APJ. 5(3):1-9, Autumn 2024

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Examining the Security Dimensions of Blockchain with a Focus on the E-Commerce Financial Transactions

A. Hamidpoor[*,1], M. Rahimi[2]

[1] Computer Department, Islamic Azad University, Bandar Abbas Branch, Iran
[2] Computer Department, Islamic Azad University, Bandar Abbas Branch, Iran

ABSTRACT

RESEARCH PAPER

Received: 25 June 2024
Accepted: 12 October 2024

KEYWORDS:
Blockchain,
Smart Contract,
Cyber Attacks,
Security,

Blockchain is a new technology whose purpose is to store and transfer any type of data in a decentralized manner. In this system, nodes are responsible for confirming and registering transactions, each of these nodes are distributed around the world and use different algorithms to perform their tasks correctly. In blockchain technology, data security has a very high value, and this technology can make our private information more secure and prevent the disclosure of this information. Blockchain security is ensured through various mechanisms, including advanced encryption techniques and mathematical models of behavior and decision making. Blockchain technology is the basic structure of most cryptosystems and what prevents the repetition or destruction of this type of digital currency and interference in the cycle of purchasing digital currency. In this article, in particular, blockchain security in the field of e-commerce is examined and cyber attacks against blockchain and challenges in this field are introduced.

[1] **Corresponding author:**
hamidpoor@iau.ac.ir

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۳، پاییز ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

بررسی ابعاد امنیتی بلاک چین با تمرکز بر تراکنش های مالی تجارت الکترونیک

علی حمیدپور*[۱]، مهدی رحیمی[۲]

[۱] گروه مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد بندرعباس، ایران

[۲] گروه مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد بندرعباس، ایران

چکیده

مقاله پژوهشی

بلاک چین، فناوری نوینی به شمار می‌رود که هدف از ایجاد آن ذخیره‌سازی و انتقال هر نوع داده به صورت غیرمتمرکز است. در این سیستم نودها وظیفه تایید و ثبت تراکنش‌ها را دارند، هرکدام از این نودها در سراسر دنیا توزیع شده و برای انجام درست وظایف خود، از الگوریتم‌های مختلفی استفاده می‌کنند. در فناوری بلاک چین امنیت داده‌ها از ارزش بسیار بالایی برخوردار است و این فناوری می‌تواند تا حد زیادی اطلاعات خصوصی ما را امن‌تر کرده و از افشای این اطلاعات جلوگیری کند . امنیت بلاکچین ازطریق سازوکارهای مختلفی ازجمله تکنیک‌های پیشرفته رمزنگاری و مدل‌های ریاضی رفتار و تصمیم‌گیری تضمین می‌شود. فناوری بلاکچین ساختار اساسی اکثر سیستم‌های رمزنگاری و همان چیزی است که از تکرار یا نابودی این نوع ارز دیجیتال و تداخل در چرخه خرید ارز دیجیتال مانع می‌شود. در این مقاله به طور خاص، امنیت بلاکچین درحوزه تجارت الکترونیک مورد بررسی قرار گرفته و حملات سایبری علیه بلاکچین و چالش‌های این حوزه معرفی می‌گردد.

واژگان کلیدی:
بلاکچین،
قرارداد هوشمند،
حملات سایبری،
امنیت،

مقدمه

اخیرا فناوری بلاک چین شیوه همکاری افراد و کسب و کارها در حوزه اقتصاد دیجیتال را متحول کرده است و بستری غیرمتمرکز و شفاف برای تبادل ارزش ارائه می‌دهد. بلاک چین[1] شبکه‌ای است که با استفاده از تکنولوژی‌های غیرمتمرکز[2] و رمزنگاری، تاریخچه تمام تراکنش‌های انجام شده با دارایی‌های دیجیتال مانند بیت کوین را در یک دفتر کل دیجیتال و عمومی ذخیره می‌کند. اساسا امکان تغییر در اطلاعات ذخیره شده در بلاک چین وجود ندارد و تمام اطلاعات ثبت شده در آن به صورت شفاف در اختیار کاربران قرار می‌گیرد. شبکه بلاک چین همان چیزی است که حذف بانک‌ها و مؤسسات مالی از تراکنش‌های دارایی‌های دیجیتال را امکان‌پذیر کرده و امنیت ارزهای دیجیتال را تضمین می‌کند؛ موضوعی که باعث شده دارایی‌های دیجیتال طرفداران زیادی پیدا کنند. بلاک چین‌ها بیشتر به دلیل نقش حیاتی در سیستم‌های ارزهای دیجیتال برای حفظ یک رکورد امن و غیرمتمرکز در تراکنش‌ها شناخته می‌شوند، اما موارد استفاده از آن‌ها به ارزهای دیجیتال محدود نمی‌شود. عموما بلاک چین‌ها را می‌توان برای تغییرناپذیر کردن داده‌ها در هر صنعتی مورد استفاده قرار داد. از آن‌ها می‌توان برای ایجاد برنامه‌های غیرمتمرکز ، سیستم‌های مدیریت زنجیره تأمین، سیستم‌های رای‌گیری، حسابداری نامتمرکز بانکی و موارد دیگر استفاده کرد. فناوری بلاک چین این پتانسیل را دارد که صنایع مختلف را با ایجاد اعتماد، امنیت و کارایی متحول نماید [۱] .

اساسا در بلاک چین، داده‌ها در یک دفتر کل توزیع شده نگهداری می‌شوند. این فناوری زنجیره بلوکی برای ارائه یکپارچگی و در دسترس بودن است که به شرکت‌کنندگان در شبکه بلاک چین اجازه می‌دهد تراکنش‌های ثبت‌شده در یک دفتر کل توزیع‌شده را بنویسند، بخوانند و تأیید کنند. با این حال، عملیات حذف و اصلاح تراکنش‌ها و سایر اطلاعات ذخیره شده در دفتر کل آن را مجاز نمی‌داند. سیستم بلاک چین توسط پروتکل‌ها و پروتکل‌های رمزنگاری، پشتیبانی و ایمن می‌شود، به‌عنوان مثال، امضای دیجیتال، توابع هش، و غیره. این موارد اولیه تضمین می‌کنند که تراکنش‌هایی که در دفتر ثبت می‌شوند از نظر یکپارچگی محافظت می‌شوند، از نظر اصالت تأیید می‌شوند و رد نمی‌شوند [۲] . علاوه بر این، فناوری بلاک چین به‌عنوان یک شبکه توزیع‌شده برای اینکه به کل مجموعه شرکت‌کنندگان اجازه دهد بر روی یک رکورد یکپارچه به توافق برسند، به یک پروتکل اجماع نیاز دارد که اساساً مجموعه‌ای از قوانین است که باید توسط هر شرکت‌کننده دنبال شود تا به دیدگاهی یکپارچه در سطح جهانی دست یابد. در یک محیط غیرقابل اعتماد، بلاک چین ویژگی های مطلوبی از جمله عدم تمرکز، استقلال، یکپارچگی، تغییرناپذیری، تأیید، تحمل خطا، ناشناس بودن، قابلیت حسابرسی و شفافیت را در اختیار کاربران قرار می‌دهد، که با این ویژگی‌های پیشرفته در چند سال اخیر توجه بخش زیادی از جامعه دانشگاهی و صنعتی را به خود جلب کرده است [۳].

براساس بررسی های انجام شده، کاربردهای بلاک چین شامل ارز دیجیتال، امور مالی (بورس اوراق بهادار،خدمات مالی بازار های مالی دیجیتالی، اینترنت اشیا، مراقبت‌های بهداشتی، بیمه، برنامه‌های کاربردی جامعه (موسیقی بلاک چین، دولت بلاک چین)، برنامه‌های کاربردی تلفن همراه، زنجیره تامین، اجرای قانون، ردیابی دارایی، سوابق دیجیتال، مدیریت مالکیت دیجیتال، ثبت عنوان مالکیت و غیره، کاربردهای فزاینده مارپیچی فناوری بلاک چین می باشند و انتظار می رود موارد استفاده بیشتر و بیشتری از سیستم‌های بلاک چین در آینده نزدیک در حال ظهور باشد [۴].

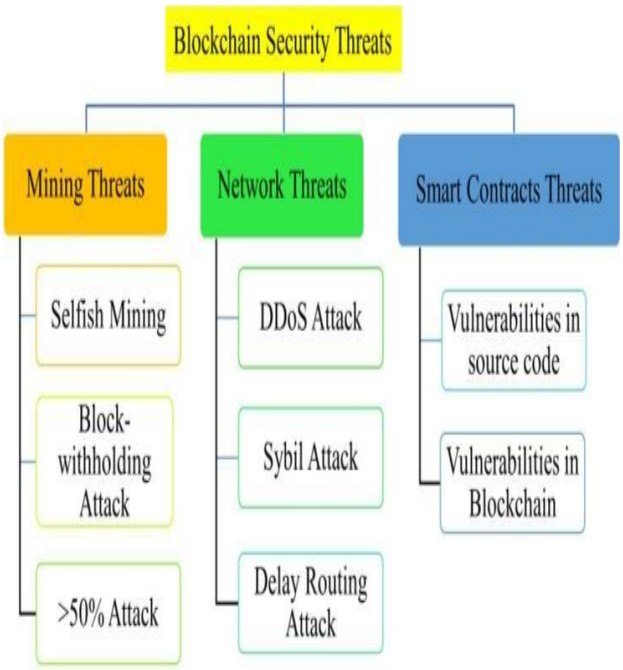
امنیت بلاک چین که مهم ترین اصل بکارگیری آن می باشد، یک سیستم یکپارچه در مدیریت ریسک برای یک شبکه بلاکچ ین، با استفاده چهارچوب ها و ابزارهای امنیت سایبری، سرویس ها تأمین امنیت کاربری و رویکردهای برنامه‌نویسی ضد هک، فیشینگ و کلاهبرداری است. منظور از امنیت بلاک چین، مجموعه تمهیداتی است که در قالب اصول رمزنگاری، تمرکززدایی و نظارت جمعی برای برخورد با هر فعالیت خرابکارانه یا کلاهبرداری اتخاذ می‌شود. هدف اصلی در امنیت بلاک چین، افزایش سطح اعتماد کاربران به سیستم در مورد حفظ اطلاعات و عملکرد مناسب و متناظر با انجام تراکنش ها و سایر خدمات تعریف شده بر بستر بلاک چین است [۵]. در بلاک چین تمام افراد نقش مدیر را دارند و می توانند خودشان به صورت مستقیم دارایی های خود را کنترل نمایند. این امر می تواند امنیت بلاک چین را افزایش دهد. علاوه بر این، دیجیتال بودن داده ها، تغییر ناپذیری آنها، وجود ویژگی اجماع، امضای دیجیتال، زنجیره ای بودن، غیرمتمرکز بودن بلاک چین، ناشناس ماندن و بسیاری از ویژگی های دیگر مانند حفظ حریم شخصی که در بلاک چین وجود دارند درصد این امنیت را بیشتر می کنند. در این مقاله ابعاد امنیت بلاک چین را با تمرکز بر تراکنش های مالی حوزه تجارت الکترونیک بررسی می نمائیم. در بخش اول انواع خطرات امنیتی و حملات در حوزه بلاک چین را بررسی می نمائیم.

خطرات امنیتی و حملات در بلاکچین

امنیت در بلاکچین یکی از مؤلفه‌های کلیدی موفقیت برنامه‌های تجاری بلاکچین است که همواره می‌بایست برای ارتقای آن تلاش نمود. با افزایش روزافزون محبوبیت حوزه رمز ارز و ورود صنعت امور مالی دیجیتال به آن و همچنین بروز حملات متعدد هکرها به این حوزه، کاربران دنیای کریپتو بیش از پیش نگران ویژگی امنیت شبکه های بلاک چین و سرمایه گذاری در آن هستند . فناوری بلاک چین مفهوم کاملاً جدیدی از عدم تمرکز، شفافیت و امنیت را به صنایع مختلف آورده است. این پتانسیل را دارد که انقلابی در نحوه ذخیره و اشتراک گذاری داده ها ایجاد کند.

[1] Blockchain

[2] Decentralized



شکل ۱. تهدیدات امنیتی بلاکچین در حوزه تجارت الکترونیک

شکل بالا شمای کلی تهدیدات امنیتی این حوزه را نمایش می دهد. لازم به ذکر است، بلاک چین یکی از امن ترین و مطمئن ترین راه ها برای انتقال اطلاعات و پول است، اما مجموعه ای از تهدیدات و معایب خود را نیز دارد . در نگاهی کلی خطرات امنیتی و حملات در بلاکچین به شرح ذیل می‌باشد [۸-۶]:

- حملات شبکه:

پروتکل دروازه مرزی، حملات مسیریابی، حمله Eclipse، حملات Stealthier، حملات DNS، حملات کانال جانبی از راه دور.

- امنیت نقطه پایانی:

آسیب پذیری۵۱٪ ، حملات Sybil، امنیت کلید شخصی، بدافزار استخراج، حملات Cryptojacking.

- سوء استفاده عمدی:

تزریق، سریال زدایی، آسیب پذیری ۵۱ درصد ، فعالیت های جنایی، دوبار خرج کردن، استخراج خودخواهانه، حمله به تعادل، حمله زمان‌گیر، حمله فینی، حمله رقابتی، حمله SelfHolding.

- آسیب‌پذیری‌های کد:

- کد نرم افزار اصلی (بلاکچین ۱،۰، ۲،۰):تزریق، استفاده از مؤلفه‌های با آسیب‌پذیری‌های شناخته‌شده، پیکربندی نادرست امنیتی، احراز هویت شکسته، کنترل دسترسی شکسته، عدم امنیت نامطلوب، XSS، نشت حریم خصوصی تراکنش‌ها، دوبار خرج کردن، امنیت کلید.
- خصوصی امنیت کیف پول قرارداد هوشمند (بلاکچین ۲،۰): آسیب‌پذیری‌های قرارداد هوشمند، عملیات کمتر از قیمت، قرارداد هوشمند کم تر بهینه‌شده.

- چالش های حفاظت از داده‌ها:

چالش مواجهه و قرار گرفتن در معرض داده های حساس و نشت حریم خصوصی امهیت حفاظت صحیح از داده ها در این حوزه را ایجاب می نماید.

- حملات و باگ‌های قرارداد هوشمند

یکی از نمونه‌های واقعی حملات به قراردادهای هوشمند این است که وقتی یک قرارداد هوشمندخاص (سازمان خودمختار غیرمتمرکز) بر روی اتریوم برای صندوق سرمایه‌گذاری مخاطره‌آمیز مبتنی بر جمعیت ساخته شد، یک هکر از ضعف کد آن سوء استفاده کرد و بیش از ۵۰ میلیون دلار رمزنگاری را دزدید [۹].

- حملات شبکه:

در آگوست ۲۰۱۴، یک تیم تحقیقاتی در Dell SecureWorks Counter Threat Unit کشف کردند که یک رباینده BGP اتصالات ماینرهای رمزارز ارز دیجیتال را به یک استخر ماینینگ کنترل شده توسط هواپیما ربایان هدایت کرده و در عرض چهار ماه ۸۳۰۰۰ دلار سود به ماینرها رسیده است. در سپتامبر ۲۰۱۶، یک حمله DDoS رای حمله به شبکه اتریوم کشف شد به طوری که یک کد EXTCODESIZE حدود ۵۰،۰۰۰ بار در هر بلوک توسط تراکنش های حمله فراخوانی شد و از این رو سرعت شبکه را به شدت کاهش داد [۱۰].

- حملات نقطه پایانی:

بدافزار یکی از حملات نقطه پایانی است. بر اساس این گزارش، بدافزار بیش از یک میلیون رایانه را آلوده کرده است که توسط مهاجمان برای استخراج ۲۶ میلیون توکن ارزهای دیجیتال مورد استفاده قرار می‌گیرد. Cryptojacking یکی دیگر از حملات نقطه پایانی است که در هنگام بازدید از وب، ارز دیجیتال در مرورگر وب کاربر استخراج می‌شود. مهاجمان اسکریپت‌های استخراج کریپتو را به Pirate Bay، Showtime CBS در سال ۲۰۱۷ و صفحات وب دولت هند در سال ۲۰۱۸ هک و تزریق کردند و با استفاده از رایانه‌های بازدیدکنندگان برای استخراج، جایزه ماینینگ بازدیدکنندگان را به دست آوردند [۱۱].

اقدامات امنیتی و راه حل های پیشنهادی بلاکچین

امنیت بلاک چین، تلفیقی از اصول، ابزارها و بهترین رویه‌ها در حوزه امنیت سایبری جهت کاهش ریسک و جلوگیری از حملات مخرب و دسترسی تایید نشده در شبکه‌های بلاکچین است. هر چند تمامی بلاک چین ها با فناوری گسترده (DLT) اجرا می‌شوند، اما تمامی آنها از نظر عملکردی، یکسان نیستند و یا سطح امنیت آنها، مشابه نیست. هر

چند بلاک چین های عمومی و خصوصی مزایا و معایب خاص خود را دارند، مدل‌های امنیتی آنها به‌دلیل ماهیت باز و بسته شبکه‌هایشان، متفاوت است. لذا، در این حوزه مهمترین رویکردهای امنیتی به شرح زیر می باشد [۱۵-۱۲]:

- تحلیل امنیتی و تحلیل آسیب پذیری "بایت کد" قرارداد هوشمند: در سال ۲۰۱۶، Oyente برای یافتن اشکالات امنیتی احتمالی در قراردادهای هوشمند توسعه یافت. در سال ۲۰۱۸، Securify به عنوان یک تحلیلگر امنیتی برای اثبات خودکار قراردادهای هوشمند اتریوم به عنوان ناامن/ایمن معرفی شد. در سال ۲۰۱۸، ZEUS از بررسی مدل نمادین و تفسیر انتزاعی برای تأیید انصاف و تأیید صحت قراردادهای هوشمند استفاده کرد و حدود ۹۴٫۶٪ از قراردادها به عنوان آسیب پذیر ارزیابی شدند. ابزارهای معروف تجزیه و تحلیل آسیب‌پذیری "بایت" کد قرارداد هوشمند شامل Oyente، Securify و ZEUS و غیره می‌باشد [۱۵].
- شناسایی کدهای مخرب و اشکالات:

ReGuard یک تحلیلگر مبتنی بر فازی را در مقاله آزمایشی خود برای شناسایی خودکار "اشکالات ورود مجدد"که از رایج ترین نوع باگها در قراردادهای هوشمند است ارائه کردند و Hydra توسط Breidenbach و همکاران برای استفاده از پاداش‌های باگ برای فعال کردن پاداش اشکالات مهم و شناسایی زمان اجرا توسعه داده شد [۱۶].

- امنیت کدهای نرم افزار اصلی:

در سال ۲۰۱۷، SmartPool به عنوان یک استخر استخراج غیرمتمرکز برای جلوگیری از این پدیده طراحی شد که نزدیک به ۸۰ درصد از اتریوم و ۹۵ درصد از قدرت استخراج بیت‌کوین به ترتیب در کمتر از شش و ده استخر استخراج قرار دارند. در سال ۲۰۱۹، Drijvers و همکاران. به اشکالات ظریف طرح چند امضایی دو دور اشاره کرد و سپس mBCJ را به عنوان یک جایگزین مطمئن و در عین حال بسیار کارآمد پیشنهاد کرد.

- حفظ حریم خصوصی:

در سال ۲۰۱۶، هاوک برای محافظت از حریم خصوصی تراکنش‌ها از طریق یک قرارداد هوشمند خصوصی توسعه یافت. در سال ۲۰۱۸، Obscuro برای ارائه یک میکسر بیت‌کوین ایمن و کارآمد ارائه شد تا پرداخت کنندگان و دریافت کنندگان پرداخت نتوانند برای دستیابی به پرداخت های ناشناس به یکدیگر مرتبط شوند [۱۷].

- قابلیت اعتماد و الگوریتم های اجماع:

توافق اضافه کردن یک بلوک به زنجیره بلوکی از طریق الگوریتم‌های اجماع است. این الگوریتم‌های اجماع از این واقعیت بهره می‌برند که اکثر کاربران در یک بلاکچین علاقه مشترکی به صادق نگه داشتن زنجیره بلاک دارند. یک سیستم بلاکچین از یک الگوریتم اجماع برای ایجاد اعتماد استفاده می‌کند و تراکنش‌ها را به درستی روی بلوک ها ذخیره می‌کند. بنابراین، الگوریتم‌های اجماع را می‌توان قلب تمام تراکنش‌های بلاکچین در نظر گرفت. پروتکل اجماع اساساً مجموعه‌ای از قوانین است که باید توسط هر شرکت کننده رعایت شود. به عنوان یک فناوری توزیع شده بدون اعتماد جهانی، بلاکچین به یک مکانیسم اجماع توزیع شده نیاز دارد تا همه شرکت‌کنندگان در مورد وضعیت فعلی بلاکچین به توافق برسند. اجماع بلاکچین مبتنی بر کمبود است که کنترل بیشتر یک منبع کمیاب، کنترل بیشتری بر عملکرد بلاکچین می‌دهد

PoW، PoS، DPoS و PBFT رایج‌ترین الگوریتم‌های اجماع هستند . DAG ، بیشترین تفاوت را با سایر الگوریتم‌های اجماع دارد و PoET توسط شرکت اینتل توسعه یافته و در Hyperledger Sawtooth استفاده می‌شود. بنابراین، در ادامه بیشتر توضیح داده شده است.

PoW مشکلی را انتخاب می‌کند که فقط با حدس زدن قابل حل است. به عنوان مثال، وقتی زمان ایجاد و اعتبارسنجی یک بلوک کامل است، مشکل، حدس زدن یک مقدار nonce است به طوری که هنگام استفاده از داده‌های تراکنش و مقدار nonce به عنوان ورودی برای یک تابع هش، خروجی هش آن باید با مشکل مطابقت داشته باشد. به عنوان مثال، با چهار صفر اول شروع می‌شود. هر گره (که گره ماینینگ نیز نامیده می‌شود) در شبکه مقادیر nonce مختلف را به طور تصادفی حدس می‌زند تا زمانی که ابتدا یک گره برای یافتن مقدار nonce که با مشکل مطابقت دارد اتفاق بیفتد. بنابراین یک گره ماینینگ باید منابع محاسباتی زیادی را روی آن خرج کند و مشکل را سریعتر از دیگران حل می‌کند تا بتواند در ایجاد یک بلوک برای پیوند به بلاکچین موفق شود و پاداش استخراج انگیزشی را به دست آورد که اغلب ارز دیجیتال است. از سوی دیگر، توابع هش به عنوان یک پازل رمزنگاری در مرکز الگوریتم اجماع PoW مهم هستند. شبکه رمزارز بیت‌کوین از تابع هش رمزنگاری SHA-256 استفاده می‌کند [۱۸]. در بخش زیر بیشتر در مورد تابع هش صحبت خواهیم کرد. بلاکچین‌های عمومی بیت‌کوین و در گذشته اتریوم ۱,۰ نیز از PoW به عنوان الگوریتم اجماع خود استفاده می‌کنند. یک مشکل بزرگ در مورد فرآیند اجماع PoW این است که برای تکمیل آن به زمان و برق زیادی نیاز دارد.

PoS [۵،۹] دومین روش اجماع برجسته است و به محاسبات کمتری برای استخراج نسبت به PoW نیاز دارد. PoS مشکلات زمان و مصرف برق را که PoW دارد حل می‌کند، زیرا نیاز به برق با ماینرها مرتبط است که nonce را پیدا می‌کنند و این فرآیند نیاز به زمان دارد. PoS دارای گره‌هایی برای قرار دادن سهام است تا به عنوان سازنده بلوک بعدی انتخاب شود. هنگامی که یک بلوک انتخاب می‌شود، سازنده کارمزد تراکنش های مرتبط با آن بلوک را دریافت می‌کند. اگر برنده بلوک سعی کند یک بلوک نامعتبر اضافه کند، سهام خود را از دست خواهد داد. در اولین مرحله از ارتقای اتریوم ۲,۰، «کامپیوترهای جهانی» بلاکچین از الگوریتم اجماع PoW به PoS تغییر می‌کند [۱۹].

DAG ها از رئوس و یال ها (خطوط متصل کننده آنها) تشکیل شده‌اند که با سایر الگوریتم‌های اجماع متفاوت است. رئوس و لبه‌ها به این دلیل جهتدار می‌شوند که در یک جهت حرکت می‌کنند و غیرچرخه‌ای هستند زیرا راس‌ها به خودشان حلقه نمی‌زنند. هر رأس در ساختار، یک تراکنش را نشان می‌دهد. در اینجا هیچ مفهومی از بلاک وجود ندارد و برای افزودن تراکنش‌ها نیازی به استخراج نیست. به جای جمع‌آوری تراکنش‌ها در بلوک‌ها، هر تراکنش بر روی دیگری ساخته می‌شود. با این حال، یک عملیات PoW کوچک وجود دارد که زمانی انجام می‌شود که یک گره تراکنش را ارسال می‌کند. این تضمین می‌کند که شبکه اسپم نشده و همچنین تراکنش‌های قبلی را تأیید می‌کند. IOTA از الگوریتم اجماع DAG استفاده می‌کند [۲۰].

- قرارداد هوشمند:

قرارداد هوشمند بخش زیبای دیگری از بلاکچین را ایجاد می‌کند که بلاکچین نه تنها یک رکورد توزیع شده و غیرقابل تغییر از تمام رویدادهای مختلف رخ داده ارائه می دهد، بلکه امکان نوشتن کدهای کامپیوتری بسیار غیر ذهنی را نیز فراهم می‌کند که دقیقاً نحوه مدیریت آن فرآیند و اینکه چه اقداماتی قرار است در هنگام وقوع آن رویداد انجام شود را مشخص می‌کند. یکی از اهداف قرارداد هوشمند پیشنهاد شده در اتریوم، شکستن محدودیت‌های بیت‌کوین بود. قرارداد هوشمند درباره کدهای کامپیوتری است که برای پاسخگویی به انواع خاصی از رویدادهای مهم نوشته شده است. قرارداد هوشمند لازم نیست دو یا چند طرف را درگیر کند و لازم نیست قانوناً الزام آور باشد [۲۱].

قرارداد هوشمند که به عنوان کد زنجیره‌ای نیز شناخته می‌شود:

- قوانین برنامه و تصمیم‌گیری به تراکنش‌ها و فرآیندهای بلاکچین اشاره می‌کند.
- تراکنش‌ها را خودکار می‌کند تا مطمئن شوید که همه آنها از قوانین یکسانی پیروی می کنند.
- این فناوری اساسا روی بستر بلاکچین اجرا می‌شود.

قرارداد هوشمند نحوه انجام تجارت ما را متحول خواهد کرد و سنگ‌بنای برنامه‌های بلاکچین سازمانی است. هر کسی می‌تواند بدون نیاز به واسطه، قراردادهای هوشمند ایجاد کند. قرارداد هوشمند استقلال، کارایی، دقت و صرفه جویی در هزینه را فراهم می‌کند.

- رمزنگاری:

بلاکچین، لایه‌ای از اعتماد بین طرف‌های غیرقابل اعتماد ایجاد می‌کند تا سوابق و تراکنش‌های امن و مطمئن را امکان‌پذیر کند. بدون بلاکچین برای ایجاد سوابق و تراکنش های قابل اعتماد، یک واسطه شخص ثالث ضروری است. بلاکچین از رمزنگاری و همکاری برای ایجاد این اعتماد استفاده می‌کند و در نتیجه، نیاز به یک موسسه متمرکز را برای عمل به عنوان یک واسطه اجرایی را از بین می برد. اطلاعات مربوط به بلاکچین با استفاده از رمزنگاری در دفتر کل ذخیره می‌شود. بلاکچین از برخی از بلوک‌های سازنده رمزنگاری به شرح زیر استفاده می‌کند.

برای اثبات اینکه یک معامله توسط شخص مناسب ایجاد شده است استفاده می‌شود. در بلاکچین، کلید خصوصی در یک کیف پول دیجیتال، یا یک کیف پول سخت افزاری یا هر کیف پول نرم‌افزاری نگهداری می‌شود. یک کاربر به کلید خصوصی خود دسترسی پیدا می‌کند تا پیامی به نام امضای دیجیتال را امضا کند که به زنجیره بلوکی منتقل می‌شود و کلید عمومی آن برای تأیید این است که پیام واقعاً از طرف کاربر آمده است. از آنجایی که کلید خصوصی فقط توسط مالک آن به صورت ایمن نگهداری می‌شود، لذا امضای دیجیتالی مربوطه از ایجاد تراکنش اطمینان می‌دهد. این الگوریتم امضای دیجیتال را در هر تراکنش بسته به کلید خصوصی فردی هر کاربر فعال می‌کند. جفت کلید عمومی و کلید خصوصی به عنوان ستون فقرات بلاکچین در بلاکچین قرار می‌گیرند و برای امضا و تأیید تراکنش‌هایی که کاربر انجام می‌دهد استفاده می‌شود.

- توابع هش:

توابع هش یک فناوری کلیدی است که در بلاکچین استفاده می‌شود. تابع هش یک معادله ریاضی با پنج ویژگی مهم برای رمزنگاری است. تابع هش رمزنگاری راهی برای پیوند دادن همه بلوک‌های روی بلاکچین به یکدیگر فراهم می‌کند. در سطح بلوک، هش هدر بلوک i-2 قبلی در بلوک i-1، هش هدر بلوک i-1 قبلی در بلوک i، هش هدر بلوک i قبلی در بلوک ذخیره می‌شود. i+1، و غیره را مسدود کنید. در یک بلوک، چندین تراکنش وجود دارد. بلاکچین همچنین هر تراکنش را هش می‌کند و برای یک سه راهی مرکل در قسمت پایین شکل و ریشه Merkle در هدر بلوک ذخیره می‌شود. به این ترتیب، بلاکچین یک دفتر کل توزیع شده ایجاد می‌کند که تغییرناپذیر، ایمن و بسیار قابل اعتماد است. اگر هر بلوک یا هر تراکنش یا اطلاعاتی در آن بلوک اصلاح شود، مهم نیست که چقدر کوچک باشد، بلافاصله کشف می‌شود و پیوند بین آن بلوک و تمام بلوک های بعدی قطع می‌شود [۲۲].

- مقیاس پذیری:

مقیاس پذیری در تراکنش‌ها. PoW قادر است بین 10 TPS تا TPS 27 در سراسر جهان پردازش کند. Ethereum 2.0 ارتقا می یابد و به پروتکل کارآمدتر PoS تغییر می‌کند تا اتریوم مقیاس پذیرتر شود و از TPS 1000 پشتیبانی می‌کند. تعداد کمی از نمایندگان در EOS که از الگوریتم اجماع DPoS استفاده می‌کنند، حق رای دادن و اعتبارسنجی بلوک‌ها را دارند، و از این رو EOS متمرکزتر است و برای برخی نمایندگان آسان‌تر است که با هم ترکیب شوند تا حملات ۵۱٪ را انجام دهند. مقیاس پذیری در اشتراک گذاری داده های زنجیره ای. برای افزایش مقیاس‌پذیری و همچنین بهره‌گیری از فناوری بلاک‌چین، داده‌ها را می‌توان در یک کانال اختصاصی خارج از زنجیره به اشتراک گذاشت و پیوند یا حتی اثبات اشتراک‌گذاری داده‌ها را می‌توان در زنجیره بلوک برای ردیابی و ممیزی ثبت کرد. راه حل های به اشتراک گذاری داده خارج از زنجیره، نیاز به کانال‌های بین شرکتی دارد که بار

شرکت را برای ایجاد و نگهداری این کانال‌ها افزایش می دهد. علاوه بر این، این راه‌حل‌ها نمی‌توانند یکپارچگی داده های به اشتراک گذاشته شده توسط یک شرکت را تضمین کنند.

- حفظ حریم خصوصی:

با افزایش روزافزون داده های ذخیره شده در بلاکچین، نگرانی سازمان و افراد، نشت حریم خصوصی است. برخی از تکنیک‌های مبهم‌سازی کد،رمزگذاری همریختی، پلتفرم اجرایی قابل اعتماد و قرارداد هوشمند برای حفظ حریم خصوصی، مسیرهای امیدوارکننده ای خواهند بود.

نقش ارزهای دیجیتال در امنیت بلاک چین

ارزهای دیجیتال، معمولاً به عنوان ارزهای رمزنگاری‌شده یا ارزهای دیجیتال نیز شناخته می‌شوند، نقش مهمی در امنیت بلاکچین ایفا می‌کنند. این ارزها ابزارهای اساسی در اکوسیستم بلاکچین هستند و برخی از نقش‌های مهم آنها در امنیت به شرح زیر است:

- امضای دیجیتال :ارزهای دیجیتال از امضای دیجیتال برای تأیید اصالت تراکنش‌ها و انتقال دارایی‌ها استفاده می‌کنند. این امضاها با استفاده از کلیدهای خصوصی (Private Keys)که تنها در اختیار صاحبان حساب‌ها قرار دارند، ایجاد می‌شوند و امکان اثبات هویت و اصالت را فراهم می‌کنند.
- تأیید تراکنش‌ها :ارزهای دیجیتال به عنوان وسیله‌ای برای تأیید تراکنش‌ها در شبکه بلاکچین عمل می‌کنند. فرآیند ماینینگ (استخراج) در بلاکچین‌های مبتنی بر Proof of Work (PoW)و Proof of Stake (PoS) با استفاده از ارزهای دیجیتال انجام می‌شود و امنیت تراکنش‌ها را تضمین می‌کند.
- پاداش برای ماینرها :در بلاکچین‌هایPoW ، ماینرها به عنوان افرادی که تراکنش‌ها را تأیید و بلوک‌ها را استخراج می‌کنند، ارزهای دیجیتال به عنوان پاداش دریافت می‌کنند. این نقش اقتصادی، ماینرها را ترغیب به حفظ امنیت شبکه می‌کند.
- پیشرفت در فناوری امنیتی :ارزهای دیجیتال معمولاً از فناوری‌های رمزنگاری برتر استفاده می‌کنند. به عنوان مثال، بیت‌کوین از الگوریتم SHA-256 برای ایجاد امنیت استفاده می‌کند .پیشرفت‌های در زمینه رمزنگاری از اهمیت بسزایی برای امنیت بلاکچین و ارزهای دیجیتال استفاده می‌کنند.
- هویت دیجیتال :ارزهای دیجیتال به عنوان ابزارهایی برای ایجاد و مدیریت هویت دیجیتال افراد مورد استفاده قرار می‌گیرند. کلیدهای خصوصی و عمومی که برای کنترل دارایی‌ها و امضای تراکنش‌ها استفاده می‌شوند، ابزارهای مهم در ساختار هویت دیجیتال هستند.
- تسهیل در اجرای قراردادهای هوشمند :ارزهای دیجیتال، به ویژه در بلاکچین‌هایی مانند اتریوم که قابلیت اجرای قراردادهای هوشمند را دارند، به عنوان وسیله‌ای برای انجام تراکنش‌ها و اجرای قراردادهای هوشمند به کار می‌روند. این قابلیت به امنیت اطلاعات و اجرای قوانین منطبق با قراردادها کمک می‌کند.
- استفاده از تکنولوژی‌های تعاملی :برخی از ارزهای دیجیتال از تکنولوژی‌های تعاملی مانند اشتباه‌یابی کوانتومی برای افزایش امنیت استفاده می‌کنند. این تکنولوژی‌ها در مقابل حملات کوانتومی مقاوم هستند و به دنبال افزایش امنیت بیشتر هستند.

به عنوان جمع بندی، ارزهای دیجیتال در امنیت بلاکچین نقش محوری ایفا می‌کنند و تضمین می‌کنند که تراکنش‌ها ایمن و اصیل باشند . همچنین، این ارزها به عنوان ابزارهای اقتصادی و امنیتی در اکوسیستم بلاک چین شناخته می‌شوند. درپایان لازم به ذکر است، امنیت بلاک چین به واسطه الگوریتم‌های رمزنگاری قوی، هویت دیجیتال، و توزیع گسترده قدرت محاسباتی بسیار بالاست . با این حال، برای بهره‌مندی بهتر از این فناوری، لازم است توسعه‌دهندگان و کاربران با چالش‌ها و راهکارهای امنیتی آشنا شوند و از ابزارهای تست امنیت برای ارتقاء امنیت بلاک چین استفاده نمایند.

نتیجه گیری

بلاکچین یک تکنولوژی فناور محور و فناوری نوین است که به عنوان پایه‌ای برای ایجاد سیستم‌های اطلاعاتی بسیار امن و شفاف شناخته می‌شود. این تکنولوژی اصلی‌ترین مبنای پشتیبانی ارزهای دیجیتال مانند بیت‌کوین است، اما کاربردهای آن به مسائل مختلفی از جمله حوزه‌های مالی، مدیریت زنجیره تأمین، حقوق تأمین انرژی، حوزه سلامت و غیره گسترده شده است. این مقاله ابتدا یک بررسی در مورد بلاکچین انجام داده است. فناوری از نظر نمای کلی چالش ها و راه حل ها، الگوریتم های اجماع، قراردادهای هوشمند و رمزنگاری برای بلاکچین بررسی شده است. سپس الگوریتم‌های متداول اجماع مورد توجه قرار گرفته است. رمزنگاری کلید عمومی و توابع هش مورد استفاده در بلاکچین به تفصیل برای یکپارچگی، احراز هویت، عدم انکار و غیره مورد نیاز در سیستم‌های بلاکچین توضیح داده شده است. این مقاله سپس کاربردهای جامع بلاکچین را فهرست کرده است و اقدامات امنیتی را در زمینه‌های تجزیه و تحلیل امنیت، امنیت کدهای نرم‌افزار، حفظ حریم خصوصی و غیره ارائه کرده است. همچنین ابزار تحلیل آسیب‌پذیری بایت کد قرارداد هوشمند را ارائه کرده است. در نهایت،

چالش‌ها و روندهای تحقیقاتی برای ساخت سیستم‌های بلاکچین مقیاس‌پذیرتر و ایمن‌تر برای استقرار گسترده ارائه شده‌اند.

مراجع

[1] Arora A, Sharma M, Bhaskaran S. Blockchain technology transforms E-commerce for enterprises. InData Science and Analytics: 5th International Conference on Recent Developments in Science, Engineering and Technology, REDSET 2019, Gurugram, India, November 15–16, 2019, Revised Selected Papers, Part II 5 2020 (pp. 26-34). Springer Singapore.

[2] Reddy VM. Blockchain Technology in E-commerce: A New Paradigm for Data Integrity and Security. Revista Espanola de Documentacion Cientifica. 2021 Dec 30;15(4):88-107.

[3] Reddy VM. Blockchain Technology in E-commerce: A New Paradigm for Data Integrity and Security. Revista Espanola de Documentacion Cientifica. 2021 Dec 30;15(4):88-107.

[4] Zhang A, Zhang L, Zhu W. Safety and security of e-commerce transactions based on blockchain technology. Journal of Electrical Systems. 2024;20(6s):237-46.

[5] Dahal SB. Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions. International Journal of Information and Cybersecurity. 2023 Feb 20;7(1):1-2.

[6] Shaikh JR, Iliev G. Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security. In2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN) 2018 Nov 23 (pp. 155-158). IEEE.

[7] Shaikh JR, Iliev G. Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security. In2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN) 2018 Nov 23 (pp. 155-158). IEEE.

[8] Moubarak J, Filiol E, Chamoun M. On blockchain security and relevant attacks. In2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) 2018 Apr 18 (pp. 1-6). IEEE.

[9] König L, Unger S, Kieseberg P, Tjoa S, Blockchains JR. The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. J. Internet Serv. Inf. Secur.. 2020 Aug;10(3):110-27.

[10] Zamani E, He Y, Phillips M. On the security risks of the blockchain. Journal of Computer Information Systems. 2020 Nov 1;60(6):495-506.

[11] Siddiqui ST, Ahmad R, Shuaib M, Alam S. Blockchain security threats, attacks and countermeasures. InAmbient Communications and Computer Systems: RACCCS 2019 2020 (pp. 51-62). Springer Singapore.

[12] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems. 2018 May 1;82:395-411.

[13] Anita N, Vijayalakshmi M. Blockchain security attack: A brief survey. In2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019 Jul 6 (pp. 1-6). IEEE.

[14] Siddiqui ST, Ahmad R, Shuaib M, Alam S. Blockchain security threats, attacks and countermeasures. InAmbient Communications and Computer Systems: RACCCS 2019 2020 (pp. 51-62). Springer Singapore.

[15] Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access. 2021 Jan 14;9:13938-59.[15] König L, Unger S, Kieseberg P, Tjoa S, Blockchains JR. The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. J. Internet Serv. Inf. Secur.. 2020 Aug;10(3):110-27.

[16] Islam MR, Rahman MM, Mahmud M, Rahman MA, Mohamad MH. A review on blockchain security issues and challenges. In2021 IEEE 12th control and system graduate research colloquium (ICSGRC) 2021 Aug 7 (pp. 227-232). IEEE.

[17] Park JH, Park JH. Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry. 2017 Aug 18;9(8):164.

[18] Cheng J, Xie L, Tang X, Xiong N, Liu B. A survey of security threats and defense on Blockchain. Multimedia Tools and Applications. 2021 Aug;80:30623-52.

[19] Stephen R, Alex A. A review on blockchain security. InIOP conference series: materials science and engineering 2018 Aug 1 (Vol. 396, No. 1, p. 012030). IOP Publishing.

[20] Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023 Jan 20;12(3):546.

[21] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain: research and applications. 2022 Jun 1;3(2):100067.

تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.