فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال هشتم، شماره ۹۴، پاییز ۱۴۰۳، ص ۱۰۳۰-۱۰۰۷

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

بررسی جنبه‌های فنی مهم قراردادهای هوشمند مبتنی بر بلاک‌چین در صنعت مالی در جهان و ارائه بهترین شیوه‌های بهینه‌سازی عملکرد و بهبود مقیاس‌پذیری در بانکداری الکترونیکی

رسول چراغ سحر [۱]
محمد هادی بحرانی [۲]
محمد ساسان‌پور [۳]

تاریخ دریافت: ۱۴۰۳/۰۷/۰۱ تاریخ چاپ: ۱۴۰۳/۰۹/۱۵

چکیده

زمینه تحقیقات صنعتی و محاسباتی در دهه های گذشته در جهات مختلف متحول شده است. قرارداد هوشمند مبتنی بر بلاک چین به دلیل ویژگی‌های فنی متمایز آن مانند ذخیره‌سازی غیرمتمرکز تراکنش‌ها، اجرای مستقل کدهای قرارداد و ایجاد غیرمتمرکز اعتماد، به عنوان یک علاقه تحقیقاتی قابل توجه، مورد بررسی محققان بسیاری بوده است. قراردادهای هوشمند مبتنی بر بلاک چین می‌توانند معماری کاری تقریباً همه صنایع را به سمت استانداردهای خدماتی بالاتر تغییر دهند. مطالعه حاضر با هدف شناسایی جنبه‌های فنی مهم قراردادهای هوشمند مبتنی بر بلاک چین در صنعت مالی و ارائه بهترین شیوه های بهینه سازی عملکرد و بهبود مقیاس پذیری در بانکداری الکترونیک در ایران انجام شده است. این مطالعه در دسته مطالعات کتابخانه ای/کیفی با هدف توسعه ای- اکتشافی قرار دارد. نتایج بیانگر شناسایی جنبه‌های فنی قراردادهای هوشمند مبتنی بر بلاک چین برای بهبود بیشتر و تشدید قابلیت‌های آن در بانکداری الکترونیک در ایران می باشد.

واژگان کلیدی

قراردادهای هوشمند مبتنی بر بلاک‌چین، بانکداری الکترونیک، بهینه سازی عملکرد، بهبود مقیاس پذیری

[۱] عضو هیات علمی وابسته، گروه مدیریت بازرگانی، دانشگاه آزاد اسلامی، واحد یاسوج، ایران. Rasol.chraghsahar@gmail.com

[۲] دانشجوی دکتری مدیریت بازرگانی، گروه مدیریت بازرگانی، دانشگاه آزاد اسلامی، واحد یاسوج، ایران. Mohammadhadibahrani@yahoo.com

[۳] دانشجوی دکتری مدیریت بازرگانی، گروه مدیریت بازرگانی، دانشگاه آزاد اسلامی، واحد یاسوج، ایران. M.sasanpuor@gmail.com

مقدمه

«بلاک‌چین»[1] یک سیستم غیرمتمرکز است که می تواند اشتراک گذاری اطلاعات را تسهیل کند. از بلاک‌چین برای ارتباط مستقیم اطلاعات با کاربران شبکه استفاده می شود. به دلیل مکانیزم امنیتی قوی، فناوری بلاک‌چین برای مشاغل مختلف جذاب است. فناوری بلاک چین می‌تواند مشکل وجود زمان و نیروی کار را را با امکان ثبت بی‌درنگ اطلاعات معاملات، قراردادی و سایر اطلاعات در یک دفتر کل مشترک برطرف کند. این به این معنی است اولاً تأیید خودکار انطباق قانونی انجام خواهد شد؛ ثانیاً اثربخشی عملیات سازمان به میزان قابل توجهی افزایش خواهد یافت و ثالثاً تراکنش‌های داده و هویت‌ها ایمن‌تر خواهد شد[2]. با پیشرفت انقلاب دیجیتال، بلاک‌چین می تواند به حفظ تعادل بین فناوری، داده های کاربر و حریم خصوصی کمک کند. تاکید بر محرمانگی ممکن است افزایش یابد در حالی که مدیریت داده ها نیز ممکن است سودمند باشد. بلاک چین بر اساس یک مفهوم دفتر کل توزیع شده است که هر تراکنش را ثبت می کند و جدول زمانی و صحت آن اطلاعات را در یک شبکه جهانی امن و بدون دستکاری حفظ می کند[3].

«هوش مصنوعی»[4] و بلاک چین دو فناوری بسیار متفاوت با کاربردهای بسیار متنوع هستند. هوش مصنوعی به داده های امنی که قابل دسترسی یا تکرار نیستند متکی است و یک سرویس بسیار متمرکز است. مزایای متعددی از همکاری این دو فناوری به ویژه در بخش مالی ناشی می شود[5]. فناوری بلاک چین امکان ارتباط یکپارچه بین طرفین درگیر در تراکنش‌ها را فراهم می‌کند و نیاز به نگهداری سوابق در فرآیندهای سفارش به نقد، ثبت به گزارش و خرید تا پرداخت را از بین می‌برد[6].

«قراردادهای هوشمند»[7] فعال شده توسط فناوری بلاک چین می‌تواند به همه طرف‌ها کمک کند تا توافق‌نامه‌های مالی الزام‌آوری ایجاد کنند که پس از برآورده شدن همه پیش‌نیازها، با تضمین اجرا می‌شوند. همانند قراردادهای سنتی، قراردادهای هوشمند شرایط را در زمان واقعی و بدون ابهام بر روی یک زنجیره بلوکی اجرا می‌کنند و واسطه‌ها را قطع می‌کنند و مسئولیت همه طرف‌ها را به گونه‌ای افزایش می‌دهند که قراردادهای معمولی نمی‌توانند[8]. از آنجایی که یک شبکه غیرمتمرکز از رایانه ها وظایف واسطه را از طریق اینترنت انجام می دهد، راه حل دفتر کل توزیع شده به شخص ثالث قابل اعتماد نیاز ندارد. هر تراکنش در یک دفتر کل دیجیتال ثبت می شود، برای هر عضو شبکه منتشر می شود و در دسترس عموم قرار می گیرد. شبکه می‌تواند مالکیت دارایی و تراکنش‌های شفاف را تأیید کند، زیرا هر یک از

[1] Blockchain
[2] (Lahkani et al, 2020. No.3.)
[3] (Chang et al, 2020. No.2.)
[4] Artificial intelligence
[5] (Poongodi et al, 2020. No.14.)
[6] (Javaid et al, 2022. No.2.)
[7] Smart contracts
[8] (Kowalski et al, 2021. No.7.)

اعضای شبکه یک نسخه قانونی از دفتر دارند که آن را به مکانیزم امن‌تری نسبت به رویکرد دفتر کل مرکزی موجود تبدیل می‌کند[۱].

با توجه به مرور ادبیات پیرامون فناوری‌های دیجیتال، مشاهده می شود که این نوع از فناوری، فرصت های جدیدی را برای افزایش همکاری در بخش های مختلف صنعت مالی به خصوص در بخش بانکی ایجاد کرده است. رویه‌های حسابداری بانکداری در جهان امروز، توسط برنامه‌های کاربردی «مبتنی بر ابر»[۲] با تحلیل‌های تخصصی برای موارد استفاده خاص مانند حساب‌های پرداختنی و دریافتنی، مدیریت قرارداد، گزارش‌دهی و موارد دیگر تغییر یافته است. امن‌ترین روش‌های پرداخت، پول نقد، چک‌های نقدی و حواله‌های بانکی است. با این حال اینها نمی‌توانند حواله‌های سیمی را که زمان و پول نقد می‌طلبد، جبران کند. پرداخت هایی که با استفاده از فناوری بلاک‌چین انجام می شود، این مشکلات را برطرف می کند و اعتماد مشتری را افزایش می دهد. همچنین این فناوری، انتقال پول نقد بین مؤسسات مالی را در زمان واقعی امکان پذیر می کند، اصطکاک را کاهش می دهد و تسویه حساب را تسریع می کند. این فناوری پتانسیل اتوماسیون را ارائه می دهد و برای ردیابی تراکنش ها ایده آل است. ارائه دهندگان خدمات مالی در بخش بانکداری می توانند از قراردادهای هوشمند برای نظارت بر پرداخت ها و تحویل های مشتریان استفاده کنند[۳]. با توجه به موارد مطرح شده، در این مطالعه به بررسی جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاک‌چین در صنعت مالی در جهان پرداخته خواهد شد. همچنین بخش دوم مطالعه به ارائه بهترین شیوه های بهینه سازی عملکرد و بهبود مقیاس پذیری در بانکداری الکترونیکی با توجه به استفاده از قرارداد های هوشمند مبتنی بر بلاک چین می پردازد.

مبانی نظری

در حال حاضر هدف موسسات مالی و بانک ها خودکارسازی اطلاعات، داده ها و تراکنش های پولی خود است[۴]. علاوه بر این، این هدف با چالش‌های زیادی روبرو است زیرا اتوماسیون به معنای حملات و هک‌های خطرناک بسیاری است تا زمانی که اطلاعات در اینترنت یا از طریق بانکداری الکترونیک در دسترس باشد؛ بنابراین، اعتماد و امنیت بین مشتریان و ذینفعان بسیار مهم است. بانک‌ها و سازمان‌های مالی مختلف دائماً تحت فشار هستند تا تعادلی بین امنیت سیستم، هزینه‌ها و توانایی تکمیل رویه‌ها در زمان واقعی ایجاد کنند[۵] که این یک چالش بزرگ است زیرا تهدیدات سایبری به طور فزاینده‌ای در حال توسعه هستند و به طور مداوم شکل‌های جدیدی به خود می‌گیرند. از اینرو صنعت مالی در جهان پیشرفته امروز به فناوری هایی همچون قرارداد های هوشمند و بلاک چین روی نموده است. این بخش از مطالعه شامل بخش فرعی ۱,۲. است که بلاک چین و موارد استفاده در بانکداری الکترونیکی را توضیح می دهد. زیر بخش ۲,۲. قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی را خلاصه می کند. همچنین بخش فرعی ۳,۲. به مشارکت اصلی

[1] (Dong et al, 2023. No.3.)
[2] Cloud-based
[3] (Wang, Wu, 2021. No.3.; Wang et al, 2022. No.2.)
[4] (Garg et al, 2023. No.11.)
[5] (Javaid et al, 2022. No.3.)

مطالعه حاضر می پردازد و به بررسی جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی بروز جهان پرداخته خواهد پرداخت.

پیشینه ای در مورد بانکداری الکترونیکی و روش های مورد استفاده

این بخش در بخش های فرعی سازماندهی شده است که جزئیات رویه های بانکداری الکترونیک و اقدامات امنیتی را ارائه می دهد. هدف ما محافظت از تراکنش‌ها در برنامه‌های بانکداری الکترونیکی است تا یک نمای کلی کاملاً ذهنی از استراتژی‌های بانکداری الکترونیک ارائه کنیم.

➢ آداب بانکداری الکترونیکی

با گذشت زمان و به دلیل توسعه فناوری، روش‌های فنی و الکترونیکی نسبت به روش‌های سنتی در بانک‌ها و مؤسسات مالی به کار گرفته شد[1]. از این رو اصطلاح بانکداری الکترونیکی به عنوان راهی سریع، آسان و کارآمد برای دسترسی الکترونیکی مردم به حساب های بانکی خود ارائه شده است. علاوه بر این، بانکداری الکترونیکی به افراد این مزیت را می دهد که به حساب های خود در ۲۴ ساعت شبانه روز و ۷ روز هفته دسترسی داشته باشند.

بلاک چین و موارد استفاده در بانکداری الکترونیکی

فناوری بلاک چین، به عنوان یک فناوری تکاملی برای تخمین اهداف امنیتی، حفاظت از داده ها و حذف نقش های شخص ثالث در طول تراکنش های پولی پیشنهاد شده است[2]. تراکنش ها از طریق فرآیند «همتا به همتا»[3] انجام می شود. سپس، کل فرآیند با استفاده از «اصل هش»[4] در یک دفتر کل غیرمتمرکز ذخیره می شود؛ بنابراین، از زمان ایجاد فناوری بلاک‌چین، این فناوری به کاهش استثنایی در هزینه در مقایسه با مزایای قابل توجهی که ارائه می دهد، ادامه داده است[5]. یک بلاک چین از بلوک ها، زنجیره ها، گره ها و گره های اصلی تشکیل شده است. گره ها مسئول بلوک های شبکه هستند. افزودن بلاک ها به بلاک چین یک عملیات چالش برانگیز است که نیاز به حل مسئله ریاضی دارد. ظرفیت شبکه بلاک چین برای گسترش بی‌پایان با حل معماهای چالش‌برانگیز ریاضی محدود شده است. هک، تقلب یا تغییر شبکه بلاک چین به دلیل منحصر به فرد بودن کدهای هش، عملا غیرممکن است. بلاک چین یک دفتر کل توزیع شده است که در آن یک کپی از دفتر کل در هر کامپیوتر متصل نگهداری می شود. این شبکه زنجیره بلوکی نامیده می شود زیرا از بلوک های به هم پیوسته تشکیل شده است که سوابق تراکنش ها را ارائه می دهند. ایده و عملکرد ارزهای دیجیتال به شبکه بلاک چین بستگی دارد[6]. طبق مطالعات انجام شده در مورد بانکداری الکترونیکی و استاندارد مراقبت از مشتری، مردم خدمات بانکداری الکترونیکی را به سیستم های بانکداری سنتی ترجیح می دهند. در نتیجه،

[1] (Garg et al, 2023. No.4.)
[2] (Thommandru, Chakka, 2023. No.1.)
[3] peer-to-peer
[4] hashing principle
[5] (Riad, Elhoseny, 2023. No. 14.)
[6] (Scott et al, 2017. No.3.)

توسعه‌دهندگان/محققان شروع به بهبود خدمات آنلاین و ایجاد سیستم‌های جدیدی کرده‌اند که می‌توانند از داده‌های کاربر محافظت کنند و دسترسی ساده به حساب‌های بانکی را فراهم کنند. یکی از این فناوری‌ها و سیستم‌های شگفت‌انگیز قرارداد های هوشمند مبتنی بر بلاک چین است.

علاوه بر این، بلاک چین را می توان به انواع اصلی زیر تقسیم کرد[1]:

- «بلاک چین عمومی»[2] غیرمحدود است و با این نوع بلاک چین، نیازی به مجوز برای دسترسی نیست؛ بنابراین، هر کسی که به اینترنت دسترسی دارد می تواند به این نوع بلاک چین دسترسی داشته باشد؛ بنابراین، مزیت اصلی این نوع ارز دیجیتال این است که کاملا مستقل است و اکثر ارزهای رمزپایه بر روی بلاک چین عمومی اجرا می شوند.

- «بلاک چین خصوصی»[3] نوعی محدود کننده است که برای ورود به آن نیاز به مجوز دارد و تحت کنترل یک نهاد واحد است. فقط کاربران معتبر می توانند به این نوع بلاک چین دسترسی داشته باشند.

- «بلاک چین ترکیبی»[4]، ترکیبی از بلاک چین عمومی و خصوصی است که در آن به مجوز نیاز است و یک سیستم بدون مجوز از این نوع است. برخی از بخش ها توسط یک سازمان مدیریت می شوند، اما برخی دیگر عمومی هستند.

- «بلوک کنسرسیوم»[5] یک رویکرد خلاقانه است که در آن برخی از بخش ها عمومی و برخی دیگر خصوصی هستند، اما می تواند توسط بیش از یک سازمان تعدیل شود.

در مطالعه حاضر، بلاک چین خصوصی مد نظر می باشد، زیرا کنترل حریم خصوصی و مقیاس‌پذیری بیشتری را در مقایسه با سایر انواع بلاک چین در امور مالی و بانکداری ارائه می‌دهد. در امور مالی، حریم خصوصی به دلیل داده‌های حساسی که با آن سروکار دارد، موضوع بسیار حساسی در نظر گرفته می‌شود، به همین دلیل است که بلاک چین خصوصی دسترسی مجاز را ارائه می‌دهد که دسترسی افراد به شبکه و انجام تراکنش را محدود می‌کند. علاوه بر این، یک بلاک چین خصوصی به تراکنش های سریعتر اجازه می دهد تا نیازها و الزامات خاص یک موسسه مالی را برآورده کند.

قرارداد های هوشمند مبتنی بر بلاک‌چین در صنعت مالی

قرارداد هوشمند به عنوان یک برنامه غیرمتمرکز پیشنهاد شده است که بسیار نزدیک به ایده قراردادها در زندگی واقعی در نظر گرفته شده است. این بدان معناست که هر معامله بین دو همتا توسط قرارداد هوشمند بر اساس یک شرایط از پیش تعیین شده کنترل و شناسایی می شود. اگر این شرایط محقق شود، معامله انجام می شود. در غیر این صورت، معامله

[1] (Shrivas, Yeboah, 2019. No.13.)
[2] Public blockchain
[3] A private blockchain
[4] Hybrid blockchain
[5] A consortium block

رد می شود. در نتیجه، هرگونه مبادله پول یا اجرای هر نوع محتوای محدود شده توسط قوانین خاص می تواند از اجرای قرارداد هوشمند بهره مند شود[1]. سوال این است که این قراردادها چگونه کار می کنند. پاسخ به سادگی، (اگر/ زمانی که) سپس خواهد بود، به این معنی که کدی توسط یک توسعه دهنده یا برنامه نویس نوشته شده است تا اطمینان حاصل شود که هیچ اقدامی انجام نمی شود مگر اینکه شرایط برآورده شود. به عنوان مثال، اگر یک مشتری (قرارداد هوشمند) بخواهد با یک ذینفع پول معامله کند، یک قرارداد هوشمند به گونه ای نوشته می شود که گویی تاریخ آن ۲۰۲۳/۱۰/۲۱ است و قرارداد هوشمند از یک رمز عبور خاص استفاده می کند و سپس پول را به ذینفع می فرستد. به این معنی که فرآیند تراکنش هرگز انجام نمی شود مگر اینکه دو شرط مربوط به تاریخ و رمز عبور انجام شود[2].

➢ مراحل قراردادهای هوشمند

پیشنهاد: اولین جزء معامله را شروع می کند. طرف اول از یک زبان برنامه نویسی خاص برای نوشتن قراردادی استفاده می کند که شامل یک بند «اگر/زمانی که»[3] است. سپس، قرارداد از طریق بلاک چین انجام می شود.

مذاکره: قرارداد پس از ارسال در بلاک‌چین برای همه طرف های درگیر قابل مشاهده است. شرایط قرارداد توسط طرفین قابل مذاکره است. پس از امضای آن، هیچ بازگشتی وجود ندارد، بنابراین افراد درگیر در این مرحله تمام شرایط را بررسی می کنند.

تایید: رویدادهای محرک پس از تایید همه طرفین با شرایط قرارداد رخ می دهد. طرفین ممکن است شرایط دیگری را نیز تعیین کنند، مانند تاریخ انقضا، تاریخ سررسید، مجوز اعتصاب یا توقف ضرر یا تاریخ دیگری. پس از آن توافق نامه پذیرفته و نهایی می شود. **رویداد ماشه**: هنگامی که الزامات برآورده می شوند، دارایی ها منتقل می شوند، یا نتیجه اساسی رخ می دهد، قرارداد هوشمند فعال می شود.

➢ جنبه‌های مثبت استفاده از قرارداد هوشمند در کنار بلاک‌چین در سیستم‌های مالی

استفاده از قرارداد هوشمند در کنار بلاک‌چین در سیستم‌های مالی دارای مزایای متعددی است، از جمله:

اتکا به خود: قرارداد های هوشمند امکان دستکاری قرارداد توسط اشخاص ثالث را از بین می‌برند زیرا به کارگزاران یا سایر واسطه‌ها برای تأیید آن نیاز ندارند. علاوه بر این، صرفه جویی مالی با قرارداد های هوشمند وجود دارد زیرا هیچ واسطه ای وجود ندارد.

امنیت: به دلیل اتکا به خود، قرارداد های هوشمند از امنیت بالایی برخوردار هستند.

شتاب: با استفاده از پروتکل های کامپیوتری، قرارداد های هوشمند وظایف را به طور خودکار انجام می دهند و ساعات کار را در انواع فرآیندهای مالی صرفه جویی می کنند.

---

[1] (Sai et al, 2023; No.8.)
[2] (Al-Zubaidie, Jebbar; 2024. No. 5.)
[3] if-then

قابلیت اطمینان: با استفاده از قرارداد های هوشمند، خطاهایی که از پر کردن فرم های متعدد با دست به وجود می آیند، از بین می روند.

اهداف پژوهش

مطالعه حاضر با دو هدف اصلی انجام پذیرفته است که در ادامه ارائه شده است:

۱. شناسایی جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاک چین در صنعت مالی در جهان

۲. رتبه بندی راهکار های جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاک چین در بهینه سازی عملکرد و بهبود مقیاس پذیر در بانک مرکزی

روش پژوهش

پژوهش حاضر از نوع پژوهش های ترکیبی با استفاده از مطالعات کتابخانه ای و کیفی و با استفاده از نظر سنجی ۸ نفر از خبرگان حوزه فناوری اطلاعات در بانکداری الکترونیک انجام شده است. هدف شماره یک مطالعه با استفاده از مطالعات کتابخانه ای محقق شده است. همچنین برای رسیدن به هدف شماره ۲. از تکنیک تصمیم گیری چند شاخصه «سوارا»[1] استفاده شده است.

شناسایی جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاک چین در صنعت مالی در جهان

بلاک چین یک دفتر کل غیرمتمرکز و غیرقابل تغییر است که از یک زنجیره رمزنگاری مرتبط از رکوردهای مسدود شده تشکیل شده است. مجموعه رکوردها را بلوک و رکوردها را معمولاً تراکنش یا رویداد می نامند. دفتر کل غیرمتمرکز در بین تمام اعضای مشارکت کننده در شبکه بلاک چین به اشتراک گذاشته شده است[2]. معاملات پس از تأیید و فرآیند توافق بین طرفین در بلاک چین به دفتر کل اضافه می شود. پیوند رمزنگاری ستون فقرات بلاک چین است. کلیدواژه های مهم مرتبط با بلاک چین عبارتند از عدم تمرکز، تغییر ناپذیری و پیوند رمزنگاری.

«تمرکززدایی»[3]: تمرکززدایی نشان دهنده قابلیت تراکنش (ذخیره و بازیابی داده) قراردادهای هوشمند مبتنی بر بلاک چین بدون یک نقطه شکست است. دفتر کل در هر گره در دسترس است و برخلاف سیستم های مدیریت پایگاه داده متمرکز[4]، دسترسی به داده ها به یک سرویس متمرکز بستگی ندارد.

«تغییرناپذیری»[5]: رکوردهای دفتر کل پس از ثبت غیرقابل تغییر هستند[6]. تلاش برای جعل رکورد دفتر کل در یک بلوک خاص، آن را رد صلاحیت می‌کند و یکپارچگی داده‌های کل بلاک چین را از بین می‌برد. تغییر ناپذیری دفتر کل

[1] SWARA
[2] (Pilkington, 2016; No.3.)
[3] Decentralization
[4] (Chowdhury et al, 2018; No.9.)
[5] Immutability
[6] (Hofmann et al, 2017; No.6.)

با استفاده از تکنیک های رمزنگاری مانند هش و امضای دیجیتال که در ادامه توضیح داده خواهد شد، تضمین می شود. تغییرات دفتر کل یک کار محاسباتی پرهزینه است.

«**پیوند رمزنگاری**»[1]: پیوند رمزنگاری ستون فقرات کل بلاک چین است[2]. تغییرناپذیری بلاک چین از طریق پیوند رمزنگاری ایجاد شده با هش و امضاهای دیجیتال به دست می آید. تراکنش یا بلوک را نمی توان تغییر داد زیرا نیاز به تغییر تمام بلوک های بعدی دارد.

➢ جنبه های فنی قراردادهای هوشمند مبتنی بر بلاک چین

تحقیقات علمی در مورد قراردادهای هوشمند مبتنی بر بلاک چین در جهات مختلف تخصص فنی مسحور شده است. فناوری بلاک چین که به عنوان یک دفتر کل غیرمتمرکز حداقلی آغاز شد، به لطف مشارکت تحقیقاتی که در سرتاسر جهان انجام شده، ویژگی‌های حیاتی مانند امنیت بهبود یافته، مقیاس‌پذیری و عملکرد بهینه ظاهر شد. جنبه های فنی مهم قراردادهای هوشمند مبتنی بر بلاک چین در این بخش مورد بحث قرار می گیرد.

حملات امنیتی، آسیب پذیری ها

قراردادهای هوشمند به طور گسترده در صنعت مالی جهان شروع به پذیرش کرده است. امنیت در در نظر گرفتن قراردادهای هوشمند از اهمیت حیاتی برخوردار است زیرا بر عملکرد کل بلاک چین تأثیر می گذارد. حملات متعددی در زمینه قرارداد هوشمند وجود دارد[3]. این حملات به دلایل متعددی مانند خطاهای برنامه نویسی، محدودیت در زبان های برنامه نویسی و حفره های امنیتی منجر می شوند. نتایج این حملات شامل پیچیدگی‌های زیادی برای شبکه‌های بلاک چین و دقت آن‌ها، از دست دادن ارز دیجیتال بومی و خاتمه در دسترس بودن سیستم است. این حملات را می توان در هر دو پلتفرم بلاک چین عمومی و خصوصی شناسایی کرد. نقش قراردادهای هوشمند و دقت آنها می تواند در بلاک چین های عمومی مهم تر از بلاک چین های خصوصی باشد. اشکال زدایی یا هر اصلاحی یک فرآیند دست و پا گیر است، زیرا قراردادها برای همه گره ها در یک شبکه بلاک چین اتخاذ شده است.

آسیب پذیری ورود مجدد

به طور کلی، آسیب‌پذیری ورود مجدد زمانی مورد سوء استفاده قرار می‌گیرد که یک قرارداد هوشمند، قرارداد هوشمند دیگری را به طور مکرر فراخوانی می‌کند و قرارداد هوشمندی که فراخوانی را آغاز می‌کند، مخرب است. چنین حملاتی در پلتفرم اتریوم زیاد بود. در نهایت، اترهای قرارداد هوشمند فراخوانی به حساب قرارداد مخرب منتقل می شود. مهر و همکاران[4] حمله «دی. ای.او»[5] را توصیف کردند، یک هکر ناشناس ۵۰ میلیون دلار اترها را از ۱۶۸ میلیون دلار سرمایه گذاری شده از طریق افزایش سرمایه مجازی در سال ۲۰۱۶ دزدید. یک کدگذار حفره هایی پیدا کرد،

[1] Cryptographic Link
[2] (Anjum et al, 2017; No.8.)
[3] (Liu et al, 2019; No.21.)
[4] (Mehar et al, 2019; No.7.)
[5] DAO

هنگامی که یک تابع تقسیم فراخوانی شد، کد ابتدا اتر را بازیابی می کند و به روز می شود. بعداً تعادل برقرار شد و بررسی نشد که آیا تماس بازگشتی است یا خیر. مهاجم به صورت بازگشتی توابع تقسیم را فراخوانی می کند و وجوه آنها را قبل از اینکه کد موجودی را بررسی کند، بازیابی می کند.

۱. خطاهای سرریز

سرریز زمانی رخ می دهد که نتیجه یک عملیات حسابی خاص کمتر یا بیشتر از حداقل یا حداکثر نوع داده عددی مورد استفاده در پلت فرم قرارداد هوشمند باشد. برنامه نویسان موظفند چنین شرایطی را هنگام کدگذاری قرارداد در نظر بگیرند[۱].

۲. حملات سیبیل

«حمله سیبیل»[۲] زمانی اتفاق می‌افتد که یک عضو تلاش می‌کند تا با درک هویت‌های جعلی آشکارا، شبکه همتا را در اختیار بگیرد. چنین شرایطی منجر به کنترل نامتناسب شبکه می شود که می تواند منجر به ربودن اکوسیستم همتا بلاک چین توزیع شده شود. به عنوان مثال، اگر اجماع بر اساس رای اکثریت یک بلاک چین خاص باشد، اعضایی که به صراحت در حمله ایجاد شده اند می توانند اجماع شبکه را در اختیار بگیرند. زمانی که فرآیند ورود به بلاک چین بسیار کم و خودکار باشد، سیستم مستعد چنین خطری است[۳].

۳. تصادفی بد

تصادفی بودن در قراردادهای هوشمند مورد نیاز است. علاوه بر آن، توابع سودمندی وجود دارند که نیاز به تصادفی بودن دارند. رویکردهای تولید اعداد تصادفی یا شبه تصادفی در برخی شرایط آسیب پذیر خواهند بود. استفاده از متغیرهای بلوک و هش بلوک به عنوان منابع آنتروپی می تواند آسیب پذیر باشد[۴].

٤. حملات دوگانه خرج کردن

استفاده از توکن بومی تقریباً در تمام پلتفرم‌های قرارداد هوشمند رایج است. در هر تراکنش، این خطر وجود دارد که همان کاربر بتواند یک توکن خاص را دو یا چند بار خرج کند. این نوع حملات به عنوان حملات دوگانه خرج کردن شناخته می شود[۵].

۵. حملات اکثریت

اکثر حملات زمانی رخ می دهند که برخی از کاربران یا گروه های مخرب کنترل را برای بازنویسی تاریخچه تراکنش ها یا جلوگیری از تایید تراکنش های جدید به دست می گیرند. این حمله زمانی رخ می دهد که یک کنسرسیوم بلاک

[1] (Kim, Ryu, 2020; No.11.)
[2] Attack Sybil
[3] (Cai, Zhu, 2016; No.7.)
[4] (Chatterjee et al, 2019; No.3.)
[5] (Zhang, Lee, 2019; No.14.)

چین خاص با اجماع اکثریت رای پذیرفته شود. بسته به نیاز کاربر، گاهی اوقات استخراج بلوک و تأیید تراکنش به برخی از همتایان برجسته اختصاصی هر یک از اعضای کنسرسیوم بارگذاری می شود. اگر اکثر همتایان پیشرو توسط کاربر مخرب ربوده شوند، شرایط مشابهی رخ داده است[۱].

٦. قراردادهای قابل تخریب

آسیب‌پذیری خود تخریبی محتوای یک قرارداد هوشمند را با حذف بایت کد در آدرس‌های خاص حذف می‌کند. علاوه بر این، تمام وجوه قرارداد را به یک آدرس هدف خاص ارسال می کند و قرارداد را غیر کاربردی می کند[۲].

۷. اختلال استثنایی

اختلال استثنایی به این دلیل رخ می دهد که استثناهایی که به درستی مدیریت نشده اند منجر به شکست می شوند. رسیدگی به استثناها یک عمل مهم در برنامه نویسی است، چه در بلاک چین یا هر زمینه دیگری. مدیریت نادرست استثناها، به ویژه زمانی که یک قرارداد دیگر را فراخوانی می کند، بر عملکرد کل شبکه تأثیر می گذارد. از این رو، اختلال استثنا به عنوان آسیب پذیری اصلی برجسته می شود[۳].

۸. آسیب پذیری پشته تماس

عمق پشته تماس تا یک مقدار معین در محیط اجرای قرارداد هوشمند محدود شده است. به عنوان مثال، در اتریوم عمق پشته تماس به ۱۰۲۴ فریم محدود شده است. هنگامی که عمق تماس به محدودیت برسد، عملیات با شکست مواجه می شود. این می تواند به دلایل مختلفی مانند خطاهای برنامه نویسی رخ دهد[۴].

۹. عملیات فشرده توان محاسباتی نامحدود

هر عملیات روی قراردادهای هوشمند نیاز به مصرف توان محاسباتی دارد. به عنوان مثال، هزینه توان محاسباتی در اتریوم گاز نامیده می شود. گاز مورد استفاده برای ارزیابی مصرف منابع محاسباتی یک عملیات خاص در قرارداد هوشمند استفاده می شود. عملیات فشرده توان محاسباتی نامحدود منجر به خطاهای مختلفی می شود و در نهایت سیستم را تحت تأثیر قرار می دهد[۵].

مسائل و راه حل های فنی حریم خصوصی

تمرکززدایی یک اصل اصلی قراردادهای هوشمند مبتنی بر بلاک چین است. تمرکززدایی در بلاک چین باعث می شود دفتر کل تراکنش ها و قراردادهای هوشمند به عنوان یکی از ویژگی های امنیتی برای همه همتایان در شبکه شفاف شود. شفافیت برای شرایط خاص توصیه نمی شود. شفافیت داخلی یک نگرانی مهم در خصوص حفظ حریم خصوصی در

[1] (Moubaraket al, 2018; No.3.)
[2] (Groce et al, 2020; No.1.)
[3] (Hasanova et al, 2019; No.18.)
[4] (Li et al, 2020; No.3.)
[5] (Tosh et al, 2020; No. 5.)

قراردادهای هوشمند مبتنی بر بلاک چین است. جنبه های فنی حریم خصوصی در قرارداد های هوشمند دامنه وسیعی دارد. با توجه به ماهیت توزیع شده قراردادهای هوشمند، نگرانی های عمده کمی درباره حریم خصوصی وجود دارد. نگرانی های حفظ حریم خصوصی، باید به منظور افزایش قابلیت استفاده از قراردادهای هوشمند مبتنی بر بلاکچین در صنعت مالی و بانکداری الکترونیک مورد توجه قرار گیرد. جدول ۱. راه حل های فنی مربوط به حفظ حریم خصوصی قراردادهای هوشمند مبتنی بر بلاک چین در صنعت مالی را نشان می دهد.

جدول ۱. مسائل و راه حل های فنی حفظ حریم خصوصی قراردادهای هوشمند مبتنی بر بلاک چین در صنعت مالی (بانک الکترونیک)(ماخذ: یافته های پژوهش)

توضیحات	حریم خصوصی داده های تراکنش	حریم خصوصی منطق قرارداد هوشمند	حریم خصوصی کاربر	حریم خصوصی در اجرای قرارداد های
هک	*			
سیستم معاملاتی با افزایش حریم خصوصی کاربر			*	
حفظ حریم خصوصی و هزینه جمع سنجی بهینه با استفاده از قرارداد های هوشمند و زنجیره بلوک			*	
Prov chain			*	
فضای زنجیره ای	*			
Arbitrum			*	
Ekiden				*
town crier				*
shadoweth				*
پشتیبانی از داده های خصوصی با محاسبات امن چند جانبه	*			
معما			*	
Zether		*		

➢ حریم خصوصی داده های تراکنش

در شرایط خاص، اعضای شبکه شفافیت را ترجیح نمی دهند زیرا برخی از اطلاعات حساس مانند اسرار تجاری، اطلاعات قیمت گذاری را فاش می کند. حتی اگر سیستم مرتبط با بلاک چین، اقدامات لازم برای حفظ حریم خصوصی را یکپارچه کرده باشد[1].

- **راه حل های بالقوه فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی جهان پیرامون حریم خصوصی داده های تراکنش**

ایبا نز و همکاران[2] بینش های قابل توجهی در مورد جنبه های مختلف فناوری بلاک چین از جمله مقررات عمومی حفاظت از داده ها و کاربرد آن در زنجیره بلوکی به عنوان یک توانمند برای محافظت از داده ها ارائه کردند. نویسندگان درباره کاربرد قراردادهای هوشمند بر روی بلاک چین های مجاز و بلاک چین های بدون مجوز در ارتباط با کنترل کننده های داده مناسب بحث کردند. نویسندگان این دو نوع راه‌حل را در زمینه امکان‌پذیری انطباق، به‌عنوان ادغام توابع رمزنگاری مختلف و طرح‌های محاسباتی خصوصی بدون افشای محتوای تراکنش‌ها و کاربرد زنجیره‌های بلوکی به‌عنوان ماشین‌های تأیید غیرمتمرکز دسته‌بندی کردند.

جولز و همکاران[3] ظهور قراردادهای هوشمند جنایی در زمینه مالی را نشان دادند که افشای اطلاعات محرمانه را تسهیل می کند. نویسندگان چند موضوع از جمله سرقت کلیدهای رمزنگاری شده توسط قراردادهای هوشمند جنایی را نشان دادند. نتایج آنها بر ایجاد سیاست‌ها و اقدامات حفاظتی فنی در برابر قراردادهای هوشمند جنایی برای اطمینان از اهداف سودمند قراردادهای هوشمند تأکید کرد.

کوسبا و همکاران[4]، چارچوبی را پیشنهاد می کنند که یک برنامه نویس غیر متخصص را قادر می سازد تا یک قرارداد هوشمند حفظ حریم خصوصی بنویسد. ایشان حریم خصوصی زنجیره ای را پیشنهاد می کنند که به صورت رمزنگاری جریان پول و پنهان کردن مبلغ از دید عموم را انجام می دهد.

➢ حریم خصوصی منطق قرارداد هوشمند

قرارداد هوشمند به طور عمومی در تمام گره های بلاک چین مستقر شده است[5]. به دلیل برخی الزامات، منطق تجاری باید در بلاک چین گنجانده شود. منطق کسب و کار ممکن است شامل اطلاعات حساس مانند کمیسیون، پاداش باشد. افشای چنین اطلاعات حساسی از طریق قرارداد هوشمند یکی از دغدغه های سازمان ها خواهد بود.

---

[1] (Gupta et al, 2020; No.12.)
[2] (Ibáñez et al, 2018; No.13.)
[3] (Juels et al, 2016. No.1.)
[4] (Kosba et al, 2016. No.1.)
[5](Bünz et al, 2024; No.17.)

- **راه حل های بالقوه فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی جهان پیرامون حریم خصوصی در منطق**

الباسام و همکاران[1]، «فضای زنجیره ای[2]» را ارائه می‌کنند که توسعه‌پذیری سازگار با حریم خصوصی را در پلت فرم قرارداد هوشمند ارائه می‌دهد. این پلتفرم مقیاس‌پذیری بالاتری نسبت به پلتفرم موجود ارائه می‌دهد که از طریق تقسیم کردن گره‌ها با استفاده از یک پروتکل جدید اتمی توزیع‌شده به نام «اس-بی.ای.سی[3]» به دست می‌آید. همچنین از قابلیت حسابرسی و شفافیت پشتیبانی می کند.

کالودنر و همکاران[4]، «آربیتروم[5]» را ارائه کردند که یک سیستم ارز دیجیتال با قراردادهای هوشمند است. مدل آربیتروم برای قراردادهای هوشمند خصوصی سازگار است که وضعیت داخلی را برای تأییدکنندگانی که در شرایط خاص در تأیید تراکنش‌ها دخیل هستند، آشکار نمی‌کند. آربیتروم طرفین را تشویق می کند تا در مورد رفتار ماشین مجازی به توافق برسند، به این معنی که ماینرهای آربیتروم فقط باید امضاهای دیجیتال را بدون افشای قرارداد تایید کنند تا طرفین بر روی رفتار ماشین مجازی توافق کرده اند.

- **حریم خصوصی کاربر**

حریم خصوصی کاربر در برخی از کاربردهای مهم قراردادهای هوشمند مبتنی بر بلاک چین بسیار مورد توجه است. کاربرانی که قراردادهای هوشمند را وارد می‌کنند، در شرایط خاصی ملزم به خصوصی بودن هستند. به عنوان مثال، راه حل هایی مانند سیستم های اطلاعات سلامت توسط کاربران در صورتی که اطلاعات هویت شخصی در دفتر فاش شود، ترجیح نمی دهند. حفظ حریم خصوصی هویت کاربر نیز یک نگرانی مهم در اجرای قراردادهای هوشمند مبتنی بر بلاک چین است[6].

- **راه حل های بالقوه فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی جهان پیرامون حریم خصوصی کاربر**

نیا و همکاران[7] طراحی و اجرای یک برنامه تجاری را نشان دادند که از قراردادهای هوشمند اتریوم استفاده می کرد. این برنامه با انعطاف پذیری در درخواست هویت کاربر به طور مستقیم توسط فروشنده و خریدار توسعه یافته است. بلاک چین سبک وزن برای تسهیل تبادل داده در کانال های دستگاه به دستگاه ایجاد شده است.

[1] (Al-Bassam et al, 2017; No.1.)
[2] Chain Space
[3] S-BAC
[4] (Kalodner et al, 2018; No.1.)
[5] Arbitrum
[6] (Dorri et al, 2017; No.5.)
[7] (Niya et al, 2018; No.1.)

چاتزوپولوس و همکاران[1] یک معماری جدید شامل وظایف سنجش جمعیت فضایی مبتنی بر رویداد در ارتباط با بلاک چین و فناوری با حفظ حریم خصوصی کاربر پیشنهاد کرد. این معماری از قراردادهای هوشمند استفاده می کند تا به ارائه دهندگان خدمات سنجش جمعیت اجازه دهد درخواست های خود را ارسال کنند، حراج های بهینه هزینه را اجرا کنند و پرداخت ها را انجام دهند.

لیانگ و همکاران[2]، «پرووچین[3]» را طراحی و اجرا کردند که یک معماری غیرمتمرکز برای منشأ داده های ابری قابل اعتماد است. پرووچین ویژگی های امنیتی قابل توجهی مانند منشأ ضد دستکاری و حفظ حریم خصوصی کاربر را ارائه می دهد. مراحل اصلی عملیاتی عبارتند از جمع‌آوری داده‌های منشأ، ذخیره‌سازی داده‌های منشأ و اعتبارسنجی داده‌های منشأ که سوابق ضد دستکاری را فراهم می‌کند تا شفافیت و پاسخگویی داده‌ها را در ابر فراهم کند.

➢ حریم خصوصی در اجرای قراردادهای هوشمند

قراردادهای هوشمند برنامه هایی هستند که بر روی زیرساخت محاسباتی اجرا می شوند. در بلاک چین، قراردادهای هوشمند بر روی گره ها اجرا می شوند. دسترسی به دستورالعمل های اجرا شده بر روی ماشین را می توان با استفاده از رویکردهای متعدد برقرار کرد. به عنوان مثال، رمز عبور وارد شده توسط کاربر باید در حافظه بارگذاری شود و با استفاده از ابزارهای تخلیه حافظه به شکل واضح قابل مشاهده است. این نوع سرقت‌های داده‌های سطح پایین‌تر در هنگام اجرا به عنوان نقض حریم خصوصی در شرایط خاص در نظر گرفته می‌شوند[4].

- **راه حل های بالقوه فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی جهان پیرامون حریم خصوصی در اجرای قراردادهای هوشمند**

الف) محیط اجرای مورد اعتماد (TEE[5])

محیط اجرای قابل اعتماد مانند «Intel SGX[6]»، محرمانه بودن و حفظ حریم خصوصی را در طول اجرای کد قراردادهای هوشمند تضمین می کند.

ژانگ و همکاران[7] یک سیستم خوراک داده تایید شده را ارائه کرد که به عنوان «Town Crier» نامگذاری شده است. این سیستم، پلی بین قراردادهای هوشمند و وب سایت های موجود که معمولاً برای برنامه های غیر بلاک چین قابل اعتماد هستند، فراهم می کند. قسمت جلویی و باطن سخت افزار با راه حلی ترکیب شده است که در صورت لزوم با حریم خصوصی فعال می شود.

---

[1] (Chatzopoulos et al, 2018; No.1.)
[2] (Liang et al, 2017; No.1.)
[3] Prov chain
[4] (Bao et al, 2020; No. 11.)
[5] Trusted Execution Environment
[6] *Intel Software Guard Extensions*
[7] (Zhang et al, 2016; No.1.)

چنگ و همکاران[1]، «Ekiden» را ارائه کردند که زنجیره بلوکی را با محیط اجرای مورد اعتماد ترکیب می کند. نویسندگان از معماری جدیدی استفاده کردند که اجماع را از اجرا جدا می‌کند و محرمانگی را برای حفظ قراردادهای هوشمند در محیط اجرای قابل اعتماد فعال می‌کند. نویسندگان قصد داشتند کار خود را گسترش دهند تا محاسبات چند جانبه ایمن را در آینده فراهم کنند.

یوان و همکاران[2] «ShadowEth» را ارائه کردند که سیستمی است که از یک محصور سخت افزاری برای اطمینان از محرمانه بودن قراردادهای هوشمند در بلاک چین عمومی مانند اتریوم استفاده می کند. این سیستم همچنین یکپارچگی و در دسترس بودن را تضمین می کند. نویسندگان نمونه اولیه را با استفاده از «Intel SGX» در شبکه اتریوم برای تجزیه و تحلیل امنیت و آسیب پذیری سیستم پیاده سازی کردند.

ب) محاسبات ایمن چند طرفه

بنهامودا و همکاران[3] روشی را برای سازگار کردن پلت فرم بلاک چین «Hyperledger Fabric» با داده های خصوصی با استفاده از محاسبات چند جانبه ایمن ارائه کرد. نویسندگان یک سرور کمکی را مرتبط کردند که محاسبات چند طرفه را به خارج از زنجیره جدا می کند.

زیسکین و همکاران[4]، «Enigma» را ارائه کردند که یک مدل محاسباتی مبتنی بر یک نسخه بسیار بهینه از محاسبات چند جانبه ایمن است که طرح‌های اشتراک‌گذاری راز قابل تأیید را تضمین می‌کند و از محرمانه بودن اطمینان می‌دهد. نویسندگان از یک جدول هش توزیع شده اصلاح شده برای نگهداری داده های مخفی به اشتراک گذاشته شده با یک بلاک چین خارجی به عنوان کنترل کننده شبکه برای کنترل دسترسی و مدیریت هویت استفاده کردند.

ج) کاهش سربار محاسباتی قراردادهای هوشمند

اجرای قرارداد هوشمند فرآیندی با منابع فشرده است. ذینفعان قرارداد هوشمند باید نسبت به اجرا برای طرف های مربوطه بهینه باشند. قراردادهای هوشمند غیربهینه در محاسبات گران هستند و در نهایت هزینه اضافی را برای کاربران قراردادهای هوشمند به همراه خواهند داشت. علاوه بر این، مصرف بیش از حد منابع قراردادهای هوشمند کل سیستم را از کار می اندازد؛ بنابراین شرایط اجرای بهینه در زمینه قراردادهای هوشمند بسیار پیش بینی می شود.

- **راه حل های بالقوه فنی**

ایدلبرگر و همکاران[5] بینش های مهمی را با مزایا و معایب فنی قراردادهای هوشمند مبتنی بر منطق در هنگام ارائه قراردادهای معمولی ارائه کردند. نویسندگان ثابت کردند که یک رویکرد مبتنی بر منطق می تواند به طور سودمندی بر

[1] (Cheng et al, 2019; No.1.)
[2] (Yuan et al, 2018; No.1.)
[3] (Benhamouda et al, 2019; No.1.)
[4] (Zyskind et al, 2015; No.1.)
[5] (Idelberger et al, 2016; No.1.)

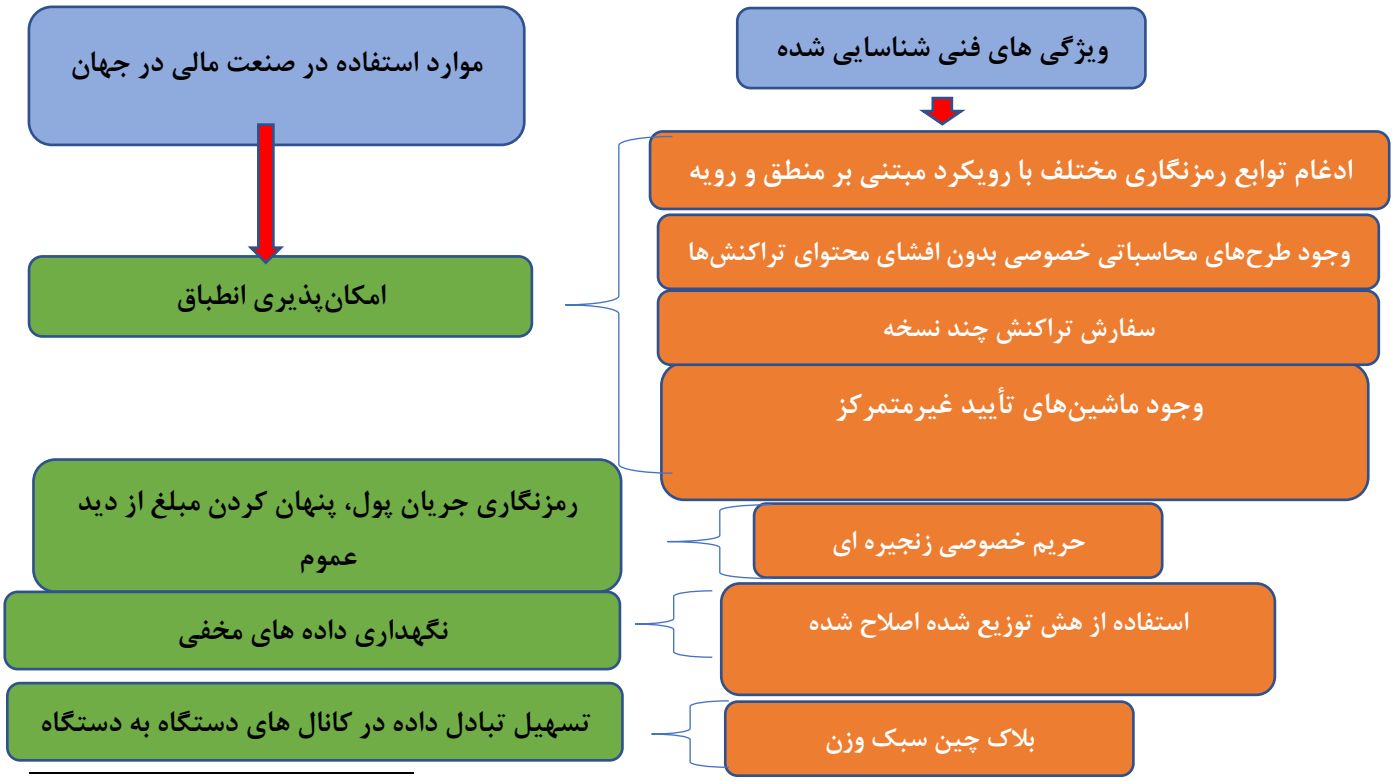
روی مؤلفه رویه ای خود در ابعاد کمی از جمله مذاکره، شکل گیری، ذخیره سازی تکمیل شود. نویسندگان تاکید کردند که رویکردهای منطقی و رویه ای در قراردادهای هوشمند ناسازگار نیستند.

د) بهبودهای همزمان

زمانی که قراردادهای هوشمند بر روی یک بلاک چین مستقر شدند، انتظار می رود که در چندین نمونه اجرا شوند. برای بهبود کارایی، چندین مطالعه رویکردهایی را برای بهبود همزمانی قراردادهای هوشمند پیشنهاد کرده‌اند. دو دسته اصلی از رویکردها، از جمله سفارش پایه زمانی مهر (BTO[1]) و سفارش تراکنش چند نسخه (MVTO[2]) پیشنهاد شد. BTO به هر تراکنش یک مهر زمانی اختصاص می‌دهد و ترتیب سریال‌سازی تراکنش‌ها را برای اجرا یا دسترسی به یک منبع بر اساس مُهر زمانی تعیین می‌کند. MVTO تضمین می کند که اگر ناسازگاری بین دو تراکنش که به اقلام داده مربوطه دسترسی دارند شناسایی شود، یکی از آنها لغو می شود. یک طرح همزمان برای اجرای قراردادهای هوشمند به صورت همزمان می تواند ۲,۵ برابر سرعت پردازش در اعتبارسنجی بلوک با سه رشته کاری را به همراه داشته باشد.

۳,۵. استخراج جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی جهان با توجه مطالعات موجود

با توجه به مرور مطالعات پیرامون قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی، تعدادی از جنبه ها و ویژگی های مهم فنی قرارداد های هوشمند مبتنی بر بلاکچین شناسایی شدند. در شکل شماره ۱. ویژگی های فنی و کاربرد های هر ویژگی به طور خلاصه ارائه شده است.



[1] Basic Timestamp Ordering
[2] Multi-Version Transaction Ordering

شکل شماره ۱. استخراج جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در صنعت مالی و کاربرد های آن

ارائه بهترین شیوه های عملکرد و بهبود مقیاس پذیری در بانک مرکزی با استفاده از جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در بانک مرکزی

بخش قبلی مطالعه حاضر، جنبه‌های فنی مهم قراردادهای هوشمند مبتنی بر بلاک چین را از منظری گسترده‌تر شناسایی و منعکس کرد. این بخش با بینش‌های قابل توجهی از جنبه‌های فنی قراردادهای هوشمند و دستورالعمل‌های منحصر به فرد برای بهبود بیشتر در جهت بهینه سازی عملکرد و بهبود مقیاس پذیری در بانک مرکزی با استفاده از تکنیک سوارا می پردازد.

۱,٦. تجزیه و تحلیل های مرتبط با تکنیک سوارا

در این بخش از پژوهش به منظور وزن دهی به جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در بانکداری الکترونیکی، از خبرگان حوزه فناوری اطلاعات خواسته شد که هرکدام از شاخص ها را با توجه به میزان تأثیر آنها در بهینه سازی عملکرد و بهبود مقیاس پذیری بانکداری الکترونیک بر اساس تجربیات خود رتبه بندی کنند. سپس با میانگین گرفتن رتبه هر کدام از جنبه های فنی، رتبه بندی انجام گردید. در ادامه پس از به دست آمدن اهمیت نسبی

هرکدام از جنبه های فنی، برای وزن دهی عوامل بر اساس تکنیک سوارا از فرمول های زیر استفاده کرده که نتایج حاصله در جدول شماره ۲. قابل مشاهده است.

فرمول ۱. $$K_j = S_j + 1$$

فرمول ۲. $$W_j = \frac{W_{j-1}}{K_j}$$

فرمول ۳. $$Q_j = \frac{W_j}{\sum_{j=1}^{n} W_j}$$

جدول ۲. وزن دهی به جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در بانکداری الکترونیک

جنبه های فنی	متوسط اهمیت نسبی هر معیار SJ	Kj=Sj +1	وزن اولیه هرمعیار qj	وزن نرمال wj
بلاک چین خارجی	۰,۹۶۲۵	۱,۹۶۲۵	۱,۹۶۲۵	۰,۴۸۹
وجود ماشین‌های تأیید غیرمتمرکز	۰,۹۷۵	۱,۹۷۵	۰,۹۹۴	۰,۲۴۸
فضای زنجیره ای	۰,۸۲۵	۱,۸۲۵	۰,۵۴۴	۰,۱۳۶
سفارش تراکنش چند نسخه	۰,۶۷۵	۱,۶۷۵	۰,۳۲۵	۰,۰۸۱
پروتکل سازگار اجماع خارج از زنجیره	۰,۷۶۲۵	۱,۷۶۲۵	۰,۱۸۴	۰,۰۴۶
			۴,۰۱۰	۱,۰۰۰
سناریو ذخیره سازی ابری	۰,۹۳۷۵	۱,۹۳۷۵	۱,۹۳۷۵	۰,۵۲۴
ادغام توابع رمزنگاری مختلف با رویکرد مبتنی بر منطق و رویه	۰,۹۷۵	۱,۹۷۵	۰,۹۸۱	۰,۲۶۶

جنبه های فنی	متوسط اهمیت نسبی هر معیار SJ	Kj=Sj+1	وزن اولیه هرمعیار qj	وزن نرمال wj
بلاک چین سبک وزن	۰,۹۳۸	۱,۹۳۸	۰,۵۰۶	۰,۱۳۷
سفارش پایه زمانی مهر	۰,۸۷۵	۱,۸۷۵	۰,۲۷۰	۰,۰۷۳
			۳,۶۹۵	۱,۰۰۰
استفاده از هش توزیع شده اصلاح شده	۰,۷۱۲۵	۱,۷۱۲۵	۱,۷۱۲۵	۰,۴۷۴
معماری بر اساس سنجش جمعیت فضایی مبتنی بر رویداد	۰,۹۳۷۵	۱,۹۳۷۵	۰,۸۸۴	۰,۲۴۵
محاسبات ایمن چند طرفه	۰,۷۸۷۵	۱,۷۸۷۵	۰,۴۹۴	۰,۱۳۷
وجود طرح‌های محاسباتی خصوصی بدون افشای محتوای تراکنش‌ها	۰,۸	۱,۸	۰,۲۷۵	۰,۰۷۶
زنجیره بلوکی	۰,۷۱۲۵	۱,۷۱۲۵	۰,۱۶۰	۰,۰۴۴
حریم خصوصی زنجیره ای	۰,۸۷۵	۱,۸۷۵	۰,۰۸۶	۰,۰۲۴
			۳,۶۱۲	۱,۰۰۰

در نهایت با استفاده از تکنیک سوارا، وزن هر یک از جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در بانکداری الکترونیک به دست آمد که نتایج در جدول ۳. ارائه شده است.

جدول ۳. وزن هر یک از جنبه های فنی مهم قرارداد های هوشمند مبتنی بر بلاکچین در بانکداری الکترونیک

جنبه های فنی	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
وزن نهایی	۰,۲۵۹۱	۰,۱۳۱۲	۰,۰۷۱۹	۰,۰۴۲۹	۰,۰۲۴۴	۰,۲۷۷۶	۰,۱۴۰۶	۰,۰۷۲۶	۰,۰۳۸۷	۰,۲۵۱۱	۰,۱۲۹۶	۰,۰۷۲۵	۰,۰۴۰۳	۰,۰۲۳۵	۰,۰۱۲۵
رتبه	۲	۵	۹	۱۰	۱۳	۱	٤	۷	۱۲	۳	٦	۸	۱۱	۱٤	۱۵

بحث و نتیجه گیری

با گسترش حوزه های کاربردی قراردادهای هوشمند به خصوص در بانکداری الکترونیکی، کدها باید به طور رسمی تأیید شوند. تأیید رسمی مستلزم آن است که قرارداد هوشمند خاص، در نهایت یک برنامه رایانه ای مطابق با مشخصات رسمی پیش بینی شده توسط ذینفعان اجرا شود. مشخصات رسمی قراردادهای هوشمند مستلزم آن است که با حمایت کارشناسان به وضوح تعریف شود. به‌ویژه زمانی که بلاک‌چین‌های زیربنایی با سیستم‌های حیاتی ادغام می‌شوند، تأیید رسمی یک الزام اجباری خواهد بود. تأیید رسمی نباید به مداخله شخص ثالث نیاز داشته باشد. به عنوان مثال، تشخیص آسیب‌پذیری به آزمایش‌کنندگان نفوذ متخصص برای شبیه‌سازی حملات امنیتی و شناسایی آسیب‌پذیری‌ها نیاز دارد. ممیزی های امنیتی ممکن است به مداخله متخصص نیاز داشته باشد؛ اما تأیید رسمی فقط مستلزم ایجاد مشخصات رسمی است که می تواند تخصص توسعه دهندگان بانکداری الکترونیکی باشد. توسعه‌دهندگان قرارداد هوشمند در بانکداری الکترونیکی باید از روش‌های تأیید رسمی برای تأیید قراردادهای هوشمند قبل از استقرار آگاه باشند. راستی‌آزمایی رسمی آسیب‌پذیری‌های مهمی مانند قفل کردن وجوه، ارسال وجوه به حساب‌های دیگر به طور مداوم بدون رضایت مالک حساب و غیره را شناسایی می‌کند. تأیید رسمی بهترین روش اجباری برای توسعه دهندگان قرارداد هوشمند آینده است.

منابع و مآخذ

1. Al-Bassam, M., Sonnino, A., Bano, S., Hrycyszyn, D., & Danezis, G. (2017). Chainspace: A sharded smart contracts platform. *arXiv preprint arXiv:1708.03778*.

2. Al-Zubaidie, M., & Jebbar, W. (2024). Transaction Security and Management of Blockchain-Based Smart Contracts in E-Banking-Employing Microsegmentation and Yellow Saddle Goatfish. *Mesopotamian Journal of CyberSecurity*, *4*(2), 1-19.

3. Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing*, *4*(4), 84-90.

4. Bao, Z., Wang, Q., Shi, W., Wang, L., Lei, H., & Chen, B. (2020). When blockchain meets SGX: An overview, challenges, and open issues. *Ieee Access*, *8*, 170404-170420.

5. Benhamouda, F., Halevi, S., & Halevi, T. (2019). Supporting private data on hyperledger fabric with secure multiparty computation. *IBM Journal of Research and Development*, *63*(2/3), 3-1.

6. Bünz, B., Agrawal, S., Zamani, M., & Boneh, D. (2024, February). Zether: Towards privacy in a smart contract world. In *International Conference on Financial Cryptography and Data Security* (pp. 423-443). Cham: Springer International Publishing.

7. Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*, 1-10.

8. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technological forecasting and social change*, *158*, 120166.

9. Chatterjee, K., Goharshady, A. K., & Pourdamghani, A. (2019, May). Probabilistic smart contracts: Secure randomness on the blockchain. In *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 403-412). IEEE.

10. Chatzopoulos, D., Gujar, S., Faltings, B., & Hui, P. (2018, October). Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain. In *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)* (pp. 442-450). IEEE.

11. Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., ... & Song, D. (2019, June). Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 185-200). IEEE.

12. Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain versus database: A critical analysis. In *2018 17th IEEE International conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 1348-1353). IEEE.

13. Dong, L., Qiu, Y., & Xu, F. (2023). Blockchain-enabled deep-tier supply chain finance. *Manufacturing & Service Operations Management*, *25*(6), 2021-2037.

14. Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE communications magazine*, *55*(12), 119-125.

15. Garg, P., Gupta, B., Kapil, K. N., Sivarajah, U., & Gupta, S. (2023). Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector. *Annals of Operations Research*, 1-34.

16. Garg, P., Gupta, B., Kapil, K. N., Sivarajah, U., & Gupta, S. (2023). Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector. *Annals of Operations Research*, 1-34.

17. Groce, A., Feist, J., Grieco, G., & Colburn, M. (2020). What are the actual flaws in important smart contracts (and how can we find them)?. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (pp. 634-653). Springer International Publishing.

18. Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE access*, *8*, 24746-24772.

19. Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060.

20. Hofmann, F., Wurster, S., Ron, E., & Böhmecke-Schwafert, M. (2017, November). The immutability concept of blockchains and benefits of early standardization. In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)* (pp. 1-8). IEEE.

21. Ibáñez, L. D., O'Hara, K., & Simperl, E. (2018, July). On blockchains and the general data protection regulation. EU Blockchain Forum and Observatory.

22. Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of logic-based smart contracts for blockchain systems. In *Rule Technologies. Research, Tools, and Applications: 10th International Symposium, RuleML 2016, Stony Brook, NY, USA, July 6-9, 2016. Proceedings 10* (pp. 167-183). Springer International Publishing.

23. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073.

24. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073.

25. Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 283-295).

26. Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S. M., & Felten, E. W. (2018). Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 1353-1370).

27. Kim, S., & Ryu, S. (2020, September). Analysis of blockchain smart contracts: Techniques and insights. In *2020 IEEE Secure Development (SecDev)* (pp. 65-73). IEEE.

28. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

29. Kowalski, M., Lee, Z. W., & Chan, T. K. (2021). Blockchain technology and trust relationships in trade finance. *Technological forecasting and social change*, *166*, 120641.

30. Lahkani, M. J., Wang, S., Urbański, M., & Egorova, M. (2020). Sustainable B2B E-commerce and blockchain-based supply chain finance. *Sustainability*, *12*(10), 3968.

31. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, *107*, 841-853.

32. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, May). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)* (pp. 468-477). IEEE.

33. Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y. C., & Kim, D. I. (2019). A survey on blockchain: A game theoretical perspective. *IEEE Access*, *7*, 47615-47643.

34. Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., ... & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in

blockchain: the DAO attack. *Journal of Cases on Information Technology (JCIT)*, *21*(1), 19-32.

35. Moubarak, J., Filiol, E., & Chamoun, M. (2018, April). On blockchain security and relevant attacks. In *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* (pp. 1-6). IEEE.

36. Niya, S. R., Shüpfer, F., Bocek, T., & Stiller, B. (2018, April). Setting up flexible and light weight trading with enhanced user privacy using smart contracts. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-2). IEEE.

37. Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations* (pp. 225-253). Edward Elgar Publishing.

38. Poongodi, M., Sharma, A., Vijayakumar, V., Bhardwaj, V., Sharma, A. P., Iqbal, R., & Kumar, R. (2020). Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system. *Computers & Electrical Engineering*, *81*, 106527.

39. Riad, K., & Elhoseny, M. (2022). A blockchain-based key-revocation access control for open banking. *Wireless Communications and Mobile Computing*, *2022*(1), 3200891.

40. Sai, B. D. S., Nikhil, R., Prasad, S., & Naik, N. S. (2023). A decentralised KYC based approach for microfinance using blockchain technology. *Cyber Security and Applications*, *1*, 100009.

41. Scott, B., Loonam, J., & Kumar, V. (2017). Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strategic change*, *26*(5), 423-428.

42. Shrivas, M. K., & Yeboah, T. (2019). The disruptive blockchain: types, platforms and applications. *Texila International Journal of Academic Research*, *3*, 17-39.

43. Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, *65*, 263-274.

44. Thommandru, A., & Chakka, B. (2023). Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks. *Sustainable Futures*, *5*, 100107.

45. Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A., & Njilla, L. (2017, May). Security implications of blockchain cloud with analysis of block withholding attack. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)* (pp. 458-467). IEEE.

46. Wang, L., Luo, X. R., Lee, F., & Benitez, J. (2022). Value creation in blockchain-driven supply chain finance. *Information & management*, *59*(7), 103510.

47. Wang, R., & Wu, Y. (2021). [Retracted] Application of Blockchain Technology in Supply Chain Finance of Beibu Gulf Region. *Mathematical Problems in Engineering*, *2021*(1), 5556424.

48. Yuan, R., Xia, Y. B., Chen, H. B., Zang, B. Y., & Xie, J. (2018). Shadoweth: Private smart contract on public blockchain. *Journal of Computer Science and Technology*, *33*, 542-556.

49. Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016, October). Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security* (pp. 270-282).

50. Zhang, S., & Lee, J. H. (2019). Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE transactions on Industrial Informatics*, *15*(10), 5715-5722.

51. Zyskind, G., Nathan, O., & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, *14*.