



Oracle Architecture in the Blockchain Data Structure Management

A. Sobhani^{*,1}

¹ Department of Electrical and Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Received: 12 October 2022
Accepted: 28 December 2022

KEYWORDS:

Oracle,
Blockchain,
Distributed Database,
Architecture,
Smart Contract,

Corresponding author
✉ A_Sobhani@yahoo.com

Blockchain is a revolution in the field of information and communication technology, which was able to create outstanding developments in technology and the daily life of users and affect the internet payment process, by its benefits and applications. Investing in digital currencies has always been associated with a lot of risk due to the fact that their use is separate from the real world. Recently, this risk was largely covered by smart contracts. But the reality is that a smart contract without the use of strong information management systems like Oracle is often worthless. For the global adoption of blockchains, a reliable mechanism that facilitates communication between smart contracts and the outside world is critical. Without blockchain-based oracles, smart contracts are forced to rely solely on in-network information, which significantly limits their capabilities. Decentralized oracles have the potential to create security mechanisms that remove many systemic risks from the blockchain ecosystem. Blockchain oracles are one of the most important elements that make up the blocks, which operate with a safe, reliable function and without the need for mutual trust, to improve the blockchain ecosystem. In this article, we examined the application of Oracle architecture in the management of data structures in the field of blockchain.



NUMBER OF REFERENCES
20



NUMBER OF FIGURES
2



NUMBER OF TABLES
0

بکارگیری معماری اوراکل در مدیریت ساختارهای داده های حوزه بلاکچین

علی سبحانی^{۱*}

^۱ گروه کامپیوتر، دانشکده برق و کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

بلاکچین انقلابی در حوزه فناوری اطلاعات و ارتباطات است که توانست تحولات برجسته‌ای در تکنولوژی و زندگی روزمره کاربران ایجاد کند و پروسه پرداخت اینترنتی را تحت تاثیر مزایا و کاربردهای خود قرار دهد. سرمایه‌گذاری بر روی ارزهای دیجیتال به علت جدا بودن کاربرد آن‌ها از دنیای واقعیت همیشه با خطر و ریسک فراوانی همراه بوده است. اخیراً این ریسک را قراردادهای هوشمند تا حد زیادی پوشش دادند. اما واقعیت این است که یک قرارداد هوشمند بدون بهره‌گیری از سیستم‌های مدیریت اطلاعات قوی مانند اوراکل غالباً بی‌ارزش باشد. برای پذیرش جهانی بلاکچین‌ها، مکانیزم قابل اتکایی که ارتباط میان قراردادهای هوشمند و دنیای خارج را تسهیل می‌کند، حیاتی است. بدون اوراکل‌های بر بستر بلاکچین، قراردادهای هوشمند مجبورند که تنها به اطلاعات درون شبکه اتکا کنند که به طور قابل توجهی قابلیت‌های آنها را محدود می‌کند. اوراکل‌های غیرمتمرکز، پتانسیل ایجاد مکانیزم‌های امنیتی که بسیاری از ریسک‌های سیستمی را از اکوسیستم بلاک چین حذف کنند را دارند. اوراکل‌های بلاکچینی، از مهمترین عناصر تشکیل دهنده بلوک‌ها هستند که با عملکردی ایمن، قابل اطمینان و بدون نیاز به اعتماد متقابل، برای ارتقاء اکوسیستم بلاکچین فعالیت می‌کنند. در این مقاله بکارگیری معماری اوراکل در مدیریت ساختارهای داده در حوزه بلاکچین را بررسی نمودیم.

واژگان کلیدی:

اوراکل،
بلاکچین،
پایگاه داده توزیعی،
معماری،
قرارداد هوشمند،


تعداد مراجع
۲۰


تعداد شکل‌ها
۲


تعداد جداول
۵

لایه امنیتی (پایگاه‌های داده دیگر فقط یک لایه امنیتی دارند)

- سرعت بالا و دسترسی سریع به اطلاعات در حجم انبوه
- توانایی نگهداری حجم انبوه و بالای اطلاعات
- سرویس دهی همزمان به تعداد زیادی کاربر (بدون کاهش زمان پاسخگویی سیستم)
- دارای قابلیت کنترل همزمانی در سیستم شبکه
- دارای قابلیت عملیات پشتیبان‌گیری از اطلاعات به صورت اتوماتیک
- قابلیت آرشیو Online اطلاعات
- امکان بازیابی سریع و راحت اطلاعات با استفاده از ابزار Recovery Manager
- امکان کنترل و مدیریت بانک اطلاعاتی به طور ساده با استفاده از ابزار EnterPrise Manager
- امکان مدیریت و کنترل سیستم به صورت Remote Access و متصل شدن کاربران از محل‌های دیگر تنها با یک خط تلفن و کنترل و مدیریت بانک اطلاعاتی
- مدیریت دیسک تحت عنوان ASM و جاسازی Data File ها، Control File ها و Log File ها روی گروه‌های تعریف شده
- قابلیت ایجاد Snapshot برای بازگشت به یک نقطه زمانی خاص
- راه‌اندازی دیتابیس‌های پشتیبان توزیعی
- دارای قابلیت راه‌اندازی و اتصال چندین پایگاه داده در نقاط مختلف جغرافیایی به یکدیگر
- سفارشی سازی در استفاده از منابع سرور مانند CPU، Disk و RAM

در حوزه سیستم‌های مدیریت داده امروزه زنجیره بلوکی نیز سیستمی برای ثبت و ضبط داده‌ها به حساب می‌آید. این داده‌ها می‌توانند برای نمونه تراکنش‌های بانکی باشند یا اسناد مالکیت، قراردادها، پیام‌های شخصی یا دیگر اطلاعات. ویژگی زنجیره بلوکی این است که کار ذخیره این داده‌ها بدون وجود یک مدیر و صاحب‌اختیار مرکزی امکان‌پذیر است و نمی‌توان با تخریب یک نقطه مرکزی داده‌های ذخیره‌شده را تحریف یا نابود کرد. معروف‌ترین کاربرد زنجیره‌های بلوکی، رمز ارز بیت‌کوین است. در یک تعریف کلی، می‌توانیم بگوییم بلاک چین یک دفتر کل توزیع شده، غیرمتمرکز و اشتراکی است که به صورت زنجیره‌ای از سوابق بنام بلاک ساخته شده است. هر بلاک در این زنجیره، مسئول ذخیره‌سازی نوعی از اطلاعات است. در فضای بلاکچین، اوراکل اساساً یک منبع داده است که به عنوان یک پل ارتباطی

بانک اطلاعاتی یا همان پایگاه داده^۱ مجموعه‌ای سازمان‌یافته از داده‌ها است. پایگاه‌های داده از ذخیره‌سازی الکترونیکی و ایجاد تغییر در داده‌ها پشتیبانی می‌کنند. اساساً ذخیره، بازیابی و مدیریت داده‌های نامتمرکز به وسیله پایگاه داده بسیار آسان می‌شود. برای مدیریت داده‌ها در یک بانک اطلاعاتی از سیستم مدیریت پایگاه داده^۲ یا همان DBMS استفاده می‌شود. بهره‌گیری از پایگاه داده‌های کارآمد در سیستم مدیریت داده‌های سازمانی موجب امنیت بالا و پیشرفته داده‌ها، کاهش افزونگی داده‌ها، افزایش ماندگاری داده‌ها، یکپارچگی و استقلال داده‌ها، بهبود دسترسی به داده‌ها برای کاربران و تسهیل توسعه برنامه‌های کاربردی جدید می‌گردد [۱-۲].

اوراکل یک سیستم مدیریت پایگاه داده رابطه‌ای است که توسط شرکت Oracle ایجاد و اداره می‌شود. این سیستم مدیریت پایگاه داده در حال حاضر، از چندین مدل داده مانند سند، نمودار، رابطه‌ای و مقدار-کلید در پایگاه داده واحد پشتیبانی می‌کند. در آخرین نسخه‌های خود نیز در محاسبات ابری مورد استفاده قرار گرفت. مجوز موتور دیتابیس اوراکل کاملاً اختصاصی است و گزینه‌های رایگان و پولی در دسترس است. بانک اطلاعاتی اوراکل مجموعه‌ای از داده‌ها است که به عنوان یک واحد جهت مدیریت ذخیره و بازیابی داده‌ها مورد استفاده قرار می‌گیرد. سرور بانک اطلاعاتی، کلید حل مشکلات مدیریت اطلاعات است. به طور کلی، یک سرور با اطمینان قابل توجهی می‌تواند مقدار زیادی از داده‌ها را در یک محیط چند کاره مدیریت کند تا بسیاری از کاربران بتوانند همزمان به همان داده‌ها دسترسی پیدا کنند. همه این قابلیت‌ها در حین ارائه کارایی بالا انجام می‌شود. سرور پایگاه داده همچنین از دسترسی غیرمجاز جلوگیری می‌کند و راه حل‌های کارآمدی برای بازیابی خرابی ارائه می‌دهد. مهم‌ترین مزایای این سیستم مدیریت پایگاه داده در ادامه لیست شده‌اند [۳-۵]:

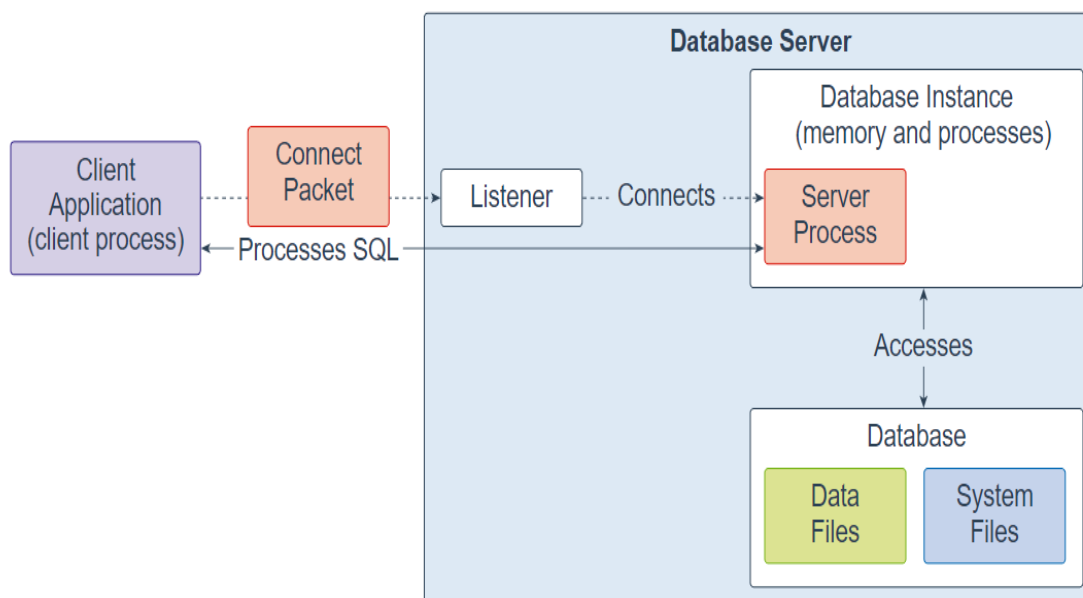
- رابط کاربری قوی و وجود نسخه‌های متنوع با قابلیت‌های متفاوت برای این پایگاه داده
- امکان نصب و استفاده از آن روی تمامی سیستم‌عامل‌ها و پلتفرم‌های مختلف و خدمات پشتیبانی قوی کمپانی اوراکل
- قابلیت کنترل صحت اطلاعات به صورت اتوماتیک و جلوگیری از ورود اطلاعات غیر معتبر
- عدم وجود خرابی، بهم ریختگی و از بین رفتن اطلاعات
- ضریب امنیتی بالای سیستم و جلوگیری از دسترسی غیر مجاز کاربر به اطلاعات با داشتن ۱۴

² Database Management System (DBMS)

¹ Database

معماری اوراکل

اوراکل یکی از بزرگ‌ترین سیستم‌های مدیریت پایگاه‌های داده در صنعت است. در این قسمت قصد داریم ابتدا با معماری اوراکل آشنا شویم و آن را به صورت جزئی بررسی کنیم. اوراکل از Database و حداقل یک Database Instance تشکیل شده است. هر Database Instance یا به اختصار Instance، مجموع Memory و Process و هر Database مجموعه‌ای از فایل‌ها است. تصویر زیر معماری Oracle Database Server را به خوبی نشان می‌دهد [۸-۹]:



شکل ۱. معماری سرویس دهنده پایگاه داده اوراکل

به طور کلی هر Database Instance رابطی بین کاربر و Database می‌باشد. هر Database Instance شامل سه بخش به شرح زیر می‌باشد.

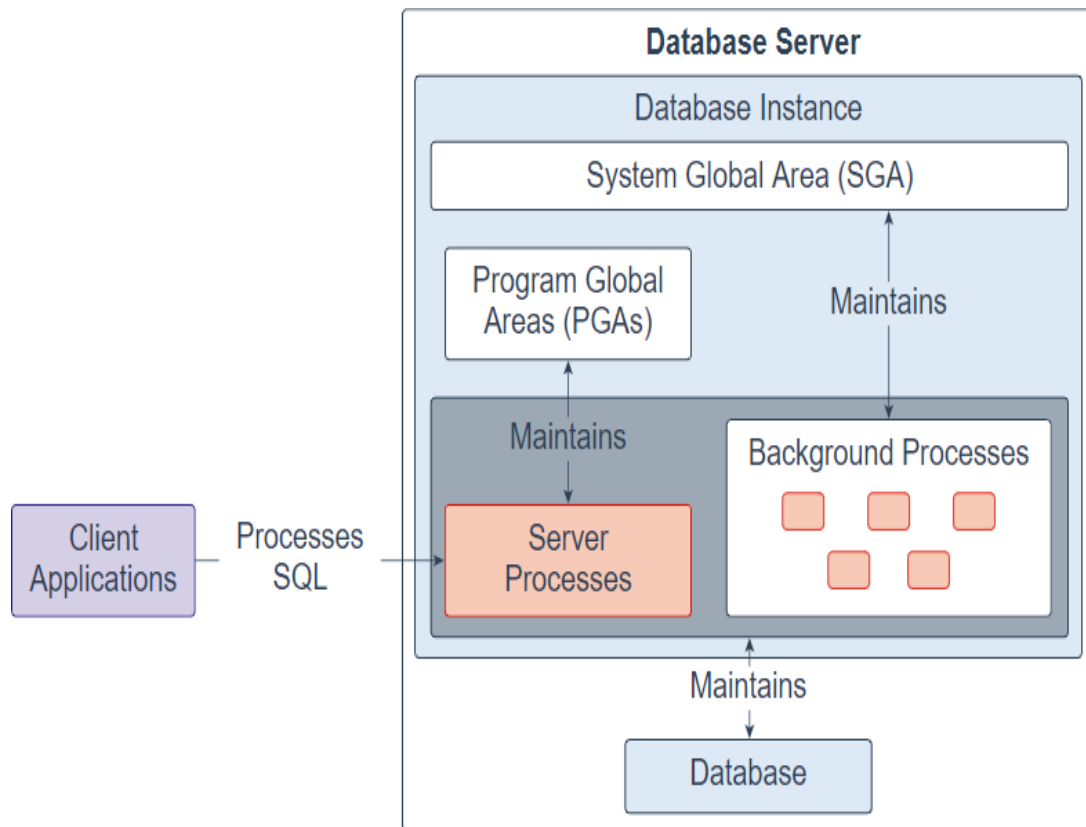
- System Global Area (SGA)
- Program Global Area (PGA)
- Background Processes

هنگام شروع Database Instance یک SGA ایجاد می‌شود. این بخش یک فضای حافظه اشتراکی است که زمان خاموش شدن Database Instance از حافظه آزاد می‌شود. در طرف دیگر این زیرساخت PGA را داریم که در دسترس همه Process‌ها می‌باشد و به ازای هر Session ایجاد شده و در پایان از حافظه آزاد می‌شود. شکل زیر معماری کلی Database Instance را به خوبی نمایش می‌دهد [۱۱].

بین قراردادهای هوشمند و دیگر منابع خارجی مورد استفاده قرار می‌گیرد. به طور تخصصی‌تر می‌توان گفت که یک واسط مدیریت داده اوراکل عاملی است که نه تنها با منابع داده خارجی ارتباط برقرار می‌کند، بلکه به تایید و بررسی صحت داده‌های فراهم شده نیز می‌پردازد [۶-۷]. اخیراً در سیستم‌های مدیریت داده اوراکل‌ها یکی از مولفه‌های اصلی در فناوری بلاکچین محسوب می‌شوند و در تعیین نحوه پاسخگویی بلاکچین به درخواست‌های کاربران، نقشی کلیدی را ایفا می‌کنند. از آنجا که فرایندهای سختگیرانه‌ای جهت ارتباط قراردادهای هوشمند با منابع داده خارجی وجود دارد، اوراکل وظیفه این تبادل داده‌ها را ایفا می‌کند. در ادامه این مقاله پس از معرفی معماری اوراکل به بررسی و موارد استفاده از اوراکل در بلاکچین خواهیم پرداخت.

لازم به ذکر است، هر instance تنها می‌تواند به یک database دسترسی داشته باشد. همچنین می‌توانیم چند instance تعریف کرده که همه آن‌ها به یک database دسترسی داشته باشند. هر Database مجموعه‌ای از فایل‌ها را شامل می‌شود. اوراکل برای مدیریت فایل‌ها ساختاری ارائه کرده است که می‌توانیم Database خود را به صورت ریزدانه مدیریت کنیم. واحدهای مختلفی برای مدیریت حافظه وجود دارد که عبارتند از [۱۰]:

- Data blocks
- Extents
- Segments
- Tablespaces



شکل ۲. ساختار معماری Database Instance

لازم به ذکر است، پل ارتباطی کاربر و Database Instance در معماری ارائه شده، Listener است. در ابتدا دستورات از طرف کاربر به Listener می‌رسد و در ادامه Listener آن را به Database Instance می‌فرستد. درواقع، اگر Listener در دسترس نباشد، نمی‌توانیم با Database Instance ارتباط برقرار کنیم. امروزه، اوراکل‌ها یکی از مولفه‌های اصلی در فناوری بلاکچین محسوب می‌شوند و در تعیین نحوه پاسخگویی بلاکچین به درخواست‌های کاربران، نقشی کلیدی را ایفا می‌کنند. در قسمت‌های بعدی مقاله حاضر بصورت مبسوط تر به این موضوع می‌پردازیم [۱۲].

بکارگیری اوراکل در بلاک چین در مدیریت ساختارهای داده در بلاکچین

بلاک چین‌ها و شبکه‌هایی که جدیداً بحث‌های داغی در مورد آنها ایجاد شده است و محصولاتی به شدت پربازده را عرضه کردند، یکی دیگر مواردی هستند که Oracle برای خود یک کارایی جدید را دست و پا کرده است. بلاک چین‌ها در واقع داده‌های رمزنگاری شده‌ای را بر مبنای بلاک‌های داده‌ای پشت سر هم ایجاد می‌کنند. این داده‌ها به یک سیستم مدیریتی نیاز دارند که بتواند این حجم عظیم از داده‌ها را مدیریت کند. اوراکل همانند یک پل، دنیای خارج فناوری محور را به شبکه داخلی بلاکچین متصل می‌کند. بلاک چین یا قرارداد هوشمند، شبکه‌های بسته‌ای هستند که به داده‌های دنیای بیرون دسترسی ندارند و از آنجا که این شبکه‌ها باید اطلاعات را از دنیای خارج دریافت کنند به اوراکل نیاز دارند. نقش پایگاه داده Oracle در بلاکچین بسیار مهم و حیاتی است و در صورت نبود آن، به علت اینکه بلاک چین فقط به داده‌های درون شبکه خود دسترسی دارد، دامنه فعالیت قراردادهای هوشمند به طور قابل توجهی کاهش پیدا می‌کند. آماده کردن داده‌های ورودی اصلی‌ترین و مهم‌ترین نقش اوراکل در بلاکچین محسوب می‌شود. همچنین اوراکل‌ها امکان تولید قراردادهای هوشمند (مجموعه از کدهای قابل اجرا بدون نیاز به نیروی انسانی) را نیز دارند [۱۳].

همچنین اوراکل‌ها مکانیسمی به منظور فراهم کردن اطلاعات مهم و قابل اعتماد برای قراردادهای هوشمند هستند که این قراردادها هم به نوبه خود وظایف معینی را انجام می‌دهند. پس مفهوم اوراکل در فضای بلاک چین کمی با فناوری‌های دیگر متفاوت است. اهمیت اوراکل‌ها بر این حقیقت استوار است که قراردادهای هوشمند بلاکچینی تنها قادر به دسترسی به داده‌هایی هستند که در داخل زنجیره آنها قرار گرفته است. بنابراین آنها به عنوان یک ابزار ارتباطی

ایفای نقش می‌کنند که رویدادهای جهان واقعی را به داده‌های دیجیتال تبدیل می‌کنند. اوراکل‌ها مسیری را برای اکوسیستم غیرمتمرکز وب مهیا می‌کنند تا بتوان از این طریق آنها به منابع داده‌های موجود، سیستم‌های سنتی و محاسبات پیشرفته دسترسی داشت. شبکه‌های غیرمتمرکز اوراکل امکان شناخت قراردادهای هوشمند ترکیبی را فراهم می‌کنند. این قراردادها بستری را در اختیار ما قرار می‌دهند تا بتوان کد آچین یا درون زنجیره و زیرساخت آچین یا بیرون زنجیره‌ای را برای پشتیبانی از برنامه‌های غیرمتمرکز ترکیب کرد و به رویدادهای دنیای واقعی و سیستم‌های سنتی واکنش نشان داد. اوراکل‌های بلاکچین را می‌توان بسته به تعدادی از کیفیت‌های مختلف طبقه‌بندی کرد [۱۴-۱۶]:

اوراکل‌های نرم افزاری

اوراکل‌های نرم افزاری با منابع اطلاعاتی آنلاین ارتباط برقرار می‌کنند و آن را به بلاکچین منتقل می‌کنند. این اطلاعات می‌تواند از پایگاه‌های داده آنلاین، سرورها، وب سایت‌ها (اساساً هر منبع داده در وب) بدست آید. این واقعیت اوراکل‌های نرم افزاری به اینترنت متصل هستند نه تنها به آنها امکان می‌دهد اطلاعات را به قراردادهای هوشمند عرضه کنند بلکه می‌توانند این اطلاعات را به صورت بدون معطلی انتقال دهند. همین امر آنها را به یکی از متداول‌ترین اوراکل‌های بلاکچین تبدیل می‌کند. اطلاعاتی که معمولاً توسط اوراکل‌های نرم افزاری ارائه می‌شوند می‌توانند شامل نرخ ارز، قیمت دارایی‌های دیجیتال یا اطلاعات پرواز در زمان واقعی باشند.

اوراکل‌های سخت افزاری

برخی از قراردادهای هوشمند باید با دنیای واقعی ارتباط برقرار کنند. اوراکل‌های سخت افزاری برای به دست آوردن اطلاعات از دنیای فیزیکی و در دسترس قرار دادن قراردادهای هوشمند طراحی شده‌اند. چنین اطلاعاتی را می‌توان از طریق سنسورهای الکترونیکی، اسکنر بارکد و سایر دستگاه‌های خواندن اطلاعات ارسال کرد. یک اوراکل سخت افزاری اساساً وقایع دنیای واقعی را به مقادیر دیجیتالی تبدیل می‌کند که با قراردادهای هوشمند قابل درک است. به عنوان مثال می‌توان سنسوری را بررسی کرد که آیا کامیونی که یک کالا را حمل می‌کند به محل بارگیری رسیده است یا خیر. اگر انجام شود اطلاعات را به یک قرارداد هوشمند انتقال می‌دهد که می‌تواند تصمیمات مبتنی بر آن را اجرا کند.

اوراکل‌های ورودی و خروجی

اوراکل‌های ورودی اطلاعات را از منابع خارجی به قراردادهای هوشمند منتقل می‌کنند در حالی که اوراکل‌های خروجی اطلاعات قراردادهای هوشمند را به دنیای خارج می‌فرستند.

اوراکل های متمرکز و غیرمتمرکز

یک اوراکل متمرکز توسط یک نهاد واحد کنترل می شود و تنها ارائه دهنده اطلاعات قرارداد هوشمند است. استفاده از تنها یک منبع اطلاعاتی می تواند مخاطره آمیز باشد چرا که اثربخشی قرارداد کاملاً به نهادی بستگی دارد که این اوراکل را کنترل کند. همچنین هرگونه تداخل مخرب توسط یک بازگر بد تأثیر مستقیم در قرارداد هوشمند خواهد داشت. مشکل اصلی اوراکل متمرکز وجود یک نقطه شکست است که باعث می شود قراردادهای در برابر آسیب پذیری ها و حملات مقاومت کمتری داشته باشند. اوراکل های غیر متمرکز برخی از اهداف مشابه بلاکچین های عمومی را دارند یعنی جلوگیری از خطر طرف مقابل. آنها با اطمینان از اعتماد نکردن به یک منبع صادق، قابلیت اطمینان به اطلاعات ارائه شده به قراردادهای هوشمند را افزایش می دهند. قرارداد هوشمند برای تعیین اعتبار و صحت داده ها از چندین اوراکل استفاده می کند. به همین دلیل است که از اوراکل غیرمتمرکز می توان به عنوان اوراکل اجماع نیز نام برد.

اوراکل های مخصوص قرارداد

اوراکل مخصوص قراردادی است که برای استفاده در یک قرارداد هوشمند طراحی شده است. این بدان معناست که اگر کسی بخواهد چندین قرارداد هوشمند را به کار بگیرد باید متناسب با مبلغ خاص قرارداد تهیه شود. این نوع اوراکل بسیار وقت گیر و نگهداری آن گران قیمت در نظر گرفته می شود. شرکت هایی که می خواهند از منابع مختلف داده استخراج کنند ممکن است این روش را بسیار غیر عملی تشخیص دهند. از طرف دیگر از آنجا که می توان اوراکل های خاص قرارداد را از ابتدا برای استفاده در یک مورد خاص استفاده کرد، توسعه دهندگان انعطاف پذیری بالایی دارند تا آنها را متناسب با نیازهای خاص تنظیم کنند.

اوراکل های انسانی

بعضی اوقات افراد با دانش تخصصی در یک زمینه خاص می توانند به عنوان اوراکل عمل کنند. آنها می توانند صحت اطلاعات را از منابع مختلف تحقیق و بررسی کنند و این اطلاعات را به قراردادهای هوشمند ترجمه کنند. از آنجا که اوراکل های انسانی می توانند هویت خود را با استفاده از رمزنگاری تأیید کنند احتمال جعل هویت توسط یک کلاهبردار و ارائه داده های خراب نسبتاً کم است. از سوی دیگر، مشکل اوراکل در بلاک چین نشان دهنده یک محدودیت بنیادین از قراردادهای هوشمند است. این قراردادهای توانایی ذاتی تعامل داشتن با داده ها و سیستم های موجود در بیرون از محیط بلاک چین بومی خود را ندارند. منابع خارج از بلاک چین به صورت آفچین یا بیرون زنجیره ای به حساب می آیند، این در

شرایطی است که داده هایی که در درون بلاک چین ذخیره شده اند به صورت آفچین یا بیرون زنجیره ای در نظر گرفته می شوند. با قطع کردن عمدی این بستر از سیستم های خارجی، بلاک چین ها با ارزش ترین ویژگی های خود مانند اجماع قوی اعتبار تراکنش های کاربر، جلوگیری از حملات، هزینه مازاد و کاهش میزان زمان از دسترس خارج بودن شبکه را برای ما به ارمغان می آورند. تعامل ایمن با سیستم های خارج از زنجیره یک بلاک چین به زیرساخت اضافه ای تحت عنوان اوراکل برای ایجاد پلی بین دو محیط نیاز دارد.

از سوی دیگر، اوراکل ها می توانند با حفظ جنبه های امنیتی ارزشمند بلاکچین، یک درگاه جهانی از منابع بیرون زنجیره ای را به منظور گسترش کاربردهای صنعت بلاکچین، برای این صنعت فراهم کنند. صنایع بزرگ از ترکیب اوراکل ها و قراردادهای هوشمند و کاربردهایی از جمله قیمت دارایی ها در امور مالی، اطلاعات آب و هوا برای بیمه، قابلیت تصادفی درون بازی ها، حسگرهای اینترنت اشیا (IoT) برای زنجیره تامین، احراز هویت برای دولت و غیره منفعت می برند. با توجه به اینکه داده های ارسال شده از اوراکل ها به بلاکچین ها تأثیر مستقیمی بر روی نتایج حاصل شده از قراردادهای هوشمند دارد، صحیح بودن مکانیسم مورد استفاده اوراکل برای اطمینان حاصل کردن از اجرای دقیق توافقنامه به صورت مورد انتظار ما، از اهمیت بالایی برخوردار است. مکانیسم های اوراکل در بلاک چین با استفاده از یک موجودیت متمرکز برای تحویل دادن داده به قرارداد هوشمند، نشان دهنده نقطه ضعف بزرگی است. این امر به از بین رفتن کل کاربرد غیرمتمرکزسازی بلاک چین منجر می شود. اگر یک اوراکل واحد در این مثال به صورت آفلاین در بیاید، قرارداد هوشمند دیگر به داده های مورد نیاز برای اجرای صحیح دسترسی نخواهد داشت و یا به صورت نادرست و بر اساس داده های قدیمی به کار خود ادامه می دهد [۱۷].

علاوه بر این، با توجه به اینکه تراکنش های بلاکچین خودکار بوده و غیرقابل تغییر هستند، نتایج یک قرارداد هوشمند مبتنی بر داده نادرست نیز غیرقابل بازگردانی است. این بدان معناست که منابع مالی کاربران به صورت دائمی از بین می رود. بنابراین اوراکل های متمرکز رویکرد مناسبی برای شروع کار برنامه های غیرمتمرکز نیستند. امروزه شناخته شده ترین نوع اوراکل در بلاک چین تحت عنوان اوراکل ورودی نامگذاری می شود، که داده ها را از دنیای واقعی (آفچین) دریافت کرده و آن را به یک شبکه بلاک چین و برای مصرف در قراردادهای هوشمند تحویل می دهد. سه نوع از اوراکل ها برای تامین فیدهای قیمت در شبکه چین لینک مورد استفاده قرار

می‌گیرند تا قراردادهای هوشمند دیفای بتوانند به صورت آنچین به داده‌های امور مالی بازار دسترسی داشته باشند [۱۸].

یکی از جدیدترین انواع اوراکل‌هایی که به صورت گسترده مورد استفاده برنامه‌های قراردادهای هوشمند قرار گرفته است اوراکل‌های محاسباتی هستند، که از محاسبات ایمن بیرون زنجیره‌ای برای ارائه خدمات غیرمتمرکزی استفاده می‌کنند که به دلایل فنی، قانونی یا محدودیت‌های مالی در بستر آنچین بدون کاربرد هستند. یکی از انواع این اوراکل‌ها که توسط شبکه چین لینک معرفی شده است، Chainlink Keepers نام دارد. این قابلیت امکان اجرای خودکار قراردادهای هوشمند در هنگام اتفاق افتادن یک رویداد از پیش تعریف شده، فراهم می‌کند. توسعه‌دهندگان قراردادهای هوشمند از اوراکل‌های استفاده می‌کنند تا برنامه‌های غیرمتمرکز پیشرفته‌تری را در طیف گسترده‌تری از کاربردهای بلاکچین بسازند. در حوزه کاربردهای پروژه ای، اوراکل‌های میان زنجیره‌ای، یک میان‌افزار امن بلاک چین را به شرکت‌ها ارائه می‌دهند، این میان‌افزار به آن‌ها اجازه می‌دهد تا اپلیکیشن‌های خود را به هر یک از شبکه‌های بلاک چینی متصل کنند. با انجام این کار، توسعه‌دهندگان می‌توانند اطلاعات مورد نیاز خود را در تمامی بلاک چین‌ها بخوانند یا در آنها ثبت کنند. نتیجه این امر این است که موسسات می‌توانند به سرعت به بلاک چین‌های مختلف بپیوندند و به سرعت انواع خدمات مورد نیاز کاربران خود را در بلاکچین‌های مختلف ایجاد کنند [۱۹-۲۰].

لازم به ذکر است، سازوکاری قابل اعتماد که ارتباط بین قراردادهای هوشمند و دنیای خارجی را تسهیل کند برای پذیرش جهانی بلاک چین‌ها حیاتی است. بدون اوراکل بلاکچین، قراردادهای هوشمند باید فقط به اطلاعات موجود در شبکه‌های خودشان اعتماد کنند، که به طور قابل توجهی توانایی‌های آنها را محدود می‌کند. اوراکل‌های غیرمتمرکز توانایی معرفی مکانیسم‌های محافظتی را دارند که می‌تواند، بسیاری از خطرهای سیستمی را از اکوسیستم بلاکچین برطرف کند. اوراکل‌های بلاک چین همچنان یکی از مهمترین عناصر سازنده ای است که برای رشد اکوسیستم بلاک چین به صورت ایمن، قابل اعتماد و بدون نیاز به اعتماد به دیگران، اجرا می‌شود.

نتیجه گیری:

امروزه اوراکل به عنوان یکی از قدرتمندترین پایگاه داده‌های جهان شناخته شده است و درحال حاضر، شرکت‌های مختلفی از آن استفاده می‌کنند. در فضای بلاکچین، اوراکل اساساً یک منبع داده است که به عنوان یک پل ارتباطی بین قراردادهای هوشمند و دیگر

منابع خارجی مورد استفاده قرار می‌گیرد. به طور تخصصی‌تر می‌توان گفت که یک اوراکل عاملی است که نه تنها با منابع داده خارجی ارتباط برقرار می‌کند، بلکه به تایید و بررسی صحت داده‌های فراهم شده نیز می‌پردازد. شبکه‌های غیرمتمرکز اوراکل امکان شناخت قراردادهای هوشمند ترکیبی را فراهم می‌کنند. اخیراً در سیستم‌های مدیریت داده، اوراکل‌ها یکی از مولفه‌های اصلی در فناوری بلاکچین محسوب می‌شوند و در تعیین نحوه پاسخگویی بلاکچین به درخواست‌های کاربران، نقشی کلیدی را ایفا می‌کنند. از آنجا که فرایندهای سختگیرانه‌ای جهت ارتباط قراردادهای هوشمند با منابع داده خارجی وجود دارد، اوراکل وظیفه این تبادل داده‌ها را ایفا می‌کند. در این مقاله پس از معرفی معماری اوراکل به بررسی و موارد استفاده از اوراکل در بلاکچین پرداختیم.

منابع:

- [1] Gao Z, Zhuang Z, Lin Y, Rui L, Yang Y, Zhao C, Mo Z. Select-Storage: A New Oracle Design Pattern on Blockchain. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) 2021 Oct 20 (pp. 1177-1184). IEEE.
- [2] Kyte T, Kuhn D. Expert Oracle Database Architecture. Apress; 2014 Nov 10.
- [3] Kuhn D, Kyte T. Expert Oracle Database Architecture: Techniques and Solutions for High Performance and Productivity. Apress; 2021.
- [4] Caldarelli G. Understanding the blockchain oracle problem: A call for action. Information. 2020 Oct 29;11(11):509.
- [5] Peasland B. Oracle DBA Mentor: Succeeding as an Oracle Database Administrator. Apress; 2019 Mar 29.
- [6] THYWISSEN JA. An Overview of the Mechanisms of Oracle RDBMS Transactions and Logs. 2013.
- [7] Yu L, Zichichi M, Markovich R, Najjar A. Enhancing trust in trust services: Towards an intelligent human-input-based blockchain oracle (ihibo). In Proceedings of the 55th Annual Hawaii International Conference on System Sciences 2022.
- [8] Caldarelli G. Overview of Blockchain Oracle Research. Future Internet. 2022 Jun 8;14(6):175.
- [9] Gryglewicz-Kacerka W, Kacerka J. Analysis of the effect of chosen initialization parameters on database performance. In Beyond

- [19] Daif A, Eljamiy F, Azzouazi M, Marzak A. Review current CRM architectures and introducing new adapted architecture to Big Data. In 2015 International Conference on Computing, Communication and Security (ICCCS) 2015 Dec 4 (pp. 1-7). IEEE.
- [20] Du Y, Li J, Shi L, Wang Z, Wang T, Han Z. A Novel Oracle-aided Industrial IoT Blockchain: Architecture, Challenges, and Potential Solutions. IEEE Network. 2022 Aug 8.
- Databases, Architectures and Structures: 11th International Conference, BDAS 2015, Ustroń, Poland, May 26-29, 2015, Proceedings 11 2015 (pp. 60-68). Springer International Publishing.
- [10] Widiyanto SR, Rahman R, Kulsum LK, Yahtadi M. Enterprise Architecture Blending Cycle. Jurnal Mantik. 2020 Nov 1;4(3):1825-30.
- [11] Adler J, Berryhill R, Veneris A, Poulos Z, Veira N, Kastania A. Astraea: A decentralized blockchain oracle. In 2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) 2018 Jul 30 (pp. 1145-1152).
- [12] Purnama SA. PERENCANAAN ARSITEKTUR SISTEM INFORMASI PT. MA'SOEM ARIAS DENGAN MENGGUNAKAN ORACLE ENTERPRISE ARCHITECTURE FRAMEWORK. Jurnal Accounting Information System (AIMS). 2018 Dec 12;1(2):125-41.
- [13] Sheldon MD. Auditing the blockchain oracle problem. Journal of Information Systems. 2021;35(1):121-33.
- [14] Beniiche A. A study of blockchain oracles. arXiv preprint arXiv:2004.07140. 2020 Mar 19.
- [15] Lo SK, Xu X, Staples M, Yao L. Reliability analysis for blockchain oracles. Computers & Electrical Engineering. 2020 May 1;83:106582.
- [16] Macías SG, Gaspary LP, Botero JF. Oracle: An architecture for collaboration of data and control planes to detect ddos attacks. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM) 2021 May 17 (pp. 962-967). IEEE.
- [17] Hess Z, Malahov Y, Pettersson J. Æternity blockchain. Online]. Available: <https://aeternity.com/aeternity-blockchainwhitepaper.pdf>. 2017 Jan 23.
- [18] Lv P, Zhang X, Liu J, Wei T, Xu J. Blockchain Oracle-Based Privacy Preservation and Reliable Identification for Vehicles. In Wireless Algorithms, Systems, and Applications: 16th International Conference, WASA 2021, Nanjing, China, June 25-27, 2021, Proceedings, Part III 2021 Sep 9 (pp. 512-520). Cham: Springer International Publishing.