هنگامی که هارد فورک رخ می دهد نودها حتما باید خود را بروز رسانی کنند و تیم توسعه دهنده آن ارز دیجیتال همواره آپدیت هایی را برای آنها فراهم می کنند تا با شبکه جدید همساز شوند. اگر نودهای قدیمی خود را بروز رسانی نکنند دیگر نمی‌توانند به شبکه جدید وارد شوند و نودهای آپدیت شــده دیگر بلاک هایی که نودهای قدیمی اســتخراج می کنند را نمی پذیرند. به بیان ســاده، اگر آپدیت جدید برایبک کوین داده شود و نود آن را روی سیستم خود نصب کند، بعد از آن به تراکنش‌های روی بلاکچین قبلی دسترسی نداشته باشد، در حقیقت فعالیت خود را رویبک بلاکچین جدید، برایبک ارز جدید و تراکنش‌های جدید ادامه خواهد داد. یعنی با اتفاق افتادن هارد فورک، یک ارز جدید با بلاکچین و گره‌های جدید ایجاد خواهد شد.

در سافت فورک، برعکس هارد فورک، کوینیا توکن جدیدی ایجاد نمی شود. با اعمال کردن اصلاحات و آپدیت روی نســخه اصــلی، گره ها همچنان به فعالیت خود روی بلاک چین قبلی ادامه خواهند داد. در واقع تغییراتی اعمال نمی شــود که بلاکچین قبلی به روند خود ادامه ندهد و چندین تغییر در بلاکچین جدید ایجادمی شود که با بلاکچین قبلی مطابقت دارد و نودهای قدیمی که بروز رسانی نکرده اند می توانند بدون بروز رسانی به فعالیت در بلاکچین جدید نیز ادامه دهند. در فورک نرم معمولا اصــلاحات و تغییرات به حدی جدی نیســت که بلاکچین جدیدی ایجاد شود.

شاید به نظربرخی این مساله سبب سلامت زنجیره شود ولی به نظر برخی دیگر ممکن است مشکلات زیر را نیز به همراه داشته باشد:

- ✓ شاید برخی از افراد همیشه به دنبال فورک جدید بیت‌کوین باشند، اما معمولا بسیاری از افراد شناخته شده در ارزهای دیجیتال نگاه و دید مثبتی نســبت به فورک‌ها ندارند و هدف اینگونه اقدامات را صــرفا ســودجویی می‌دانند.
- ✓ برخی از این فورک‌ها دارای پشتیبانی قوی نیستند.
- ✓ پس از انجام فورک‌ها، معمولا تعداد زیادی ســایت و کیف پول از طرف هکرها ســاخته می‌شــود تا با معرفی خودشان به عنوان کیف پول ارز جدید، موجودی کاربران را بدزدند(گروه دیتافلیر[1]، ۲۰۱۸).

یکی دیگر از مشکلات بلاکچین، تعادل بین مقدار گره‌ها و هزینه های مناسب برای کاربران است. در حال حاضر گره‌ها برای بلاکچین به طور درست و قدرتمند کار نمی کنند. در این مورد، هزینه ها بالاتر است، زیرا گره ها پاداش های بیشــتری دریافت می کنند؛ اما تراکنش ها به آرامی انجام می شــود، زیرا گره‌ها فشــرده نمی شــوند .بلاکچین هنگامی که بلوک های جدید به زنجیره اضــافه می‌شــوند و بار محاســباتی افزایش پیدا می کند افزایش پیدا می کنند. تمام گره ها نمی‌توانند ظرفیت لازم را ارائه دهند. دو مشــکل وجود دارد: اول، مرجع کوچکتر

[1]Dataflair team

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

اسـت؛ زیرا گره ها قادر به حمل نسـخه کامل بلاکچین نیسـتند و باعث می شـود تغییرات و شـفافیتبلاکچینخراب شود؛ دوم، بلاکچین سیستم متمرکزتری می شود.

هزینه های بالا یک مشـکل بزرگ بلاکچیناسـت. میانگین هزینه معامله بین ۷۵ تا ۱۶۰ دلار اسـت و اکثر آن مربوط به مصرف انرژی می شود. یکی از دلایل این وضعیت در بالا توضیح داده شده است. دلیل دوم هزینه های اولیه سرمایه بلاکچین است(دیتا فلیر تیم، ۲۰۱۸).

حملات و مشکلات دیگر بلاکچین[1]

٪۵۱ حملات اتفاقا زمانی رخ خواهد داد که دو معدنچی[2] در یک زمان محاسبه هش بلوک و نتایج مشابه ی را دریافت کنند. در این حالت بلاکچین تقسـیم می شـود و در نتیجه کاربران دو زنجیره متفاوت دارند و هر دو به درستی در نظر گرفته می شوند.

دوبرابر کردن اصل ، این حمله مشابه حمله قبلی است، اما در اینجا می توان از تقسیم زنجیره ای برای صرف پول دوباره استفاده کرد.

حمله Sybil، این ممکن اسـت وقتی که، یک گره چندین معنا را می پذیرد زیرا شـبکه نمی تواند به طور واقعی ماشـین های فزیکی ر تشـخیص دهد. این می تواند منجر به دو حمله قبلی و توانایی دیدن همه معاملات با برنامه های خاص شود.

حمله DDos حمله شـامل یک مقدار زیادی از درخواسـت‌های مشـابه اسـت. حفاظت در حمله DDos ها وجود دارد – اندازه بلوک تا ۱ مگابایت، اندازه هر اسـکریپت تا ۱۰۰۰۰ بایت، تا ۲۰۰۰۰ امضـا می تواند بررسـی شود و حداکثر امضای چندگانه ۲۰ کلید است.

کرک کردن رمزنگاری[3]: اگر از الگوریتم های کوانتومی مانند «شـورا[4] » اسـتفاده شـود که می تواند رمزگذاری RSA را خراب کند، این مساله امکان پذیر است.

در مقاله ای که تو سط جیمی سانگ از یکی از مطرح ترین کار شنا سان بیت کوین و ارز های دیجیتالی در سال ۲۰۱۸ منتشر شده است،در ارتباط با، توهم بلاکچین راه حل مشکلات صنایع و اقتصاد، مباحث زیر را مطرح کرده است:

بلاک چین به یک کلمه محبوب برای برخی افراد تبدیل شـده که معنایش «حل بزرگ‌ترین چالش‌ها در صنایع» ا ست. این افراد با ا ستفاده از واژگان فنی و پیچیده سعی می‌کنند اهمیت این فناوری را به دیگران تو ضیح

[1]BitFury Group ؛۲۰۱۵ ،D. Balaban ؛۲۰۱۸ ،J. Golosova, A. Romānovs, 2018
[2]minner
[3]Cracking of the cryptographic
[4]Shora

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دهند. اما واقعیت متفاوت است. بیشتر این استارتاپ‌ها به این نتیجه رسیدند که بلاک چین، نوش‌دارویی برای درمان همه مشکلات نیست. آنها ابتدا در حل مشکلاتی قدیمی نظیر مسأله اوراکل[1]، مسأله اجماع[2] و مسأله تحلیل‌پذیری قراردادهای کامل تورینگ[3] با مانع روبرو شدند. مشخص شد که بلاک چین نه تنها کلید طلایی حل همه مشکلات نیست، بلکه مانعی برای ایجاد راه‌حل است، زیرا غیرمتمرکز سازی نمی‌تواند شیوه درست حل این مسائل باشد.از آن بدتر اینکه توسعه‌دهندگان سامانه‌های بلاکچینی معمولا آن قدر درگیر جزئیات فنی می شوند که از کاربران و انگیزه نودها که به ایجاد ثبات و سلامت شبکه کمک می‌کنند غافل می‌شوند. نتیجه این وعده‌های توخالی کاملا قابل پیش‌بینی است. وقتی وعده‌ای می‌دهید که نمی‌توانید با توان معمولی در فناوری پیچیده‌ای که تعداد کمی از افراد به آن تسلط دارند از پس انجامش برآیید، نمی‌توانید دستاورد ارزشمندی هم داشته باشید. بسیاری از این تلاش‌ها هیچ نتیجه‌ای به همراه نداشته‌اند. آنهایی که به یک محصول اولیه رسیده‌اند هم نتوانسته‌اند محصول نهایی را ارائه کنند. چند سامانه انگشت‌شماری که موفق به نسخه نهایی شده‌اند هم تراکنشی بسیار اندک (کمتر از ۲۰۰۰ کاربر در روز که یک شکست برای اپلیکیشن و یا وب سایت به شمار می‌رود) داشتند.حتی اگر به‌صورت اتفاقی،یک اپلیکیشن پرطرفدار بر روی بلاک چین قرار گیرد،یک اپلیکیشن مشابه ولی متمرکز و بدون استفاده از بلاک چین در نهایت ارزان‌تر، سریع‌تر و اصلاح‌پذیرتر خواهد بود و درعین‌حال، امکان بروز مشکل در آن تفاوتی با نسخه بلاک چینی ندارد. به عبارت دیگر، هر نرم‌افزار غیرمتمرکز(dApp) در برابر مشابه متمرکز خود محکوم به شکست است که دلیل آن نیز هزینه، سرعت، قابلیت‌ها و امکان مقیاس‌پذیری بهتر است.مفهوم «بلاک چین، نه برای بیت کوین» به‌هیچ‌وجه جدید نیست. طی پنج سال گذشته، فناوری بلاک چین نتوانسته هیچ محصول یا خدمت ارزشمندی را به بازار عرضه کند و احتمال چنین اتفاقی در پنج سال آینده نیز بسیار ضعیف است. این پروژه‌های بلاک چینی که با هدف حل بزرگ‌ترین چالش‌های صنایع مختلف وارد میدان می‌شوند، سرمایه زیادی را مصرف کرده‌اند ولی دستاورد خاصی ندارند.

سایر چالش‌های بلاکچین:

- ✓ جدید بودن و عدم بلوغ تکنولوژی و کمبود استانداردهای صنعتی (آدامز و دیگران، ۲۰۱۷؛ گوخال، ۲۰۱۶؛ بورلی، ۲۰۱۵؛ گئو و لیانگ، ۲۰۱۶)
- ✓ عدم اثبات توانایی تکنولوژی در مدیریت چالش‌های پردازشی(بورلی، ۲۰۱۵؛ دهار و بئوس، ۲۰۱۶؛ گوخال، ۲۰۱۶)
- ✓ ناآشنایی مردم و فعالان عرصه مالی و تکنولوژی (Mthethwa، ۲۰۱۶؛ دشپاند و دیگران، ۲۰۱۷)
- ✓ عدم بلوغ‌ساز و کارهای قانونی، مقرراتی حاکمیتی(دشپاند، ۲۰۱۷؛ Mthethwa، ۲۰۱۶؛ گئو و لیانگ، ۲۰۱۶؛ کترر، ۲۰۱۷)

[1]oracel problem
[2]Consensus problem
[3]analyzability of Turing-complete contracts

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

- ✓ مساله حفظ حریم خصوصی و و مبارزه با فعالیت‌های مالی مجرمانه(پاپادو، ۲۰۱۵)
- ✓ نیاز به توان پردازشی بالا و مقیاس‌پذیری(Mthethwa، ۲۰۱۶؛ دهار و بئوس، ۲۰۱۶)
- ✓ عدم سازگاری با سیستم‌های سنتی(بورلی، ۲۰۱۵؛ دهار و بئوس، ۲۰۱۶)
- ✓ نوسانات قیمتی ارزها و تبدیل آن‌ها به ارزهای رایج، مخفی بودن هویت کاربران ارزهای دیجیتال برای نهادهای حاکمیتی و نظارتی، متوازن سازی مساله حفظ حریم خصوصی و مبارزه با فعالیت‌های مالی مجرمانه، عدم بلوغ ساختارمدیریت ارزهای دیجیتال(پاپادو، ۲۰۱۶)
- ✓ نیاز به ارزیابی‌های زیاد تکنولوژیک رگولاتوری، مشکل بودن توسعه پروتکل‌های اجماع و رمزنگاری، توسعه پروتکل‌ها و مکانیزهای حاکمیتی برای دسترسی و قراردادهای هوشمند مورد نیاز سیستم‌های چند عاملی با ریسک افشای بالا(دهار و بئوس، ۲۰۱۶)
- ✓ نیاز به نقش‌های جدید در توسعه برنامه‌ها، سازو کارهای امنیت و قابلیت اطمینان در توسعه برنامه‌ها، چالش‌های معماری نرم‌افزار، شاخص‌های جدید ارزیابی عملکرد برنامه‌ها، نیاز به محیط‌های توسعه جدید(رورئو و دیگران، ۲۰۱۷)
- ✓ ایجاد اخلال در بازار، واکنش فعالان صنعت خدمات مالی، نیاز به شبکهبا پهنای باند بالا، تغییرات پیشبینی‌نشده فضای پرداخت، زمان‌بر بودن فرآیند کاوش و استخراج، عدم امکان حذف کامل واسطه در موارد کاربرد واقعی،نیاز به تعریف مکانیزهای سخت‌تر دسترسی به اطلاعات به دلیل تغییر ناپذیریاطلاعات ورودی(گوخال، ۲۰۱۶؛ کترر، ۲۰۱۷، دوری، ۲۰۱۶؛ گئو و لیانگ، ۲۰۱۶)

هوش مصنوعی

دراین قسمت به بیان مفهوم هوش‌مصنوعی می‌پردازیم و به یکی سری از دستاوردهای مهم آن می‌پردازیم که نتایج و آثار قابل توجهی داشته و ما را در درک مسائل مربوط به آن یاری می‌هد.

مفهوم هوش مصنوعی

هوش مصنوعی که به اختصار به آنAI یا ML[1]نیز گفته می شود، بههو شمند شدن ما شین‌ها ا شاره دارد.در علوم کامپیوتر به انجام پژوهش در زمینه «هوش مصنوعی»، مطالعه «عامل‌های هوشمند» نیز می گویند. هر دستگاهی که محیط خود را درک کند و بر اساس ادراکش اقدامی انجام دهد که شانس دستیابی موفقیت‌آمیز به هدف را بیشینه کند، یک عامل هو شمند ا ست. به عبارت دیگر، ما شینی که بتواند محیط را درک کند و بر ا ساس ادراکی که از محیط به دست آورده برای رسیدن به یک هدف خاص تصمیم‌گیری کرده و اقدامی را انجام دهد که امکان موفقیت آن بیشترین میزان ممکن است، یک عامل هوشمند نامیده می‌شود. در واقع، عبارت «هوش مصنوعی» زمانی به‌کار می‌رود که ماشین عملکردهای «شناختی» مانند «یادگیری» و «حل مساله» را که مرتبط با مغز انسان

[1]Artificial Intelligence & Machine Learning

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

است تقلیدمی کند(بوروویس و دیگران[1]، ۲۰۱۸).

درتعریفی دیگر منظور از هوش مصنوعی[2] ماشین‌های هوشمندی است که توانایی فکر کردن دارند. در حال حاضر، هوش مصنوعی پیشرفت سریعی در ارتباط با تقلید هوش انسانی دارد. این عقیده در واقع، هوش ماشینی را می خواهد با فعالیت های مرتبط با فکر انسان مانند تصمیم گیری و یادگیری حل مساله مرتبط کند(مت رحیم و دیگران[3]،۲۰۱۸). پروفسور مک کارتی[4] (۱۹۹۵) مفهوم هوش مصنوعی را برای اولین بار در کنفرنس بورنموث در سال ۱۹۵۶ بیان کرد. این انقلاب، هوش مصنوعی، و مفهوم آن توسط بوگو[5](۲۰۱۴) تکمیل شد که هوش مصنوعی را به عنوان یک سیستم عامل هو شمند تو صیف کرد که احتمال موفقیت را در انجام یک وظیفه خاص افزایش می دهد. پن[6](۲۰۱۶) به این مساله اشاره کرد که استفاده از هوش مصنوعی در تکنولوژی بسیار حائز اهمیت ا ست.بر ا ساس مطالعات و گزار شات در حوزه مصنوعی این انتظار می رود که بازار مربوط به AI تا سال ۲۰۲۲ ارزش ۰۶,۱۶ بیلیون دلاری داشته باشد. این بازار انتظار می رود نرخ رشد ۹,۶۲ درصدی را با توجه به ترکیب نرخ رشد سالیانه طی سال های ۲۰۱۶ تا ۲۰۲۲ داشته باشد(ریسرچ و مارکتز، ۲۰۱۶[7]). در ۲۵ آپریل ۲۰۱۶ تا ۲۷ می ۲۰۱۶، گزارش ویژه ای تحت عنوان « چشم انداز هوش مصنوعی در سرمایه گذاری و کسب وکار ۲۰۱۶» توسط Narrative Science با همکاری موسسه تحقیقات کسب وکار ملی[8] تهیه شده است. این گزارش با توجه به ارزیابی پاسخ ۲۳۵ هزار نفر، در یک نظر سنجی آنلاین، نشان می‌دهد که ۵۸ درصد از پاسخ‌دهندگان معتقدند که AI در اکثر موارد باید قادر به تجزیه و تحلیل و پیشبینی باشد. که این امر شامل استفاده از داده کاوی، آمار، مدلسازی و یادگیری ما شین می با شد. شاید مهمتر از این مساله این با شد که بازار مربوط به خدمات و تکنولوژی داده های حجیم[9] تا سال ۲۰۱۹ به ارزش ۶,۴۸ بیلیون دلاری برسد(نریتیو ساینس[10]، ۲۰۱۶).

امروزه آن دسته از مشتریانی که خبره‌تر و آگاه‌تر هستند، ترجیح می دهند تراکنش های مالی خود را در تعامل کمتر با انسان و دخالت کمتر آن انجام دهند. حوزه تکنولوژی برای بهبود و کارامدی سیستم های مالی سراسری بسیار گسترده و دارای شرایط بالقوه ای برای تحقق این امر است. یکی از این ابزار های محبوب قرارداد های هوشمند است، یک برنامه کامپیوتری که شرایط قرارداد ها را اجرا می‌کند(سارتور و دیگران[11]، ۲۰۱۶). قراردادهای هو شمند و خودکار می‌تواند تکمیل کننده یا به طور کامل جانشین قراردادهای معمولی قانونی شوند. این مساله از این جهت که قراردادهای هوشمند در صنایع و زمینه های مختلفی مانند مراقبت های پزشکی، املاک و مستغلات و اوراق بهادار بسیار حیاتی و مهم ا ست واضح می با شد. البته امکان ا ستفاده از قراردادهای هو شمند

[1]Borowiec
[2]Artificial Intelligence
[3]Siti Rohaya Mat Rahim, Zam Zuriyati Mohamad, Juliana Abu Bakar, Farhana Hanim Mohsin, & Norhayati Md Isa
[4]Professor J. McCarthy
[5]Bogue
[6]Pan
[7]Research & Markets, 2016
[8]National Business Research
[9]Big data
[10]Narrative Science
[11]Idelberger, Governatori, & Sartor, 2016

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

در زمینه‌های دیگری مانند سیستم بانکداری، بیمه، مدیریت و .... نیز وجود دارد. قرارداد های هوشمند و هوش مصنوعی به عنوان فناوری و نوآوری های که جدیدا طراحی شده است، ممکن است که در بعضی از محصولات بانکی اسلامی قابل استفاده و کاربردی باشد(مت رحیم و دیگران، ۲۰۱۸). ضمن اینکه کمید[1](۲۰۱۷) دریافت که هوش مصنوعی دارای ابزارهای چون یادگیری ما شین و شبکه عصبی عمیق ا ست که می‌تواند یک تجربه کاملا جدیدی را در برای صنعت مالی به ارمغان آورد.

کاربردهای هوش مصنوعی در اقتصاد وبانکداری

کشف کلاهبرداری مالی

سیستم‌های قدیمی کشف کلاهبرداری مالی تا حد زیادی وابسته بهمجموعه‌های پیچیده‌ای از قوانین و قواعد بودند اما سیستم کشف کلاهبرداری مدرن، فراتر از دنبال کردن فاکتورهای خطرآفرین می‌رود و بر مبنای آن پتانسیل‌های جدید تهدیدات امنیتی در مورد اطلاعات شرکت‌ها را قاعده‌مند می‌کند. با استفاده از یادگیری ماشین، سیستم‌ها می‌توانند فعالیت‌ها یا رفتارهای منحصربه‌فرد آ شفتگی را کشف کنند و آنها را برای تیم امنیتی ار سال کنند.

هوش مصنوعی وبازارهای سهام

بازارهای مالی ازجمله حوزه‌هایی است که اخیراهوش مصنوعیدرآن راهپیداکرده است وشرکت‌های بزرگ حوزه بازارهای سهام وارز از این ابزار برای تجزیه و تحلیل داده‌ها از آن استفاده می‌کنند. سوالی که در اینجا مطرح می‌شود این است که هوش مصنوعی چگونه می‌تواند در بازارهای سرمایه مورد استفاده قرار بگیرد؟ والا ستریت با ا ستفاده از هوش مصنوعی و بخش‌ها و ابزارهای مهم آن مانند «یادگیری ما شین» و یادگیری عمیق می‌تواند میلیون‌ها داده‌ای را که در زمان واقعی[2] اتفاق می‌افتد، تجمیع کند و بسیاری از همبستگی‌ها که با روش سنتی نمی‌توان به دست آورد، با استفاده از هوش مصنوعی به راحتی به دست می‌آیند(مک کینزی، ۲۰۱۸).

تشخیص کلاهبرداری در بیمه

چندین روش یادگیری ماشین برای شناسایی تقلب در مسائل مربوط به متقاضیان بیمه موفق بوده است [3]. رویکرد سنتی برای شناسایی تقلب مبتنی بر ویژگی هایی است که باید توسط یک متخصص استخراج شود(چالاپاتی و چائولا[4]، ۲۰۱۹). البته این روش‌ها برای شناسایی تقلب و پولشویی در نظام بانکی نیزقابل استفاده است.

[1]Kmeid
[2] Real Time
[3]Joudaki et al, 2015; Roy and George, 2017
[4]Chalapathy and Chawla

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

هوش مصنوعی صنعت بانکداری را بیش از هر صنعت دیگری تحت تأثیر قرار داده است. سازمان‌هایی که در صنعت بانکداری فعال هستند، به طور فزاینده ای برای تثبیت جایگاه خود به عنوان یک شرکت نوآور، در حال رقابت‌اند. تصویر زیر نشان دهنده دلایل استفاده گسترده از هوش مصنوعیدر خدمات بانکداری و مالی است.

دلایل استفاده از هوش مصنوعی در بانکداری

هوش مصنوعی چندین برنامه در صنعت بانکداری ارائه کرده است. در این قسمت به معرفی۴ زمینه کاربردی و کلیدی هوش مصنوعی، در حوزه صنعت بانکداری، پرداخته می شود. این زمینه ها می توانند در پنج سال آینده انقلابی در صنعت ایجاد کنند.

❖ ضد پول‌شویی[1]، مجموعه ای از رویه ها، قوانین و مقررات طراحی شده برای توقف درآمدهای حاصل از اقدامات غیرقانونی و پول شویی است. پول شویی، تبدیل سود حاصل از خلافکاری و فساد به دارایی‌های به ظاهر مشروع است. در فرایند پول شویی، پول حاصل از اقدامات غیرقانونی تبدیل به پول یا ثروتی می شود که

[1](AML)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

در ظاهر از راه‌های قانونی بد ست آمده‌ا ست و به این طریق «پول شسته شده» وارد اقتصاد می شود. در اغلب موارد، پول شـویان با به کارگیرییک سـری اقدامات پنهانی، این کار را انجام می دهند.اکثر بانک های بزرگ در سرتاسر دنیا، در حال انتقال از قوانین مبتنی بر سیستم های نرم افزاری به سیستم‌های مبتنی بر هوش مصنوعی هستند. سیستم‌های مبتنی بر هوش مصنوعی، از الگوریتم های ضدپول‌شویی قوی‌تر و هوشمندانه‌تری استفاده می کنند. در طول سال های آینده،این سیستم ها با توجه به نوآوری های مداوم و پیشرفت های حوزه هوش مصنوعی، دقیق‌تر و سریع‌تر می‌شوند.

- ❖ ربات های چت هوشمند مبتنی بر هوش مصنوعی، سیستم‌های چت خودکار هستند که گفتگوهای انسانی را بدون دخالت هیچ انسانی شبیه سازی می‌کنند. این سیستم ها براساس شناسایی محتوا و احساسات در چت‌های متنی با کاربران نهایی کار می‌کنند. آن‌ها متن کاربر را بررسی نموده و مناسب ترین پاسخ را ارسال می‌کنند. با گذشـــت زمان، این ربات‌های چت، داده‌های فراوانی در مورد رفتار و عادت‌های کاربر دریافت می‌کنند. یادگیری رفتار کاربر، به آن‌ها کمک می کند تا با نیازها و خلق و خوی کاربر نهایی سازگار شوند. ربات‌های چت در حال حاضر به طور گسترده در صنعت بانکداری استفاده می شوند. این ربات ها در مدیریت ارتباط با مشتری، در سطح خصوصی تغییرات اساسی ایجاد کرده‌اند. بانک مرکزی آمریکا قصد دارد یک دستیار مجازی به نام "اریکا" را به مشتریان ارائه دهد. این دستیار مجازی با استفاده از هوش مصنوعی پیشنهادآتی را برای بهبود امور مالی کاربران در تلفن همراه آن ها، ارائه خواهد داد. آلوو[1] ، یکی دیگر از موارد تحقق ربات‌های چت است که توسط گوگل منتشر شده است.
- ❖ پیشنهاد به مشتریان،موتورهای پیشنهاد، بخش مهمی از هوش مصنوعی در صنعت بانکی هستند. این ابزار، با اســتفاده از داده های گذشــته درباره کاربران/ یا پیشــنهادهای مختلف بانک مانند طرح های کارت اعتباری، استراتژی های سرمایه گذاری، صندوق ها و ...مناسبترین توصیه ها را براساس اولویت ها و پیشینه کاربران، به آن‌ها ارائه می‌دهد.با داده های بزرگ و محاسبات سریع تر، ماشین ها به الگوریتم های دقیق هوش مصنوعی مجهز شده‌اند که نقش مهمی در چگونگی ارائه پیشنهادات در بخش بانکی دارند.
- ❖ قراردادهای هوشمند در سال‌های آتی به تنهایی با استفاده از الگوریتم‌های یادگیری ماشین و یا در ترکیب با استفاده از سیستم‌های غیر متمرکز ، در جهت کاهش هزینه‌ها و افزایش امنیت و حذف شخص ثالث به شدت مورد توجه قرار گرفته‌اند(مک‌دونل[2]، ۲۰۱۹).

مزیت ها و عدم مزیت‌های قراردادهای هوشمند مبتنی بر هوش مصنوعی

در قسمت قبل به بیان ساختار کلی قراردادها از منظر پیاده سازی، انواع قراردادها، مقایسه آن‌ها، برتری ها و عدم مزیت‌های قراردادهای هوشمند بر بستر بلاکچین، مفهوم کلی قراردادهای هوشمند مبتنی بر هوش مصنوعی، ساختار کلی این نوع از قراردادها پرداختیم. لذا در این قسمت سعی شده است آنچه قراردادهای هوشمند مبتنی بر

[1]Allo
[2]Phil McDonnell

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

هوش مصنوعی می‌تواند برای عرضه داشته باشد صحبت کنیم. بیان این نکته ضرورت دارد که ماهیت قراردادهای هوشمند مبتنی بر هوش مصنوعی و قراردادهای هوشمند مبتنی بر بستر بلاکچین در پایه و اساس مشابه هم هستند هر دو درنهایت به دنبال اجرای قراردادهای خودکار و حذف شخص ثالث در اجرای این قراردادها هستند ولی در بستر پیاده سازی تفاوت دارند. که همین تفاوت در نوع پیاده‌سازی و اجرا موجب مزیت‌ها و عدم مزیت‌هایی می‌شوند.

یکی از مشکلات اصلی در ارتباط با بلاکچین و قراردادهای هوشمند بلاکچینی مباحث مربوط به مصرف انرژی بالا و فورک و هزینه بالا بود که در قراردادهای هوشمند مبتنی بر هوش بواسطه اینکه بستر آن‌ها بر اساس سیستم‌های شبه نامتمرکز و الگوی گراف جهت‌دار غیرمدور است اصلا زنجیره‌ای تشکیل نمی‌شود که مشکلات مربوطه برای آن ایجاد شود. و از آنجا که بیس اصلی این قراردادها الگوریتم های یادگیری ماشین و یا الگوریتم‌های مرتبط با آن مانند الگوریتم‌های مرتبط با بحث گراف است و سرورها و شبکه‌ها موردنیاز می‌تواند همان شبکه های رایج باشد که برای مثال در شبکه بانکی استفاده می‌شود لذا از نظر سخت‌افزاری نیازی به دستگاه‌ها و سرورهایی با پردازنده‌ها و سایر سخت‌افزارهای شبیه دستگاه‌ها و سرورهای مورد نیاز برای شبکه بلاکچین نیست. لذا از نظر هزینه و سخت‌افزاری می‌تواند نسبت به قراردادهای هوشمند بلاکچینی مزیت داشته باشد.

از آنجا که در این شبکه ارتباط بین نودها و کاربرانی که وارد شبکه شده‌اند به شکل گراف می‌باشد و با استفاده از الگوریتم شبکه های نیمه خودمختار[1] از طریق ماشین مجازی تبدیل به گرافی می‌شود که دارای چند نود اصلی است که مراکزاینودهامی‌توانند بانک‌ها یا حتی بانک مرکزی باشد لذا این مساله که نهادها و سازمان‌های قانون‌گذار از جریان این تراکنش‌ها خارج و مسائل مربوط به پولشویی و مالیات مطرح می‌شود تا حدی حل می شود چراکه اولا بانک‌ها و بانک مرکزی می‌توانند در مراکز اصلی این شبکه قرار گیرند، ثانیا، این تراکنش‌ها می‌تواند بر اساس ارز تعریف شده جدیدی باشد یا می‌تواند با استفاده از رابط کاربری کاربردی همان حساب بانکی افراد در تراکنش‌ها و انجام معاملات بر اساس قرارداد هوشمند مورد استفاده قرار بگیرد و از آنجا که می‌توان برخی از نودها را به عنوان نود اصلی قرار داده تا تراکنش‌ها در آن‌ها ذخیره شوند از جنبه نظارت نسبت به بلاکچین برتری دارد ولی این برتری، عدم برتری را نیز به همراه دارد که در این شبکه اگرچه از الگوهای رمزنگاری و کلید عمومی و خصوصی استفاده می شود ولی در صورت وجود بانک‌ها و بانک مرکزی به عنوان نودهای اصلی شناسایی و احراز هویت نودها از طریق روش‌ها و تکنیک‌های داده‌کاوی و بررسی و هک API میتواند به راحتی انجام شود. که این مساله بستگی به نحوه پیاده‌سازی الگوریتم دارد. و از طرفی با استفاده از الگوریتم جستجوی اول عمق بین دو نودی که تراکنش انجام می‌دهند مسیری از نودها را که کوتاه‌ترین زمان ممکن برای تایید کلی و ذخیره تراکنش و یا معامله را دارد انتخاب و تایید نودهایی که دراین مسیر قراردارند

[1]Semi-Autonomous Networks

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

موجب ذخیره تراکنش در این نودها و نودهای اصلی می‌شوند لذا از آنجا که این مسیر و الگو برای تمام نودها نمی‌باشد میزان زمان سپری شده برای این امر بسیار کاهش پیدا خواهد کرد(جکسون[1]، ۲۰۱۸).
نکته‌ی دیگری که در ارتباط با قراردادهای هوشمند وجود دارد بحث امنیت می‌باشد. قراردادهوشمند مبتنی بر بستر بلاکچین در مقایسه با قراردادهای هوشمند مبتنی بر هوش مصنوعی به دلیل شبکه بلاک‌چین از امنیت بیشتری برخوردار است که دلیل آن عدم تغییرپذیری و مقاوم بودن شبکه بلاکچین است ولی همین امر نیز یک نقطه ضعف برای آن به حساب می‌آید از آنجا که این قراردادها باید کد آن توسط اشخاص نوشته شود، در صورت اشتباه در بندها و مفادقرارداد و استفاده نودها از این قراردادها، به دلیلی تغییر ناپذیری این شبکه نتایج زیان‌باری دارد و به دلیل مکانیسم اجماع در چنین شبکه‌هایی حل چنین مشکلاتی واقعا زیان‌بار است ولی در پروتکل پیشنهادی مربوط به قراردادهای هوشمند مبتنی بر هوش مصنوعی ، از آنجا که بانک‌ها به عنوان نود اصلی قراردارند و حتما درمسیر تایید معاملات و تراکنش‌ها قراردارند(حداقل یکی از آن‌ها) در صورت وجود چنین مشکلاتی می‌تواند دراسرع وقت وارد عمل شده و بواسطه اینکه ماشین مجازی در سرورهای آن‌ها طراحی شده می‌تواند تغییرات لازم را اجرایی کند و البته ابتدا باید اجرای آن را متوقف سازد. و همچنین با استفاده از شبکه تخاصمی مولد ارزیابی‌هایی بصورت پویا و ایستا در روند اجرا و قبل از اجرای قراردادها صورت می‌گیرد که احتمال بروز چنین مشکلاتی را نسبت به قراردادهوشمند مبتنی بر بستر بلاکچین به بهای امنیت کمتر، کاهش می‌دهد.

کاربردها و فواید قراردادهای هوشمند و تاثیر آن بر بانکداری

در سال ۱۹۹۴ نیک سازبو[2]محقق حقوق و استاد رمزنگاری متوجه شد که از فناوریسیستم‌های غیر متمرکز می‌توان برای فرایند قراردادهای هوشمند استفاده کرد[3]. فرایندی که با عنوان قراردادهای اجرای خودکار، قرارداد دیجیتال هم شناخته می شود. در این فرمت از قراردادها، اسناد به کدهای کامپیوتری تبدیل شده و در کل شبکه ذخیره و کپی می شوند. سپس فرایندهای مربوط به این اسناد و قراردادها توسط کامپیوترهای حاضر در شبکه‌ی بلاک‌چین نظارت می شود. قراردادهای هوشمند حتی می‌توانند با فرایندهای مرتبط با دفتر کل (حسابداری) مانند تراکنش پول و ارسال و دریافت کالا و خدمات نیز ادغام شوند.جری کومو[4]معاون بخش بلاک چین شرکت IBM اعتقاد دارد قراردادهای هوشمند را می‌توان در گستره‌ی وسیعی از کاربردها از خدمات مالی و بانکداری تا سلامت و بیمه به کار گرفت.

[1]Jackson
[2]Nick Szabo
[3] باز این نکته قابل ذکراست که آثار و نتایج smart contract و intelligent contract تا حدی مشابه هم هستند ولی ساختار و شکل پیادهسازی آن‌ها با هم متفاوت می‌باشد.
[4]Jerry Cuomo

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کاربردها

کاربرد دولتی قرارداد هوشمند

کارشناسان متعدد اعتقاد دارند بهینه‌سازی و امن‌تر کردن سیستم‌های رأی‌گیری کنونی دشواری‌های زیادی دارد. دراین‌میان قراردادهای هوشمند می‌توانند نمامی نگرانی‌های موجود را با ارائه‌ی سیستمی امن‌تر برطرف کنند.دسترسی به رأی‌هایی که با استفاده از دفتر کل توزیع‌شده حفاظت می‌شوند، نیاز به منابع پردازشی بسیار زیاد دارد. به‌علاوه پس از دسترسی احتمالی نیز باید آنها را رمزگشایی کنیم که امری تقریبا غیرممکن خواهد بود. البته تقریبا هیچ‌کس آن‌چنان منبع پردازشی ندارد و نفوذ به سیستم را می‌توان تقریبا غیرممکن دانست[1](بارتولتی[2]، ۲۰۱۷).یکی از حوزه‌های کاربردی قراردادهای هوشمنددر حوزه دولتی و بانکی صدور ضمانت‌نامه الکترونیکی، از مرحله درخواست تا مرحله صدور، ابطال یا اجرا و ...است که طی یک قرارداد هوشمند انجام می‌پذیرد. در این میان چه میزان از هزینه‌های این عملیات کاسته شده و به چه میزان از تقلب‌های رایج در این زمینه کاسته خواهد شد؟

کاربرد مدیریتی قرارداد هوشمند

بلاک چین نه‌تنها یک دفتر کل ثابت به‌عنوان منبع اعتماد و امنیت ارائه می‌کند، بلکه احتمال ایجاد تداخل در ارتباط و فرایندهای کاری را نیز به‌خاطر دقت، شفافیت و سیستم خودکار از بین می‌برد.فرایندهای کسب‌وکاری معمولا مجبور به تحمل رفت‌وآمدهای متعدد هستند که با صبر کردن برای تأییدیه‌های داخلی و خارجی زمان زیادی را از نیروها تلف می‌کنند. درنتیجه منظم شدن فرایندهای کسب‌وکار عملی طاقت‌فرسا و زمان‌بر است. استفاده از دفتر کل مبتنی بر سیستم‌های غیر متمرکز، فرایند بالا را سرعت می‌بخشد. به‌علاوه باعث می شود که اختلافات معمول در کسب‌وکار کاهش پیدا کنند. اختلاف‌هایی که به‌دلایل متعدد همچون تفسیرهای شخصی در کسب‌وکار ایجاد می‌شوند و حتی به دعواهای حقوقی هم منجر خواهند شد. به‌عنوان نمونه‌ای از کاربرد قرارداد هوشمند در حوزه‌ی کسب‌وکار می‌توان شرکت Deposity Trust & Clearing Corp را نام برد که در سال ۲۰۱۵ اوراقی به ارزش ۱,۵ کوادریلیون دلار از ۳۴۵ تراکنش را به‌کمک قراردادهای هوشمند پردازش کرد(مکینزی، ۲۰۱۶).

کاربرد قرارداد هوشمند در زنجیره تأمین

قرارداد هوشمند بر اساس روند جملات شرطی کار می‌کند. به‌بیان ساده‌تر برای اجرای هر فرایند در قراردادهای مذکور، باید شرطی اجرا شود. جف گارزیک[3] یکی از توسعه‌دهنده‌های اولیه‌ی بیت کوین درباره‌ی

[1] بیان این نکته در اینجا ضرورت دارد که پژوهشگر در این قسمت با بیان قید غیر ممکن چندان موافق نیست و دلایل این عدم موافقت را در قسمت محدودیت‌های بلاکچین بیان کرده‌ایم.

[2] Bartoletti

[3] Jeff Garzik, 2017

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قرارداد هوشمند این‌گونه توضیح می‌دهند:

زنجیره‌های تأمین عموما با سیستم‌های مبتنی بر فرایندهای کاغذی دچار کاهش سرعت و بازدهی می‌شوند. در آن سیستم‌ها باید فرم‌ها را از طریق کانال‌های بی‌شمار برای تأیید ردوبدل کرد که احتمال گم شدن کالا وحتی کلاهبرداری را افزایش می‌دهد. سیستم‌های نامتمرکز مشکل مذکور را با ساخت ورژن دیجیتالی امن و قابل د سترس از همه‌ی طرف‌های درگیر در زنجیره‌ی تأمین حل می‌کند. به‌علاوه وظایف و پرداخت‌ها نیز به‌کمک آن خودکارسازی می‌شوند.از نمونه‌های زنده‌ی کاربرد قرارداد هوشمند می‌توان به بانک برکلیس[1] اشاره کرد. بانک مذکور از قرارداد هوشمند برای ردگیری تغییرات مالکیت استفاده می‌کند. به‌علاوه انتقال خودکار پرداخت‌ها به موسسه‌ی مالی دیگر در زمان تحویل مرسوله نیز به‌کمک این فناوری انجام می‌شود(حسن و دیگران[2]، ۲۰۱۹).

بانکداری و خدمات مالی

۱- عرضه اولیه سکه(ICO[3]) و DAICO

قراردادهای هوشمند بیشترین کاربرد را در صنعت بانکداری و بخش‌مالی دارد و این قراردادها در قسمت رهن و اجاره، ارتباطات کشوری و پرداخت‌ها و بیمه هستند. عرضه اولیه سکه[4] و عرضه اولیه سکه سازمان‌های خومختار غیر متمرکز[5] قراردادهای هوشمند اتریوم کل فرایندعرضه اولیه سکه و فروش توکن‌ها را بهتر، شفاف‌تر و معقول‌تر می‌کنند. به تازگی ویتالیک بوترین موسس اتریومیک مدل DAICO ارائه‌داده که یک مدل ترکیبی از عرضه اولیه سکه وسازمان-های خودمختار غیر متمرکز[6] است.

$$DAO + ICO = DAICO$$

در تامین مالی عرضه اولیه سکه از طریق سازمان-های خودمختار غیر متمرکز، تیم سازنده، یک قرارداد هوشمند بوجود می‌آورد که "تپ"نام دارد و کمی با ICOهای قدیمی متفاوت است. اما تپ نیز با حالت مشارکت آغاز می‌شود و سرمایه‌گذاران می‌توانند با قوانین ICO در اتر مشارکت کنند. اما تفاوت‌هایی نیز وجود دارد که مثلا هر تپ نشان می‌دهد که سرمایه گذاران چند اتر در ثانیه می‌توانند از قرارداد را دریافت کنند و همچنین محدودیت هایی برای آن وجود دارد. (این امر تو سعه‌دهندگان را زیر نظر می‌گیرد تا ناگهان همه میزان مشارکت را دریافت کنند و با همه پول‌ها فرار نکنند)(ژانگ و دیگران[7]، ۲۰۱۸).

۲- حساب وثیقه

---

[1]Barclays

[2] Haya Hasan, Esra AlHadhrami, Alia AlDhaheri, Khaled Salah, Raja Jayaraman

[3]عرضه اولیه سکه یا همان آی‌سی‌اوICO ، روشی برای جذب سرمایه و فرصتی برای سرمایه‌گذاری است که در آن توکن‌ها (همان ارزهای دیجیتال) یک پروژه، پیش از راه‌اندازی پروژه فروخته می‌شوند و افراد می‌توانند با خریدن توکن‌ها در آن سرمایه‌گذاریکنند.

[4]Initial coin offering

[5]DAICO

[6] Decentralized autonomous organization

[7]YinghuiZhang, Robert H.Deng, Ximeng Liu, DongZheng

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

از قراردادهای هوشـــمند می‌توان هنگام جایگزین کردن کردن خدمات اســتفاده کرد. در این صـــورت، قراردادها باید خیلی هو شمند با شند و همه ویژگی‌های آن‌ها به خوبی تست شده با شند تا باعث ضرر نشوند. مثلا قراردادهای هوشـــمند اتریوم می‌توانند نقش یک حســـاب وثیقه[1] را در یک صـــرافی همتا به همتای اتریوم به نام لوکال اتریوم[2] ایفا کنند. به طور مشابه، می‌توان در بخش املاک، وراثت و غیره از آن‌ها استفاده کرد. مثال دیگری درباره قراردادهای هو شمند در بازارهایی مثل آپ‌ورک[3] است که آن‌ها نقش حساب وثیقه را ایفا می‌کنند(همان) و در اینصورت بانک‌ها نیز می‌توانند از این مکانیسم برای دریافت وثیقه در هنگام ارائه تسهیلات استفاده کنند.

۳- هویت دیجیتالی

قراردادهای هوشمند به شما اجازه کنترل هویت دیجیتالیرا مثل داده‌ها و سایر موارد را داده و اجازه می‌دهند تا با به اشتراک‌گذاری چیزهایی که خودتان می‌خواهید، به شرکت‌ها در شناختن مشتریان‌شان کمک کنید. طرفین قرارداد لازم نیست که اطلاعات حساس را برای تراکنش‌ها نگه دارند. این کار باعث کاهش مسئولیت و بالارفتن میزان انعطاف و همکاری خواهد شد.

۴- سوابق

قراردادهای هوشـــمند کد تجاریکنواخت را دیجیتالی می‌کنند و فرآیند تمدید و انتشـــار آن را خودکار می‌سازند. همچنین می‌توانند در ایجادیک وام مطمئن، سهیم باشند. آن‌ها می‌توانند قوانینی را که در آینده به از بین بردن سوابق نیاز دارند، خودکار سازند و با تمدید و انتشار خودکار، قراردادهای هوشمند می‌توانند مخارج قانونی را کاهش دهند.

۵- اوراق بهادار

قراردادهای هوشمند می‌توانند مدیریت جدول سپرده‌گذاری را ساده‌تر کنند. آن‌ها همچنین واسطه‌ها را در زنجیره نگهداری اوراق بهادار نگه می‌دارند و با کاهش خطرات عملیاتی، تقســیم ســهام و مدیریت مســئولیت را آســان‌تر می‌کنند. اما باید به مواردی نیز توجه داشــت. امضــای تایید ایالتDelaware ممکن اســت نیاز به ایجاد قانونی داشته باشد که اجازه ثبت خود در دفتر توزیعی را بدهد. در حالی که صادرکنندگان این اوراق از خریداران اســتقبال می‌کنند، برخی شــرکت‌ها ممکن اســت در مورد این اطلاعات محافظ کارانه عمل کنند(وانگ و دیگران[4]،۲۰۱۸).

۶- تجارت مالی

[1]Escrow
[2]Local Ethereum
[3]Upwork
[4]C. Wang, J. Shen, Q. Liu, Y. Ren, T. Li

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قراردادهای هوشمند می‌توانند انتقال‌های بین‌المللی را ساده‌تر سازند و نقدینگی بیشتری برای دارایی‌ها فراهم کنند و همچنین برای خریداران، تولیدکنندگان و موسسات عملکرد بهتری در زمینه اقتصادی فراهم کند. در این زمینه ملاحظاتی نیز وجود دارد. استانداردهای صنعتی برای پشتیبانی گسترده از قراردادهای هوشمند بایدبالا با شند و مفاد قانونی باید تعیین شوند. ادغام سیستم‌های توافقی، فناوری‌های لازم و اکو سیستم‌های غیرزنجیره‌ای برای موفقیت لازم و مهم است(همان).

۷- مشتقات

قراردادهای هوشمند می‌توانند پردازش‌های بعد از معامله را ساده‌تر سازند و کارهای اضافی تایید معامله را از میان بردارند. آن‌ها یک شرایط استاندارد برای پردازش بهتر کارهای بعد از معامله بوجود می‌آورند و همچنین به شکل همزمان به دنبال نظارت و حل و کاهش مشکلات احتمالی خواهند بود. هنگام استفاده از قراردادهای هوشمند، مهم است که تغییرات پروتکل مرتبط با اصلاحات قانونی، توجه داشته باشیم(همان).

۸- سوابق داده‌های مالی

سازمان‌های مالی می‌توانند از قراردادهای هوشمند برای بدست آوردن اطلاعات دقیق و شفاف مالی استفاده کنند و گزارش‌های مالی خود را بهبود یابند و مخارج حسابرسی آن‌ها را کاهش دهند. بدین طریق، این قراردادها به بهبود یافتن ثبات بازار کمک می‌کنند و مخارج حسابرسی را از طریق اشتراک مخارج بین سازمان‌ها، کاهش می‌دهد. قابلیت همکاری در میان شبکه‌های لجستیک توزیع شده و سیستم‌های موروثی[1] در گزارش‌های مالی بسیار مهم است(همان).

۹- وام‌های مسکن

قراردادهای هوشمند می‌توانند قراردادهای وام و رهن مسکن را از طریق اتصال خودکار بخش‌های مختلف، ساده‌تر سازند و یک پروسه بدون مشکل و آسوده‌ای را فراهم کنند. آن‌ها می‌توانند به شکل خودکار پرداخت‌ها را پردازش کنند و در هنگام واریز مبلغ وام، اتفاقات را یادداشت کنند. آن‌ها همچنین امکان ملاحظه سوابق و پیگیری و تایید پرداخت‌ها را ساده‌تر می‌کنند و مشکلات و هزینه‌های بین راه را کم‌تر می‌کنند. داشتن هویت دیجیتالی برای این پروسه لازم است.

۱۰- ثبت قراردادهای املاک

قراردادهای هوشمندی که قراردادهای انتقال املاک را کنترل می‌کنند، می‌توانند موارد جعلی را شناسایی کنند و این‌گونه به شفافیت و بهینه بودن تراکنش‌ها کمک کنند و اطمینان لازم را به ما بدهند. آن‌ها همچنینمی‌توانند هزینه‌های حسابرسی را کاهش دهند. پروتکل‌های متداول باید برای ثبت موارد الکترونیکی ایجاد

[1] legacy systems

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شوند(تیان و دیگران[1]، ۲۰۱۸).

منافع استفاده از قراردادهای هوشمند برای بانک‌ها و مشتریان

قراردادهای هوشـمند احتمالا برای بخش‌هایمختلف خدمات مالی به کار گرفته خواهد شـد. موارد کلیدی کاربرد قراردادهای هوشمند در صنعت خدمات مالی عبارتند از:

بازار های سرمایه و بانکداری سرمایه گذاری[2]

تامین مالی شرکتی:عرضه اولیه سهام، سرمایه گذاری خصوصی

تامین مالی ساختار یافته: وامهای سندیکا و وامهای اهرمی[3]

زیرساخت بازار بورس اوراق بهادار

بانکداری خرد و بانکداری تجاری[4]

تجارت بین الملل[5]: مستندسازی زنجیره تامین، صورتحساب و پرداختها

قرض وام رهن[6]

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

با توجه به کاربردهای قراردادهای هوشمند منافعی را در پی دارد:

تأمین مالی جمعی برای سهام خصوصی در استارتاپ‌ها، یکی از موارد کلیدی هوش مصنوعی به شمار می‌آید که اولویت روش‌های دیگر نیز می با شد. فیلیپ دنیس[7] به برر سی دو مثال از این موارد می‌پردازد که بیشترین تأثیر را دارا اســت، تخمین تحلیل این نوع کســب وکارها حاکی از این اســت که اتوماســیون از طریق منطبق شــدن با قراردادهای هوشمند، فرایندهای مرتبط و تغییراتسازمانی منافع اساسی را ایجاد خواهد کرد. این تخمین‌ها بر مبنای تحلیل تکنولوژی، تحلیل فرایندها و عناصــر هزینه مقرراتی اســت که در محیط امروزی وجود دارد و با تکامل سیستم، این تخمین‌ها نیز تغییر خواهد یافت.

۱-صرفه جویی با کاهش زمان تسویه وام:

بازار وام اهرمی با مشــکلات حادی روبرو اســت. درحالیکه معاملات اوراق قرضــه با نرخ بازده بالا[8]در t + ۳ روز دوره تسـویه برای وام های اهرمی با هر مبلغی تقریبا ۲۰ روز طول می کشـد. این مسـئله ریسـک بالا و چالش های نقدینگی دربازار وام اهرمی به دنبال خواهد داشــت و به جذابیت و رشــد آن صــدمه میزند. از ســال ۲۰۰۸، بازار جهانی وام اهرمی، شاهد رشد منفی بوده در حالی که بازار اوراق قرضه با نرخ بازده بالا ، بالای ٪۱۱رشد را تجربه کرده اســت. چنین ســازمانهایی بر اینباورند که قراردادهای هوشــمند می تواند باعث کاهش دادن تأخیر در

[1]Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, X. Cu
[2]Investment Banking
[3]leveraged loans
[4]Commercial and Retail Banking
[5]Trade Finance
[6]Mortgage Lending
[7]Philippe Denis
[8]High-Yield Bond trades

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فرایندهای مستندسازی، تأیید فروشنده و خریدار، چککردن قوانین ،قوانین ضدپولشویی[1] شناسایی اولیه مشتری[2] با کمک دفتر همگانی دارای مجوز شـــود.دوره تســـویه وامهای اهرمی میتواند تا طیف t + ۱۰و t + ۶ یابد و منجر به افزایش نقدینگی وام[3]های اهرمی شود.تخمینزده می شود که با کاهش زمانهای تسویه، اگر وامهای اهرمی نصف وامهای اوراق قرضه با بازده بالا یعنی در حدود ۵٪ تا ۶٪ رشد داشته باشند، تقاضای بازار وام را با پیشرفت ۱۴۹ میلیارد دلاری مواجه خواهند ساخت. این وامها معمولا ۱٪الی ۵٪کارمزد سازمانی دارند که درآمدی در حدود ۵,۱ الی ۴,۷میلیارد دلار برای بانک های سرمایه گذار به ارمغان خواهدآورد. به علاوه، هزینه های عملیاتی، سرمایه مورد نیاز جهت نظارت و هزینههای مربوط به خسارت تأخیر تأدیه در طول تسویهوام را های اهرمی با کوتاه شدن دوره تسویه، کاهش خواهند داد.

۲-افزایش سود صنعت رهن

فرایند وام اهرمی به اکوسیستمی پیچیده برای ایجاد، تامین و سرویس دهی رهن تکیه می کند که با خود هزینه و تأخیر بههمراه دارد. روبرتو[4]می گوید "حال حاضر، بهترین زمان برای حل مشکلات سیستماتیکپردازش وامهای رهنی است. وامها یکی از بهترین عوامل برای رشد به حساب می آیند 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 هزینه و زمان مورد نیاز فرایند را ازطریق اتوماسیون، بازطراحی فرایند و دسترسی تمامی طرفین قرارداد به اسناد فیزیکی حقوقی، کاهش خواهد داد و این امر رااز طریق به اشتراک گذاشتن این اسناد و دسترسی به اطلاعات بیرونی انجام می دهد.

تحقیقات صورت گرفته اخیر در مورد اتوماسیون پشت باجه بانکی پیش بینی می کند که وام دهندگان رهنی[5] می توانند ازطریق سیستمهای مدیریت فرایند کسب و کار، پلتفرمهای بانکداری متمرکز الکترونیکی[6] و نیز سیستمهای مدیریت اسناد[7]هزینه‌های خود را بین ۶٪ الی ۱۵٪ کاهش دهند. این اعداد در کنار تجربه و بحث‌های صورت گرفته با مجربان صنعت، موجب‌کاهش دادن هزینه‌های فرآیندهای وام دهی می‌شود. برای مثال در بازار مسکن آمریکا، تقریبا ۱,۶ میلیون خانه در سال ۲۰۱۵ به فروش رسید. بر اساس میانگین های آماری از صاحب خانهها با وام رهنی این خانهها را خریده بودند و تخمین زده شد که وام دهندگان حداقل ۵,۱ میلیارد دلار از طریق اتوماسیون فعالیت‌ها برای سازمان‌های خود صرفهجویی به همراه خواهندداشت. همچنین تخمین زده می شود که با انطباق قراردادهای هوشمند، هزینه های پردازش وام رهنی مشتریان حدود ۱۱٪ الی۲۲٪ کاهش خواهد یافت . در واقع، به ازای هر وام مبلغ ۴۸۰ تا ۹۶۰ دلار صرفه جویی خواهد شد؛ میانگین هزینه پردازش ۴۳۵۰ دلار است. میزان وام‌های معلق در سال ۲۰۱۴ در کشورهای ایالات متحده و اروپا ۹۸,۲۰ دلار بوده است. در موردبازار رهن

[1]Anti-money laundering
[2]Know your customer

۳

[4]Roberto Mancone
[5]banking back-office automation
[6]core banking platforms
[7]document management systems

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

آمریکا و اروپا، قراردادهای هوشـــمند می‌تواند در فرایند جدید ایجاد وام رهنی به طور بالقوه بین ۳ الی ۱۱میلیارد دلار کاهش هزینه داشته باشند.

در ادامه می‌توان به تأثیر مثبت بر ســـود خالص از طریق کاهش هزینه های خدمات و اداری نیز اشـــاره نمود. قراردادهای هوشـــمند با خودکار نمودن فرایندهای کســـب وکار 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 می دهد. قدرت و منفعت این تکنولوژی بیشتر ازکاهش هزینه‌ها، ریسک‌ها، نرخ‌های خطا و فرایندهای مغایرتگیری ا ست چرا که امکان داشتن زیرساختی مشترک را برایاعضاء فراهم می کند و منجر به آزاد نمودن سرمایه و گزارشدهی قانونی می گردد(کنگ و هی، ۲۰۱۷).

همچنین مایکل ســـالو در مقاله‌ای در ســـال ۲۰۱۸ تحت عنوان " از قراردادهای هوشـــمند تا امنیت " در مزایای قراردادهای هوشمند به این موارد اشاره می کند:

۱- تاییداطلاعات‌افزایش‌یافته: با انتخاب استفاده ازشـــــرکت‌های بلاکچینی می‌توان دو مشکل را فوراًحل کرد: کنتـــرل اطلاعات درتراکنش‌های دیجیتالی و اجتناب از تکرارها.

۲- اعتبارسنجی‌سرعت‌بالایی‌دارد: نیازی نیست منتظر تایید تراکنش از سوی بانک باشید.

۳- پایداری‌پیشرفته: وقتی هیچ رگولاتورمرکزی ای وجود ندارد نقطه مرکزی ای برای شکســـت نیز وجود ندارد و بلاکچین مقاومت بیشـــتری در برابر انواع حملات مخرب دارد.

۴- شـــفافیت: هیچ تراکنش بلاکچینی رانمی‌توان تغییـــر داد یـــا حذف کـــرد. همه تغییـــرات در بلاکچین‌های عمومی قابل مشاهده‌اند.

۵- توانمندسازی کاربر: هر بخشـــی در استفاده از بلاکچین مســـتقیما تحت کنتـــرل اطلاعات و تاریخ تراکنش است.

۶-کاهش‌هزینه‌های‌عملیاتی: بلاکچین می‌تواند هزینه‌هـــا را کاهش دهـــد. بر اســـاس آخرین تحقیق، اکسنچر اســـتقرار بلاکچین برای خودکارســـازی فرایندهای مالی خاص می‌تواند به بانک‌ها کمک کنـــد که ســـالانه ۱۲میلیارد دلار ذخیره کنند.ازنظر مشـــتریان اســـتفاده از بلاکچین برای انجـــام پرداخت‌های بین‌المللی می‌توانـــد منجر به کاهش هزینه‌هایی شـــود که توسط بانک‌ها به مشتریان تحمیل می‌شود[1].

بررسی قرارداد های اتوماتیک و هوشمند از نظر منظر مبانی قرارداد های اسلامی

دراین قســـمت به طور مختصـــر به بیان موارد اصـــلی ویژگی‌های قرارداد هوشـــمند در ارتباط با قراردادهای اســـلامی می‌پردازیم . و مواردی که مرتبط با موارد فقهی مشـــابه با موارد قرارداد الکترونیکی اســـت، از بیان آن‌ها

[1] مواردی که در مزایای بلاکچین و قرارداد هوشمند بر بستر بلاکچین مطرح شده تا حدی ازنظر پژوهشگر اغراق آمیز است که دلیل مربوطه در قسمت محدودیت‌ها و عدم مزیت‌های قرارداد هوشمند و بلاکچین آمده است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

خوداری می‌کنیم چرا که تا حدی در قســمت ماهیت قراردادهای الکترونیکی به آن‌ها پرداخته شــده و تاکیدا که هدف اصلی پژوهش بررسی ماهیت این قراردادها از نظر فقهی و اسلامی نمی‌باشد.

الحاقی بودن

در قرارداد های الحاقی اختیار گفتگو درباره شــرایط قرارداد بکلی از یک طرف گرفته می شــود و طرف دیگر از پیش، تمام شرایط و آثار آن را معین می کند. کسی که مایل به بستن پیمان ا ست، یا باید از آن منصرف شــود یا تمام شــرایط طرف را بپذیرد، ود واقع به طرحی بپیوندد که او به طور مســتقل تنظیم کرده اســت. به همین جهت هم این گروه از قرارداد ها را الحاقی یا انضمامی می نامند.

قرار داد های خودکار که در محیط الکترونیکی منعقد می شــوند از جمله قرارداد های الحاقی محســوب می شوند زیرا فرو شنده کالا و خدمات خود را توام با اطلاعات لازم و شرایط از پیش تعیین شده در این سیستم ها طراحی کرده ا ست و خریدار و مصرف کننده در صورت تمایل به خرید فقط تحت شرایط می تواند آن را قبول کند و عموما دیگر جایی برای مذاکره وجود ندارد.

رضایی بودن

قرارداد های ر ضایی قرارداد هایی اند که هر گاه قصد انشا در آن مقرون به چیزی با شدکه دلالت بر قصد نماید صحیح شناخته می شود و احتیاج به الفاظ و عبارات مخصوص و یا تشریفات خارجی دیگری ندارد. ماده ۱۹۱ قانون مدنی " صرف مقرون بودن عقد به چیزی که دلالت بر قصد انشاء نماید" را در تحقیق عقد کافی دانسته اســت. درانعقاد قرار داد از طریق ســیســتم های خودکار نیز اصــل بر رضــایی بودن اســت، مگر اینکه قانون گذار تشریفات خاصی را برای آن لازم بداند.

آنی بودن

قرارداد آنی قراردادی ا ست که تمام اجزای مورد آن در لحظات معین زمان تحقق دارد مانند عقد بیع که دو مورد آن مبیع و ثمن، در زمان معین، شــخصــا یا توعا محقق می باشــد. قرارداد های اتوماتیک را به ســبب ســرعت مبادله ی اطلاعات در محیط اینترنت می توان از قرارداد های آنی قلمداد کرد.

زیر ساخت‌های ضروری پیاده‌سازی قراردادهای هوشمند

۱- پیاده سازی فرایند انعقاد قراردادهای هو شمند در حقوق ایران منوطبه پیشبینی و پیاده سازیزیر ساخت‌های این قراردادها ا ست. مهمترین زیر ساخت‌های این قراردادها امضائات دیجیتالی و بستر شبکه می‌با شد. امضائات دیجیتالی، امضایی ا ست که از طریق تغییر شکل داده پیام از طریق ا ستفاده از یک سیستم رمزنگاری نامتقارن و یک تابع هش تولیدمی‌شود. این امضا دنباله‌ایاز بیت‌هایی است که با اجرای یک پیامالکترونیکی از طریق تابع هش یکطرفه و سپس رمزگذاریپیام نتیجه که از طریق کلید شخصی فرستنده خلاصه می گردد، ایجاد می‌شود(Blythe,

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

.(2007

۲- دومین مساله، مساله سخت‌افزاری است که قراردادهای هوشمند مبتنی بر بلاکچین به دلیل اینکه در بستر بلاکچین هستند نیاز به سخت‌افزارهای قویتر نیاز دارد ولی در ارتباط با قراردادهای هوشمند هوش مصنوعی، چون از ابزارها و الگوریتم‌های AI استفاده شده است نسبت به بلاکچین از لحاظ سخت‌افزاری، از سطح پایین‌تری برخوردار است.

۳- یکی دیگر از زمینه‌های پیاده‌سازی قراردادهای هوشمند، آماده سازی اجرای این قراردادها از لحاظ حقوقی است . چالش عدم وجود ظرفیت کامل آن‌ها برایبرخورداری از تمامی جنبه‌های حقوقی انواع قراردادها در نظامات حقوقی است؛ برای مثال، اگرطرفین عقد مبادرت به انعقاد عقودی مانند صلح محاباتی در نظام حقوقی ایران کنند، چنین عقدیبه دلیل عدم تطابق میان ارزش عوضین معامله، قابلیت انعقاد در قالب قراردادهای هوشمند را نخواهدداشت؛ چراکه هوش مصنوعی از تأیید این قرارداد خودداری میکند. البته چنین ویژگی میتواندموجب ازبینرفتن غبن در معاملات مغابنی شود(صادقی، ۱۳۹۷). لذا ابتدا باید زمینه‌های حقوقی قراردادها باید مورد توجه قرار بگیرد و از آنجا که این قراردادها به صورت خودکار اجرایی می‌شوند در صورت لزوم باید قوانین مربوطه در کتابخانه قانون در پروتکل پیشنهادی قرار بگیرد و یا تمام قراردادهایی که در این پروتکل و به صورت هوشمند می‌خواهند اجرا شوند، با توجه به مبانی حقوقی و با توجه به امکان پیاده‌سازی در کتابخانه قرار بگیرند.

۴- از آنجا که انعقاد قراردادهای هوشمند از لحظه انجام مذاکراتمقدماتی تا امضای قرارداد توسط طرفین،تحت نظارت هوش مصنوعی انجام می‌گیرد. هوش مصنوعی مطابق با دستورالعمل داده شده، مفادقرارداد را تجزیه و تحلیل و در صورت مطابقتمفاد قرارداد با پروتکل‌های داده شده، آن‌ها را تأییدمی‌کند.تأیید قرارداد توسط هوش مصنوعی به منزله نهایی شدن قرارداد است. در صورتی که مفادقرارداد با دستورالعمل داده شده به هوش مصنوعی تطابق نداشته باشد، امکان انعقاد قرارداد نیست(کیویات[1]، ۲۰۱۵).

پیشینه تحقیق

ژیگئو[2](۲۰۱۹)در مقاله خود به بررسی سیاست های ضد اعتماد که در برنامه های بلاکچین مورد توجه قرار می گیرد بحث می کند. در این تحقیق بیان می شود که تکنولوژی بلاکچین سیستم های غیر متمرکز را گسترش می دهد و به طور بالقوه فضای قراردادی را از طریق قرارداد های هوشمند گسترش می دهد.در ضمن، اجرای سیستم غیر متمرکز در محیط اطلاعاتی شامل اطلاعاتی است که لازم است اصلاح شوند. همین طور ادعا می شود که قرارداد های هوشمند عدم تقارن اطلاعاتی را کاهش می دهند و مازاد رفاه مصرف کننده را از طریق افزایش رقابت و ورود رقبا بیشتر افزایش می دهد. به طور کلی، بلاکچین تعادل اقتصاد و بازار در محدوده گسترده تری از

[1]Kiviatt
[2]Zhiguo (2019)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

اقتصاد حفظ می کند.

اندرسون و دیگران [1](۲۰۱۹)در تحقیق خود به شیوه عملکرد قرارداد های هوشمند در بستر بلاک چین پرداختند. در رویکرد تولید قرارداد های هوشمند در بستر بلاک چین،یکیا تعداد بیشتری پردازنده کامپیوترییک تقاضا را برای خدمت مالی دریافت می کنند. یکیا تعدا بیشتری پردازنده کامپیوتری، یک یا تعداد بیشتری ویژگی از تقاضای مورد نظر مشخص می کنند. یک یا چند پردازنده کامپیوتری یک یا تعداد بیشتری از نمونه های قرارداد های هوشمند که مرتبط با تقاضای مورد نظر است را مشخص می کنند، حداقل در بخشی، که یک سری ویژگی با تقاضا مرتبط است. یک یا چند پردازنده کامپیوتری،یکیا تعداد بیشتری از پاسخ به تقاضا را از یکیا تعدا بیشتری از ارائه دهنده خدمات دریافت می کنند. یک یا چند پردازنده کامپیوتری،یک قرارداد هوشمند پیشنهادی را ایجاد می کنند، حداقل در بخشی از یک یا چند قالب قرارداد هوشمند و یک یا چند پاسخ دریافت شده.

وانگ و دیگران [2](۲۰۱۸)در توصیف قرارداد هوشمند این گونه بیان می‌کند که قرارداد هوشمند عملکرد خاصی در مورد کاربران ناشناس بدون سیستم متمرکز اجرا می کند. همین امر تسهیل شدن پرداخت های عادلانه و قانونی در تجارت را از طریق ایجاد و انجام تراکنش های تغییر ناپذیر فراهم می کند.چنین قرارداد هایی مانند قرارداد های هوشمند کیفری(CSC)که در CSC'16 پیشنهاد شده است می تواند با توجه به زبان های برنامه نویسی موجود کارآمد باشد.

رحیم و دیگران [3](۲۰۱۹)در مقاله خودبه بررسی مسائل اسلامی و شریعت فین‌تک پرداخته اند. تکنولوژی مالی،یک تکنولوژی در حال ظهور در تراکنش ها و مبادلت مالی است. این تکنولوژی یک تکنولوژی نفاق‌افکن است چراکه رفتار بانکداران را برای سهامداران تغییر می‌دهد. رشد این تکنولوژی در حال ظهور نه تنها بر صنعت مالی متعارف تاثیر گذار است بلکه بر صنعت مالی اسلامی نیز تاثیر گذار است و دلیل آن این است که فین‌تک اسلامی ادعا کرده است که اصول و مبانی شریعت با سیستم و مکانیزم های اصلی این تکنولوژی سازگار است و انطباق دارد.

وانگ و دیگران [4](۲۰۱۹)سیستم های مدیریت مالی وام در حال حاضر به صورت سیستم های تک سرویسه استفاده می شوند،همچنین تراکنش ها و مبادلات مالی در این سیستم شفاف و قابل پیگیری نیستند. داده ها و اطلاعات خصوصی و امنیتی آن ها در برابر حملات سایبری به اندازه کافی از امنیت برخوردار نیست. در این مقاله پیشنهاد شده است که برای چیره شدن بر این مشکلات، یک سیستم مدیریت مالی جدید برای وام،LOC ، مبتنی بر قرارداد های هوشمند طراحی شود.

[1]Anderson & et.al (2019)
[2]Wang & et.al (2018)
[3]Rahim & et.al (2019)
[4]Wang & et.al (2019)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فنگ و دیگران [1](۲۰۱۹)در مقاله خود به بررسی رشد و توسعه قرارداد های هوشمند پرداخته اندو نشان دادند که ارزش قرارداد های هوشمند در پلتفرم اتریوم در بازار مربوطه افزایش پیدا کرده است. در سال ۲۰۱۶، مردم به دلیل از دست رفتن نزدیک به ۵۰ میلیون دلار ارزرمزنگاری شده در حمله مربوط به سازمان DAO شوکه شده بودند. و با توجه میزان و حجم بزرگی از مبالغ که در این بازار ها وجود دارد امنیت این بازار ها بعد از این اتفاق مورد توجه زیادی قرارگرفته است. در این مقاله در مورد مواردی که ممکن است امنیت این بازر ها را به خطر بیاندازد و اسیب پذیری انها بحث شده است.

سازبو [2](۱۹۹۸)بنیانگذار قرارداد هوشمند، این ایده را مطرح کرد که می توان با استفاده از پروتکل ها و رابط های کاربری تمام امکانات و شرایط لازم را برای همه مراحل مربوط به فرآیند قرارداد را تسهیل کرد. این قرارداد هو شمند بسیار کارآمدتر از قرارداد سنتی ا ست. برا ساس مقاله سازبو قرارداد های هو شمند تسهیلات و خدمات زیادی را در عرصه ی مالی برای وام های اعتباری و کارت های اعتباری می توانند ارائه دهند. معتقد است قراردادهای هوشمند توانایی حمایت از بسیاری از صنایع مانند بانکداری، بیمه، انرژی، دولت الکترونیک، مخابرات، صنعت موسیقی و فیلم، هنر، آموزش و بسیاری دیگر را دارد.

ساولیو [3](۲۰۱۷) در مقاله خود به تجزیه و تحلیل عنصر کلیدی بین قرارداد هوشمند و قرارداد سنتی می پردازد. او قرارداد هوشمند را اینگونه تعریف می کند: " قرارادد های که به صورت کد نرم افراری در بستر بلاکچین اجرا می شوند". اصل قرارداد هوشمند بر اساس یک سری عوامل و فاکتور های از پیش تعیین شده است.

میک [4](۲۰۱۷)در مورد مشکلات ادغام این قرارداد هوشمند با دنیای واقعی بحث می کند. این مقاله برخی محدودیت های فنی و حقوقی دستور العمل های مربوط به قراردادی هوشمند را بررسی می کند.

میک و نورتلس (۲۰۱۷)در مقاله خود به بررسی کاربرد های قرارداد های هوشمند می پردازند و نشان می دهند که قرارداد های هوشمند برای بانک ها ، وکلا و دادگاه ها مفید است.

دریک تجزیه و تحلیل دقیق تر ، جیانکاسپرو [5] (۲۰۱۷) فرض می کند که یک قرارداد هوشمند می تواند برای خریدیک کالای خاص با یک قیمت مشخص طراحی شود. این قراردادباید شامل ضمانت محصولات نیز باید باشد. کاربرد های جدید قراردادهای هوشمند ، یک مساله و عنصر مهمی است نه از جهت ار تباط فروشنده با خریداران شخصی و اطلاعات مالی از طریقیک واسطه مورد اعتماد، بلکه به عنوان یک سیستمی که به طور معمول مستقیما با کیف دیجیتالی افراد در ارتباط است.

[1]Feng & et.al (2019)
[2]Szbo (1997)
[3]Savelyev
[4]Mik (2017)
[5]Giancaspro

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

جیانکا سپرو[1] (۲۰۱۷) در مقاله خود حتی این مساله را بیان می کند که قرارداد های هو شمند می تواند برای شناسایی طرفین قرارداد، پیش شرایط و مقررات لازم برای اجرای قرارداد ها در کل پیش قراردادو مهلت برای ارجاع به قیمت مبادله سهام به کار رود.

دیریکان [2](۲۰۱۵) در تحقیق خود به روشنی بیان می‌کند که نه تنها هوش مصنوعی بلکه، مطالعات معنایی، توسعه رباتیک، کلان داده، داده کاوی و .... می‌توانند زمینه‌هایی برای جهت گیری هایی در آینده برای بهبود و پیشرفت خدمات مالی و بانکی مورد توجه قرارا بگیرد. در این تحقیق این موضوع بیان می شود، دانشی که ربات ها استفاده می کنند از مقدار زیادی از اطلاعات، که کلان داده نامیده می شود، استفاده می کنند که از پایگاه داده‌های زیادی که با محا سبات ابری ارتباط دارند یا تو سط هوش مصنوعی مدیریت می شوند به د ست می آید. این پیشنهاد می‌تواند در جهت تولید خط‌ها و منابع انسانی که مورد بحث روز هستند استفاده شود.

الزایدی و کازاکوو[3](۲۰۰۸) پیشنهاد کردند که برای بهبود شرایط موجود از هوش مصنوعی ا ستفاده شود. آنها پیشنهاد کردند که زنجیره تامین باید جریان داده را اداره کند و آن را به شرکت های مختلف شبکه زنجیره تامین (به عنوان مثال وام گیرندگان، بانک ها، تامین کنندگان و انبارها) مرتبط سازد. این سیستم اجازه می دهد هر عاملی در شبکه حسلب خود را کنترل کند و تبادلات و تراکنشات خود را تنها با فشردن یک کلید انجام دهد. همچنین می توان این سیستم را از طریق تاجران و کارگزاران بین المللی و بازار های بین المللی توسعه و بهبود داد. بانک با افزایش سود کل و سپس فرو ختن محصولات به تاجران دیگر از طرف خودشان این فرایند را توسعه خواهد داد. سپس بانک دوباره با یکی سری از این تاجران و کارگزاران قرارداد امضاء می کند تا دوباره به مبادلات و خید و فروش ان در در بازار های بین المللی بپردازد.

پن [4](۲۰۱۶)در مقاله خود شرکت هایی که از هوش مصنوعی برای خدمات مالی و بانکییا در پروژه هایخود استفاده کرده اند را مورد بررسی قرارداد. با این حال بیشتر سرمایه گذاری ها و ابتکارات و خلاقیت ها به دوره آغاز و شروع بر می گردد. مایکروسافت یک چت باتی رو با عنوان Xiaobing توسعه داد. در همین حال IBM سیستم واتسون[5] را توسعه داد. این سیستم غربالگری رکورد های مبتنی بر تاریخ بیماران سرطانی را در تعداد زیادی از بیمارستان ها انجام می دهد. در چینBaidu بر روی توسعه سیستم های هوشمند و همچنین توسعه هوش مصنوعی در بخش مالی تمرکز کردند.

خان[6](۲۰۱۷)در مقاله خود به بررر سی کاربردهای هوش مصنوعی در حوزه مالی و بانکی پرداخته است. که یکی از مهم ترین کاربرد های هوش مصنوعی توسعه پروژه ای به نام مشاورین رباتیک است. یشرفت در

[1]Giancaspro
[2]Dirican (2015)
[3]Alzaidi and Kazakov
[4]Pan (2016)
[5]Watson
[6] Khan (2017)

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

"مشاوران روبو" به ویژه مهم است، زیرا می تواند به عنوان یک مشاور مالی خودکار عمل کند که به کاربر کمک می کند تا تصـمیمات مالی خود (به عنوان مثال مدیریت مالی شـخصـی) را انجام دهد. او در زمانهای قدیم اذعان داشت، AI به دلیل ویژگی های منحصر به فرد خود در ارتباط با سرعت و دقت به سمت تحلیل مالی، تخصیص دارایی، بیمه نامه، پیش بینی و گزارش حرکت می کند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل سوم:

روش تحقیق

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

در فصل دوم به بیان مبانی نظری در ارتباط با، شکل قراردادها، قراردادهای هو شمند، محدودیت‌های بلاکچین و قراردادهای هو شمند مبتنی بر بلاکچین و ساختار کلی قراردادها پرداختیم. همچنین زیر ساخت‌ها و زمینه‌های لازم برای اجرای این قراردادها را شـرح دادیم. لذا از آنجا که هدف اصـلی پژوهش، طراحی سـاختاری به صـورت پروتکل برای قراردادهای هو شمند با ا ستفاده از هوش م صنوعی می‌با شد می‌خواهیم با ا ستفاده از بستر گسترده هوش مصنوعی به چنین هدفی با روش مشخصی که به طور خلاصه در فصل اول در قسمت روش تحقیق بیان شده است برسیم.

مقدمه

از آنجایی که هر پژوهش علمی با ظهور مسـاله و یا مجهولی در ذهن محقق شـروع می شـود، هدف اصـلی تحقیق علمی را باید معلوم نمودن مجهول و به عبارتی حل م ساله و یافتن پا سخ منا سبی برای آن دان ست، اما یک پژوهش علمی یک هدف اولیه و یک هدف نهایی دارد. هدف اولیه محقق روشن نمودن مساله خاصی است که با آن روبرو شده است ولی هدف نهایی او دستیابی به معلوم کلی و به عبارتی قضایای علمی کلی است.روش شناسی تحقیق عبارت است از مطالعه مجموعه اصول و قوانین و کندوکاوهایی که ما را به شناخت علمی هدایت می کند. علم یعنی مطالعه واقعیت. واقعیت عبارت است از هر چیزی یا پدیده ای که قابل لمس و حس کردن است. بنابراین روش شنا سی تحقیق کاری علمی بر مبنای واقعیت شنا سی ا ست. واقعیت‌هایی که به و ضعیت و شرایط صفات بیرونی انســانها مثل نحوه لباس پوشــیدن و غذاخوردن و قیافه آن‌ها و به ویژگی درونی آدم‌ها مثل گرایش، احســاســات، تعصــبات و تعلقات و نیز عواملی که موجب بروز تغییرات ظاهری و پدیده‌های مختلف می‌شــود و همچنین چگونگی کنش متقابل اجتماعیو نحوه مشـارکت مردم در یک عمل اجتماعی مربوط می شـود(فراهانی، ۱۳۹۰).

انواع روش تحقیق میدانی، کتابخانه ای، تحلیل محتوا و منوگرافی است(ابراهیم زاده، ۱۳۹۲).

مطالعات کتابخانه ای، موضوعات مورد مطالعه در دسترس محقق قرار ندارد و غالبا به گذشته دور یا نزدیک مربوط می شود. به همین دلیل اصطلاح مطالعات کتابخانه ای را مترادف با مطالعات تاریخی به کار می برند.

مونوگرافی یا تک نگاری یکی از شیوه هایی ا ست که در روش ژرفایی برای مطالعه جوامع محدود بکار می رود. تک نگاری توصـیفی ژرف و همه جانبه از یک خانواده و یک روسـتا یایک طایفه اسـت. در تک نگاری اوضـاع اجتماعی، اقتصــادی، جمعیتی و فرهنگی، نهادها و هنجارها و بطور کلی همه جزئیات زندگی مردم روســتا مورد بررسی قرار می گیرد.

تحلیل محتوا به عنوان یک روش عبارت ا ست از شناخت و برجسته ساختن محورها یا خطوط ا صلی یک متن یا متون مکتوب، یک یا مجموعه ای از سخنرانی ها، تصاویر، نوارها و غیره... .

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

به هرحال انتخاب روش از این نظر اهمیت دارد که هر روش دارای مجموعه از فنون و ابزار اســت. لذا از این نظر، روش تحقیق مورد نظر ما کتابخانه‌ای اســت و بر اســاس مطالعات علمی و مقاله‌ها و همچنین مشـاهدات تجربی در خصوص زمینه‌های بخصوصی است. برای مثال در زمینه انتخاب بستر و شبکه برای پروتکل موردنظرمان از مبانی تئوریک موجود درباره بستر و شبکه استفاده کردیم و در ارتباط با انتخاب یک الگوریتم هش، ازمطالعه موردی و تجربی شرکت مایکروسافت استفاده کرده‌ایم.

این پژوهش از نظر اهداف اکتشافی است زیرا منابع زیادی برای آن وجود ندارد. روش شناسی این پژوهش از نوع مطالعات اکتشافی و رویکرد تحقیق نیز کیفی است. پایه هر علمی در حقیقت، روش شناسی آن علم است. د ست یابی به اهداف علم و یا شناخت علمی در هر ر شته ای میسر نخواهد بود، مگر زمانی که با روش شنا سی درســتی همراه شــود. به عبارت دیگر هر تحقیق علمی از باب روش انجام اســت که اعتبار مییباد و نه موضــوع تحقیق(خاکی، ۱۳۸۷).

اما به طور خاص، روش ما برای پا سخ‌گویی به سوالات تحقیق و خصو صا سوال ا صلی تحقیق که طراحی یک مدل است بر اساس نوع روش تحقیقی است که (عبدالطیف و بروسمیچ[1]، ۲۰۱۸) و (کاسادو وارا و دیگران[2]، ۲۰۱۸)که در مقاله خود برای پا سخگویی به سوالات خود ا ستفاده کرده‌اند. که این روش تحقیق بر ا ساس روش تطبیقی – مقایسه‌ای و تحلیلی می‌با شد. عبدالطیف و برو سمیچ در مقاله خود که به برر سی قراردادهای هو شمند زنجیره‌ای که امکان اجرای آن درمحیط‌های کم اعتماد می‌باشــد پرداختند به ارائه یک مدل جدید برای اثبات رفتار قرارداد هوشمند و نحوه عملکرد آن پیشهادکردند. و کاسادو ورا و دیگران در مقاله خود به طراحی مدلی از قراردادهای هوشمند، برای نظارت و کنترل فعالیت‌های لجستیکی پرداختند.

در مقاله اولی ابتدا، نویسندگان در مقاله خود در بخشی تحت عنوان محیط تعیین و مدل‌سازی اجزا و عناصر اصلی را برای طراحی قرارداد هوشمند تعیین کردند و سپس با توجه به همین عناصر به طراحی مدل خود پرداختند. تعیین اجزا و تعیین عناصر اصلی بر اساس مطالعات پیشین و نتایج تجربی حاصل از مدل‌های شبیه‌سازی شده است.

در مقاله دومی، نیز هر چند ماهیت تحقیق متفاوت است، ولی با مشخص کردن عناصر درگیر با قرارداد هوشمند را در ۴ لایه مشـتری، منابع، مدیریت جریان کار و خرید را مشـخص کرده اسـت. و در هر کدام از این لایه‌ها اجزای مربوط به قراردادهای هوشــمند را مشــخص کرده اســت و در نهایت مدلی ارتباطی آن‌ها رادر قســمت تجزیه و تحلیل(بحث) بیان کرده است.

لذا در این تحقیق، بر این اسـاس که قرارداد هوشـمند شـکل جدیدی از قراردادهاسـت لازم اسـت اسـاس و پایه‌های شــکل گیری این قراردادها مشــخص شــود در واقع اینکه چگونه میخواهیم چنین مدلی طراحی کنیم بر اســاس مطالعات کتابخانه‌ای و بررســی مقالات و تحقیقات نظری و تجربی در مورد هر کدام از بخش‌های اصــلی

[1]Abdellatif & Brousmiche
[2]Casado-Vara & et.al

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شکل‌گیری این قرار دادها ست. و پایه‌های ا صلی طراحی این قراردادها نیز برا ساس قراردادهای هو شمند مبتنی بر بلاکچین ا ست چراکه ماهیت آن دو یک‌سان ولی شکل پیاده سازی آن‌ها متفاوت ا ست. در واقع ما با ا ستفاده از قسمت‌های مختلف و ویژگی‌های مختلف قراردادهای هوشمند، به نحوه پیاده‌سازی این قراردادها در نظام بانکداری توجه کردیم. و همچنین با توجه به نحوه پیاده سازی و اجرایی شدن قراردادهای هوشمند به پارامترهایی مشخص، فریم ورک، حفاظت، ایمنی، تایید، ارتباط کاربران، شناسایی باگ‌ها، ارزیابی پویا و استا و قضاوت عقلانی رسیدیم. لذا در این فصل به بیان این پارامترها و توضیح مفاهیم مربوط به آن‌ها و راهها و روش‌های اجرای بهینه این پارمترها در حد مطلوب اشاره می‌کنیم. سپس در فصل بعدی به انتخاب روش بهینه جهت بهینه‌سازی پارامترها و نحوه اجرا و عمل روش‌های انتخاب شده می‌پردازیم.

نکته مهم در این تحقیق این ا ست که این تحقیق به دنبال طراحی مدلی برای قرارداد های هو شمندا ست که بتواند در بانکداری با توجه به قرارداد های اسلامی، با توجه به شرایط و امکانات موجود قابل پیاده سازی با کارکرد های قرارداد هو شمند مورد استفاده در حال حاضر باشد که جهت طراحی چنین قرارداد هایی میخواهیم از روش های هوش مصنوعی و ابزار ها و الگوریتم های هوش مصنوعی استفاده کنیم. که برای پاسخ به این مساله از ترکیب روش مقایسه تطبیقی و تحلیل محتوایی استفاده کرده ایم.

متنا سب با هدف ا صلی پژوهش که طراحی مدلی از قراردادهای هو شمند بوده از ترکیب روش‌های مقایسه تطبیقی و تحلیل محتوایی استفاده کرده‌ایم.

- بررسی الگوها و معیارهای نظری در مورد قراردادهای هوشمند مبتنی بر بلاک‌چین

- مقایسه تطبیقی قراردادهای هو شمند مبتنی بر بلاکچین با قراردادهای هو شمند مبتنی بر هوش مصنوعی با توجه به همین معیارها و الگوها

- در را ستای طراحی مدل قرارداد هو شمند مبتنی بر هوش مصنوعی، با توجه به مقایسه تطبیقی و معیارها و الگوهای نظری اقدام به طراحی مراحل و الزامات موردنیاز طراحی قرارداد هوشمند بر بستر هوش مصنوعی و درحوزه بانکداری کرده‌ایم.

این مراحل و الزامات بر اساس موارد زیر تدوین شده‌اند:

۱- تحلیل محتوایی الگوها و معیارهای نظری و فنی

۲- بررسی و مقایسه تطبیقی

۳- تحلیل محتوایی مدل طراحی شده از قراردادهای هوشمند در نظام بانکداری

با توجه به روش بالا و از آنجایی که ما می‌خواهیم در تحقیق خود به جای استفاده از بلاکچین، از هوش

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مصنوعی و ابزار های و الگوریتم های آن برای ایجاد قرارداد های هو شمند ا ستفاده کنیم بایدیک سیستم محافظ کامل و جامع طراحی کرده که شامل جزئیات زیر باشد. و درهر قسمت برای رسیدن به هدف مورد نظر در آن بخش ابتدا با بیان خلاصه وار شیوه پیاده سازی در قراردادهای هو شمند الگوریتم‌ها و روش‌های مورد نظر خود را بیان می‌کنیم. باتوجه به اینکه این پژوهش در حوزه بانکداری و در دانشکده اقتصادمی‌باشد در هر قسمت توضیحات لازم به صورت ساده آورده می‌شود وتوضیحات مفصل‌تر و پیچیده‌تر در پیوست آورده می‌شود.

بستر و شبکه

همانطور که در مبانی نظری و تئوری بیان کردیم اولین قسمت و مهمترین قسمت قراردادهای هو شمند بستر و فریم ورک آن است. بستر و محیطی که قراردادهای هوشمند معمول در آن‌ها اجرایی می‌شوند یک بستر و سیستم غیر متمرکز[1] و توزیع شده[2]است که همین غیر متمرکز بودن و توزیع بودن آن موجب امنیت بالا و اعتماد بالا به آن شده است. ولی همان‌طور که اصول بلاکچین (اصل پایداری[3]، اصل تغیرناپذیری[4]، اصل تصاحب‌پذیری[5]، اصل معیار[6] و اصل غیر متمرکز بودن) نشان می‌دهد در این بستر سلسله گزارش‌ها و سوابق تغییرناپذیر که توسط افراد خاص کنترل نمی‌شوند، مشخصا سودمند است، اما برای ایجاد چنین سازوکاری بهایی نیز باید پرداخت شود. و دقیقا مساله نیزهمین بهایی است که باید پرداخت شود. که این بها شامل، توسعه سخت‌تر و آهسته تر ، سخت‌تر شدن سازوکارهای تشویق کننده، داوطلبانه بودن به روز رسانی و .... است(جیمی سانگ[7]، ۲۰۱۸).

حفاظت پیشگیرانه

حوزه حفاظت پیشگیرانه مربوط به به فرآیندکد نویسی، استاندارد سازی در فرآیند نوشتن کد ها و شناسایی باگ ها و نقاط خلاء در خروجی کد نهایی می‌باشد.

زبان‌های برنامه نویسی مورد نیاز برای نوشتن قرارداد هوشمند

مطمئنا یکی از موارد مهم و اصلی در ایجاد یک پروتکل هوشمند برای اجرای قراردادهای هوشمند در بانک‌ها و شبکه مورد نظر استفاده از زبان برنامه نویسی درست و مشخص است. از آنجا که زبان‌های برنامه نویسی زیادی وجود دارد و با توجه به نوع شبکه مورد نظر ما که یک شبکه توزیع شده و شبه نامتمرکز است و نوع اجرای قراردادهای هو شمند هوش مصنوعی در ما شین مجازی بهتر ا ست از زبان‌های برنامه نویسی منا سب برای

[1]Decentralized system
[2]Distributed
[3]Principle of Sustainability
[4]Principle of Invariance
[5]Principle of Acquisition
[6]Criterion and Decentralization Principle
[7]Jimisong

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

طراحی شبکه و قراردادها استفاده شود(stackoverflow, 2019)[۱].

استانداردسازی کدها

همانطور که قبلا گفتیم قراردادهای هوشمند کدهای کامپیوتری هستند که در محیط یا بستری که قرار گرفته اند به صـــورت خودکار و اتوماتیک اجرا می‌شـــوند. و از آنجا که قرار اســـت این قراردادها در یک محیط برای کاربران و بانک اجرایی شـود لازم اسـت از اسـتاندارد های لازم برخوردار باشـد تا در فرآیند پیاده سـازی و اجرا مشکلی پیش‌نیاید. استاندارد بودن کدها از دو جهت مهم است. اول از دیدگاه برنامه نویسی است.عنصر اصلی در کدنویسی امن با زبان های مختلف برنامه نویسی، مستند سازی خوب و استفاده از استانداردهای قابل اجرا است. استانداردهای کدنویسی، برنامه نویسان را ترغیب به پیروی از مجموعه ای متحدالشکل از قوانین و راهنمایی‌ها می کند که بر اساس نیازمندی های پروژه و سازمان تعیین شده است، نه بر اساس سلایق و مهارت های مختلف برنامه نویســان. به محض تعیین اســتانداردهای مذکور، می توان از آن به عنوان معیاری برای ارزیابی کدهای منبع، چه به صورت دستی و چه به صورت اتوماتیک استفاده کرد.

از استانداردهای معروف در این زمینه می توان به استاندارد CERT برای کدنویسی امن اشاره کرد که یک ســری از قوانین و پیشــنهادات را برای کد نویســی امن با زبان های برنامه نویســی C، C++ و جاوا ارائه می دهد. هدف از این قوانین و پیشنهادات، حذف عادت های کدنویسی ناامن و رفتارهای تعریف نشده است که منجر به آسیب پذیری های قابل سوءاستفاده می شود[۲].

شناسایی باگ‌ها

شناسایی باگ‌ها در مراحل اجرای قرارداد هوشمند در ماشین مجازی و پیاده سازی کدها و تایید آن‌ها در حال انجام فرآیند بسیارحائز اهمیت است. برای مثال نوامبر سال گذشته یک کاربر به‌صورت تصادفی بیش از ۱۵۵ میلیون دلار از سرمایه خود را در سرویس کیف الکترونیکی «پریتی» متعلق به ارز دیجیتال اتریوم از دست داد. این کلاهبرداری در نتیجه وجود یک باگ بزرگ در این نرم‌افزار اتفاق افتاد که دامن این کاربر را گرفت. این اتفاق البته اولین حادثه‌ای نبود که در کیف پول هوشمند پریتی رخ می‌داد. یک ماه قبل از این اتفاق، یک باگ دیگر در این سرویس باعث شد هکرها بتوانند مبلغی معادل ۳۰ میلیون دلار از ارزهای دیجیتال این برنامه را به سرقت ببرند. البته پریتی تنها کیف پول متعلق به اتریوم نیســـت که از این قبیل آســـیب‌پذیری‌های قرارداد هوشـــمند (Smart Contrat) ضرر می‌کند. در سال ۲۰۱۶، هکرها موفق شدند مبلغی برابر با ۱۵ درصد از سرمایه در گردش اتریوم را به ســرقت ببرند. این اتفاق باعث ایجادیک شــکاف بزرگ در کســب و کار اتریوم شــد و در نتیجه آن، اتریوم مجبور شد سیستم بلاک چین و ارز دیجیتال خود را به‌طور کامل تغییر دهد و نسخه جدیدی از پول مجازی برای مشتریانش معرفی کند. همانند بسیاری دیگر از سرقت‌ها که از زمان ظهور اتریوم در سال ۲۰۱۵ تا به حال در این

[۱] زبان‌های برنامه‌نویسی قابل استفاده جهت نوشتن کدها در پیوست توضیح داده شده است.
[۲] درپیوست در مورد استانداردسازی CERT مفاهیم آن ارائه شده است

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

زمینه صـورت گرفته، اکثر این اتفاقات و باگ‌ها به «پروتکل‌های هوشـمند» مربوط می‌شـود(سـانگ، ۲۰۱۹). در ارتباط با قراردادهای هوشمند مبتنی بر هوش مصنوعی، تحقیقات در ارتباط با نقاط ضعف آن، بیشترین مشکل به قوانین و سـاختار قرارداد ها و قوانین و کتابخانه قوانین برمی‌گردد. الگوریتم‌هاو ابزارها و فریم‌ورک‌های متفاوتی برای رفع ا شتباهات و باگ‌های کدنویسی وجود دارد. از آن‌جایی که قراردادهای هو شمند کد آن تو سط انسان نوشـته می‌شـود پس امکان دارد انواع خطاهای برنامه‌نویسـی پیش آید و لذا می‌توان از توسـعه و بهبود کامپایلرها، الگوریتم‌های کلاس‌بندی مانند الگوریتم‌های مبتنی بر معنا (name-based) جهت بهبود کدها و شـناسـایی باگ‌ها استفاده کرد(کابالرو، ۲۰۱۷).[1]

تایید در حال انجام فرآیند

در تحقیقاتی که در آزمایشگاه هشگارد، مو سسه تحقیقاتی هشگارد و مو سسه تحقیقاتی BKFUND به طور مشترک در ارتباط با زمینه‌های ایجاد قراردادهای هوشمند انجام شده است، که شامل موارد زیر می‌باشد:

قرارداد هو شمند، با یک حس محدود، یک برنامه کامپیوتری ا ست که بر روییک دفتر توزیع شده با قوانین، حالت و واکنش مشروط کار می‌کند، که می‌تواند شامل ریزکپسوله سازی، تایید، و اجرای رفتارهای پیچیده گره توزیع شده، تبادل اطلاعات کامل ، انتقال ارزش و مدیریت دارایی با شد. در مفهوم و سیع‌تر، قرارداد هو شمند یک توافقنامه تجاری رایانه‌ای اسـت که به واسـطه‌گری نیاز ندارد و می‌تواند به طور خودکار شـرایط قرارداد را اجرا کند.

در حال حاضـر ، سـه روش فنی برای تحقق و بررسـی مکانیزم‌های فرآیند تایید قراردادهای هوشـمند وجود دارد: حالت اسکریپت ، حالت کانتینر شده و حالت ماشین مجازی.

اجرای کدها و ارزیابی امنیتی پویا

در این قسمت چه برنامه‌نویس بخواهد و چه نخواهد، هر کد منتشر شده از طریق بررسی و تایید، به صورت پیوسـته و خودکار مورد ارزیابی قرار می‌گیرد، تا این اطمینان حاصـل شـود کدهای اسـتاتیک می‌توانند از مرحله بررسی عبور کنند و نقاط ضعف آن شناسایی شوند و حلقه کد دچار over flow نشود یا به عبارت دیگرشرطی گذاشته نشود که enforce coding به سمت بی‌نهایت میل نکند.

تایید پویا گره‌ها در هنگام اجرای قراردادها

تایید پویا [2] با استفاده از ماشین مجازی ، تایید قراردادها و قراردادهای مرتبط را تحت پوشش قرار می‌دهد و روند اجرای قرارداد بررسـی خواهد شـد. حتی اگر یک هکر شـکاف و اخلالی ایجاد کند، چون روند بررسـی

[1] در پیوست در ارتباط با مفهوم باگ و انواع خطاها در برنامه نویسی توضیح داده شده است.

[2] dynamic verification

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

قراردادها و بررسی فرآیند اجرای قراردادها به صورت اتوماتیک و خودکار انجام می‌گیرد و از آنجا که قراردادهای هوشمند مبتنی بر هوش مصنوعی به دلیل ساختار و و بستر شکل گیری و نوع طراحی ماشین مجازی انعطاف پذیری مشخصی دارند، به محض مشاهده هر نوع اخلال غیر قابل‌حل در فرآیند اجرای قرارداد، مجریان آن را به حالت تعلق در می‌آورند.

قضاوت عقلانی بعد از اجرای قرارداد

نتایج بعد از اجرای قرارداد از طریق قوانین خاصی داوری می‌شود و در عین حال هوش مصنوعی برای تجزیه و تحلیل دامنه منطقی اجرای قراردادها معرفی می‌شود. تا در مورد نتیجه نهایی قرادادها تصمیم گیری شود، و مساله تصمیم و قصد کاربران مورد بررسی قرار گیرد. برای مثال سناریوی دوبار خرج کردن در مورد حساب ها و یا سطوح بالاتر آن بررسی شود.

مکانیزمی برای فرآیند شکایات و روش هایی برای قضاوت اتوماتیک

در میان گره ها،در جریان اجرای قرارداد هوشمند ، دارای یک مکانیزم داوری داخلی و مکانیسم داوری و قضاوت هوش مصنوعی برخوردار هستند و از تصمیم گیری مبتنی بر رأی[1] پشتیبانی می کنند ، تا فرصت های خاصی و معینی برای بازیابی یک ضرر فراهم کنند.

دراین قسمت منظور از تکنیک‌های مورد نیاز، استفاده از ابزارها و الگوریتم‌ها و طراحی کتابخانه برای تایید پویای قرارداد و حل کردن یا به تعلیق درآوردن قرارداد در صورت ایجاد یک مشکل در فرایند اجرای قرارداد است. به طور خلاصه در این قسمت به بیان آن‌ها می‌پردازیم.

ارزیابی و چک های ترکیبی بر اساس کتابخانه قانون

کتابخانه قانون موجود در پروتکل موردنظر از نظر ماهیت و کاربرد مانند کتابخانه داوری قرارداد هوشمند است و لذا به دلیل اهمیت و کاربردی که دارد باید استفاده شود. تا با استفاده از سیستم عامل در روند اجرای قرارداد، مفاد اصلی و پایه‌ای قرارداد غیر قابل تغییر باشد و حتما اجرا شود. لذا این کتابخانه در حقیقت شامل قوانین و مقرراتی پایه‌ای است که در روند هر قراردادی باید اجرا شود و همین‌طور شامل قراردادهایی است که بانک به عنوان یکی از نودهای اصلی به عنوان پایه‌گذار این شبکه، جهت انجام معاملات و تراکنش‌ها و مبادلات در آن قرار می‌دهد تا با استفاده از الگوریتم‌های یادگیری ماشین مانند یادگیری عمیق و شبکه تخاصمی مولد در ماشین مجازی به عنوان سیستم عامل موجود در ساختار(فریم‌ورک) بتواند ارزیابی‌های لازم را انجام دهد.

[1]vote-based decision-making

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تعیین مدل تراکنش ها و تبادلات و ارزیابی امنیتی بر اساس تجزیه و تحلیل معنایی

در سطح معنایی[1] کامپایلر معمول در فریم‌ورک مربوط به قراردادهای هوشمند، ارزیابی‌های مفهومی برای تعیین عملیات مشخص، قوانین را به درستی اجرا نمی‌کنند و ایمن نیستند.که عبارتند از:

۱- بررسی اشیاء و روش‌هایی که برای بررسی میزان ضرورت و نقص‌های احتمالی آن‌ها که در محیط‌های خارجی قرار دارند.

۲- ارزیابی اینکه آیا شاخه‌های دیگر از قرارداد ی فرآیند پردازش اوراکل کامل شده و آیا عملیات‌های آنومالی در زمان فراخوانی قرارداد وجود دارد یا خیر

۳- ارزیابی (عبارات) شرطی یکسان در آپشن‌های مختلف برای اجتناب از آنومالی ها به عنوان یک نتیجه متفاوت از نتیجه.

بررسی امنیت قرارداد های هوشمند بر اساس الگوریتم‌هایAI

ماشین مجازی هوش مصنوعی مجهز به یک چارچوب تأیید رسمی برای تأیید ویژگی های امنیتی قراردادهای هوشمند مبتنی بر هوش مصنوعی است. این چارچوب براساس یک زبان برنامه نویسی کاربردی، یک حل کننده SMT را در اختیار دارد و تعداد زیادی مدل و ابزار دارد. از آن برای تأیید نرم افزارهای مختلف و برنامه های رمزگذاری استفاده شده است.

جریان تایید قراردادهای هوشمند: زنجیره ابزار تایید، توانایی پردازش امنیت کدها را در دو سطح کد منبع و بایت کد دارد. کد منبع ترجمه در معادل برنامه[2]به یک زبان برنامه نویسی کاربردی ترجمه خواهد شد. مدل برنامه نویسی کاربردی ، در افشای منطق پنهان[3] و سهولت در انجام عملیات رسمی موفق است.بایت کد بر روی ماشین مجازی اجرا خواهد شد و کدها از هم جدا می شوند[4] و به یک برنامه کاربردی معادل تبدیل خواهند شد. و یک عملیات ارزیابی معادل و ارزیابی‌های پیوسته دیگر بر روی برنامه‌های کاربردی انجام می‌شود.یکی از ویژگی های اصلی استفاده از هوش مصنوعی برای شناسایی خودکار از نظر نحوی برای شناسایی مدل های معمولی است و سپس به طور خودکار، به دنبال شناسایی خواصی است که الزامات امنیتی را برآورده می کند. با توجه به برنامه قرارداد هوشمند ، موتور ماشین مجازی هوش مصنوعی به طور خودکار تطبیق جزئی و تطبیق کامل را برای پیشبینی مدل رفتار کدها تشخیص می دهد.

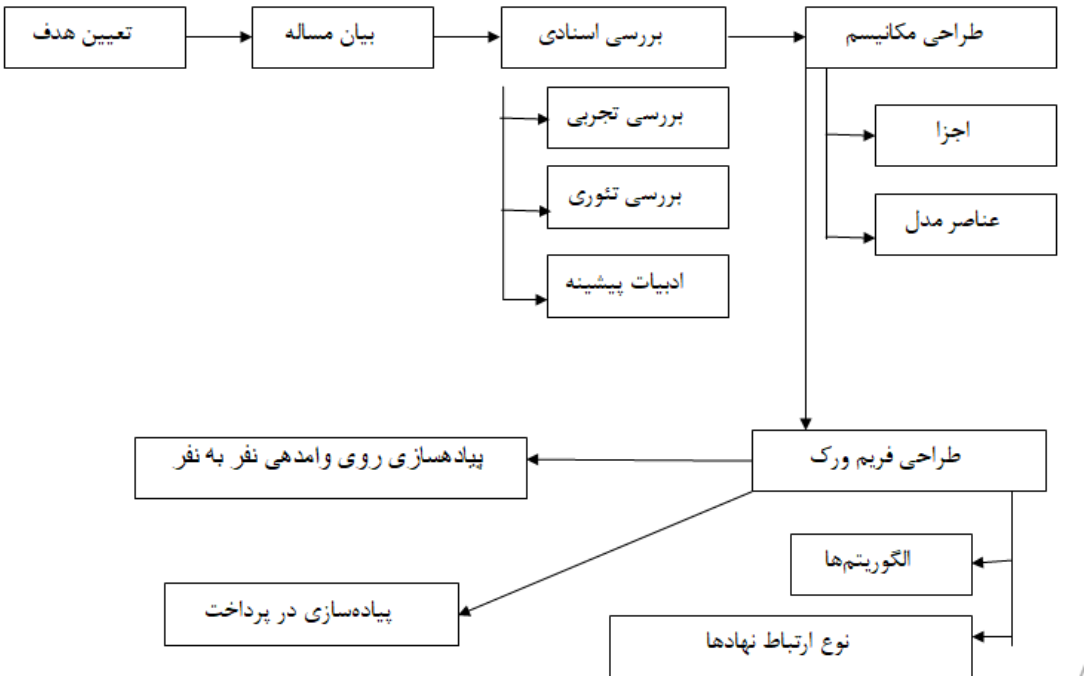
[1]semantic level
[2]equivalent program
[3]hidden logic
[4]disassembled

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بهینه سازی پویا و بهینه سازی امنیت بر اساس مدل شبکه تخاصمی مولد

ماشین مجازی فقط به کاربران نیاز دارد تا عناصر اصلی (مانند ورودی ، خروجی و شرایط معامله) یک قرارداد را با یک زبان برنامه نویسی وارد کنند. سپس، یک ژنراتور کد بر ا ساس یک شبکه عصبی عمیق قادر به تبدیل خودکار اسکریپت به یک برنامه معادل است. ماشین مجازی برای دستیابی به تأیید امنیت پویا ، شبکه مخالف تولیدی اخیراً توسعه یافته را تطبیق می دهد. روش تأیید پویا را می توان با چارچوب تولید کد در یک حلقه بسته همراه کرد. چارچوب شبکه تخاصمی مولد از دو شبکه عصبی تشکیل شده است. از شبکه عصبی برای تجدید نظر در برنامه های موجود برای قراردادهای هو شمند ا ستفاده می شود، در حالی که دیگری یاد می گیرد که از طریق نمونه های تصادفی توزیع احتمال داده شده، برنامه های هکر تولید کند. پس از ایجاد برنامه های قرارداد هو شمند ، آن‌ها در "شبکه شبیه سازی (شبکه ای که شبیه سازی۷ که شبیه یک شبکه شبه نامتمرکز و توزیع شده ا ست و در آنجا آزمایش ها می تواند به صورت کنترل شده انجام شود)" به همراه کدهای مربوط به هکرها مستقر می شوند. توابع هزینه این دو شبکه به هم گره خورده اند به طوری که وقتی کل سیستم به یک تعادل نش رسید ، نتیجه مطلوب کلی حاصل می شود. در این مرحله ، برنامه اصلاح شده برای قراردادهای هوشمند دارای بالاترین سطح امنیتی خواهد بود(بیل‌لی[1]، ۲۰۱۸).

خلاصه روش تحقیق



[1]Bill li

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۱- تعیین هدف تحقیق: طراحی مدلی از قراردادهای هوشمند در نظام بانکی

۲- بیان مساله: بواسطه مزیت‌های قراردادهای هوشمند در نظام بانکی ومالی ، چرا باید به جای قرادادهای هوشمند معمول، باید از قراردادهای هوشمند مبتنی بر هوش مصنوعی استفاده کنیم. و در زمینه پرداخت و تسهیلات نفر به نفر چگونه می‌توانیم مدلی بر اساس قراردادهای هوشمند طراحی کنیم.

۳- بررسی اسنادی، ادبیات پیشینه، مقالات و نتایج تجربی(روش کتابخانه‌ای)

این مرحله از بررسی، با توجه به تجزیه و تحلیل اسنادی در ارتباط با سه بخش انجام شده است:

- ✓ بررسی مزیت‌ها وعدم مزیت‌های بلاک‌چین
- ✓ مقایسه تطبیقی قرادادهای هوشمند مبتنی بر بلاکچین و هوش مصنوعی
- ✓ بررسی موارد استفاده از قراردادهای هوشمند

روش اصلی این مطالعات در پاسخ به سوال دوم این تحقیق بصورت ترکیبی از شیوه مقایسه تطبیقی- مقایسه‌ای و تحلیلی (با محوریت دو مقاله مذکور)می‌با شد به طوری که در طراحی مکانیسم و طراحی فریم‌ورک و اجزاء آن از روش تطبیقی و مقایسه‌ای استفاده شده است و در طراحی مدل‌نهایی قراردادهای هوشمند مبتنی بر هوش مصنوعی در نظام بانکداری از روش تحلیل محتوایی استفاده شده است.

۴- بررسی روش فریم‌ورک در دومقاله سال۲۰۱۸ ,Abdellatif & Brousmiche و Vara & et.al جهت طراحی مدل

۵- طراحی مراحل و ساختار اجزا و عناصر مدل قراردادهای هوشمند بر اساس فریم‌ورک و ساختار دو مقاله مربوطه

۶- مشخص نمودن اجزا و عناصر فریم ورک کلی طراحی قرارداد هوشمند جهت تعیین و مشخص کردن الگوریتم‌های هوش مصنوعی برای هر جزء

۷- تعیین الگوریتم‌های هوش مصنوعی در مراحل و اجزا مورد نظر

۸- اجرای دو مورد پرداخت به کارکنان و وام‌دهی نفر به نفر در بستر و فریم‌ورک طراحی‌شده در نظام بانکی

خلاصه فصل

در این فصل بر اساس، مبانی و ساختارهای کلی قراردادهای هوشمند، که در فصل ۲ بیان شده است به پارامترهای ا صلی شکل‌گیری قراردادهای هو شمند ر سیدیم و بر همین مبنا، به تو ضیح ا صولی که بر ا ساس آن

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

میخواهیم پروتکل خود را طراحی کنیم پرداختیم. در فصل بعد نیز بر اساس همین اصول و ترتیب به طراحی مدلی از قراردادهای هوشمند که برای کاربران من جمله بانک‌ها و نظام بانکی کاربردی باشد خواهیم پرداخت.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل چهارم:

پروتکل پیشنهادی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقدمه

ما دراین تحقیق به دنبال طراحی یک پروتکل، به شکل پروتوتایپ برای قراردادهای هو شمند بودیم. لذا در فصل سوم به بیان و برر سی بستر این قراردادها، ابزارها و الگوریتم‌های امنیتی و ساختار و نوع کدنویسی، ما شین مجازی و نوع آن پرداختیم. در حقیقت در فصل سوم به بیان ابزارها و الگوریتم‌هایی از هوش مصنوعی پرداختیم که می‌توانیم از آن‌ها برای طراحی قراردادهای هوشمند در بستر هوش مصنوعی استفاده کنیم به‌طوری که کارکردهای قرادادهای هوشمند مبتنی بر بلاکچین را داشته باشد و یا حداقل در حد قابل قبولی از ویژگی‌های قرادادهای هوشمند مبتنی بر بلاکچین باشد و همچنین نقاط ضعف قرادادهای هوشمند مبتنی بر بلاکچین را که در قسمت مبانی نظری بر ا ساس مباحث تئوریک و موردهای تجربی مطرح کردیم ندا شته با شد. لذا در این فصل بر اساس و به ترتیبی که مباحث،در فصل روش تحقیق بیان‌شده، به بیان و تحلیل تئوریک ابزارها و الگوریتم‌های مطرح شده در هر قسمت می‌پردازیم و نحوه عملکرد پروتکل پیشنهادی را بر ا ساس الگوریتم‌های پیشنهادی بیان می کنیم.

در قسمت اول این فصل به فریم‌ورک موردنظر بر اساس شبکه‌های تعریف شده‌می‌پردازیم. قراردادهو شمند بر بستر بلاکچین که یک دفتر همگانی‌توزیع‌شده است، می‌باشد. این فریم ورک لیستی از رکوردهای در حال رشد را به صورت بلاک‌هایی نگهداری کرده و آن‌ها را از خطرات مداخله و بازدید امن نگه می دارد. هر بلاک شامل یک وقفه زمانی[1]بوده و یک لینک به بلاک قبلی دارد، در واقع هر بلاکیک امضای رمز شده از بلاک قبلی را دا شته و این گونه یک رکورد امنی را فراهم می کند. طبق طراحی، بلاکچین به طور ذاتی در برابر د ستکاری و تغییر داده‌ها مقاوم بوده و داده‌ی ذخیره شده در بلاکچین قابل تغییر نمی‌باشد. پایگاه داده‌ی بلاکچین از طریق استفاده از یک شبکه‌ی همتا به همتا و یک سرور وقفه زمانی توزیع شده، به صورت خودگردان مدیریت می شود. بلاکچین‌هایک دفتر کل باز و توزیع شده هستند که می توانند تراکنش های بین دو شخص را از روی کفایت و به صورت تحقیق پذیر و پایدار ثبت کنند. خود دفتر کل نیز می تواند برای تراکنش های راه اندازی شده به صورت اتوماتیک برنامه نویسی شود.

فریم‌ورک

همانطور که قبلا اشاره شد قرارداد هوشمند در بستر یک شبکه توزیع شده (وب) است که افراد از طریق آن وارد شده و اقدام به پردازش و استخراج و انجام تراکنش می‌کنند. لذا ما در قدم اول باید به طراحی یک مدل برای فریم‌ورک مورد نظر خود بپردازیم. فریم ورک مدنظر ما دو قسمت ا صلی دارد. اول اینکه این فریم ورک به صورت شبه نامتمرکز است و ارتباط بین نودها بر اساس گراف جهت‌دار غیرمدور[2] است.

[1]time stamped
[2]Directed acyclic graph

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

از آنجا که این پروتکل برای طراحی قراردادهای هو شمند در حوزه بانکداری می‌با شد لذا بانک را به عنوان یک نود اصلی در این شبکه در نظر گرفته که شبکه شبه نامتمرکز را با ایجاد چند سرور مختلف و مبتنی بر سیستم توزیع شده ایجاد خواهد کرد.مسلما برای ایجاد چنین شبکه ای باید این شبکه را در د سته شبکه بزرگ قرارداد . فارغ از مسائل مرتبط با اندازه و نیاز شبکه، اجرای موفق طراحی شبکه نیاز به پیروی از اصول مهندسی در زیرساخت دارد[1].

فریم ورک مدنظر ما از چند نود اصلی تشکیل شده است که سایر نودها وگره‌ها بر اساس الگوریتم گراف جهت دار غیر مدور به هم مربوط می شوند. در حقیقت این نودهای اصلی مربوط به بانک می‌باشد. و دلیل آن این امر می‌باشد که برای مبادلات و انجام تراکنش‌ها از یک سری اطلاعات بانکی و داده‌های بانکی باید استفاده شود . در حقیقت برای اینکه نودها و گره ها بتوانند تراکنش انجام دهند باید دارای یک حساب مالی و به اصطلاح دارای یک والت باشند که این والت می‌تواند دارای یک حساب مرتبط با حساب بانکی طرف باشد یا یک واحد پولی جدید باشد و از طریق یک رابط برنامه ریزی کاربری(API[2]) به حساب مربوطه بانکی وصل شود وتغییرات لازمه حاصل از تراکنش و انجام قرارداد را در حساب‌ها اعمال کند. ورود کاربران به این شبکه مانند هر شبکه دیگری در بستر وب می‌با شد و بر ا ساس ا صول اولیه لاگین کردن وارد شبکه شده و به عنوان یک نود اصلی محسوب می‌شوند و بانک‌ها و شعبه‌های آن ها هر کدام تشکیل یک نود بدهند.

الگوریتم‌های نوع اجماع ابزارهای موثری برای به اشتراک‌گذاشتن و کنترل اطلاعات توزیع شده برای سیستم‌های شبکه‌ای و چند عاملی فراهم می‌کنند.ما به این کلاس از سیستم ها به عنوان شبکه های نیمه خودمختار اشاره می کنیم. در چنین تنظیمات، ما اثربخشییک کنترل متوسط ثابت را بررسی می کنیم ، که در آن عوامل (کنترل کننده) خارجی سیگنال را با میانگین ثابت به عوامل بومی همسایه در شبکه تحویل می دهند(چپمن[3] و دیگران، ۲۰۱۵).

در حقیقت بعداز اینکه هر یک از کاربران عمللاگین را بر اساس اطلاعات پایه و مورد نیاز انجام دادند به عنوان یک نود و گره وارد فریم ورک و شبکه می شوند و در نهایت بر ا ساس شبکه‌های نیمه خودکار از طریق ما شین مجازی تبدیل به گرافی می شود که دارای چند نود ا صلی ا ست که مراکز این نودها بانک‌ها هستند که به شکل زیر می‌شود.[4]

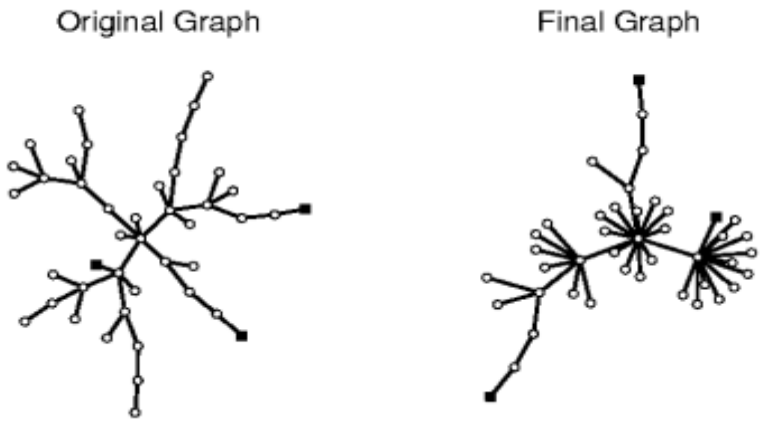
[1] پیوست الف، مربوط به فصل ۴

[2] Application Programming Interface

[3] Chapman

[4] پیوست ب، فصل چهارم

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.



حفاظت پیشگیرانه

در این قسمت به بیان روش‌ها و الگوریتم‌هایی می‌پردازیم که در نهایت منجر به افزایش امنیت فریم‌ورک و کاهش باگ‌ها می‌شود.

زبان برنامه نویسی

اخیرایکی از شرکت های دیده بان امنیتی به بررسی آسیب پذیری زبان های برنامه نویسی مختلف پرداخته و در نهایت طی گزار شی و ضعیت این زبان‌ها را مشخص کرده ا ست. این گزارش طی برر سی ده سال فعالیت این زبان ها و گزارشات امنیتی دریافت شده از آنها می باشد. طبق این گزارش امنیتی زبان های برنامه نویسی دارای بیشترین نقص امنیتی به ترتیب عبارتند از: C، پی اچ پی، جاوا، جاوا اسکریپت، پایتون، ++C و روبی که درصد آسیب پذیری در هر یک متفاوت می باشد. جالب این که زبان معروف و قدیمیC در رتبه اول این لیست قرار گرفته و دارای بیشترین آسیب پذیری بوده است. جالب تر این که تقریبا نیمی از گزارش های امنیتی ثبت شده مربوط به این زبان می باشد.آمار ارائه شده به معنی ناامنیC و امنیت بالای پایتون نمی باشد و در استفاده از هر زبان باید نکات امنیتی را رعایت کرد. در حقیقت این توسعه دهنده و برنامه نویس است که امنیت را به برنامه خود می دهد. تو سعه دهنده باید از خلاقانه ترین و ایمن ترین کدها در نرم افزار خود ا ستفاده کند و برای جلوگیری از آسیب پذیری آن حفره های مختلف کدهای خود را کشف کند. لذا با توجه به توضیحاتی که در فصل روش تحقیق آورده شده بهتر ا ست قرادادهای هو شمند با زبان پایتون که هم یک زبان سطح بالا ا ست و هم با توجه به گزارش بالا از امنیت نسبتا خوبی، در صورت رعایت اصول برنامه‌نویسی که در پیوست توضیح داده شده، برخوردار می‌باشداستفاده شود.

استاندارد سازی کدها و شناسایی باگ‌ها

از آنجا که مدل و پروتکل پیشنهادی ما برای قراردادهای هو شمند قرار ا ست در حوزه بانکداری با شد و لذا این قراردادها دارای ا صطلاحات تخصصی خا صی هستند و لازم ا ست مفاد قرارداد به صورت کامل کدنویسی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شود،بنابراین لازم است علاوه بر شناسایی باگ‌های برنامه نویسی، قراردادهای هوشمند ازجنبه معنایی[1] نیز بررسی شوند. در سال ۲۰۱۸ در مقاله‌ای که توسط پارادی[2] و سن[3] منتشر شد،الگوریتمی مبتنی بریادگیری ماشین و با دیدگاه معنایی، این الگوریتم، کدها را از نظر معنایی بررسی می‌کند.

تایید قرارداد و قضاوت عقلانی بعد از تایید قرارداد

در قسمت روش تحقیق سه مرحله تایید در حال انجام فرآیند، تایید پویا گره‌ها در هنگام اجرای قرارداد و قضاوت عقلانی بعد از اجرای قرارداد به طور جداگانه توضیح داده شده است ولی از آنجا که مرکز اصلی و اجرایی این ۳ مرحله به ماشین مجازی بر میگردد، در یک قسمت به بیان آن‌ها می‌پردازیم. همانطور که در قسمت روش تحقیق بیان شد برای بررسی روند اجرای قرارداد هوشمند، سه مکانیزم وجود دارد که ما در طراحی مدل خود جهت این امر ماشین مجازی را در نظر می‌گیریم . ماشین مجازی مانند یک سیتم عامل است همانطور که شما می‌توانید از طریق سیستم عاملی مانند ویندوز کارهای خود مانند محاسبات، برنامه نویسی، .... را در کامپیوترخود انجام دهید ماشین مجازی می‌تواند براساس الگوریتم‌های پیاده شده در ماشین مجازی اهداف و کارهایی که تعریف شده را به صورت خودکار یا غیرخودکار انجام دهد.

ماشین مجازی VM AI و تایید و ارزیابی قرارداد[4]

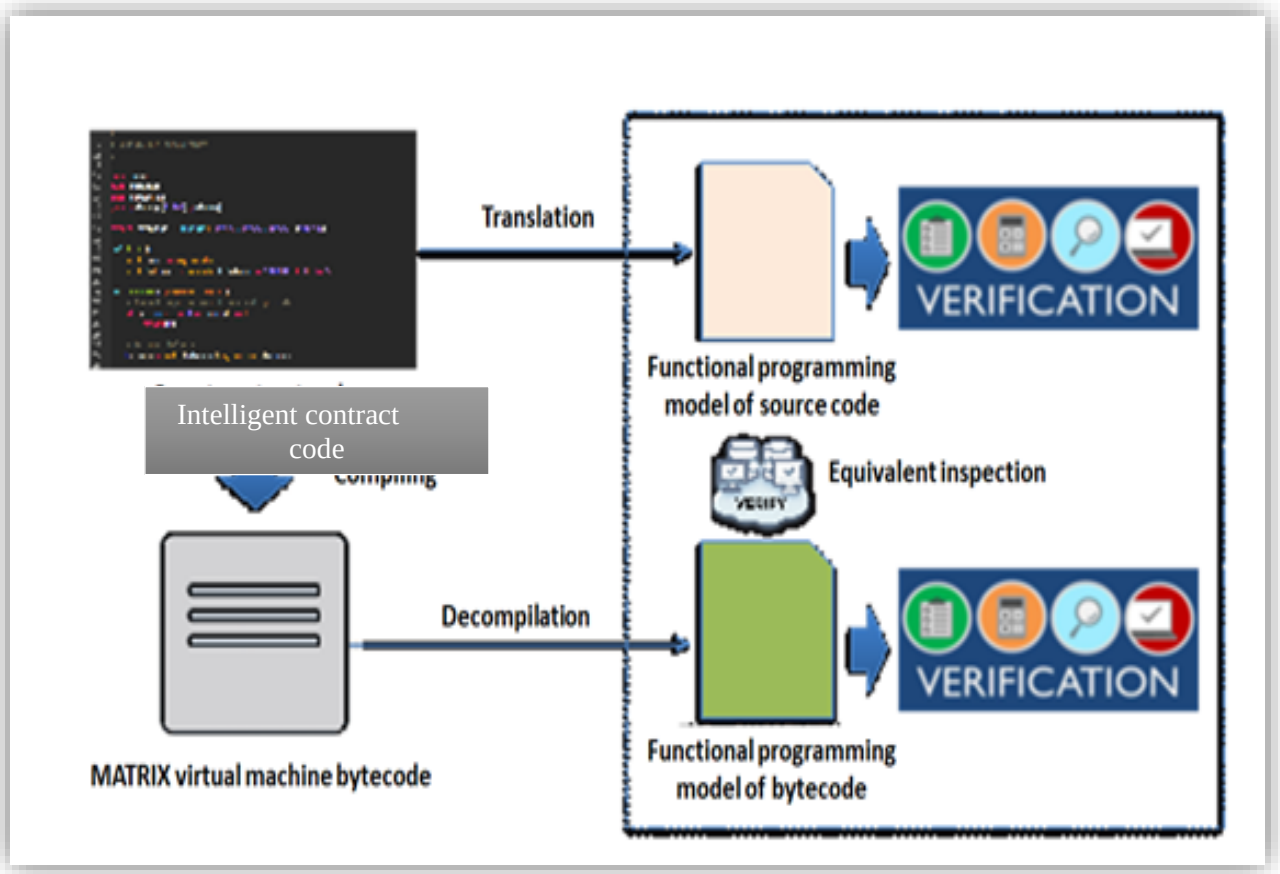
ماشین مجازی به یک چارچوب برای تایید رسمی مسائل امنیتی و سلسله اجرای مفاد قرارداد مجهز است. این چارچوب بر اساس یک زبان برنامه‌نویسی کاربردی که فریم‌ورک SMT و تعدادی ابزار و مدل جهت انجام این کاردر اختیار دارد.

[1]Segmntation
[2]PRADEl
[3]SEN

[4]پیوست د، فصل چهارم

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

تایید رسمی قراردادهای هوشمند



منبع: سایت www.seal-software.com

شکل بالا جریان تایید رسمی قراردادهای هوشمند را نشان می‌دهد. زنجیره ابزار تایید توانایی پردازش قراردادها را هم در سطح منبع[1] و هم در سطح بایت‌کد دارد. کد منبع به زبان برنامه‌نویسی کاربردی معادل با یک برنامه ترجمه می شود. اتخاذ برنامه‌نویسی کاربردی، افشای منطق پنهان و سهولت در انجام عملیات ر سمی موفق است. بایت‌کد در ماشین مجازی اجرا خواهد شد و سپس از هم جدا شده و به یک برنامه کاربردی تبدیل می‌شود. یکی از ویژگی‌های ماشین مجازی این است که برای بررسی کدها از نظر نحوی و ساختاری از الگوریتم‌های هوش مصنوعی استفاده می‌کند و به طور خودکار الزامات امنیتی را برآورد می‌کند. با توجه به برنامه قرارداد هوشمند ، موتور ماشین مجازی به طور خودکار تطبیق جزئی و تطبیق کامل را برای پیش بینی مدل رفتار کدها تشخیص می‌دهد. بر اساس چنین مدل هایی، موتور هوش مصنوعی مورد نظر(VM AI) مجموعه ای از محدودیت‌های مربوط را برای تأیید عمیقتولید خواهد کرد.این الگوها می توانند به صورت نحوییا ساختاری (یا ترکیبی از این دو) باشند. اولی معمولاً شامل گرامر و ویژگی های عملکردی است ، در حالی که دومی شامل

[1]source code

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ویژگی های ساختاری است.

تایید و ارزیابی براساس کتابخانه قانون[1]

در سطح نحوی، کامپایلر موجود درما شین مجازی ، محدودیت های مربوط به ما شین مجازی ونمودارهای جریان داده را مشخص می کند. سپس آن‌ها را بر اساس قانون ویرایش می کند.

که از مثال‌های معمول می‌توان به موارد زیر اشاره کرد:

۱- اجرای کلیه عبارات شرطی[2] به منظور جلوگیری از عدم اجرای قرارداد به دلیل کامل نشدن کاندیشن‌ها.

۲- تجزیه و تحلیل کلیه اعضای عمومی و توابعی که برای مشخص کردن سطح افشاء در قراردادها فراخوانی می‌شوند.

۳- بررسی اینکه آیا مراحل انجام تراکنش‌ها کامل شدند برای اطمینان از اجرای کامل و درست عبارات شرطی.

تعیین مدل تراکنش ها و تبادلات و ارزیابی امنیتی بر اساس تجزیه و تحلیل معنایی

با تجزیه و تحلیل معنایی استاتیک، ماشین مجازی به طور کلی می‌تواند تمام نقص‌های منطقی موجود در لایه های سطحی که تو سط انسان در قراردادهای هو شمند ایجاد شده ا ست را حذف می کند، اما هنوز نمی‌تواند مسائل منطقی را که در طول اجرای پویای قرارداد اتفاق می‌افتد را حل کند[3].

استفاده از الگوریتم‌ها جهت افزایش امنیت و ارزیابی قراردادها و تایید انجام مبادلات و تراکنش‌ها

الگوریتم SHA512

الگوریتم SHA512[4]،یک تابع هش، یک تابع ریاضی است که یک مقدار ورودی را به مقدار فشرده شده‌ی دیگر تبدیل می کند. ورودی تابع هش یک مقدار با طول نامعلوم است اما خروجی همیشه طول ثابتی دارد. توابع هش به شدت کاربردی هستند و تقریبا در همه کاربردهای امنیت اطلاعات حضور دارند.مقدار برگشت داده

[1] با توجه به برنامه قراردادهای هوشمند، کامپایلر[1] موجود در ماشین مجازی یک AST مبتنی بر BNF را به عنوان یک نماینده درونی انتخاب می‌کند.برای قراردادهای هوشمندی که داخل اسناد بایتکد وارد می‌شوند، ابتدا ماشین مجازی کدهای باینری[1] را از هم سوا کرده[1] و سپس BNF مربوطه را تولید می‌کند. بر اساس کتابخانه قانون، که بر اساس گستره دانش و تجربیات ما در این حوزه و با توجه به مفاد و محتویات قراردادها ساخته شده است، کامپایلر از RDP[1] برای ارزیابی AST برای هر گونه آسیب پذیری امنیتی[1] استفاده می‌کند.

[2] conditional clauses

[3] پیوست ذ، فصل چهارم

[4] Microsoft, 2018

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

شده توسط یک تابع هش، یک «پیام خلاصه» یا به طور ساده «مقدار هش» نام دارد.

لذا در این پروتکل جهت اینکه کاربر زمانی که وارد پروتکل می‌شود برای اینکه بتواند تراکنش انجام دهد دارای دو شناسه می‌باشد یک شناسه عمومی یا همان کلید عمومی و دیگری شناسه خصوصی یا همان کلیدخصوصی است که توسط الگوریتم SHA512، زمان ورود کاربر به شبکه برای او مشخص می شود. در واقع شناسه عمومی او برای شناسایی کاربران دیگر است و شناسه خصوصی به منزله امضای او در تایید تراکنش و انجام قراردادهای هوشمند می‌باشد. در بحث اهمیت و امنیت این الگوریتم همین قدر بس که مایکروسافت برای هش کردن جداول و متغیرها و موارد دیگر از این الگوریتم استفاده می‌کند.

الگوریتم جستجوی اول عمق(DFS)

زمانی که یک تراکنش جدیدی انجام می‌شود این تراکنش بین دو یا چند گره انجام می‌شود که انجام تراکنش منجر به تغییر شناسه عمومی دو نودی میشود که تراکنش انجام شده است سپس بر اساس الگوریتم گراف جهت دار غیر مدورهر یال از آخرین گره موجود به گره جدید وصل می‌شود. و سپس بر اساس الگوریتم جستجوی عمق اول مسیری که کوتاهترین زمان ممکن را بر اساس پیچیدگی زمانی انتخاب میکند و تایید گره‌ها منجر به تایید تراکنش و ثبت تراکنش در آن گره‌ها و تایید پویای تراکنش می‌شود[1].

شبکه‌های مولد تخاصمی GAN[2]

ماشین مجازی فقط به کاربران نیاز دارد تا عناصر اصلی (مانند ورودی ، خروجی و شرایط معامله) یک قرارداد را با یک زبان برنامه نویسی وارد کنند. سپس ، یک ژنراتور کد بر اساس یک شبکه عصبی عمیققادر به تبدیل خودکار اسکریپت به یک برنامه معادل است. ماشین مجازی برای دستیابی به تأیید امنیت پویا ، شبکه مخالف تولیدی اخیراً توسعه یافته را تطبیق می دهد. روش تأیید پویا را می توان با چارچوب تولید کد در یک حلقه بسته همراه کرد. چارچوب شبکه مولد تخاصمی از دو شبکه عصبی بازگشتی تشکیل شده است. از شبکه عصبی بازگشتی برای تجدید نظر در برنامه های موجود برای قراردادهای هوشمند استفاده می شود ، در حالی که دیگرییاد می گیرد که از طریق نمونه های تصادفی توزیع احتمال داده شده ، برنامه های هکر تولید کند. پس از ایجاد برنامه های قرارداد هوشمند ، آنها در "شبکه شبیه سازی سندباکس[3](شبکه ای که شبیه ساز یک شبکه شبه نامتمرکز و توزیع شده است و در آنجا آزمایش ها می تواند به صورت کنترل شده انجام شود)" به همراه کدهای مربوط به هکرها مستقر می شوند. توابع هزینه این دو شبکه به هم گره خورده اند به طوری که وقتی کل سیستم به یک تعادل نش رسید، نتیجه مطلوب کلی حاصل می شود.

در قسمت ابتدایی این فصل، به توضیح الگوریتم‌هایی پرداختیم که در ایجاد قرارداد هوشمند و توسعه

[1] پیوست ز، فصل چهارم
[2] پیوست ه ، فصل چهارم

[3] sandbox

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

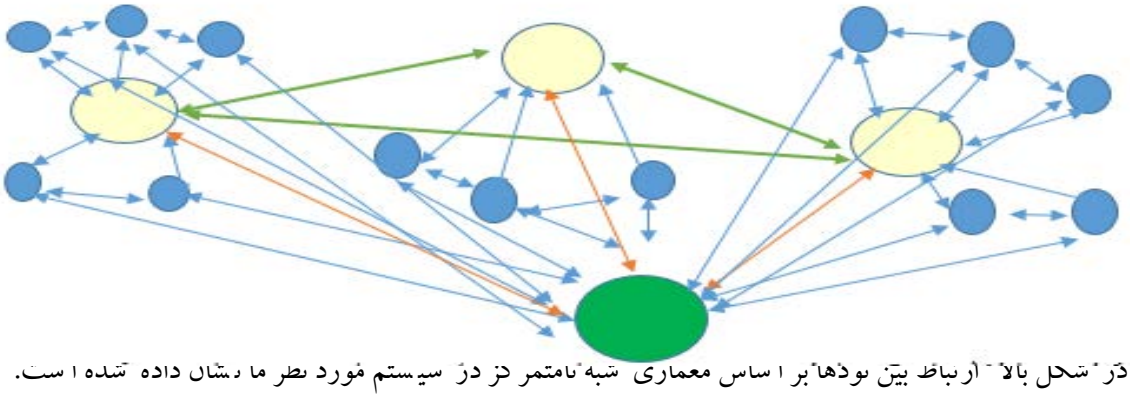
قراردادهای هو شمند مبتنی بر هوش مصنوعی پرداختیم. و از الگوریتم‌های شبکه تخا صمی مولد، جستجوی اول عمق والگوریتم شنا سایی باگ برای تو سعه و بهبود این نوع از قرادادهای هو شمند ا ستفاده کردیم. لذا در قسمت بعدی به بیان نحوه عملکرد پروتکل پیشنهادی در حوزه بانکی می‌پردازیم. لذا در این قسمت می‌خواهیم به بیان دو سناریو در مورد انجام تراکنش مالی بین دو نود در پروتکل طراحی شده بپردازیم. و با توجه به پروتکلی که طراحی کردیم اگر فردی بخواهد به یک کاربر دیگر پرداختی انجام دهد این پرداخت چگونه انجام خواهد گرفت .

نحوه عملکرد بر اساس پروتکل پیشنهادی

شکل‌گیری شبکه و نحوه و شرایط ورود یک نود به شبکه

در نظام بانکداری در نظر بگیرید که افراد حقیقی و حقوقی و بانک و شعبه‌های آن در ارتباطات مالی و تراکنش‌های مالی با یکدیگر در ارتباط اند. افراد حقیقی و حقوقی در بانک‌ها وشعبه‌های آن دارای حساب هستند و تراکنش‌ها و مبادلات مالی خود را از طریق بانک و حساب‌های خود انجام می‌دهند. لذا جهت انجام این تبادلات و تراکنش‌ها بانک‌ها دارای قوانین خاصی هستند که باید رعایت شود. حال فرض کنید بر اساس شرایط پروتکل پیشنهادی این مبادلات چگونه صورت می‌گیرد. بر اساس آنچه گفته شد این پروتکل بر اساس یکی سیستم شبه نامتمرکز است که تمام افراد حقیقی و حقوقی آن به عنوان یک نود در این شبکه هستند. و نکته اساسی و مهم این است که بانک‌ها باید به عنوان نودهای اصلی این شبکه قرار بگیرند. پس در این سیستم بانک‌ها به عنوان نودهای اصلی این شبکه هستند و افراد حقیقی و حقوقی که در این شبکه قرار دارند پیرامون این نودهای اصلی قراردارند. لذا پس از قرار گرفتن در این شبکه، نودها بر اساس معماری شبکه‌های نیمه خود مختار به صورت زیر با یکدیگر با هم در ارتباط می‌باشند:

نوع ارتباط شبکه ای نودها (کاربران) در بستر شبکه شبه نامتمرکز بر اساس پروتکل پیشنهادی



در شکل بالا[1] ارتباط بین نودها بر اساس معماری شبه نامتمرکز در سیستم مورد نظر ما نشان داده شده است.

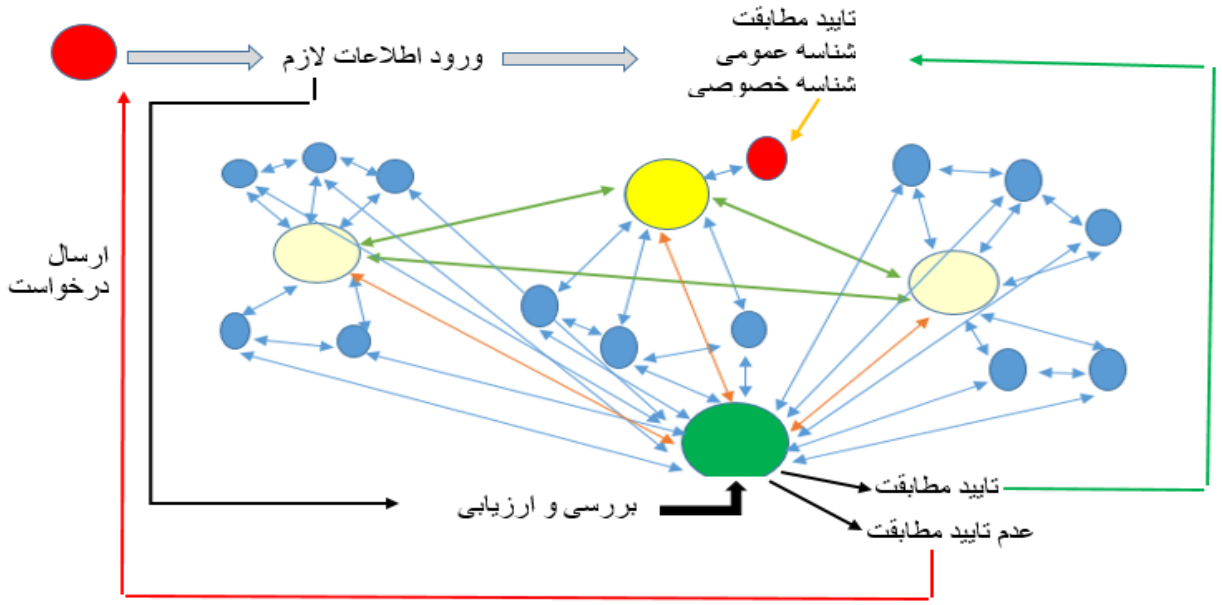
[1] این شکل بر مبنای شکل final graph، مقاله : Semi-Autonomous NetworksTheory and Decentralized Protocol می‌باشد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

دایره‌های بزرگتر (زرد کم رنگ) نشان دهنده نودهای اصلی این گروه‌ها می‌باشند که در واقع بانک‌ها و شعبه های آن‌ها می‌باشند و دایره‌های کوچکتر و آبی رنگ همان افراد حقیقی و حقوقی می‌باشند که در این شبکه قرار گرفته‌اند. تمام نودهای اصلی با هم ارتباط دارند و نودهای پیرامون نود اصلی با نود اصلی و با سایر نودهای پیرامون همان نود اصلی در ارتباط اند و ارتباط نودهای پیرامونی یک نود اصلی با نودهای پیرامونی نودهای اصلی دیگر بر مبنای ار تباط بین این نودهای ا صلی می‌با شد. بنابراین تمام این نودها یا به صورت م ستقیم یا به صورت غیرمستقیم با هم در ارتباط اند. اما نود سبزرنگ نود ا صلی این شبکه ا ست که تمام نودها باآن در ارتباط اند نکته مهم دیگر این است که در طراحی قرارداد در نظام بانکداری، طراحی این شبکه و ماشین مجازی به عنوان سیستم عامل اجرایی این قرارداد در یک مرکز اصلی مانند بانک مرکزی یا شعبه مرکزی یک بانک باشد. و دلیل آن هم بر اساس معیارهای اجرای قوانین و نظارت بر اجرای قراردادها می‌باشد چرا که از آنجایی که این قوانین حوزه پولی و مالی در بانکداری توسط بانک مرکزی تعیین می‌شود لذا بهتر است اجرای آن بر عهده بانک مرکزی با شد. نکته ای که حائز اهمیت ا ست این ا ست که این نود به عنوان سرور مرکزی در سیستم های متمرکز نیست این نود قادر به تغییر جریان مسیر تراکنش ها یا قادر به تغییر قوانین و مفاد قرارداد ها به نفع خود نیست لذا به محض هر گونه تغییر تمام نود ها در جریان این تغییر قرار می‌گیرند. در سناریوی اول در نظر بگیرید که یک بانک می‌خواهد پرداختی‌های خود را بر ا ساس پروتکل بالا انجام دهد. ابتدا هر یک از کارمندان مراحل لاگین را انجام می‌دهند و اطلاعات خود را وارد می‌کنند و به عنوان یک نود و گره وارد فریم ورک می‌شوند(دایره‌های آبی رنگ) و از طرفی خود بانک نیز از سرور مرکزی خود به عنوان یک نود وارد شبکه می‌شود و این به این معنی نیست که این سرور به عنوان مرکز اصلی پایگاه داده است (دایره زرد کم رنگ) بلکه آن هم مانند یک نود و گره در شبکه و فریم ورک مورد نظر می‌باشد. شناسه عمومی و شناسه خصوصی هر کدام از این نودها بر اساس الگوریتم SHA-512 به آن‌ها داده می شود. اما برای لاگین شدن باید فرد حتما در یکی از شعبه های بانک باید حساب داشته باشد چرا که همانطور که قبلا بیان شده بود هم می‌توان برای انجام تراکنش‌ها در این شبکه یک کیف پول با ارز جدیدی طراحی کرد که متنا سب با حساب بانکی افراد با شد هم اینکه م ستقیما به حساب بانکی افراد، از طریق رابط کاربری، البته با رعایت م سائل امنیتی، ارتباط دا شته با شد تا انجام تراکنش ها و مبادلات مالی در حوزه بانکداری امکان‌پذیر باشد. با توجه به این مساله نود قرمز در این شبکه لاگین شده است و این نود در نود زرد(شعبه بانک) حساب دارد. وقتی فرد وارد شبکه شد این درخواست به نود سبز ارسال می‌شود و پس از تایید و ارزیابی پویای مربوطه، الگوریتم هش دو شناسه عمومی و خصوصی فرد را مشخص می‌کند وفرد وارد شبکه می‌شود.

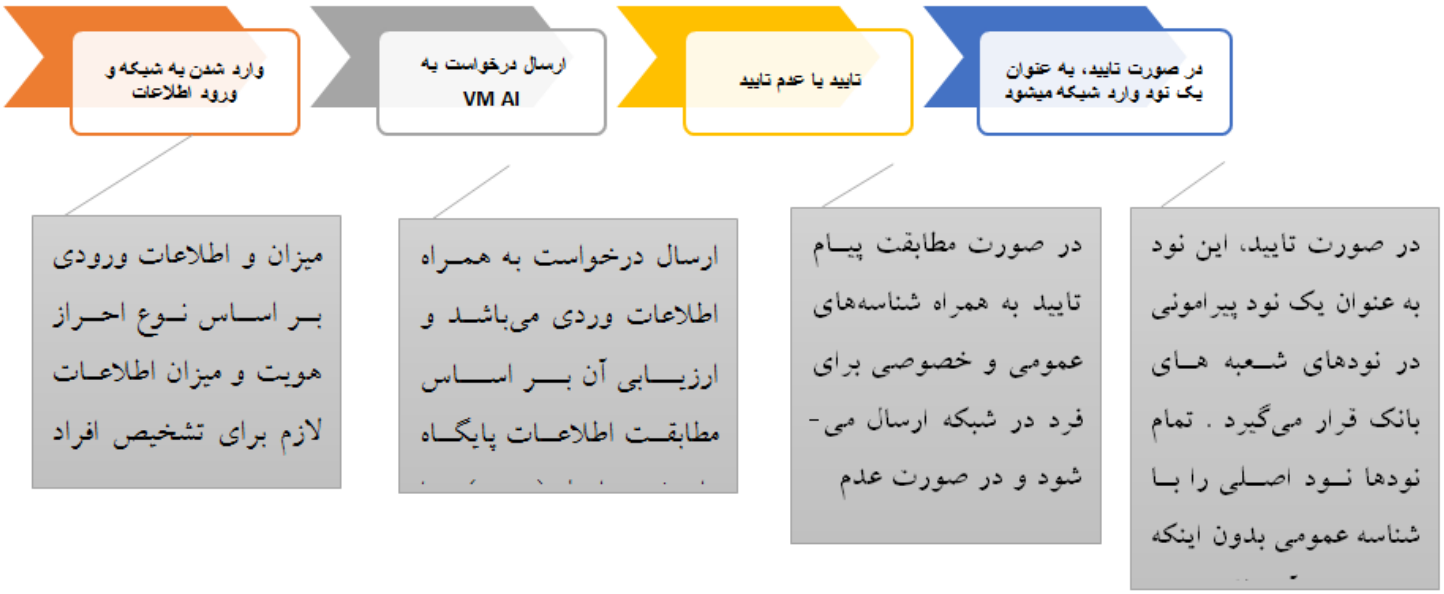
نحوه ورود یک کاربر جدید به شبکه

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.



با توجه به پایگاه داده موجود و دسترسی اطلاعات این نود به اطلاعات تمام نودها در حد ارزیابی اطلاعات و نه توانایی تغییر آن، پاسخ به صورت دو رشته تحت عنوان شناسایی عمومی و خصوصی، بعد از تایید اطلاعات می‌باشد.

مسیر جریان اطلاعات وتایید در شبکه



دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کتابخانه‌ها و ارزیابی قرارداد

در پروتکل پیشنهادی، قسمتی به نام کتابخانه قانون وجود دارد. در نظام بانکداری،برای انجام مراودات مالی و تراکنش‌های مالی یک سری قوانین وجود دارد. هر کدام از قراردادهای مالی اسلامی دارای یک سری قوانین هستند که لازمه اجرای درست این قراردادها و رسیدن به نتیجه مطلوب اقتصادی هستند. لذا این کتابخانه قانون برای این امر در نظر گرفته شده است:

اولا، انجام تراکنش‌ها و تبادلات مالی براساس قوانین مالی و پرداخت‌ها در نظام بانکداری باشد.

ثانیا، برای انجام قراردادهای مالی، این قراردادها به صورت پیشفرض و با تایید بانک مرکزی در این کتابخانه قرار گرفته باشد.

ثالثا، هر کدام از نودها برای استفاده از این قراردادها، میتوانند مانند نرم‌افزارهای برنامه نویسی تابع وقرارداد مورد نظر را فراخوانی کنند.

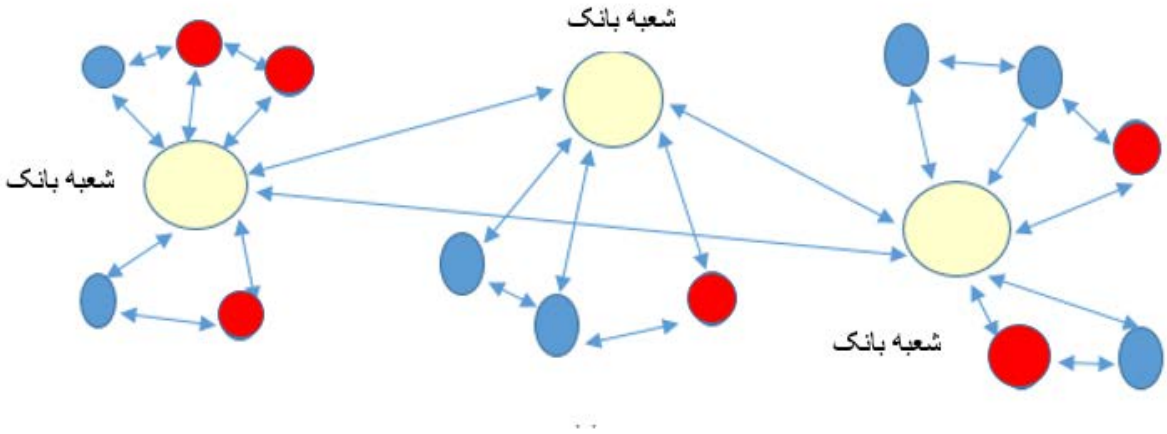
بانک به عنوان یک نود مانند سایر نودها می‌تواند قراردادهایی را طراحی و مفاد آن را در کتابخانه مشخص کند. که مسلما این قراردادها باید منطبق با قوانین نظام بانکداری باشند. زمانی که این قرارداد طراحی و در کتابخانه قانون موجود در ماشین مجازی قرارگرفته، تمام نودها به آن دسترسی داشته و می‌توانند مفاد آن را مشاهده کنند لذا این قراردادها نمیتواند مخالف با قوانین نظام بانکی باشد و مورد سوء استفاده قرار بگیرد. همانطور که قبلا توضیح داده شد، بعد از طراحی ، این قراردادها توسط الگوریتم مبتنی بر دیدگاه معنایی مورد ارزیابی قرار میگیرد و در صورتی که در کلاس درست قرار بگیرد پیاده سازی آن با مشکلی مواجه نمی‌شود و بعد از این ارزیابی نوبیت به شبکه تخاصمی مولد می‌رسد که ارزیابی لازمه را انجام دهد و همانطور که قبلا توضیح داده شد در صورت تایید ارزیابی توسط این الگوریتم ها و تایید نهایی تطبیق الگو قراردادی که به صورت کد نوشته شده است تحت یک تابع خاصی در کتابخانه قانون ماشین مجازی قرار می‌گیرد و نودهای شبکه می‌توانند با فراخوانی آن، از آن استفاده کنند. نکته ای که وجود دارد این است چون این قوانین باید به صورت کد نوشته شود، در طراحی این قراردادها یک سری محدودیت‌های وجود دارد به همین دلیل بهتر است ابتدا از قراردادهای ساده مالی در نظام بانکداری و پرداخت‌های ساده جهت پیاده سازی شروع شود.

پرداخت حقوق کارکنان بانک توسط بانک در پروتکل مورد نظر

فرض کنید بانک به عنوان یک کاربردرپروتکل پیشنهادی ما می‌خواهد به کارمندان خود پرداختی انجام دهد. تمام کارمندان بانک و خود بانک به عنوان یک نود شبکه قرار دارند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نمونه شبکه مورد نظر برای پرداخت حقوق کارکنان



دایره های قرمز کارمندان شعبه‌های بانک هستند و دایره‌های قبلی سایر کاربران هستند. در شکل بالا نود اصلی (سبز) وجود دارد ولی برای فهم بهترشکل در این قسمت نیاوردیم.

از آنجا که اساس هوشمندی این قراردادها این است که باید به صورت خودکارانجام شود لذا باید انجام اتوماتیک پرداخت‌ها در نظر گرفته شود. بانک باید ابتدا تابعی را جهت پرداخت در کتابخانه قانون تعریف کند. بعد از اینکه الگوریتم‌های موردنظر ارزیابی مورد نظر را انجام دادند و کد قرارداد با مشکلی مواجه نشد در کتابخانه قانون قرار می‌گیرد و تمام افراد می‌توانند به آن دسترسی پیدا کنند و از مفاد آن آگاه شوند. این تابع باید در تاریخ مشخصی به صورت خودکار توسط ماشین مجازی مورد نظر به نودهایی فرستاده شود که کارمندان بانک هستند و فراخوانی شود البته این کار هم امکان پذیر است که این تابع توسط خود بانک فراخوانی شود وبرای افراد فرستاده شود. تشخیص اینکه کدام نود کارمند بانک هست یا خیر به صورت زیر است:

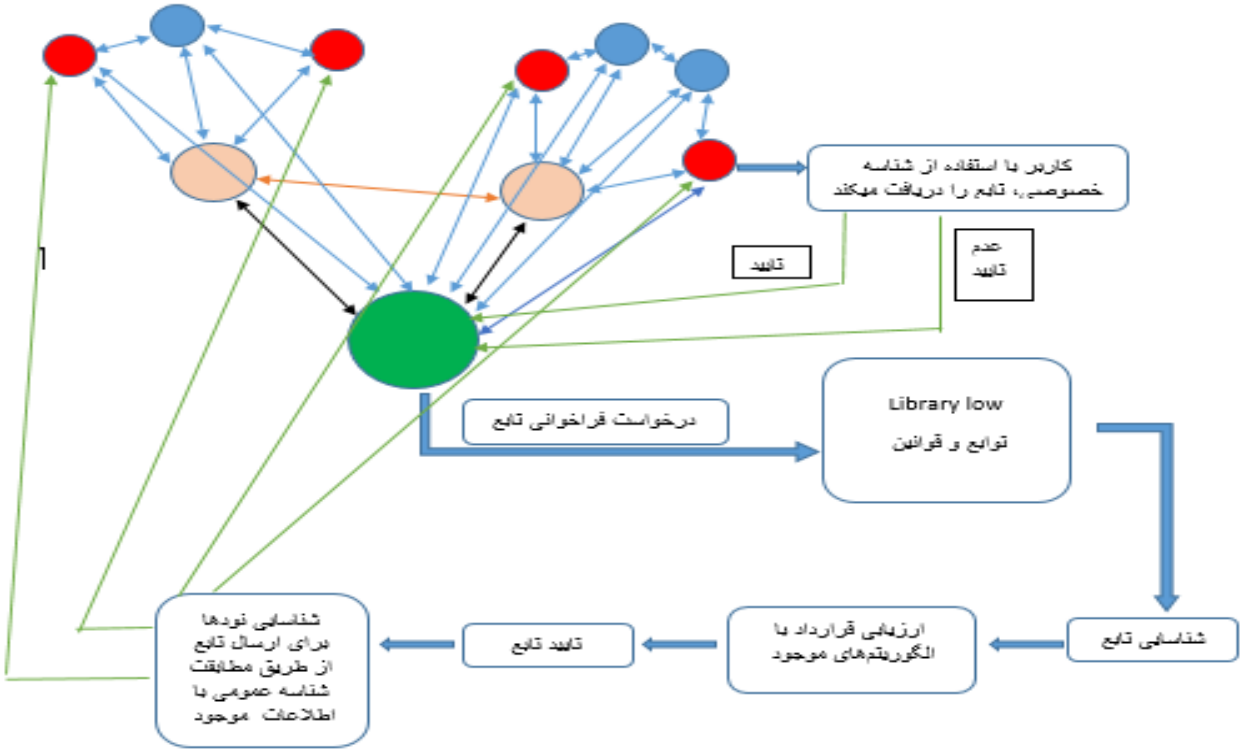
زمان لاگین شدن هر کاربر اطلاعات لازم را وارد می‌کند که بعد از تطابق و ارزیابی و تایید، شناسه عمومی و خصوصی فرد برای اوارسال می‌شود. لذا در نود اصلی (نود سبز) این اطلاعات وجود دارد که با شناسه عمومی فرد مطابقت داده می شود. لذا پس از مطابقت شناسه عمومی و اطلاعات فرد به عنوان یک کارمند تابع فراخوانی شده برای پرداخت به صورت خودکار برای نودها فرستاده می‌شود. اما ممکن است سوالی در زمینه شناسایی افراد پیش آید که در این پروتکل افراد به راحتی قابل شناسایی هستند؟

جواب این سوال این است که این پروتکل نسبت به بلاکچین در این زمینه شناس‌تر است اما این مزیت این امر است چراکه در حوزه پرداخت‌ها و تراکنش‌های مالی باید در عین خودکار انجام شدن تراکنش‌ها و قراردادهای مالی جریان مالی کلی آن‌ها به دلیل مسائلی مانند پولشویی و تقلب برخلاف بلاکچین شناسایی آن راحت‌تربا شد و نکته دیگر مهم در این زمینه این است که در خود شبکه فرد تنها شناسه عمومی آن قابل رویت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

است و سایر نودها نسبت به هویت فرد اطلاعی ندارند و تطابق شناسه عمومی با اطلاعات ورودی و سایر اطلاعاتی که برای انجام قراردادها لازم است در ماشین مجازی مورد نظر و به صورت خودکار صورت می‌گیرد.

جریان کلی پرداخت به کارکنان در پروتکل مورد نظر



بعد از شنا سایی نودها، تابع پرداخت برای هریک از نودها ار سال می شود. هر یک از این توابع همان طورکه قبلا تو ضیح داده شده ا ست دارای یک سری پارامتر یا آرگومان مانند پکیج‌های برنامه نویسی ا ست لذا در این تابع پرداخت، علاوه بر شناسایی نودهای موردنظر، با توجه به نوع نودها و اطلاعات موجود در نود اصلی، این آرگومان‌ها برای هریک از این نودها متفاوت است برای مثال میزان پرداختی به هر یک از این نودها متفاوت است . چرا که یکی ازاین آرگومان‌ها میزان پرداختی می‌باشد و با توجه به شناسه عمومی و مطابقت آن با اطلاعات افراد، این آرگومان مقادیر لازم را می‌پذیرد. پس از دریافت و تایید درخواست توسط هر یک از نودها با استفاده از امضای دیجیتالی، در صورت عدم تایید کاربر، در خواست عدم تایید و دلیل آن با توجه به مفاد موجود در قرارداد به نود ا صلی برگردانده می شود. و پس ازبرر سی و قضاوت عقلانی تو سط الگوریتم‌های موجود، موفق به تشخیص و حل مساله شدند چرخه دوباره تکرار می شود در غیر اینصورت نیاز به قضاوت انسانی ا ست. ولی در صورت تایید فرد، قرارداد بر اساس عبارات شرطی که اجرا شده ادامه پیدا می کند و مبلغ مورد نظر به فرد پرداخت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

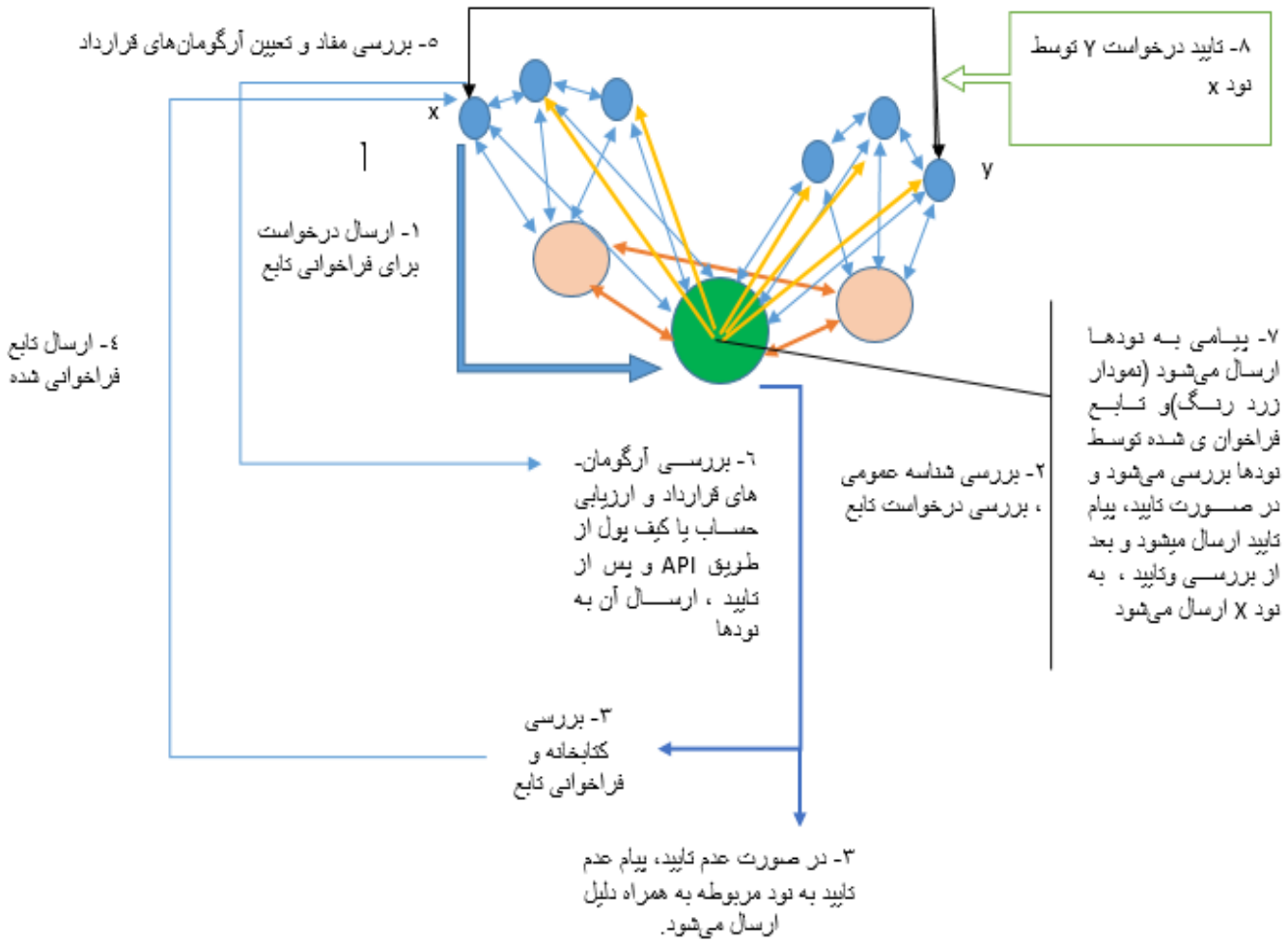
می‌شـود. این پرداخت، همان طور قبلا گفتیم می‌تواند یک ارز تعریف شـده باشـد که در کیف پول افراد ماهیت بدهکار و بستانکار آن اعمال شود و یا می‌تواند از طریق رابط کاربری هم به صورت مستقیم به حساب افراد متصل شده و ماهیت تراکنش‌ها در حساب افراد اعمال شود. بعد از تایید ، گره راس و گره ریشه مشخص می شود و از طریق الگوریتم جسـتجوی اول عمق و پروتکل گراف غید مدور جهتدار مسـیرهایی از گره‌ها ی جدید که نیاز به تایید تراکنش جدید می‌باشـد و کمترین زمان ممکن را برای تایید پویای پرداخت بانک به کارمند مورد نظر را می‌دهد انتخاب میکنند و گره هایی که در این مسیر قراردادرند شروع به پردازش بر اساس مسیرهایی که از طریق گراف جهت دار مشخص شده کرده و در نهایت هر مسیری از گره ها که توانستند تایید تراکنش را انجام دهند به این مفهوم که هش تولید شده برای نوع تراکنش را رمزگشایی کنند و جهت انجام این پردازش تمام گره هایی که در این مسـیر قرار گرفته اند و توانسـتد تایید تراکنش را به طور کامل انجام دهند درصـدی از تراکنش را به عنوان جایزه دریافت می‌کنند که این باید از طریق حسابی که به عنوان والت برای هر نود تعریف شده و یا حسابی که از طریق رابط کاربری به حساب ا صلی آن‌ها و صل شده واریز شود و پرداخت شود. تایید فرآیند پویای قرارداد و نوع قرارداد بر اسـاس الگوریتم ها و پروتکل هایی که در ماشـین مجازی تعبیه شـده انجام میگیرد ونحوه عملکرد آن نیز توضیح داده شده است.

وام دهی نفر به نفر

در سناریوی دوم فرض کنید یک قرارداد بین دو نود بر اساس قرارداد هوشمندی که در کتابخانه وجود دارد انجام شود. فرض کنید این قرارداد یک قرارداد مالی باشد. برای مثال نود x و yدارای حساب در بانک مورد نظر و دارای یک حسـاب کاربری در شـبکه باشـند. این قرارداد هوشـمند برای این می‌باشـد که فرد x دارای میزان مشـخص پول یا ارز عمومی در شـبکه می‌باشـد و می‌خواهد آن را به عنوان وام به فردی تحت عنوان یکی از قراردادها بدهد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نحوه اجرای قرارداد وام نفر به نفر در پروتکل پیشنهادی



مفاد این قرارداد و اصول اولیه این قراداد در کتابخانه تعیین شده است و لذا غیر قابل تغییر است فرد xدرخواست خود مبنی بر فراخوانی این قرارداد را انجام می‌دهد و بعد از تایید کلید عمومی و تایید آن توسط گره و نود بانک که از طریق رابط کاربری به اطلاعات حساب فرد دسترسی دارد فرد اقدام به تعیین آرگومان‌های قرارداد با توجه به مفاد قراداد می‌کند. برای مثال میزان مبلغ و مدت قراداد را مشخص می‌کند. سپس بانک با توجه به فراخوانی این قرارداد توسط فرد x و با توجه به آرگومان‌های آن اقدام به تایید اطلاعات حساب فرد x از طریق رابط کاربری متصل به سرور اطلاعات حساب فرد در بانک می‌کند بعد از تایید بانک، مفاد قراداد نهایی با استفاده از الگوریتم‌های عمیق وشبکه تخاصمی مولد مورد ارزیابی قرار میگیرد و بعد از تایید در ماشین مجازی ، قراردادها به نودها فرستاده می‌شود و بعد از تایید کلید خصوصی نودها قرارداد را مشاهده می‌کنند و نودها تایید خود را برای کلید عمومی فرد x میفر ستند و فرد x تایید، قبول y را با تایید کلید خصو صی خود انجام می‌دهد. با تایید این دو

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نود، طبق فرآیند سناریوی قبل، نودهایی با توجه به مسیرهای جهتدار که توسط پروتکل گراف جهتدار غیر مدور تعیین شده اقدام به پردازش و تایید قرارداد هوشمند می‌کنند. و حتما یکی از این گره‌ها به عنوان نود اصلی بانک می‌باشد و این تایید ها در این گره ها ذخیره می‌شود. با تایید x و y، بانک به عنوان ضمانت با توجه به مفاد قرارداد ضمانت های لازم برای پیشبرد قرارداد و نحوه ی اجرایی آن را به صورت قرارداد هوشمند پیاده سازی کرده و به ترتیب کد مراحل آن اجرایی شود. و در نهایت مفاد قرارداد، به ترتیب تایید ضمانت، تایید حساب و ..... همگی به صورت خودکار انجام شده و قرارداد به صورت خودکار اجرایی می‌شود.

در فصل چهارم با توجه به اصول و مبانی روش تحقیق، به بیان جزئیات مدل و پروتکل مورد نظر خود برای قراردادهای هوشمند مبتنی بر هوش مصنوعی، در حوزه بانکداری پرداختیم و توضیح دادیم که چگونه پروتکل مورد نظر می‌تواند برای انجام تراکنش‌های مالی و اجرای قراردادهای مالی مورد استفاده قرار بگیرد. و جهت شرح دقیق‌تر این پروتکل با طراحی دو سناریو به توضیح نحوه انجام تراکنش مالی بین دو نود(کاربر)، به عنوان سناریوی اول، و انجام یک تسهیلات نفر به نفر، به عنوان سناریوی دوم، پرداختیم.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

فصل پنجم:

پیشنهادات و تحقیقات آتی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

مقدمه

استفاده از تکنولوژی‌های جدید نیازمند امکانات و ملزوماتی است کهتنهادر صورتی که با درک درست از شرایط و نیاز و ضرورت همراه باشد می‌تواند نتیجه درستی داشته باشد و مفید واقع شود. لذا در این تحقیق با بیان مزیت ها و عدم مزیت‌های قراردادهای هوشمند مبتنی بر بلاکچین، این مسئله را مطرح کردیم که با توجه به شرایط و ساختار موجود به خصوص در حوزه بانکداری ما میتوانیم با استفاده از ابزارها و الگوریتم‌های هوش‌مصنوعی، قراردادهای هوشمند مبتنی بر هوش مصنوعی طراحی کنیم که تا حد قابل قبولی از مزیت‌های قراردادهای هوشمند مبتنی بر بلاکچین برخوردار باشد و عدم مزیت‌های آن را نداشته باشد. هر چند با توجه به فریم‌ورک طراحی شده از نظر امنیتی به حد قراردادهای هوشمند مبتنی بر بلاکچین نمی‌رسد ولی تلاش شد با استفاده از الگوریتم‌های جدید امنیتی در حوزه سایبر تا حدی این نقطه ضعف پوشانده شود. ولی از جهت انعطاف پذیری مقید دارای ویژگی‌های مثبتی می‌باشد.قابل ذکر است که این پروتکل اکثر قسمت‌های آن بر اساس مبانی نظری و تئوری و موردهای تجربی که در حال حاضر در بانک‌ها و شرکت‌های مالی یا نهادهای تکنولوژی مالی پیاده سازی شده‌است می‌باشد. و لذا قسمت‌هایی که موردهای تجربی وجود ندارد بر اساس مبانی نظری معتبر بیان شده است.

تجزیه و تحلیل

هدف اصلی در این تحقیق طراحی مدلی از قراردادهای هوشمند، با استفاده از هوش مصنوعی بود، به طوری که در حوزه نظام بانکی کاربردی باشد. لذا با توجه به مبانی و نحوه عملکرد قراردادهای هوشمند، مبانی و بستر لازم برای طراحی قراردادهای هوشمند مبتنی بر هوش مصنوعی رامشخص کردیم و با توجه به همین بستر و ساختار که تحت عنوان روش تحقیق در فصل ۳ بیان شد به طراحی و توسعه آن پرداختیم. پروتکل پیشنهادی، مزیت‌هایی دارد:

از آنجا که این پروتکل بر اساس الگوریتم‌هایی مانند شبکه تخاصمی مولد، الگوریتم کلاسبند کد و الگوی تطبیق الگو[1] طراحی شده است که در ماشین مجازی به صورت خودکار اجرا می‌شوند، مشکل عدم اثبات توانایی تکنولوژی در مدیریت چالش‌های پردازشی رانسبتا حل کرده است در واقع با بررسی پویا و ایستای قرارداد و اجرای آن در چند لایه حل کرده است و همچنین برخلاف بلاکچین،به دلیل عدم تشکیل بلاک، استفاده از

[1]Patern matching

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

الگوریتم جستجوی اول عمق و گراف جهتددار غیر مدور نیاز به توان پردازشی بالا ندارد.

قراردادهای هوشمند معمول، بر مبنای ارزهای دیجیتالی طراحی شده‌اند و این ارزها در بازار نوسانات بالایی دارند و از طرفی تبدیل این نوع ارزها به ارزهای رایج در تمام کشـــورها کار راحتی نیســـت. لذا در این پروتکل پیشنهادی، با توجه به اینکه خود بانک‌ها به عنوان یک نود در شبکه هستند می‌توان از طریق رابط کاربرهایی این تراکنش‌ها بر اساس ارز ملی انجام شود یا والتی طراحی شود که بر اساس آن تراکنش‌های مربوط به قراردادهای هوشمند انجام گیرد. لذا همین امر سبب یک نقطه ضعف در پروتکل می شود و آن هم این است که در پروتکل مورد نظر شناسایی کاربران و نودها، به دلیل نیاز مطابقت اطلاعات با داده‌ها جهت احراز هویت در نود اصلی (هر چند تمام این‌ها به صورت خودکار انجام می‌گیرد) نسبت به بلاکچین راحتر شناسایی می‌شوند.

یکی از مشـکلات بلاک‌چین بحث ناشـناس بودن و شـناسـایی سـخت کاربران بوده اسـت از آن جهت که مباحث پولشـویی و مالیات در آن مبهم بوده اسـت و زمینه را برای فرار مالیاتی و پولشـویی به دلیل سـاختار خود فراهم می‌کرده اسـت. لذا در این پروتکل همانطور که در قسـمت قبل بیان شـده اسـت شـناسـایی راحتر صـورت می‌گیرد.

در این پروتکل با توجه به قرار گرفتن بانک‌ها به عنوان نود، مانند ســـایر کاربران زمینه و بســـتر برای اجرای پیاده‌سازی قراردادهای هوشمند بیشتر فراهم است اما نکته اصلی در این ارتباط بحث قوانین و نظارت و نوع ارتباط اطلاعاتی بین نودهای اصلی و سایر کاربران است.

از سـایر مشـکلات و چالش‌های قراردادهای هوشـمند معمول ایجاد اخلال در بازار، واکنش فعالان صـنعت خدمات مالی، نیاز به شبکه با پهنای باند بالا، تغییرات پیشبینی‌نشده فضای پرداخت، زمان‌بر بودن فرآیند کاوش و استخراج، عدم امکان حذف کامل واسطه در موارد کاربرد واقعی،نیاز به تعریف مکانیزهای سخت‌تر دسترسی به اطلاعات به دلیل تغییر ناپذیری اطلاعات ورودی بوده اســـت اما از آنجا که در این پروتکل فرآیند تایید قراردادها توسط نودهای دیگر، تنها به عده بخش از نودهاست (با توجه به گراف جهت‌دار غیر مدور و جستجوی اول عمق) و عدم تشـــکیل بلاک و تطابق اطلاعات در چند لایه حجم این مشـــکلات کاهش پیدا خواهد کرد ولی هنوز هم ممکن است تغییرات پیشبینی نشده‌ای در فضای پرداخت و زمان اجرای قراردادهای هوشمند بوجود آید ولی به دلیل وجود شبکه تخاصمی مولد به محض مشاهده چنین تغییرات پیشبینی نشده ای فرآیند اجرای قرارداد با اعلام هشدار توسط ماشین مجازی، به صورت خودکار متوقف می‌شود.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

از اهداف دیگر تحقیق، بررسی قراردادهوشمند معمول و چالش‌ها و منافع آن بوده است. از آنجا که برای طراحی پروتکل مورد نظر لازم بود به مبانی و نحوه اجرای این قراردادها و بستر آن‌ها توجه شود در فصل دو تا حد امکان و تفصیلا به بیان آن‌ها پرداخته شده است. در قسمت دیگر فصل دو به عدم مزیت‌های بلاکچین و قراردادهای هوشمند و چالش‌های اجرایی آن پرداخته شد که در واقع همان دلیل اصلی ما برای پرداختن به مفهومی به نام قرارداد هوشمند مبتنی بر هوش مصنوعی است.

یکی دیگر از سوالات پژوهش زیر ساخت‌های لازم برای اجرایی کردن قراردادهای هو شمند در حوزه نظام بانکداری است که در بخش ۲-۹ توضیح دادیم. به طور کلی با توجه به پروتکل پیشنهادی این زیرساخت‌ها هم از نظر فنی و هم از نظر حقوقی باید فراهم شود.از لحاظ زیر ساخت‌های فنی نسبت به قراردادهای هوشمند معمول با توجه به نحوه عملیاتی و اجرایی شدن آن زیرساخت-های فنی و پیچیده‌ای جهت اجرا نیاز ندارد و لی به واسطه وجود الگوریتم‌هایی مانند شبکه عصبی تخاصمی و گراف جهت دار غیر مدور لازم است بستر وشبکه شبه‌نامتمرکز و طراحی ما شین مجازی به شکل کامل و در ست انجام بگیرد و در محیط‌های شبیه سازی شده ابتدا اجرایی شود. لذا با توجه به اینکه در پروتکل پیشنهادی، کتابخانه قانون منبع قراردادهای هو شمند و سایر قوانین و مشخص کننده ارتباط بین کاربران است. اما از آنجا که تمام قوانین و الگوریتم‌ها و مطابقت‌ها باید به صورت خودکار اجرایی شوند، ابتدا این قوانین و نحوه اجرا و تایید و ارزیابی قراردادها با توجه به اینکه نهادهای مالی و بانکی را نیز شامل می‌شود به تایید نهادی مرکزی مانند بانک مرکزی قرار گیرد. و مساله میزان اینکه کاربران چقدر شناس باشند یا ناشناس، نیز ذیل همین قوانین قرار می‌گیرد که از طریق الگوریتم‌های متفاوت می‌توان این شناسایی را پیچیده کرد.

صنعت خدمات مالی با نگاه چشمگیر، تحولات در فضای قراردادهای هوشمند را دنبال می کند. نوآوران در بین بانک ها و بیمه گرها آزمایش های خود را با قراردادهای هو شمند آغاز کرده اند و تعداد زیادی از آنها نسبت به تکامل و اتخاذ جریان ا صلی قراردادهای هو شمند طی چند سال آینده خوش بین ه ستند. فیلیپ دنیس ، رئیس ابتکارات بلاک‌چین سی‌آی‌بی[1] می گوید: "اکنون ، زمان شروع آزمایش در قراردادهای هوشمند در یک محیط محا سباتی ا ست. تا سال ۲۰۱۷ ، ما شروع خواهیم کرد به قراردادهای اولیه که امکان ا ستفاده از موارد کاربردی و همچنین اتصال به سکوهای میراث پیشرفت را می دهد. و تا سال ۲۰۱۹، ما حتی ممکن است شاهد افزایش مصرف پذیری مصرف کنندگان باشیم. سناریویی که یک سازمان بزرگ نمیخواهد در آن باشد این است که باید به

[1]CIB Blockchain Initiatives

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

سرعت مدرن سازی کلیه زیر ساخت های مالی خود را انجام دهد تا بتواند با اتخاذ سریع اوراق قرضه هوشمند یا مشتق قرارداد هوشمند به عنوان یک امنیت ارجح توسط بخش بزرگی از مشتریان خود ادامه دهد."

همانطور که اشاره شد این شروع و زمینه سازی باید با نیازها ی ابتدایی و اولیه از قراردادهای هوشمند باشد. و اجرا و پیاده سازی در همه راس ها و بخش‌های بانکی کاملا خطرناک و نادرست میباشد. به این معنی که ابتدا اجرا و پیاده سازی قراردادهای هوشمند را در کارهای روتین بانک مانند پرداخت‌های یکطرفه مانند حقوق کارمندان انجا بگیرد. بانک ژاپنی توکیو[1] اکنون قرارداد های دیجیتالی هوشمند را برای کار های خصوصی و درونی بانک امضا می کند و تا سال ۲۰۱۸ قراربود از قرارداد های هوشمند برای تبادلات بین بانک و آی‌بی‌ام [2] استفاده کند.

بانک‌ها علاوه بر مهیا کردن زیرساخت‌های سخت افزاری و نرم‌افزاری باید به موارد زیر نیز توجه کنند:

۱- موضوع قرارداد

این برنامه باید به محصول یا خدمات تحت قرارداد دسترسی داشته باشد تا به طور خودکار آن ها را در عرضه یا خرید کنترل کند.

۲- امضای دیجیتال

همه شرکت کنندگان با امضای قرارداد با شناسه خود، توافقنامه را آغاز می کنند.

۳- شرایط قرارداد

شرایط قرارداد هوشمند به شکل دقیق دنباله ای از عملیات است. همه شرکت کنندگان باید این شرایط را امضا کنند.

۴- پلتفرم انحصاری

قرارداد هوشمند به ماشین مجازی تحت پلتفرم خاص صادر می شود و در میان نودهای(کاربران) پلتفرم مورد نظر توزیع می شود. نکته مهمی وجود دارد در این زمینه که قراردادها از لحاظ مفاد قرارداد باید مطابق با اصول بانکی

[1]Tokyo-Mitsubishi UFJ
[2]IBM

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

و مقررات بانکی و اسلامی باشند.

پیشنهادات و تحقیقات آتی

- از آنجا که این تحقیق بر ا ساس نقاط ضعف موجود در قرادادهای هو شمند مبتنی بر بلاکچین بیان شده لذا در صورت حذف این نقاط ضعف در سال‌های آتی، مطالعات بیشتری در زمینه الگوریتم‌های مبتنی بر یادگیری ما شین و جهت ترکیب این الگوریتم با سیستم‌های نامتمرکز و بلاک‌چین صورت بگیرد. *چرا که ترکیب این دومی‌تواند باعث بهبود قراردادهای هوشمند از نظر امنیت و کارایی شود. برای مثال می‌توان از سیستم‌های نامتمرکز جهت پیاده سازی کتابخانه قانون در قراردادهای هوشمند استفاده کرد که اصول بنیادی هر قرارداد و مفاد پایه‌ای هر قرارداد در آن می‌باشد.*
- در آینده کارهای زیادی را می توان براساس پروتکل ارائه شده انجام داده و بهبودهایی را برایآن فراهم کنیم. یکی از مواردی که می توان به عنوان کارهای پیشنهادی برای بهبود پروتکل ارائهشده در آینده انجام دهیم ارتقای مدل اعتماد و افزودن یکسری مشخصه های دیگر به آن می باشد.برای مثال سناریویی از اینترنت اشیاء را در نظر می گیریم که چندین فرستنده مجزا داشته باشیمکه هر کدام براساس موقعیت های خاص و با توجه به نیاز، داده هایی را از یک مجموعه ای ازحسگرها جمع آوری کرده و آنها را با سرویس دهنده های خاصی در میان می گذارند تا بتوانندسرویس مدنظر خود را کسب کنند(اینرنت اشیاء و).
- در طول این مطالعه ذکر شد که نبود استاندارد برای محتوای قراردادهای هوشمند ، برنامه ریزی برای استقرار و استفاده از قراردادهای هوشمند را دشوار کرده است. درک این مسئله که چگونه استانداردها به سهولت ایجاد و استفاده از قراردادهای هوشمند اضافه می شوند ، مفید خواهد بود.
- این تحقیق در بخش روش تحقیق یا در واقع ابزارها و الگوریتم‌ها، با توجه به اینکه مطالعه در حوزه رشته بانکداری می‌باشد، به صورت کلی بیان شده و در تحقیقات آتی می‌توان به صورت جزئی‌تر و کاربردی تر به خصوص با توجه به پیچیدگی زمانی الگوریتم‌ها بحث و تجزیه و تحلیل کرد.
- تحقیق در مورد نحوه اجرا وپیاده سازی قراردادهای هوشمند به طور خاص برای قراردادهای بانکی خاص ازجمله قراردادهای اسلامی و پرداخت‌های اسلامی مرتبط با بانک می‌تواند مفید باشد.
- یکی از مباحثی که مطرح شده، بحث تشخیص کاهبرداری و هک در قراردادهای هوشند است هر چند این پروتکل؛ الگوریتم‌های زیادی جهت افزایش امنیت و کارایی این قراردادها ارائه کرده ولی بحث به طور خاص در مورد این مساله از جهات مختلف و در ارتباط با قسمت‌های مختلف می‌تواند مفید باشد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

- در این تحقیق در حد ضـــرورت به توضـــیح در مورد این قراردادها از جهت مباحث اســـلامی و تایید این نوع قراردادها ازمنظر ایجاب و قبول قراردادها پرداختیم. ولی با توجه به مباحث زیادی که در این حوزه مطرح شده امکان بررســـی و تایید این نوع قراردادها از منظر شـــرع و قوانین اســـلامی در حد یک تحقیق پایان‌نامه کاملا امکان‌پذیر است.
- اکتشافی عمیق از اکوسیستم نرم افزارها و خدمات شخص ثالث پیرامون قراردادهای هوشمند بسیارمفید خواهد بود.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

منابع و مآخذ :

منابع فارسی :

۱- طاهرپور، جواد؛ محمدی ،تیمور؛ فردی، رضا؛ نقش توزیع تسهیلات اعطایی بانک ها در رشد اقتصادی ایران، پژوهشنامه اقتصادی : تابستان ۱۳۹۷ , دوره ۱۸ , شماره ۶۹ # ; b00348از صفحه ۱۳۳ تا صفحه ۱۶۲ ۲- رحمانی، کورش؛ بگدلی، عباس؛ حسینی، سید ابوالفضل؛ اقتصاد API و معاملات دیجیتال در خدمات مالی ،حرکتی به سمت بانکداری باز؛ هفتمین همایش ملی بانکداری الکترونیک و نظام های پرداخت، ۱۳۹۶.

۳- شاه آبادی، ابوالفضل؛ جعفری، مهدی؛ داوری کیش، راضیه؛تاثیر مولفه های دانش بر تجهیز منابع مالی در بورس اوراق بهادار؛ سیاست علم و فناوری؛ ۱۳۹۶.

۴- میرزایی، علیرضا، قانون ثبت اسناد و املاک در نظم حقوقی کنونی،تهران، چاپپنجم، بهنامی،۱۳۹۲.

۵- نورجمشید جمشید، امضای الکترونیکی، دانشنامه حقوق و سیاست، شماره ۱۳۸۸ ،۱.

۶- وصالی ناصح، مرتضی؛ قرارداد الکترونیک و مبانی اعتبار آن؛ ماهنامه حقوقی کانون سردفتران و دفتریاران، شماره ۶۶، دی ماه ۱۳۸۵.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

منابع لاتین :

1-Tapscot Don, Tapscot Alex, Blockchain Revolution: How The Technilogy BehindBitcoin Is Changing Money, Business, And The World,social sciences and researchnetwork,2016.

2- Bourque Samuel, Fung Sara, Tsue Ling, A Lawyer 's Introduction to Smart Contracts, social sciences and research network,2014,4.

3-Reggie O'Shields,Smart Contracts: Legal Agreements For The Blockchain, North Carolina Banking Institude,2017.

4-KAREN E. C. LEVY,Book-Smart, Not Street-Smart: Blockchain-Based Smart Contractsand The Social Workings of Law,social sciences and research network,2017,1.

5- Joshua Fairfield, Bit Property, 88 S. CAL. REV. 805, 811 (2015).

6- Edward D. Baker, Trustless Property System and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange, 45 SOUTHWESTERN L. REV. 357 (2015).

7-Edward D. Baker, Trustless Property System and Anarchy: How Trustless Transfer Technology Will

Shape the Future of Property Exchange, 45 SOUTHWESTERN L. REV. 357 (2015).

8- Cheng Lim & T. J. Shaw, Smart Contracts: Bridging the Gap between Expectation and Reality OXFORD LAW FACULTY BUSINESS LAW BLOG :https://www.law.ox.ac.uk/business-lawblog/blog/2016/07/smart-contracts-bridging-gap between expectation-and-reality (last visited July 11, 2016).

9-Joshua Fairfield, Smart Contracts, Bitcoin Bots and Consumer Protection, 71 WASH & LEE L. REV. (Online) 35, 39 (2014).

10-Josh Stark, How Close Are Smart Contracts to Impacting Real-World Law?, COINDESK http://www.coindesk.com/blockchain-smarts-contracts-real-world-law/ (last visited April 11, 2016). Bitcoin

11-Nikolei M. Kaplanov, Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation, 25 LOY. CONSUMER L. REV. 111, 118 (2012)

12-Harry Surden, Computable Contracts, 46 U. C. DAVIS L. REV. 629, 632 (2012).

13- Mayuko Tani, Tokyo-Mistubishi UFJ Starts Blockchain Trial in Asia, NIKKEIASIAN REVIEW, http://asia.nikkei.com/Business/Companies/Tokyo-Mitsubishi-UFJ-starts-blockchain-trial-in-Asia(last visited Sept. 21, 2016)

14- Andy Robinson and Tom Hingley, Smart Contracts: The Next Frontier?, OXFORD LAW FACULTYBUSINESS LAW BLOG, https://www.law.ox.ac.uk/business-law-

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

blog/blog/2016/05/smart-contractsnext-frontier (May 23, 2016)

15-Ammous Dr. Saifedean (2016), Blockchain Technology: What is it good for?Social Science Research Network.

16-Jacques Vos (2017), Blockchain Based Land Registry, Illusion or Something in Between, European Land Registry Association,7Th Annual publication.

17- Szabo, Nick. "Smart contracts." Unpublished manuscript (1994).

18- Bashir, Imran. Mastering blockchain. Packt Publishing Ltd, 2017.

19- Hillbom, Erik, and Tobias Tillström. Applications of Smartcontracts and smart property utilizing blockchains. Diss. Masters of Science Thesis in Computer Science, Chalmers University of Technology and University of Gothenburg, Sweden. Febuary, 2016.

20-Paramasiven Appavoo, Mun Choon Chan, Bhojan Anand and Ee-Chien Chang, "Efficient and Privacy-Preserving Access to Sensor Data for Internet of Things (IoT) based Services," COMSNET, Jan 2016.

21- Stark, Cyril. "Recommender systems inspired by the structure of quantum theory." arXiv preprint arXiv:1601.06035 (2016).

22-ACCENTURE (2016), Fintech and the evolving landscape: landing points for the industry,available online at http://www.fintechinnovationlablondon.co.uk.

23- BELINKY, M.; RENNICK, E.; VEITCH, A. (2015), The Fintech 2.0 paper: Rebootingfinancial services, in http://www.oliverwyman.com.

24- DE FILIPPI P.; HASSAN, S. (2016), Blockchain technology as a regulatory technology:From code is law to law is code; First Monday, 2016, 21.12.

25- GUO, Y. and LIANG, C. (2016), Blockchain application and outlook in the banking industry,Financial Innovation, 2016, 2.1: 24.

26- IANSITI M. and LAHKANI K. (2017), The Truth About Blockchain, Harvard BusinessReview, January-February 2017 Issue available online at: https://hbr.org/2017/01/the-truthabout-blockchain.

27- Konstantinos Christidis, Michael Devetsikiotis,” Blockchains and SmartContractsfor the Internet of Things”,2016 IEEE, Digital Object Identifier 10.1109/ACCESS.2016.2566339.

28- C. Cachin, S. Schubert, M. Vukoli¢, 2016, “Non-determinism in Byzantine faulttolerant replication”, [Online]. Available: http://arxiv.org/abs/1603.07351.

29- Xinlei Wang, Jianqing Zhang, Eve M. Schooler, Mihaela Ion,” Performance Evaluation of Attribute-Based Encryption: Toward Data Privacy in the IoT”, IEEE ICC 2014 - Communication and Information http://www.itrans24.com/landing1.html

30- “ElementsProject/Elements: Feature Experiments to Advance the Art of

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

Bitcoin", accessed on Mar. 15, 2016, [Online]. Available: https://github.com/ElementsProject/elements
31- M. Ali, J. Nelson, R. Shea, and M. J. Freedman, Feb. 2016, "Blockstack: Design and Implementation of a Global Naming System With Blockchains", [Online]. Available:https://blockstack.org/blockstack.pdf
32- "Blockstack_How Blockstack Works", accessed on Mar. 15, 2016, [Online]. Available:https://blockstack.org/docs/how-blockstack-works
33- "Telehash_Encrypted Mesh Protocol", accessed on Mar. 15, 2016, [Online]. Available: http://telehash.org/.

34-Coy P, Kharif O, This is your company on Blockchain. Available online at: http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-onBlockchain[AccessedMar2018].
35-Dannen, C. (2017). Introducing Ethereum and Solidity. Berkeley: Available online at:https://doi.org/10.1007/978-1-4842-2535-6 [Accessed Mar 2018].

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پیوست الف

۱- انواع سیستم و شبکه

شبکه متمرکز

معماری شبکه‌ی متمرکز حول یک سرور منفرد بنا شده است که تمام پردازش‌های عمده را عهده‌دار است. ایستگاه‌های کاری که قدرت کم‌تری دارند، به سرور متصل شده و به جای این که پردازش‌ها را خود انجام دهند آن ها را به سرور مرکزی به صورت درخواست ارجاع می‌دهند. این موارد شامل اپلیکیشن‌ها، ذخیره سازی دیتا، ابزارها و ...می‌باشد.

شبکه غیر متمرکز

در اصطلاحات کامپیوتری،یک معماری شبکه غیرمتمرکز بار کاری موجود را به جای این که متکی بر یک سرور مرکزی منفرد، بین سیستم‌های مختلف توزیع می کند. این نوع شبکه به علت پیشرفت‌های سریع کامپیوترهای دسکتاپ و لپ‌تاپ، که امروزه کارایی بسیار بیشتری از نیازهای نرم افزارییک کسب و کار ارائه می دهند، تکامل یافته. به عبارت دیگر، به این روش می توان توان محاسباتی بیش‌تر را در پردازش‌های توزیع شده استفاده کرد(پرادل، ۲۰۱۸[1]).

سیستم‌های توزیع شده

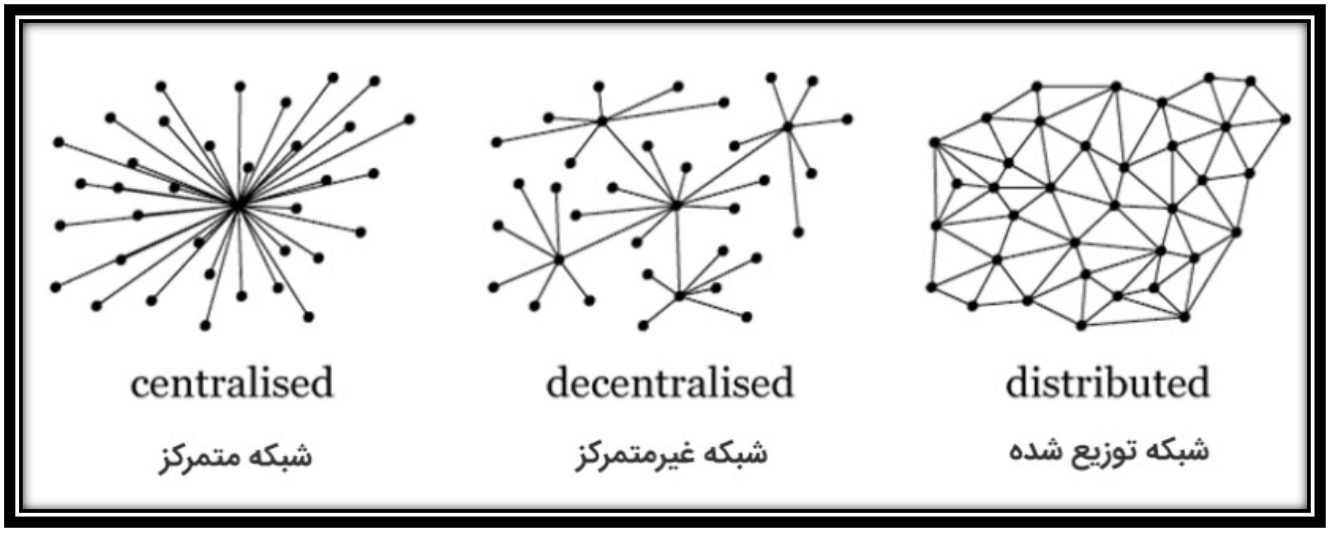
سیستم های توزیع شده مجموعه ای از چندین کامپیوتر مستقل که کاربر آن را به شکل یک سیستم واحد و متجانس می بیند، در این سیستم ها معمولا یک لایه نرم افزاری روی سیستم عامل بنام میان افزار Middleware است که مدل مورد نظر را پیاده سازی می کند.

معروف ترین سیستم توزیع شده، وب است که بر پایه اینترنت کار می کند. به این ترتیب که وب سایت های مختلفی که بر روی کامپیوترها و Server های مختلف قرار دارند،یک نوع سیستم توزیع شده محسوب می شوند.

در تصویر زیر تفاوت میان شبکه های متمرکز، غیرمتمرکز و شبکه های توزیع شده با رسم گراف میان اجزای تشکیل دهنده آن‌ها مشخص شده است:

[1]PRADEL, 2018

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.



پیوست ب

انواع روش‌های مجازی سازی

حالت اسکریپتی

این روش یک روش سنتی برای اجرای منطق قابل برنامه ریزی است که ابتدا در سیستمBTC به کار گرفته شد. مدل UTXO BTC برای تایید مشروعیت این تراکنش از یک سیستم اسکریپت نویسی امضا مانند استفاده می‌کند. تراکنش‌ها به طور کلی شامل یک اسکریپت ورودی و یک اسکریپت خروجی، که برای باز کردن خروجی تراکنش قبلی و تنظیم شرایط قفل کردن مقدار تراکنش استفاده می‌شود.

کانتینر [1]

کانتینرنوع جدیدی از تکنولوژی مجازی سازی است که در سال‌های اخیر پدیدار شده است و با ماشین‌های مجازی متفاوت است. در مقایسه با لایه اضافه شده از محیط‌های میانی در برنامه کاربر و محیط زیرین، فن‌آوری کانتینر تنها باید وابستگی‌های لازم مورد نیاز برنامه را بسته و بدون نیاز به یک محیط سیستم‌عامل مجازی دیگر بسته شود.رویکرد کانتینر شده ، در مقایسه با رویکرد ماشین مجازی ، نسبتاً مستقل تر و انعطاف پذیر است و می تواند منابع بیشتری را مستقر کند.اگرچه فن آوری کانتینر از منظر معماری کلی سیستم آسانتر و انعطاف پذیرتر است، اما اگر به فکر یک برنامه واحد باشید ، باید فاکتورهای سیستم " سنگین" تری در نظر گرفته شوند، زیرا فایل ها و سیستم ها در محیط کانتینر قابل دسترسی هستند.

[1]Containerization

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ماشین مجازی

Virtual Machineیا ماشین مجازییا به اختصار VM در واقع یک سیستم عامل است که بر روییک نرم افزار مجازی ساز که در اصطلاح Hypervisor نام دارد نصب میشود و به شما این امکان را میدهد تا مانند یک کامپیوتر واقعییا همان ماشین فیزیکی با آن کار کنید. ماشین های مجازی که در نرم افزار Hypervisor نصب میشوند در واقع از سخت افزار های سیستم اصلی تان برای کارکردشان استفاده میکنند به این معنی که CPU، حافظه RAM ، هارد دیسک ، کارت گرافیک ، کارت صدا ، کارت شبکه همه و همه بصورت اشتراکی از سیستم اصلییاHost شما می‌تواند در اختیار ماشین های مجازی‌تان قرار بگیرد(ITPRO, 2017).

ماشین‌های مجازی، بر اساس استفاده و درجه ارتباط به ماشین واقعی، به دو دسته اصلی تقسیم می‌شوند. یک ماشین مجازی سیستمییک زیرساخت محاسباتی کامل را فراهم می‌کند که از اجراییک سیستم‌عامل کامل پشتیبانی می‌کند. در مقابل، یک ماشین مجازی فرایند، برای اجراییک برنامه واحد طراحی شده، که این به این معناست که صرفاً از یک فرایند خاص پشتیبانی می‌کند. یک ویژگی مهم یک ماشین مجازی، این است که نرم‌افزاری که درون آن در حال اجراست، با منابع و سطوح انتزاعی که توسط ماشین مجازی اعمال می‌شود، محدود شده‌است – یعنی نمی‌تواند از دنیای مجازی خود خارج شود(smith, 2018)[1].

استانداردهایCERT برای کدنویسی امن شامل یک سری قوانین و پیشنهادات می شوند. در زیر تعریف هر کدام از آنها آورده شده است.

- قوانین

یک روش برنامه نویسی زمانی به عنوان قانون تعریف می شود که دارای خصوصیات زیر باشد:

سرپیچی از روش فوق احتمالاً منجر به یک نقص امنیتی شده و ممکن است به یک آسیب پذیری قابل سوءاستفاده تبدیل شود.پیروی از روش فوق را بتوان توسط تحلیل اتوماتیک، راهکارهای رسمییا تکنیک هایبازرسی دستی تشخیص داد. پیاده سازی قوانینی که در استاندارد CERT برای برنامه نویسی امن آورده شده، برای اطمینان از امنیت سیستم هایی که با زبان برنامه نویسی مربوطه ایجاد شده اند، شرط لازم است ولی کافی نیست. در این استانداردها قوانین با برچسب rule مشخص می شوند.

[1] در پیوست توضیح دقیق‌تر آن بیان شده است.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

- پیشنهادات

پیشنهادات در حقیقتیک سری از راهنمایی ها و توصیه ها است. یک روش کدنویسی زمانی به عنوان یک پیشنهاد در نظر گرفته می شود که شرایط زیر را دارا باشد:

به کارگیری روش کدنویسی مذکور، باعث ارتقای امنیت سیستم شود.

شرایطی که برای در نظر گرفتن روش مذکور به عنوان یک قانون لازم است، در مورد این روش کدنویسی صدق نکند.در هر تجربه کدنویسی، مجموعه ای از پیشنهادات با توجه به نیازمندی های امنیتی محصول نهایی مورد استفاده قرار می گیرد. پروژه هایی که نیازمند سطح امنیتی بالایی هستند، می توانند منابع بیشتری را به امنیت اختصاص دهند و در نتیجه مجموعه بیشتری از پیشنهادات را نیز به کار گیرند.

در استانداردهای CERT برای کدنویسی امن، از برچسب recommendation برای نشان دادن پیشنهادات استفاده می شود.

- استثناءها

هر قانون یا پیشنهادی ممکن است حاوی مجموعه کوچکی از استثناءها باشد که نشان می دهد تحت چه شرایطی به کار بردن قانون یا پیشنهاد مذکور برای بالا بردن سطح امنیتی محصول ضروری نیست. استثناءها فقط برای اطلاع کاربر عنوان می شوند و پیروی از آنها لازم نیست. استثناء ها در استاندارد CERT برای برنامه نویسی امن با برچسب exceptions مشخص می شوند.

- شناسه ها

در استانداردهای مذکور، هر قانون یا پیشنهاد، دارایک شناسه یکتا است.این شناسه ها از سه قسمت تشکیل شده اند:

یک بخش سه حرفی که نشان دهنده بخش استاندارد است برای مثال PRE که نشان دهنده preprocessor است. این بخش نشان دهنده روش های کدنویسی مشابه در یک گروه است.

- به کارگیری استاندارد

قوانین استانداردهای مذکور می توانند با قوانین استانداردهای داخل سازمان ترکیب شوند. البته واضح است

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

که ا ستانداردهای داخل سازمان باید با ا ستانداردهایCERT سازگاری دا شته با شند.بهتر ا ست یک سری برنامه های آموز شی برای برنامه نویسان ترتیب داد و در طی آن شیوه به کارگیری صحیح ا ستانداردهای مذکور را در برنامه نویسی آموزش داد.زمانی که یک استاندارد کدنویسی در تولید محصول پیاده سازی می شود، لازم است با استفاده از ابزارهایی، میزان تطابق محصول تولید شده با استاندارد به کار گرفته شده را سنجید. همان طور که قبلاً نیز گفته شد یکی از شرایط تبدیل شدن یک روش برنامه نویسی به قانون، امکان بررسی به کار گیری آن در نرم افزار است. بررسی می تواند به صورت دستی و یا به صورت اتوماتیک انجام شود. طبیعی است که بررسی دستی زحمت زیادی را می طلبد و همچنین احتمال خطا در آن بالا است. بررسی اتوماتیک نیز عاری از خطا نیست، زیرا برخی خطاها حالت دنباله دار دا شته و ابزار اتوماتیک باید بتواند هر گونه تخطی از قانون را تشخیص داده و دنباله آن را نیز اصلاح کند. حتی با وجود چالش های مذکور نیز، روش اتوماتیک برای بررسی همخوانی محصول با استانداردها مقرون به صرفه تر است.ابزارهای تحلیل نرم افزار می توانند گواهی همخوانی با یک استاندارد را دریافت کنند. سپس شرکت های گواهی دهنده مجاز قادرند یک نرم افزار را با استفاده از ابزارهای تحلیل نرم افزار تأیید شده مورد بازرسی قرار داده و در صورت همخوانی با استاندارد، گواهی مربوطه را مبنی بر رعایت استانداردهای کدنویسی امن ابه آن نرم افزار عطا کنند.

- معیار سنجش آسیب پذیری

معیار آسیب پذیریCERT، عددی بین ۰ و ۱۸۰ است که میزان اهمیتیک آسیب پذیری را نشان می دهد. در نگاشت یک عدد به آسیب پذیری، معیارهای متفاوتی همچون میزان شناخته شده بودن آن، وجود کد سوءاستفاده موفق از آن، در خطر قرار گرفتن زیر ساخت های شبکه، تعداد رایانه هایی که در خطر آسیب پذیری مذکور قرار دارند و غیره دخیل هستند. البته معیار مذکور خطی نبوده و به این معنی نیست که یک آسیب پذیری با درجه ۴۰ دو برابر یک آسیب پذیری با درجه ۲۰ خطرناک است.

- ارزیابی خطر

در ا ستانداردهای کدنویسی امن CERT، هر راهنما دارای بخشی به نام ارزیابی خطر یاRisk Assessment ا ست که به برنامه نویسان نشان می دهد در صورت رسیدگی نکردن به یک آسیب پذیری خاص در کد برنامه، ممکن است چه نتایج بالقوه ای به بار آید. این اطلاعات در اولویت بندی آسیب پذیری هایی که باید رسیدگی شوند، توسط تیم برطرف کننده آسیب پذیری ها به کار گرفته می شود.

نادیده انگاشتن هر قانون منجر به ایجاد آسیب پذیری هایی می شود که هر کدام از آنها از لحاظ جدیت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

خطر (severity) ، احتمال سوءاستفاده)(Likelihoodو هزینه ترمیم (Remediation Cost)متفاوت هستند. در بخش ارزیابی خطر هر راهنما، موارد مذکور نشان داده می شود. در جداول زیر دسته بندی های مذکور نشان داده شده اند.

پیوست ج

ماشین مجازی

متداول ترین روش برای اجرای قراردادهای هو شمند رویکرد د ستگاه مجازی ا ست. این برنامه یک محیط اجرای کاملاً شفاف ارائه می دهد. یک کاربرد معمول از این ایده را می‌توان به ماشین مجازی جاوا اشاره کرد. هدف اجرا "یک‌بار نوشتن و اجرا در همه جا" است, به جای اینکه توسعه دهنده نسخه‌های مختلف برنامه را برای هر سرور متفاوت بنویسید. این ویژگی دقیقاً همان چیزی است که برای گسترش و بهره‌برداری توزیع‌شده قراردادهای هو شمند مورد نیاز ا ست: تفاوت بین محیط اجرایی گره[1] اجرای بلوک در تمام گره‌ها, برای د ستیابی به ویژگی‌های قطعی.

در حال حاضر ، ماشین های مجازیsmart contractها به طور عمده شش جهت دارند:

۱. ماشین مجازی نئو (AVM هسته کامپایلر مبتنی بر .NET CLR MSILاست) ،در حال حاضر از سری زبانهای دات نت پشتیبانی می کند C#, VB.NET, #F، زبانهای سری جاوا (جاوا،کوتلین)و پایتون.

۲. ماشین مجازی وب اسمبلی Wasm، در حال حاضر از C / C ++ / RUST / Go پشتیبانی می کند.

۳. ماشین مجازی زبان اسکریپت (موتور V8 Chrome ، ماشین مجازیLua و غیره) و jsدر حال حاضر پشتیبانی می شود.

۴. ماشین مجازی RISC-Vمعماری مجموعه دستورالعمل منبع باز، در حال حاضر از Solid پشتیبانی می کند.

۵. یک ماشین و زبان مجازی جدید ، مشابه EVM ایجاد کنید. EVM و استحکام Ethereum، حرکت

[1] در اینجا مفهوم گره در smart contract ، با مفاهیم نود و کاربر فرق ندارد. و همه این‌ها معادل خود همین مفاهیم در intelligent contract هستند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

VM و حرکت Libra.

۶. پشتیبانی از چندین ماشین مجازی و چندین زبان. آنتولوژی ontologyپشتیبانی از ماشین مجازی نئو و ماشین مجازی وب اسمبلی Wasmو Thunderbolt پشتیبانی می کند، و زنجیره اصلی از ماشین مجازی نئو و EVM اتریوم پشتیبانی می کند.

خلاصه ای از اصول اولیه ماشین مجازی

هسته د ستگاه مجازی: مدیریت حافظه، بارگیری مونتاژ، امنیت، کنترل ا ستثناء، و هماهنگ سازی مو ضوع. دستگاه مجازی عمدتا بر اساس Stack و Register به دو نوع ماشین مجازی تقسیم می شود.

مترجم شفاهی

زبان منبع اجرای را تفسیر کنید (php، postcretp، javascript و غیره).

- مزایا و معایب

مترجم شروع به حرکت می‌کند و با سرعت بیشتری اجرا می‌کند، و لازم نیست قبل از اجرای این کد، کل فرآیند گردآوری را تکمیل کنید. ترجمه از خط اول و شما می‌توانید به اجرا در سفارش خود ادامه دهید. به نظر می‌رسد مفسر برای جاوا اسکریپت مناسب‌تر است. برایبک توسعه دهنده وب، مهم است که بتوانید به سرعت کد را اجرا کنید و نتایج را ببینید. به همین دلیل است که مرورگرهای اصلی از مترجم جاوا اسکریپت استفاده می‌کنند.اما، هنگام اجرای همان کد بیش از یک بار، مضرات مترجم آشکار می شود. به عنوان مثال، اگر یک حلقه را اجرا کنید، مترجم مجبور است آن را دوباره و دوباره ترجمه کند. این عملکرد ناکارآمد است.

۲- کامپایلر

کد مبدا به طور کلی در کد هدف جمع‌آوری می‌شود و کامپایلر ملزم به اجرای آن نیست، و به طور مستقیمبر روی سکویی که از کد هدف پشتیبانی می‌کند و اجرا می‌شود، به طوری که کارایی اجرایی بسیار سریع‌تر از اجرای تفسیر است.

مزایا و معایب :

مشکل کامپایلر متضاد با مترجم شفاهی است. کامپایلر نیاز دارد تا زمانی برای کامپایلر تمام کد منبع صرف

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

کند و سپس فایل را برای اجرا روی ماشین تولید کند. برای کدها با حلقه‌ها, خیلی سریع اجرا می‌شود چون نیازی به تکرار هر حلقه نیست .تفاوت دیگر این است که کامپایلر قادر است از زمان بیشتری برای بهینه‌سازی کد استفاده کند تا کد را سریع‌تر اجرا کند. مترجم شفاهی این مرحله را در زمان اجرا انجام می‌دهد که مشخص می‌کند که بهینه‌سازی زمان زیادی در طول ترجمه ممکن نیست.

- GCC

مفهوم(GNU (Gnu's Un Unix) Compiler Collection (GCC) ، مجموعه ای از کامپایلرهای زبان برنامه نویسی ، یک نرم افزار رایگان منتشر شده تحت مجوزهای GPL و LGPL، همچنین بخش مهمی از پروژه GNU و بخش اصلی ابزارهای GNU است. این اولین انتخاب کامپایلر برای نرم افزار cross-platform است. GCC از همان برنامه جلویی مشابه در تمامی سیستم عامل ها استفاده می کند و همان کد میانجیگری را تولید می کند، بنابراین این کد میانجیگری با GCC در سیستم عامل های مختلف دیگر تهیه می شود و شانس بسیار خوبی برای گرفتن برنامه صحیح خروجی وجود دارد.

زبانهای پشتیبانی شده: C، C ++، Fortran، Pascal، Objective-C، Java، Ada، Go، و غیره.

ساختارهای پردازشگر اصلی پشتیبانی شده: ARM، x۸۶ -۶۴ ، MIPS، PowerPC و غیره .

پیوست د

API

APIیا «رابط برنامه‌نویسی کاربردی»یک سری از دستورالعمل‌های مشخص و تعریف شده است که نرم‌افزارها، سخت‌افزارها، کامپوننت‌ها یا سایت‌های اینترنتی می‌توانند با استفاده از آن با یکدیگر ارتباط برقرار کنند.به عبارت دیگر API جایگزینی برای رابط کاربری است. همان گونه که کاربران می‌توانند با فشردن یک دکمه، دستوری را به سخت‌افزار ارسال کنند یا با حرکت ماوس، پیامی را به یک نرم‌افزار بفرستند، API نیز ابزاری است که نرم‌افزارها و سخت‌افزارها با کمک آن می‌توانند با هم ارتباط برقرار کنند و به یکدیگر دستورات مورد نظر را ارسال کنند. بدون وجود API، همکاری میان اجزای کوچک سیستم‌های سخت‌افزاری و نرم‌افزاری امکان‌پذیر نیست.جموعه دستوراتی که فریم‌ورک‌های برنامه‌نویسی مانند دات‌نت‌فریم‌ورکیا جاوا در اختیار برنامه‌نویسان قرار می‌دهند گونه‌ای از API به حساب می‌آید. زیرا هسته‌ی مرکزی فریم‌ورکیک نرم‌افزار است که فعالیت‌های متعددی انجام می‌دهد و برنامه‌ها با فراخوانی دستوراتی از پیش‌تعریف شده، دستورات دلخواه خود را به فریم‌ورک ارسال می‌نمایند.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

علاوه بر فریم‌ورک‌ها، هسته‌ی سیستم‌عامل‌ها مانند ویندوز و لینوکس نیز دارایAPI هستند. برنامه‌ها با فراخوانی این دستورات می‌توانند روی فعالیت‌های سیستم‌عامل کنترل داشته باشند.

API در انواع مختلف در سخت‌افزارها و نرم‌افزارها وجود دارند. برخی از انواع شناخته شده‌یAPI عبارتند از:

- API سیستم عامل ویندوز برای برنامه‌نویسی و ارتباط با هسته ویندوز
- API سایت توئیتر برای توسعه‌ی رابط کاربری سفارشی روی کامپیوترهای رومیزی و گوشی‌های موبایل
- API جاوا برای برنامه‌نویسی و ارتباط با هسته‌ی کتابخانه‌های جاوا
- API نقشه گوگل برای نمایش نقشه و دریافت اطلاعات در مورد مکان‌های مختلف جهان
- API بانک‌های مختلف برای انجام پرداخت آنلاین (Eising, 2017).

پیوست ذ

زبان‌های برنامه‌نویسی

زبان‌های برنامه‌نویسی قابل استفاده برای پیاده‌سازی قسمت‌های مختلف قراردادهای هوشمند

- زبان سی پلاس پلاس C++

این برنامه به عنوان مشتقی از زبان برنامه نویسیC ساخته شده است. زبان روندگرای C++ بر اساس زبان داده‌گرایC نوشته شده است. شاید همین بزرگ‌ترین تفاوت بین این دو زبان باشد. C++ اطلاعات و عملکرد آن‌ها را به داده‌ها تبدیل می‌کند که می‌توان آنها را به راحتی در برنامه‌های دیگر مورد استفاده قرار داد. این زبان برنامه نویسی اجازه می‌دهد تا مدیریت مؤثرتری بر روی حافظه وجود داشته باشد. محیط شبکه مورد نظر به بسیاری از کاربران اجازه می‌دهد تا به صورت سیستماتیک و همزمان عمل کنند. C++ اپلیکیشن‌هایی را ایجاد می‌کند که نه تنها بین نقاط پایانی بلکه در پروسه انجام تراکنش سریع‌تر عمل می‌کنند.

- زبان جاوا Java

جاوا به عنوان زبان جهانی اینترنت بسیار اهمیت دارد. زبان برنامه نویسیسیستم های توزیع شده و نامتمرکز زبانی قدیمی و برای ایجاد پیج های اینترنتی فعال بسیار مفید است. همچنین برای ایجادشبکه های پیچیده و تغییرناپذیر نیز کاربرد دارد. تغییر ناپذیری باعث می‌شود که هیچ کس نتواند اطلاعاتیکقسمت یا گروه را تغییردهد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

برای مثال در بلاکچین ، اطلاعات بلوک قبلی به اضـافه اطلاعات بلوک جدید را در اختیار دارد. هر تغییری که در یک بلوک ایجاد شـود باعث ایجاد تغییر جدیدی در بلوک‌های کناری آن هم خواهد شـد، و تا زمانی که اطلاعات آن بلوک با دیگر بلوک‌ها هماهنگ نشده با شد نمی‌تواند به زنجیره ا ضافه شود در نتیجه بلاک چین به این وسیله تغییر ناپذیر شده است لذا از این ویژگی میتوان در حوزه شبکه های پیچیده و نامتمرکز استفاده کرد.

- زبان پایتونPython

زبان پایتون به وسیلهیک برنامه نویس هلندی به نام گویدو وان روسام (guido van Rossum) در سال ۱۹۹۱ ابداع شد. هدف او تولید زبان برنامه نویسی آ سان و مینی مالیستی بود. ترکیب و منطق این برنامه، نشان از روحیه بلندپرواز، ابداع کننده آن دارد. در نتیجه پایتون در زمینه توسـعه نرم افزارها و وب، زبانی برتر اسـت. این زبان در میان متخصصان کامپیوتری و دانشمندان زمینه دیتا بسیار معروف است. همچنینیکی از زبان‌های برتر برنامه نویسیدر حوزه برنامه‌های کاربردی است.

- زبان سیمپلیسیتیSimplicity

سیمپلیسیتییک زبان برنامه نویسی بلاک چین ا ست که برای تنظیم قراردادهای هو شمند به کار می‌رود. این زبان برنامه نویسی بلاک چین به گفته راسل اوکان (Russell O’Connor) سازنده این برنامه بسیار ساده است. این زبان برای بهبود زبان‌های پایه‌ای ارزهای دیجیتال مانند بیت کوین و اتریوم به کار برده می‌شود.

در این زبان از تجزیه و تحلیل اسـتاتیک برای جلوگیری از هنگ کردن برنامه‌ها هنگام آنالیز و محاسـبات استفاده می‌شود. اوکانر و کمپانی او یعنی بلاک استریم (blockstream) امیدوار هستند که این زبان، پس از آنکه آزمایشش را کاملاً پس داد در بیت کوین و شبکه‌های محاسباتی مورد استفاده قرار بگیرد.

- زبان سالیدیتیSolidity

و در آخر زبان برنامه نویسی سالیدیتی،این زبان برنامه نویسی بلاک‌چین از سطح بالایی برخوردار است و بر پایه قرارداد تنظیم شـده اسـت. حروف آن مشـابه با حروفی هسـتند که در جاوا مورد اسـتفاده قرار می‌گیرند. بخش‌های هم مانند متغیرها، کلاس‌ها و عملکردهای خود را از جاوا برداشت کرده است.

یادگیری این زبان برای برنامه نویسـان بسـیار آسـان اسـت. زبان سـالیدیتی توضـیحاتی در مورد اینکه چطور کدهایش عمل می‌کنند را برای کسانی که علاقه‌مند به آموختن آن با شند تو ضیح داده ا ست این تو ضیح ممکن

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

است در ابتدا کمی مشکل به نظر بیاید.

پیوست ر

باگ و انواع خطاهای برنامه نویسی

به فرآیند اشـکال زدایی و رفع خطاییک نرم افزار عملیات دیباگ کردن یاDebugging می گویند. در زمان کدنویسییک نرم افزار، امکان دارد باگ های مختلفی در آن ایجاد شوند که اجرای صحیح آن را با اختلال رو به رو سازند. بنابراین برنامه نویسان برای برطرف سازیBug های نرم افزار باید به طور مداوم عملیات دیباگ کردن کدهای خود را انجام دهند تا Bug های آن را بر طرف سـازند.دیباگ کردن جزو مراحل اصـلی و جدا نشـدنی برنامه نویسـییک نرم افزار اسـت. در فرآیند کدنویسـی، نمی توان انتظار داشـت که کدهای نوشـته شـده، خالی از ا شتباه با شند و همواره به صورت صحیح عمل کنند. زیرا در فرآیند کدنویسی قطعا خطاهای منطقی و نو شتاری زیادی پیش می آید که باعث بروز خطا در عملکرد نرم افزار می شـوند. این خطاها می توانند در اشـکال و زمان های مختلف ظاهر شوند و در نهایت باعث شوند نتیجه نهایی و خروجی نرم افزار، با نتیجه مورد انتظار برنامه نویس تناقض داشته باشد. عملیات اشکال زدایی کدها، مانند بازبینی و ویرایشیک متن ادبی است.با توجه به این که باگ های مختلف منشا های متفاوتی دارند، عملیات ا شکال زدایی و دیباگ کردن باگ های کدهاییک نرم افزار نیز به چندین روش صورت می گیرد. متداول ترین باگ ها و روش های ا شکال زدایی آن ها در کدنویسی به صورت زیر می باشند:

خطاهای نوشتاری (Syntax)

به قوائد و نوع نوشتار کدهاییک زبان برنامه نویسیSyntax گفته می شود. یکی از متداول ترین عوامل ایجاد باگ در نرم افزارها مربوط به اشـتباهات نوشـتاری برنامه نویسـان اسـت. زمانی که برنامه نویسـان در کدهای خود اشتباه تایپیا دستوری داشته باشند، اجرای نرم افزار با اختلال رو به رو خواهد شد. زبان هایی مانند HTML و CSS به خطاهای نوشتاری حساسیت زیادی نشان نمی دهند، اما در زبان هایی مانند PHPیاPython این خطاها از اجرای نرم افزار جلوگیری می کنند.

خطاهای معنایی(Semantics)

برخی خطاها در حالی که از نظر کدنویسی صحیح هستند، اما نتیجه نهایی آن ها از نظر معنایی ا شتباه ا ست. برای مثال فرض کنید قصد داریم با کلمات سون لرن، مدر سه، ا ست، برنامه نویسی، جمله ای طبق ا صول فار سی

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

بنویسیم. اگر بنویسیم مدرسه برنامه نویسی سون لرن است در حالی که در ظاهر از کلمات صحیح استفاده کردیم اما جمله نوشته شده از نظر معنایی اشتباه است. بنابراین باید چنین نوشت سون لرن مدرسه برنامه نویسی است. در فرآیند برنامه نویسی نیز ممکن است خطاهای معنایی نیز ایجاد شوند، مثلا عددی را بر صفر تقسیم کنید که این عمل در ریاضیاتامکان پذیر نیست.

خطاهای منطقی(Logic)

این دسته از خطاها جزو سخت ترین خطاهای برنامه نویسی محسوب می شوند. برنامه نویسان زمان زیادی را باید برای رفع خطاهای منطقی صرف کنند. زمانی که کدهای نوشته شده از نظر نوشتاری کاملا صحیح هستند، اما نرم افزار به درستی اجرا نمی شود و یا در حالی که اجرا می شود خروجی آن اشتباه است، باید به دنبال یک خطایی منطقی بود. خطاهای منطقی از خود نشانه ای بر جای نمی گذارند و معمولا توسط Debugger ها شناسایی نمی شوند.گاهی برای رفع چنین خطاهایی برنامه نویس راهی جز خواندن خط به خط کدهای نوشته شده ندارد.

برخی از این خطاها شاید به راحتی شناسایی شوند ولی گاهی هم ممکن است روزها صرف برطرف کردن آن شود. برای درک بهتر این خطاها، تصور کنید که می خواهیم نرم افزاری بنویسیم که تعداد کاربران سایت را محاسبه کند. فرض کنید اطلاع داریم که ۲۰ کاربر در سایت می باشند، ولی این نرم افزار عددی غیر ۲۰ را به ما نمایش می دهد. زمانی که نرم افزار بدون هیچ خطایی اجرا شود ولی جواب صحیحی به ما نمایش ندهد، خطاییمنطقی رخ داده است.

پیوست ژ

اصول مورد نظر در طراحی شبکه

برخی از موارد مهم این اصول در ذیل آمده است:

Hierarchy : این طراحی سلسله مراتبی به طراح کمک می کند که یک شبکه مطمئن طراحی کند و مشکلات پیچیده طراحی را راحت تر و قابل مدیریتتر کند.

Modularity : طراحی ماژولار که باعث می شود عملکرد بخش های مختلف موجود در شبکه به صورت

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

یک ماژول عمل کند و به این صورت طراحی ساده تر می شود. سیسکو چندین ماژول را معرفی کرده که شامل دیتاسنتر ، لبه اینترنت ، بلوک سرویس دهی و بخش Campus می باشد.

Resiliency : شبکه باید بتواند در شرایط عادی و غیرعادی به کار خود ادامه دهد. در شرایط عادی ترافیک براساس انتظار ما جریان دارد ولی شرایط غیر عادی زمانی است که یک سخت افزار یا نرم افزار ما دچار مشکل شود یا ترافیک زیادی وارد شبکه شود یا حمله هایی مانند DoS ایجاد شود.

Flexibility : شبکه طراحی شده باید توانایی تغییرات را داشته باشد به طور مثال یک سرویس به این شبکه اضافه شود یا توان شبکه را افزایش دهیم این تغییرات باید بودن ایجاد وقفه در عملکرد و اختلال در سرویس دهی صورت پذیرد.

ب – گراف جهت‌دار غیرمدور(DAG)

این فناوری بر اساس تئوری گراف‌ها عمل می‌کند. DAG گرافی است که هیچ دوری در آن وجود ندارد و تمامییال‌های آن یک طرفه هستند. در این نوع گراف، با شروع پیمایش از گره امکان بازگشت به آن وجود ندارد. این فناوری جایگزین ارزشمندی برای رویکرد سنتی دفتر کل توزیع شده ارائه می‌دهد که با کاهش هزینه تراکنش، بهبود شفافیت و افزایش کارایی همراه است. DAGیک پلتفرم پایدار در اختیار شرکت‌ها قرار می‌دهد تا تمامیت تراکنش‌ها و دارایی‌های دیجیتال خود را حفظ نمایند. DAG نیز از یک شبکه با تعدادی از گره‌های مختلف تشکیل شده است که تراکنش‌ها را تایید می‌کنند. هر تراکنش جدید شبکه نیازمند تأیید حداقل دو تراکنش قبلی است تا با موفقیت ثبت شود. (Kotilevets & et.al, 2018).گراف مدور نوعی گراف یا شبکه‌ای از گره‌های متصل است که اطلاعات می‌توانند در مسیرهای [یال‌های] مختلف موجود از یک گره به گره دیگر منتقل شوند و با گذر از گره‌های میانی دوباره به گره اصلی بازگردند. اطلاعات باید تنهایک بار از گره‌های میانی موجود در مسیر عبور کنند تا یک گراف مدور تشکیل شود. گراف‌های غیرمدور، گراف‌هایی هستند که هیچ دوری در آن‌ها وجود نداشته باشد. اگر برای هر یک از مسیرها، دریک جهت حرکتییک طرفه تعیین شود و بین هرکدام از گره‌ها تنها یک مسیر وجود داشته باشد گراف جهت‌دار غیرمدور تشکیل می‌شود. این بدین معنی است که با شروع از یک گره نمی‌توان از تمامی گره‌های گراف عبور کرد. حرکت در گراف جهت‌دار تنها در یک مسیر امکانپذیر است. گراف، بیانگریک مرتبسازی توپولوژیک است که هر گره در یک نظم خاص قرار دارد. ساختارDAG شامل رئوسی (گره) است که توسط یال‌ها (مسیرها) به یکدیگر متصل شدهاند. الگوریتم اصلی DAGمرتبسازی توپولوژیکی نامیده می‌شود و این بدان معنی است که هر یال از آخرین گره موجود به گره جدید

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

وصل می‌شود. و چون به اینصورت عمل می‌کند و برای تایید تراکنش برخلاف بلاکچین دیگر نیازی است از اول تمام گره‌ها تایید کنند لذا انجام تایید پویای تراکنش سریعتر انجام می‌شود(S. Lee, 2018).

ج –الگوریتم بررسی کد از نظر معنایی

پایه و اساس این الگوریتم، آموزش یک طبقه‌بند، برای بررسی بین کدی است بین کدی که نمونه ای از الگوی دارای باگ می‌باشد با کدی که از دیدگاه Name-based چنین باگی را ندارد. که الگوی دارای باگ، به این مفهوم است که ما دارای یک کلاسی هستیم که از نظر کدنویسی دارای باگ‌های مشابه می‌باشند چرا که معمولا قاعده خاصی را نقض می‌کنند. برای مثال می‌توان از تعویض تصادفی آرگومان‌های منتقل شده با یک تابع، فرخوانی اشتباه یک API و استفاده از یک عمل‌کننده باینری اشتباه نام برد.

با توجه به مجموعه‌ای از کدهای نوشته شده[1]، ایجاد و استفاده از تشخیص دهنده باگ بر اساس DeepBugs شامل چند مرحله است:

۱- داده‌های آموزشی را از مجموعه کدهای نوشته شده استخراج و تولید می‌کنیم. در این مرحله احتمالا کدهایی که درست باشند برچسب ، درست و کدهایی که غلط باشند، برچسب، غلط دریافت می‌کنند، با این فرض که اکثر کدهای موجود ، بعد از رعایت اصول برنامه نویسی صحیح هستند.

۲- ارائه دادن کد بصورت یک بردار. در این مرحله هر کد به صورت یک بردار ترجمه می‌شود. برای حفظ اطلاعات معنایی که توسط نام‌های شناسه و مشخصه، منتقل می‌شود، شناسه ها را از طریق یک شبکه عصبی به نام Word2Vecبه یک بردار معنایی[2] نگاشت می‌دهیم.

۳- برای تشخیص نمونه‌های صحیح و نادرست، مدل را آموزش میدهیم. تا بین کدهای دو کلاس درست و غلط تمایز قائل شود. این طبقه بند در این الگوریتم یادگیری ماشین، یک کلاس بند براساس شبکه عصبی پیشرو[3] است.

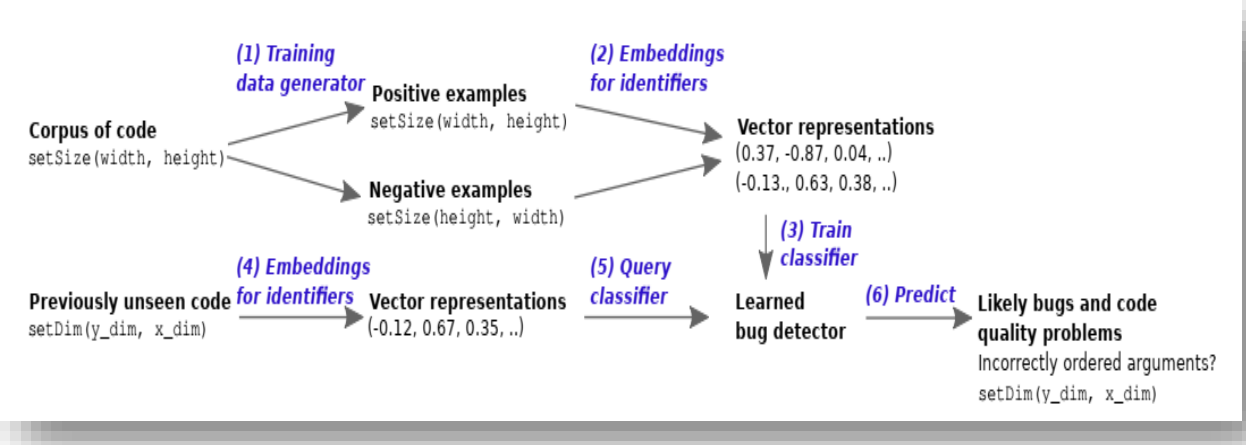
۴- این مرحله، مرحله پیشبینی است. به این مفهوم که باید پیشبینی کند که کد نوشته شده در کدام کلاس قرارمیگیرد. و اگر کد را در کلاس نادرست کلاس‌بندی کند، به توسعه‌دهنده، هشدار را گزارش می‌دهد(مرحله

[1]corpus of code
[2]semantic vector
[3]feedforward neural network

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

۴ تا ۶ در شکل(Pradel & Sen, 2018).

به طور خلاصه الگوریتم بالا به صورت خلاصه در شکل زیر نشان داده شده است:



در بحث استاندارد سازی کد همانطور که در قسمت روش تحقیق به طورخلاصه و به طور مفصل آن در پیوست الف توضیح داده شده است به طورکلی همه‌ی زبان‌های برنامه نویسی یک اصول کلی دارند که قاعده و اساسی است که در نهایت منجر به یک کد منبع خوب می‌شود که بدون هیچ خطای معنایی و منطقی و پردازش اجرا می‌شود. استفاده از ابزارهای چک کردن کد[1]، یکی از راه‌های رسیدن به یک کد استاندارد است.

د – تایید از طریق VM AI

همانطور که در قسمت روش تحقیق بیان شد، سه روش فنی برای تحقیق و بررسی مکانیزم‌های فرآیند تایید قرارداد هوشمند وجود دارد ولی به دلیل اینکه ماشین مجازی، برای اجراییک برنامه واحد طراحی شده است، از آن به عنوان مرکز پردازش و انجام فرآیندها استفاده شده است. که به این معناست که صرفاً از یک فرایند خاص پشتیبانی می‌کند. یک ویژگی مهم یک ماشین مجازی، این است که نرم‌افزاری که درون آن در حال اجراست، با منابع و سطوح انتزاعی که توسط ماشین مجازی اعمال می‌شود،محدود شده‌است –یعنی نمی‌تواند از دنیای مجازی خود خارج شود– و همچنین می‌توان از مجازی سازی برای سرورهای مرحله گذر استفاده کنید که معمولاً برای بررسی تغییرات در برنامه‌ها و آزمایش سیستم‌ها قبل از اعمال آن ها در محیط واقعی، استفاده می شوند ولذا در

[1] محصولات نرم افزاری هستند که زمان کامپایل را بررسی می کنند که آیایک برنامه نرم افزاری به مجموعه خاصی از قوانینیک استاندارد کدگذاری پایبند است. بدون وجود چنین پیش نویس کد ، اجراییک کدگذاری استاندارد در یک سازمان احتمالاً شکست خواهد خورد. دو دلیل اصلی برای این امر وجود دارد: (۱) تعداد قوانین موجود در استاندارد رمزگذاری معمولاً آنقدر زیاد است که هیچ کس نمی تواند همه آنها را یادآوری کند (به جز نویسنده) و (۲) برخی از قوانین حساس به متن که خواستار بازرسی چندین پرونده هستند. بسیار دشوار است که توسط انسان‌ها بررسی شود.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

پروتکل خود از روش فنی ماشین مجازی به عنوان مرکز و سیستم عامل پروتکل خود استفاده می‌کنیم . VM AI باعث افزایش سرعت، انعطاف‌پذیری، امنیت و هو شمندی در اجرای قرادادهای هو شمند می شود. این VM قادر است ۵۰ هزار تراکنش در ثانیه را پشتیبانی کند[1] قراردادهای هوشمند در VM AI از فرآیند پردازش طبیعی[2] و الگوهای مبتنی بر یادگیری عمیق برای Auto code استفاده می‌کنند. به همین جهت در انجام تراکنش‌ها و دقت در انجام تایید فرآیند قراردادها به مراتب بهتر عمل می‌کند. VM AI یک اکو سیستم AI-Training است که در شبکه شبه نامتمرکز و توزیع‌شده، برای اطمینان از تایید داده‌های مربوط به دارایی و مدیریت منابع قدرت محاسباتی ساخته شده است در این ماشین مجازی از مقادیر زیادی داده با کیفیت و حجیم برای آموزش مدل‌های هوش مصنوعی به کارگرفته‌شده در ماشین مجازی استفاده می‌شود. و تمام کاربرانی که در محاسبه و تکمیل فرآیندها و قراردادها شرکت می‌کنند متنا سب با قوانین موجود در کتابخانه قانون و با توجه به نوع تراکنش و نوع قرارداد پاداش خواهند گرفت. در نظر گرفتن این ماتریس در پی حل ۴ مشکل اصلی بلاک‌چین است که سرعت آهسته، موانع زیاد برای ورود، و اتلاف عظیم انرژی و عدم انطاف پذیری مطلق می‌باشد. یکی ازمزایای استفاده از VM AI این است که به کاربران این امکان را می‌دهد که الگوهای قراردادی به زبان‌های مختلف را استفاده کنند که این امکان با استفاده از الگوریتم‌های مرتبط با پردازش زبان طبیعی و یادگیری عمیق امکان‌پذیر می‌شود.

ذ – موارد مربوط به تجزیه و تحلیل معنایی

این مسائل عبارتند از:

۱- عدم موفقیت در مواجهه با شرایط قراردادهای ترکیبی، ناشی از کدهای نادرست و کامل نشده.

۲- تفاوت نسبتا زیاد بین اهداف شخصی و در نظر گرفته شده در قرارداد، با کد واقعی و نوشته شده.

۳- از آن جایی که قراردا به صورت توزیع شده اجرامی‌شود، یک تفاوت در توالی کد اجرا شده در بین همه‌ی گره‌ها وجود دارد. درنتیجه،زمانی که یک آنومالی در قرارداد محلی اتفاق می‌افتد، سایر قراردادها می توانند انواع حالت های این قرارداد را فراخوانده یا تغییر دهند ، و این باعث بروز مشکلات مختلف غیر مرتبط با امنیت می شود.

در هسته VM AI،محاسبات به کمک AI انجام می‌شود و در تمام سطوح و ویژگی‌های VM AI هوش مصنوعی وجود دارد. بنابراین برای تایید قراردادها، تایید رسمی، همچنین روش ارزیابی محدودیت پویا، بر اساس

[1] البته این مقدار بدون در نظر گرفتن گراف جهت دار غیر مدور که موجب افزایش این مقدار و سرعت انجام تراکنش‌ها می‌شود.

[2] NLP

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

هوش مصنوعی می‌باشد تا مسائل امنیتی را حل کنند.

۴- استفاده از pattern matching برای بدست آوردن محدودیت‌های واقعی تقاضای کاربران: pattern matchingبر اساس abstract syntax tree(AST) شکل گرفته شده، از طریق تجزیه و تحلیل معنایی انجام می‌شود تا مدل‌های پایه ای احتمالی از تراکنش‌هایی که توسط کاربران انجام می‌شود بدست آید. این روش می‌تواند تطبیق محلی اکثر شاخه های انتزاعی و نحوی را به روشی ثابت بدست آورد. VM مدل‌های نامزد ونماینده یا مدل‌های ترکیبی را بر اساس گستره specific matching، مشخص می کند تا بسته شدن[1] و تایید معاملات[2] و تراکنش‌ها بر اساس آن مدل صورت بگیرد.

۵- مدل طبقه بند درخت انتزاعی که بر اساس تجزیه و تحلیل معنایی استاتیک، شکل گرفته، بر اساس طبقه‌بند Bayes، که موتور VM's AI است، برای تعیین اینکه هر بخش از شاخه های درخت متعلق به کدام دسته مربوطه می باشد، استفاده می‌شود. در VM، با این وجود، برای هر دسته از معاملات باید محدودیت‌هایایستا و پویا وجود داشته باشد.

۶- به دست آوردن همه‌ی محدودیت‌های پویا و استاتیک قرارداد جاری، براساس نتایج pattern matching و نتایج طبقه‌بندی هوش مصنوعی، بلافاصله قبل از تایید کدهای قرارداد بر اساس این محدودیت‌ها، و تایید رسمی و پویا بر اساس این نتایج انجام می‌پذیرد.برای قراردادهایی که تطبیق مدل از بین نرود یا طبقه بندی انجام نشود ، VMیک هشدار امنیتی در برابر قابلیت اطمینان قرارداد به کاربران می دهد، و در حین اجرای برر سی های دقیق‌تر را انجام می‌دهد.

ر – الگوریتم هش

ویژگی‌های معمول توابع هش عبارتند از:

- **طول ثابت خروجی (مقدار هش)**

تابع هش، داده با طول متغیر را به طول ثابت تبدیل می کند.

معمولا اندازه هش بسیار کوچک‌تر از ورودی است، بنابراین توابع هش را گاهی با نام توابع فشرده‌ساز

[1]closure
[2]affirmation

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

می‌شناسند.

تابع هش با خروجیn بیتی، را تابع هش nبیتی می‌نامند.

- **اثربخشی فرآیند**

به طور کلی برای هر تابع هش h با ورودیX، محا سبه h(x)، یک عملیات سریع ا ست. انجام محا سبات در توابع هش بسیار سریعتر از رمزنگاری متقارن هستند.

برای اینکه تابع هش یک ابزار موثر رمزنگاری باشد، بایستی شرایط زیر را برآورده کند:

شرط اول

این شرط بیان می‌کند که تابع هش بایدیک تابع یکطرفه با شد. به بیان دیگر اگر یک تابع هش hیک مقدار هش z را تولید کرد، پیدا کردن یک مقدار x که هش آن با zیکی شود، بایستی فرآیند دشواری باشد. این خاصیت باعث محافظت از پیدا کردن مقدار ورودی هش توسط حمله کننده‌ای می‌شود که مقدار هش را در اختیار دارد.

شرط دوم

اگریک ورودی و هش آن را در اختیار داشته باشیم، پیدا کردن یک ورودی متفاوت که همان مقدار هش را بدهد، بایستی د شوار با شد. به بیان دیگر اگر یک تابع هش h برایک ورودیx، یک مقدار هش h(x) را بدهد، پیدا کردن مقدار ورودی دیگری که h(y) = h(x) شود، بایستی د شوار با شد. این ویژگی باعث می شود در برابر حمله کننده‌ای که یک مقدار هش ورودی و هش آن را دارد و می‌خواهدیک مقدار متفاوت را به عنوان مقدار ورودی اصلی جایگزین آن کند، محافظت شود.

شرط سوم

پیدا کردن دو ورودی متفاوت با هر طولی که منجر به یک هش مشابه شود، بایستی دشوار باشد. این ویژگی با عنوان «تابع هش بدون تصادم» نیز شناخته می‌شود. به بیان دیگر برایک تابع هش h، پیدا کردن دو ورودی متفاوت x و y به طوری که h(x) = h(y) شود، باید د شوار با شد. چون تابع هش یک تابع فشرده ساز با خروجی ثابت است، نداشتن تصادم برای آن غیر ممکن است. این ویژگی تنها بیان می‌کند که پیدا کردن این تصادم‌ها باید بسیار سخت باشد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ز – الگوریتم DFS

الگوریتم از ریشــه شــروع می‌کند (در گراف‌ها یا درخت‌های بدون ریشــه راس دلخواهی به عنوان ریشــه انتخاب می‌شود) و در هر مرحله همسایه‌های رأس جاری را از طریقیال‌های خروجی رأس جاری به ترتیب بررسی کرده و به محض روبه‌رو شدن با همسایه‌ای که قبلاً دیده نشده باشد، به صورت بازگشتی برای آن رأس به عنوان رأس جاری اجرا می‌شـود. در صـورتی که همهٔ همسـایه‌ها قبلاً دیده شـده باشـند، الگوریتم عقب‌گرد می‌کند و اجرای الگوریتم برای رأســی که از آن به رأس جاری رســیده‌ایم، ادامه می‌یابد. به عبارتی الگوریتم تا آنجا که ممکن اســت، به عمق بیشــتر و بیشــتر می‌رود و در مواجهه با بن‌بســت عقب‌گرد می‌کند. این فرایند تا زمانی که همهٔ رأس‌های قابل دستیابی از ریشه دیده شوند ادامه می‌یابد.

همچنین در مسائلی که حالات مختلف متناظر با رئوس یک گراف‌اند و حل مسئله مستلزم یافتن رأس هدف با خصوصیات مشخصی است، جستجوی عمق اول به صورت غیرخلاق عمل می‌کند. بدین‌ترتیب که هر دفعه الگوریتم به اولین همســایهٔ یک رأس در گراف جســتجو و در نتیجه هر دفعه به عمق بیشــتر و بیشــتر در گراف می‌رود تا به رأسی برسد که همهٔ همسایگانش دیده شده‌اند که در حالت اخیر، الگوریتم به اولین رأسیبر می‌گردد که همسـایهٔ داشـته باشـد که هنوز دیده نشـده باشـد. این روند تا جایی ادامه می‌یابد که رأس هدف پیدا شـود یا احتمالاً همهٔ گرافپیمایش شـود. البته پیاده‌سـازی هوشـمندانهٔ الگوریتم با انتخاب ترتیب مناسـب برای بررسـی همسـایه‌های دیده نشـدهٔ رأسـجاری به صـورتی که ابتدا الگوریتم به بررسـی همسـایه‌ای بپردازد که به صـورت موضـعی و با انتخابی حریصـانه به رأس هدف نزدیک‌تر اسـت، امکان‌پذیر خواهد بود که معمولاً در کاهش زمان اجرا مؤثر اسـت.از دیدگاه عملی، برای اجرای الگوریتم، از یک پشـته اسـتفاده می‌شـود. بدین ترتیب که هر بار با ورود به یک رأس دیده نشــده، آن رأس را در پشــته قرار می‌دهیم و هنگام عقب‌گرد رأس را از پشــته حذف می‌کنیم؛ بنابراین در تمام طول الگوریتم اولین عنصر پشته رأس در حال بررسی است. جزئیات پیاده‌سازی در ادامه خواهد آمد.وقتی در گراف‌های بزرگی جستجو می‌کنیم که امکان ذخیرهٔ کامل آن‌ها به علت محدودیت حافظه وجود ندارد، در صورتی که طول مسیر پیمایش شده توسط الگوریتم که از ریشه شروع شده، خیلی بزرگ شود، الگوریتم با مشکل مواجه خواهد شد. در واقع این راه‌حل ساده که «رئوسی را که تا به حال دیده‌ایم ذخیره کنیم» همیشـه کار نمی‌کند. چرا که ممکن اسـت حافظهٔ کافی برای این کار نداشـته باشـیم. البته این مشـکل با محدود کردن عمق جســتجو در هر بار اجرای الگوریتم حل می‌شــود که در نهایت به الگوریتم جســتجوی عمق اول عمیق‌کننده تکراری خواهد انجامید(Thomas & et.al 2015).

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

ه – الگوریتم GAN

یادگیری ما شین، ا ستخراج دانش از داده ها و ا ستفاده از آن برای هو شمند کردن ما شین ا ست. رو شی که طلایه دار پیشرفتیادگیری ماشین محسوب می شود، قطعا یادگیری عمیق است. یادگیری عمیق شاخه های مختلفی دارد که یکی از آن ها GAN، یا شبکه های مخالف مولد (Generative Adversarial Networks) است. این نوع از شبکه های عصبی در سال ۲۰۱۴ توسط گودفلو در کنفرانس NIPS ارائه شد.مدل‌های مولد بر اساس برآورد چگالی کار می‌کنند و در این مدل‌ها بر اساس اینکه تابع برآورد چگالی‌شان به چه صورت تعریف می‌شوند به دو نوع تقسیم می‌شوند. برخی از این مدل‌ها تابع برآورد چگالی آن‌ها به صورت صریح تعریف می‌شود. مانند VAEs، PixelRNN، PixelCNN و ... همین‌طور مدل‌هایی مانند(Generative Adversarial Networks(GANs از جمله مدل‌هایی به شمار می‌روند که تابع برآورد چگالی آن‌ها به صورت صریح تعریف نمی‌شود بلکه به صورت ضمنی تعریف می‌شود.

همانطور که گفتیم ازدو شبکه RNN تشکیل شده در واقع در واقع رقابت این دو شبکه مانند یک بازیminimax است که سود هر بازیکن در ضرر بازیکن مقابل است و تابع objective در این مدل‌ها به صورت زیر تعریف می‌شود:

Minimax objective function:

$$\min_{\theta_g} \max_{\theta_d} \left[\mathbb{E}_{x \sim p_{data}} \log \underbrace{D_{\theta_d}(x)}_{\text{Discriminator output for real data x}} + \mathbb{E}_{z \sim p(z)} \log(1 - \underbrace{D_{\theta_d}(G_{\theta_g}(z))}_{\text{Discriminator output for generated fake data G(z)}}) \right]$$

Discriminator outputs likelihood in (0,1) of real image

عبارت اول برای زمانی است که نمونه از توزیع داده‌های آموزش است و در اینجا فقط Discriminator نقش دارد و با تاثیر ۱ قرار دادن این عبارت(چون از مجموعه آموزش آمده)تلاش می‌کند این تابع را ماکزیمم کند و در واقع اینکه نمونه از نمونه‌های آموزش باشد، بهترین سناریو برایDiscriminator است و در عبارت دوم Discriminator برای ماکزیمم کردن تابع objective برای خودش، سعی می‌کند برای عبارت دوم تاثیر ۰ قائل شود چون از توزیع داده‌های تولید شده توسط Generator است. به این صورت که ورودییک بردار نویز به Generator داده می شود و این شبکه نمونه را تولید می‌کند و خروجیGenerator به شبکه Discriminator داده می‌شود. شبکهGenerator سعی بر این دارد که این تابع objective را مینیمایز کند به این صورت که تلاش می‌کند برای عبارت دوم که خروجی خودش را به Discriminator می‌دهد تاثیر ۱ قائل شود(انگار به

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

نحویDiscriminator را گول می‌زند که نمونه‌ای که تولید کرده از نمونه‌های واقعیا ست). همچنین وا ضح ا ست که شبکه Generator فقط در این عبارت تابع objective نقش دارد.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

Abstract:

Given the importance of the bank in the economic development and growth of countries, improving the performance of banks in terms of different performance indicators can lead to achieving the set goals. With the advent of new technologies such as artificial intelligence, blockchain, financial technology, and in recent years, banks have been using these technologies to improve their performance in the areas mentioned to reduce their costs and increase their net profit. One of these technologies is smart contracts. Since smart contracts are on the blockchain platform, in addition to their advantages, they have a number of advantages such as high processing power and scalability, incompatibility with traditional systems, the need for high regulatory technological evaluations, the difficulty of developing consensus and cryptographic protocols. Therefore, a new concept with a similar but more flexible nature, called the intelligent contract, was introduced, which relied more on artificial intelligence and its algorithms than on a completely decentralized blockchain-like structure. But since the concept is entirely new, we have examined the structure and nature of each of these contracts. By fully examining how smart contracts work, we came up with the principles behind the theoretical foundations for developing intelligent contracts. These principles include contract and network contexts, preventive protection, ongoing process verification, dynamic node verification, and rational judgment, and combined assessments and checks based on the law library. And based on these principles, in Chapter 4, we propose a protocol for the development of intelligent contracts. And finally, with respect to the proposed protocol, we outline how these types of contracts work based on the proposed protocol in the field of payment and peer-to-peer lending in the banking system. The use of such contracts seems more reasonable given the current conditions in Iranian banking and one of the main reasons for this is the flexibility of these contracts and their compatibility with traditional banking systems.

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهاده‌ها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.

Kharazmi University
Faculty of Economic

Department of Economics and Islamic Banking

Thesis Title:

Designing a Smart Contract Model in a Useless Banking System: An Application of Artificial Intelligence Models

By:
Samaneh Esfahani

Supervisor :
Dr Hossein Amiri

Advisor :
Pr Ahmad Jafari SAmimi

دسترسی به این مدرک بر پایهٔ آیین‌نامهٔ ثبت و اشاعهٔ پیشنهادهها، پایان‌نامه‌ها، و رساله‌های تحصیلات تکمیلی و صیانت از حقوق پدیدآوران در آنها (وزارت علوم، تحقیقات، فناوری به شمارهٔ ۱۹۵۹۲۹/و تاریخ ۱۳۹۵/۹/۶) از پایگاه اطلاعات علمی ایران (گنج) در پژوهشگاه علوم و فنـــاوری اطلاعات ایران (ایرانداک) فراهم شده و استفاده از آن با رعایت کامل حقوق پدیدآوران و تنها برای هدف‌های علمی، آموزشی، و پژوهشی و بر پایهٔ قانون حمایت از مؤلفان، مصنفان، و هنرمندان (۱۳۴۸) و الحاقات و اصلاحات بعدی آن و سایر قوانین و مقررات مربوط شدنی است.