APJ. 6 (2):49-58, Summer 2025

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Issn online: 2783-4549

Exploring the Security Aspects of Blockchain Technology: Challenges and Prospects

Maryam Rezae[*,1], Ali Mohammadpur[2]

[1] Department of Computer Engineering, Ar.C., Islamic Azad University, Arak, Iran
[2] Department of Computer Engineering, Ar.C., Islamic Azad University, Arak, Iran

ABSTRACT

RESEARCH PAPER

Received:
25 February 2025

Accepted:
24 June 2025

Keywords:
Blockchain,
Security,
Consensus Algorithm,
Smart Contract,

[1] **Corresponding author:**
m.rezae.research@gmail.com

Blockchain technology, with its unique features such as decentralization, transparency, security, and immutability, has brought about a significant transformation in various technological fields. This article aims to comprehensively review the security aspects of blockchain, its challenges, and future prospects. First, the fundamental concepts of blockchain, various consensus algorithms, and cryptographic techniques used in it are described. Then, the diverse applications of blockchain in fields such as finance, IoT, energy, health, and privacy are analyzed. An important part of the article is dedicated to blockchain security issues, including network attacks, code vulnerabilities, smart contract attacks, and data protection. Finally, security measures and vulnerability analysis tools are introduced, and research trends are presented to develop more scalable and secure systems. The results show that while blockchain has high potential, it cannot be used sustainably and widely without considering the existing security issues and challenges. Therefore, addressing these challenges, along with leveraging new technologies, will be the key to success in the future development of blockchain. This paper can be used as a reference for further research in the field of blockchain security and the development of related technologies.

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۲، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir
شاپای الکترونیکی: ۲۷۸۳-۴۵۴۹

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

بررسی جنبه‌های امنیتی فناوری بلاکچین: چالش‌ها و چشم‌اندازها

مریم رضائی[1*] ، علی محمدپور[2]

[1] گروه مهندسی کامپیوتر، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران

[2] گروه مهندسی کامپیوتر، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران

چکیده

مقاله پژوهشی

تاریخ دریافت مقاله:
۱۴۰۳/۱۲/۷

تاریخ پذیرش:
۱۴۰۴ /۴/۳

واژگان کلیدی:
بلاکچین،
امنیت،
الگوریتم اجماع،
قرارداد هوشمند،

فناوری بلاکچین با ویژگی‌های منحصربه‌فردی همچون عدم تمرکز، شفافیت، امنیت و تغییرناپذیری، تحول چشمگیری در زمینه‌های مختلف فناوری ایجاد کرده است . این مقاله با هدف بررسی جامع جنبه‌های امنیتی بلاکچین، چالش‌ها و چشم‌اندازهای پیش‌رو منتشر شده است. ابتدا مفاهیم بنیادی بلاکچین، الگوریتم‌های اجماع مختلف و تکنیک‌های رمزنگاری مورد استفاده در آن تشریح شده است. سپس کاربردهای متنوع بلاکچین در حوزه‌هایی نظیر مالی، اینترنت اشیا، انرژی، سلامت و حریم خصوصی مورد تحلیل قرار گرفته‌اند. بخش مهمی از مقاله به مسائل امنیتی بلاکچین، از جمله حملات شبکه، آسیب‌پذیری‌های کد، حملات قراردادهای هوشمند و حفاظت داده‌ها اختصاص یافته است. در نهایت، اقدامات امنیتی و ابزارهای تحلیل آسیب‌پذیری معرفی شده و روندهای تحقیقاتی برای توسعه سیستم‌های مقیاس‌پذیر و ایمن‌تر ارائه شده است. نتایج نشان می‌دهد که در حالی که بلاکچین ظرفیت‌های بالایی دارد، اما بدون توجه به مسائل امنیتی و چالش‌های موجود، نمی‌تواند به صورت پایدار و گسترده به کار گرفته شود. بنابراین، توجه به این چالش‌ها در کنار بهره‌گیری از فناوری‌های نوین، کلید موفقیت در توسعه آینده بلاکچین خواهد بود. این مقاله می‌تواند به عنوان مرجعی برای پژوهش‌های بعدی در زمینه امنیت بلاکچین و توسعه فناوری‌های مرتبط مورد استفاده قرار گیرد.

۱- مقدمه

فناوری بلاکچین به عنوان یک فناوری نوین ثبت داده‌ها، ساختاری غیرمتمرکز و غیرقابل تغییر را ارائه می‌دهد که اطلاعات و تراکنش‌ها در آن به صورت زنجیره‌ای از بلوک‌ها ذخیره می‌شوند. این ساختار امکان ایجاد اعتماد، شفافیت و امنیت بالا را در سیستم‌های مختلف فراهم کرده و به بسیاری از صنایع از جمله امور مالی، سلامت، زنجیره تامین و اینترنت اشیاء (IoT) خدمات ارائه می‌دهد. افزایش چشمگیر توسعه کاربردهای بلاکچین در سال‌های اخیر، این فناوری را به یکی از محورهای تحقیقاتی برجسته در حوزه فناوری اطلاعات و امنیت سایبری تبدیل کرده است [۱].

از مهمترین ویژگی‌های امنیتی بلاکچین، استفاده از ساختار هشینگ داده‌ها و الگوریتم‌های رمزنگاری است که از تغییرات غیرمجاز در داده‌ها جلوگیری می‌کند. همچنین، الگوریتم‌های اجماع مانند اثبات کار (PoW)و اثبات سهام (PoS) به عنوان سازوکارهای اصلی تایید تراکنش‌ها نقش بسزایی در امنیت و پایداری شبکه دارند. با این وجود، پیاده‌سازی و استقرار گسترده بلاکچین به دلیل برخی چالش‌ها و تهدیدات امنیتی، نیازمند بررسی دقیق‌تر و توسعه راهکارهای نوین حفاظتی می‌باشد [۲].

حملات متنوع سایبری از جمله حملات ۵۱ درصد، حملات نقطه پایانی و آسیب‌پذیری در قراردادهای هوشمند، از جمله موانع اساسی در مسیر بهره‌برداری کامل و امن از فناوری بلاکچین هستند. در نتیجه، پژوهش‌های گسترده‌ای برای شناسایی، تحلیل و رفع این تهدیدات در حال انجام است که بهبود مقیاس‌پذیری، حفظ حریم خصوصی و افزایش امنیت کدهای هوشمند را هدف قرار داده‌اند. این مقاله با ارائه بررسی جامع امنیتی و چشم‌اندازهای آتی بلاکچین، گام موثری در جهت ارتقای قابلیت اطمینان و کاربردپذیری این فناوری برداشته است [۳].

در بلاکچین اساسا، داده‌ها در یک دفتر کل توزیع شده[1] نگهداری می‌شوند. این فناوری زنجیره بلوکی برای ارائه یکپارچگی و در دسترس بودن است که به شرکت‌کنندگان در شبکه بلاکچین 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 بلاکچین 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 [۴-۵]. علاوه بر این، فناوری بلاکچین به‌عنوان یک شبکه توزیع‌شده، برای اینکه به کل مجموعه شرکت‌کنندگان اجازه دهد بر روی یک رکورد یکپارچه به توافق برسند، به یک پروتکل اجماع[2] 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، بلاکچین 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 [۶]. در بخش بعد درباره ابعاد بنیادین فناوری بلاکچین توضیح خواهیم داد.

۲- فناوری بلاکچین

فناوری بلاکچین یک ساختار داده توزیع‌شده و غیرمتمرکز است که در قالب شبکه‌ای از گره‌ها اطلاعات را به صورت شفاف و امن ذخیره می‌کند. در این فناوری، داده‌ها در قالب بلوک‌هایی قرار می‌گیرند که به صورت زنجیروار و با ترتیب مشخصی به هم متصل شده‌اند. این اتصال با استفاده از روش‌های رمزنگاری و نشانگرهای خاص انجام می‌شود، طوری که هر بلوک علاوه بر داده‌های تراکنشی، نشانگری از بلوک قبلی را نیز دارد و این امر امکان تغییر یا حذف اطلاعات قدیمی را به شدت پیچیده و غیرممکن می‌سازد. این معماری منجر به ایجاد یک دفتر کل توزیع‌شده می‌شود که تمام اعضای شبکه از آن نسخه‌ای کپی شده دارند و تراکنش‌ها تنها در صورت توافق بیشتر گره‌ها بر اساس الگوریتم‌های اجماع به زنجیره اضافه می‌شوند [۷].

کاربردهای بلاکچین شامل ارز دیجیتال، امور مالی (بورس اوراق بهادار،خدمات مالی، بازار مالیP2P ، تامین مالی جمعی و غیره)، اینترنت اشیا (ایمنی و حریم خصوصی، تجارت الکترونیک و غیره) است. سیستم های مشهور (جامعه وب، دانشگاهیان و غیره)، امنیت و حریم خصوصی (افزایش امنیت، مدیریت ریسک، حفاظت از حریم خصوصی و غیره) ، مراقبت‌های بهداشتی، بیمه، حفاظت از حق چاپ، انرژی، برنامه‌های کاربردی جامعه (موسیقی بلاکچین، دولت بلاکچین)، تبلیغات، دفاع، برنامه‌های کاربردی تلفن همراه، زنجیره تامین، خودرو، بخش کشاورزی، مدیریت هویت، رای‌گیری، آموزش، قانون و اجرای قانون، ردیابی دارایی، سوابق دیجیتال، نفوذ تشخیص، مدیریت مالکیت دیجیتال، ثبت عنوان مالکیت و غیره. شکل زیر کاربردهای فزاینده مارپیچی فناوری بلاکچین را نشان می‌دهد. انتظار می رود موارد استفاده بیشتر و بیشتری از سیستم‌های بلاکچین در حال ظهور باشد.

شکل ۱. کاربردهای بلاکچین

همچنین از دیدگاه زیرساخت، معماری بلاکچین شامل چندین لایه اصلی است که هر یک نقش کلیدی در عملکرد سیستم ایفا می‌کنند. لایه زیرساخت سخت‌افزاری شامل سرورها و گره‌های شبکه است که داده‌ها در آنها ذخیره می‌شوند و شبکه همتا به همتا (P2P) که ارتباط بین گره‌ها را ممکن می‌سازد. لایه داده از ساختار بلوک‌ها و لیست‌های متصل به هم تشکیل شده که تراکنش‌ها را ذخیره و مدیریت می‌کند. لایه شبکه مدیریت ارتباطات گره‌ها و ارسال اطلاعات را بر عهده دارد. لایه اجماع، قوانین و الگوریتم‌هایی مانند اثبات کار و اثبات سهام را تعیین می‌کند که اعتبار تراکنش‌ها را تضمین می‌کند. در نهایت، لایه کاربردها امکاناتی مثل قراردادهای هوشمند و اپلیکیشن‌های بلاکچین را فراهم می‌آورد [۸].

خصوصیات فنی بلاکچین از جمله توزیع‌شدگی، امنیت بالا، شفافیت و تغییرناپذیری داده‌ها موجب شده فناوری بلاکچین در عرصه‌های مختلف کاربردی شود. ویژگی‌های رمزنگاری مانند توابع هش و رمزنگاری کلید عمومی، امکان احراز هویت و ایمنی داده‌ها را فراهم می‌کنند. علاوه بر این، مدل‌های غیرمتمرکز باعث حذف نیاز به واسطه‌ها شده و فرآیندهای کسب‌وکار و معاملات را شفاف‌تر و باکاراتر می‌سازند. چارچوب توافق و اجماع، امنیت شبکه را تامین کرده و در مقابل حملات مخرب مقاومت ایجاد می‌کند. این ویژگی‌ها بلاکچین را به یک فناوری انقلابی تبدیل کرده که می‌تواند در صنایع مختلف تحول ایجاد کند [۱۰-۹].

با این وجود، چالش‌های فنی مانند مقیاس‌پذیری، سرعت تراکنش‌ها و مصرف انرژی، مانع‌هایی برای پیاده‌سازی گسترده بلاکچین هستند که در تحقیقات و توسعه‌های روز افزون به دنبال رفع آنها هستند. معماری‌های نوین و استفاده از فناوری‌هایی مثل شبکه‌های لایه دوم، زنجیره‌های جانبی و روش‌های اجماع پیشرفته، راهکارهای مهمی برای بهبود عملکرد بلاکچین در آینده می‌باشند. به طور خلاصه، فناوری بلاکچین با معماری متشکل از اجزای مختلف فنی و ساختار داده‌ای منحصربه‌فرد، بستری امن و مطمئن برای معاملات و ثبت داده‌ها فراهم می‌آورد که مزایای کارآمدی و امنیتی خاصی را در مقایسه با سیستم‌های سنتی ارائه می‌کند [۱۱]. در بخش بعدی ابعاد امنیتی بلاکچین را بررسی نموده‌ایم.

۳- ابعاد امنیتی بلاکچین

امنیت بلاکچین یکی از ابعاد حیاتی و کلیدی این فناوری است که آن را به یک بستر مطمئن برای ثبت و انتقال داده‌ها تبدیل کرده است. امنیت بلاکچین از طریق چندین مکانیزم هم‌افزا تأمین می‌شود که هر یک نقش متفاوتی در حفاظت از داده‌ها، جلوگیری از دستکاری و تضمین شفافیت ایفا می‌کنند. یکی از مهمترین این عوامل رمزنگاری پیشرفته است که با استفاده از الگوریتم‌های هش و امضای دیجیتال، اعتبار هر تراکنش و هویت شرکت‌کنندگان را تضمین می‌کند. این سازوکار امکان دسترسی غیرمجاز و تغییر اطلاعات را به شدت کاهش می‌دهد و امنیت پایه‌ای شبکه را فراهم می‌کند [۱۲].

غیرمتمرکز بودن شبکه بلاکچین، ابعاد مهم دیگری از امنیت را شکل می‌دهد. برخلاف سیستم‌های متمرکز که در آن‌ها یک نقطه خرابی می‌تواند کل شبکه را مختل کند، در بلاکچین داده‌ها در میان تعداد زیادی گره مستقل توزیع شده‌اند. این توزیع باعث می‌شود حتی اگر برخی از گره‌ها دچار مشکل یا حمله شوند، شبکه به فعالیت خود ادامه دهد و تغییرات مخرب به سختی قابل اجماع شوند. به علاوه، الگوریتم‌های اجماع مثل اثبات کار و اثبات سهام تضمین می‌کنند که کلیه گره‌ها در پذیرش تراکنش‌ها به توافق برسند و از حملات مخرب جلوگیری کنند، که این موضوع مقاومت شبکه را در برابر حملات افزایش می‌دهد [۱۳]. تغییرناپذیری و شفافیت دیگر ویژگی‌های برجسته امنیت بلاکچین هستند. پس از ثبت یک بلوک در زنجیره، اطلاعات آن قابل تغییر یا حذف نیست و تمامی تراکنش‌ها به صورت شفاف برای همه اعضای شبکه قابل مشاهده‌اند. این امر باعث می‌شود هرگونه تلاش برای دستکاری یا تقلب، به سرعت شناسایی شود و امکان سوءاستفاده کاهش یابد. این شفافیت به همراه ویژگی رمزنگاری باعث اطمینان مخاطبان و کاربران نسبت به صحت و اعتبار داده‌ها می‌شود [۱۴].

با این حال، چالش‌هایی از جمله آسیب‌پذیری‌های کدهای قراردادهای هوشمند، حملات شبکه‌ای، و مسائل مرتبط با حفظ حریم خصوصی وجود دارد که توسعه‌دهندگان و جامعه علمی در تلاش برای ارتقاء مکانیزم‌های امنیتی و شناخت تهدیدات نوین هستند. استفاده از فناوری‌های مکمل مانند الگوریتم های اجماع، الگوریتم‌های رمزنگاری نوین، شبکه‌های خصوصی و ابزارهای تحلیل آسیب‌پذیری از جمله راهکارهای مهم برای تقویت امنیت بلاکچین می‌باشد که در بخش های بعدی مقاله به اهم این موارد خواهیم پرداخت.

۴- الگوریتم‌های اجماع

اساسا توافق اضافه کردن یک بلوک به زنجیره بلوکی از طریق الگوریتم‌های اجماع است. 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، بلاکچین به یک مکانیسم اجماع توزیع شده نیاز دارد تا همه شرکت‌کنندگان در مورد وضعیت بلاکچین به توافق برسند. اجماع بلاکچین مبتنی بر کمبود است که کنترل بیشتر یک منبع کمیاب، کنترل بیشتری بر عملکرد بلاکچین می‌دهد [۱۴]. در ادامه مهمترین رویکردهای اجماع را بررسی خواهیم نمود.

رویکرد اثبات کار[1]

رویکرد 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 (از این رو "کار" نامیده می‌شود) 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 [۱۵]. 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.

رویکرد اثبات سهام[2]

PoS [۱۶] دومین روش اجماع 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.

گراف غیر چرخشی هدایت شده[3]

اساسا DAG ها [۱۷] 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 [۱۸]. در بخش بعدی در رابطه با قراردادهای هوشمند که از جنبه های امنیتی مهم فناوری بلاکچین می باشند صحبت خواهد شد.

۵- قرارداد هوشمند[4]

قرارداد هوشمند بخش بنیادین 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

[1] Proof of Work (PoW)
[2] Proof of Stake (PoS)
[3] Directed Acyclic Graph (DAG)
[4] Smart contract

لازم نیست دو یا چند طرف را درگیر کند و لازم نیست قانوناً الزام آور باشد [۱۹]. قرارداد هوشمند که به عنوان کد زنجیره‌ای نیز شناخته می‌شود و شامل مشخصه های زیر است [۲۰]:

- 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 قرارداد روی زیرساخت 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.

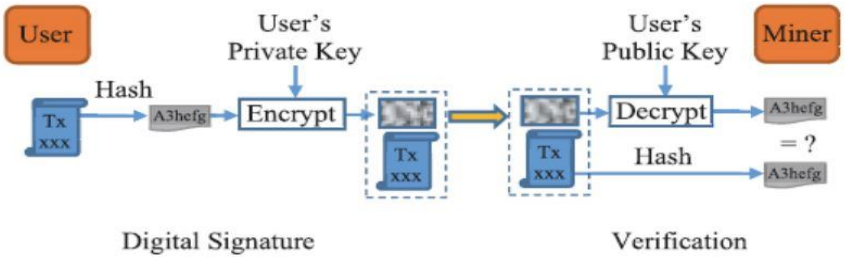
۶- رمزنگاری در بلاکچین

اساسا بلاکچین، لایه‌ای از اعتماد بین طرف‌های غیرقابل اعتماد ایجاد می‌کند تا سوابق و تراکنش‌های امن 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 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 [۲۲].

رمزنگاری کلید عمومی

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. به عنوان مثال، در شکل (۱)، کاربر داده‌های تراکنش خود را به مقدار هش ۱ درهم می‌کند و سپس با کلید خصوصی خود، روی مقدار هش ۱ امضا می‌کند تا امضای دیجیتال تولید کند. سپس کاربر امضای دیجیتال خود را همراه با داده‌های تراکنش خود به شبکه بلاکچین ارسال می‌کند. ماینر از کلید عمومی کاربر برای رمزگشایی امضای دیجیتالی دریافتی برای بدست آوردن مقدار هش A استفاده می‌کند و استخراج کننده نیز داده‌های تراکنش دریافتی را برای به دست آوردن یک مقدار هش B دیگر هش می‌کند. سپس ماینر بررسی می‌کند که آیا مقدار هش A برابر با مقدار هش B است یا خیر. اگر آنها برابر باشند، ماینر تراکنش کاربر را تأیید می‌کند.

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 [۲۳].



شکل ۲. امضای دیجیتال و هش مورد استفاده در معاملات بلاکچین

رمزنگاری کلید خصوصی

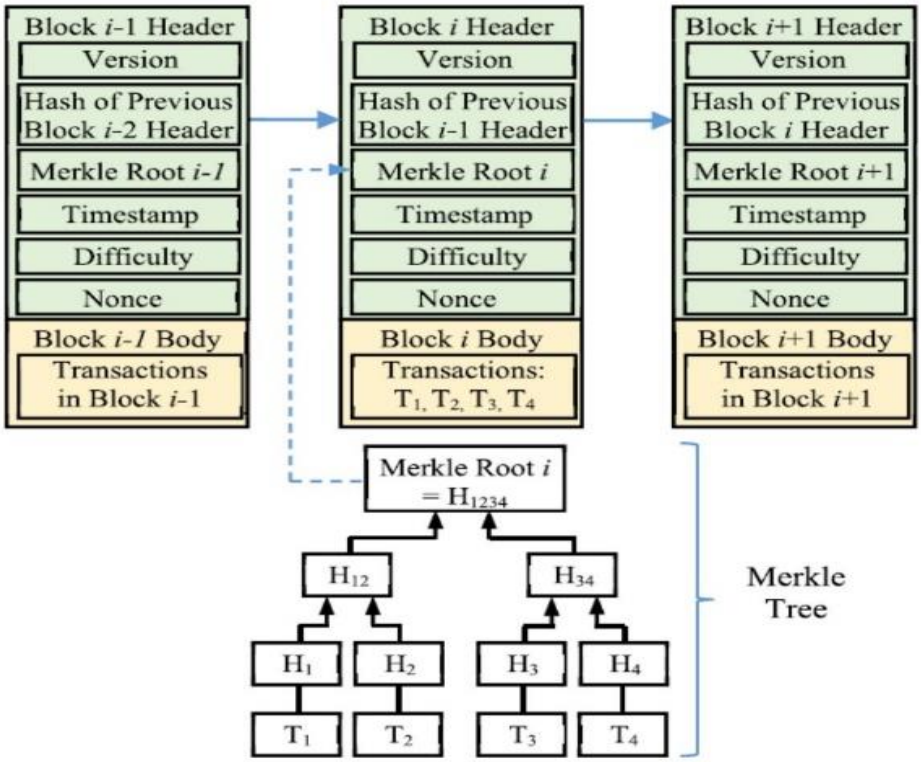
رمزنگاری با کلید خصوصی یکی از اصول بنیادین امنیت در بلاکچین است که تضمین می‌کند تنها مالک قانونی دارایی دیجیتال قادر به امضای و ایجاد تراکنش‌ها باشد .کلید خصوصی رشته‌ای طولانی و تصادفی از اعداد است که در قالب رمزنگاری نامتقارن، برای تولید امضای دیجیتال استفاده می‌شود. این امضا نشان می‌دهد که تراکنش توسط صاحب کلید خصوصی ایجاد و تأیید شده و امکان تغییر در آن وجود ندارد. برخلاف کلید عمومی که برای رمزنگاری و اعتبارسنجی امضا به صورت عمومی و قابل اشتراک استفاده می‌شود، کلید خصوصی باید به صورت کاملاً محرمانه نگهداری شود؛ زیرا دسترسی به آن به معنای دسترسی کامل به دارایی‌های دیجیتال و کیف پول است.

اهمیت کلید خصوصی به حدی است که اگر کاربر این کلید را از دست بدهد، عملاً دسترسی به دارایی‌های را از دست می‌دهد و هیچ نهادی نمی‌تواند آن را بازیابی کند. امنیت کلید خصوصی به دلیل طول بسیار زیاد و پیچیدگی ترکیبات عددی آن بسیار بالاست، به طوری که تقریباً حدس زدن آن برای قوی‌ترین کامپیوترها غیرممکن است. حفاظت دقیق از کلید خصوصی، استفاده از روش‌های ذخیره‌سازی امن مانند کیف پول

سخت‌افزاری و جلوگیری از به اشتراک‌گذاری آن، از جمله اقدامات حیاتی در حفظ امنیت دارایی‌های بلاکچینی به شمار می‌رود [۲۴].

توابع هش

تابع هش یک فناوری کلیدی است که در بلاکچین استفاده می‌شود. تابع هش یک معادله ریاضی با پنج ویژگی مهم برای رمزنگاری است. شکل زیر نشان می‌دهد که 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 (۲) 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 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 [۲۵].



شکل ۳. ساختار اتصال بلاکچین و درخت مرکل با عملکرد هش

۷- چالش‌های امنیتی و حملات در بلاکچین

اساسا، امنیت در بلاکچین یکی از مؤلفه‌های کلیدی موفقیت برنامه‌های تجاری بلاکچین است که همواره می‌بایست برای ارتقای آن تلاش نمود. در نگاهی موشکافانه، خطرات امنیتی و حملات در بلاکچین به شرح ذیل قابل رده بندی می‌باشد [۲۷-۲۶]:

- حملات شبکه: DoS، BGP (پروتکل دروازه مرزی)، حملات مسیریابی، حمله Eclipse، حملات Stealthier، حملات DNS، حملات کانال جانبی از راه دور.
- 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 Self Holding.
- 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.
- حملات مرتبط با حفاظت از داده‌ها: قرار گرفتن در معرض داده های حساس، نشت حریم خصوصی.

- حملات مرتبط با خطای انسانی، ثبت و نظارت ناکافی، پیکربندی اشتباه امنیتی
- باگ‌های واقعی در سیستم‌های بلاکچین
- حملات و باگ‌های قرارداد هوشمند: یکی از نمونه‌های واقعی حملات به قراردادهای هوشمند این است که وقتی یک قرارداد هوشمندخاص DAO بر روی اتریوم برای صندوق سرمایه‌گذاری مخاطره‌آمیز مبتنی بر جمعیت ساخته شد، یک هکر از ضعف کد آن سوء استفاده کرد و ۵۰ میلیون دلار رمزنگاری را دزدید.
- 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.

درکل، چالش‌های امنیتی بلاکچین بسیار متنوع‌اند و از حملات شبکه‌ای و آسیب‌پذیری کدها تا تهدیدات مربوط به قراردادهای هوشمند گسترده‌اند. حملات شبکه همچون حملات انکار سرویس(DoS) ، حملات مسیریابی، و حمله «ایکلیپس» از نمونه‌های بارز تهدیدات هستند که می‌توانند ثبات و عملکرد شبکه را به مخاطره اندازند . همچنین سوء استفاده‌های عمدی شامل دوبار خرج کردن، استخراج خودخواهانه، و حملات رقابتی، تهدیدهایی جدی به شمار می‌آیند. همچنین، آسیب‌پذیری در کدهای قراردادهای هوشمند یکی دیگر از چالش‌های مهم است که با ضعف در برنامه‌ریزی یا خطاهای امنیتی زمینه را برای حملات فراهم می‌کند .علاوه بر این، حملات مرتبط با حفاظت داده‌ها مانند نشت اطلاعات حساس و مسائل مربوط به حفظ حریم خصوصی نیز از موانع اصلی بهره‌گیری کامل از بلاکچین هستند. حملات نقطه پایانی مانند بدافزارها و استخراج رمزارز به صورت پنهان (Cryptojacking)نیز در این زمره قرار می‌گیرند که امنیت کاربران و گره‌ها را تهدید می‌کنند.

۸- چشم اندازها و اقدامات امنیتی برای بلاکچین

چشم‌انداز امنیتی بلاکچین در سال‌های آینده بر توسعه فناوری‌های نوین رمزنگاری و الگوریتم‌های مقاوم در برابر حملات پیشرفته، از جمله حملات با کامپیوترهای کوانتومی، متمرکز است. با پیشرفت کامپیوترهای کوانتومی، الگوریتم‌های رمزنگاری فعلی بلاکچین) مانند RSA و (ECC به چالش کشیده می‌شوند و لازم است الگوریتم‌های پساکوانتومی جایگزین و پیاده‌سازی شوند تا امنیت کلیدهای خصوصی و امضای دیجیتال حفظ شود. این موضوع باعث شده توسعه‌دهندگان بلاکچین در تلاش برای به‌روزرسانی ساختارهای رمزنگاری خود از طریق هارد فورک‌ها و الگوریتم‌های رمزنگاری مقاوم باشند [۲۸].

یکی دیگر از ابعاد مهم، حفظ حریم خصوصی و امنیت داده‌هاست. با توجه به ماهیت شفاف بلاکچین، در حالی که شفافیت یکی از محاسن آن است، حفظ محرمانگی اطلاعات شخصی و داده‌های حساس چالشی جدی محسوب می‌شود. راهکارهایی مانند استفاده از تکنیک‌های رمزنگاری پیشرفته مانند zk-SNARKs ، شبکه‌های خصوصی یا بلاکچین‌های ترکیبی به منظور افزایش حریم خصوصی مورد توجه قرار گرفته‌اند. همچنین، اقدامات قوی‌تر در حوزه مدیریت دسترسی و احراز هویت چندعاملی، به منظور کاهش احتمال نفوذهای انسانی و اشتباهات محرمانگی اهمیت یافته‌اند.

ادغام فناوری‌های نوظهور مانند هوش مصنوعی (AI) و اینترنت اشیاء (IoT)در بلاکچین فرصت‌ها و تهدیدات جدیدی ایجاد کرده است. از یک طرف، AIمی‌تواند در شناسایی تهدیدات و پیشگیری از حملات کمک کند و IoT با بلاکچین امنیت دستگاه‌ها و ارتباطات را بالا ببرد؛ اما از طرف دیگر، در صورت ضعف امنیتی در دستگاه‌هایIoT ، آنها می‌توانند نقاط ورود برای نفوذ به شبکه‌های بلاکچین شوند. بنابراین، طراحی پروتکل‌های امنیتی مخصوص برای دستگاه‌های متصل و بهبود محافظت لایه‌ای اساس امنیت بلاکچین در این حوزه است.

یکی از رویکردهای مهم، ارتقاء الگوریتم‌های اجماع است که نقش کلیدی در امنیت و پایداری شبکه دارند. الگوریتم‌های نوآورانه مانند Proof of Stake (PoS) پیشرفته‌تر، الگوریتم‌های اجماع ترکیبی، و گراف غیر چرخه‌ای هدایت شده (DAG)باعث افزایش مقیاس‌پذیری، کاهش مصرف انرژی و تقویت مقاومت در برابر حملات توزیع شده می‌شوند. همچنین، این الگوریتم‌ها با طراحی‌های مدرن می‌توانند حملات ۵۱ درصدی و تهدیدات متمرکزسازی را کاهش دهند. روند توسعه استانداردهای امنیتی جهانی و همکاری‌های بین‌المللی نیز بخش مهمی از چشم‌انداز امنیت است. تدوین قوانین دقیق، ایجاد چارچوب‌های حقوقی برای حمایت از کاربران و تضمین شفافیت و پاسخگو بودن، موجب افزایش اعتماد به بلاکچین می‌شود و گسترش کاربرد آن در حوزه‌های مالی، حقوقی و دولتی را تسریع می‌کند.

در نهایت، توسعه ابزارهای تحلیلی و سیستم‌های نظارتی امنیتی هوشمند برای پایش لحظه‌ای شبکه بلاکچین، شناسایی تهدیدات جدید و واکنش سریع به حملات از الزامات آینده این فناوری است. استفاده از یادگیری ماشین در تشخیص الگوهای مشکوک و تحلیل رفتار کاربران، امکان پیشگیری از حملات پیچیده و مهندسی اجتماعی را فراهم می‌کند. این اقدامات موجب می‌شود امنیت بلاکچین همگام با رشد فناوری‌های مرتبط، به سطح بالایی از تضمین و پایداری برسد.

۹- نتیجه گیری و راهکارهای آتی

مقاله حاضر یک بررسی جامع از جنبه‌های امنیتی فناوری بلاکچین، چالش‌ها و چشم‌اندازهای آن ارائه داده است. امنیت بلاکچین به دلیل ویژگی‌های منحصر به فردی مانند غیرمتمرکز بودن، رمزنگاری پیشرفته، و الگوریتم‌های اجماع، بستری امن برای ثبت و انتقال داده‌ها فراهم می‌کند. با این وجود، چالش‌های متعددی از جمله آسیب‌پذیری‌های کد، حملات شبکه و قراردادهای

هوشمند، و مشکلات حفظ حریم خصوصی وجود دارند که نیازمند تحقیقات و توسعه راهکارهای نوین هستند. این مقاله ابتدا یک بررسی تفضیلی در مورد بلاکچین انجام داده است. فناوری از نظر نمای کلی، 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 چشم اندازها و اقدامات امنیتی را در زمینه‌های تجزیه و تحلیل امنیت، امنیت کدهای نرم‌افزار، حفظ حریم خصوصی و غیره ارائه کرده است. همچنین، چالش‌ها و روندهای تحقیقاتی برای ساخت سیستم‌های بلاکچین مقیاس‌پذیرتر و ایمن‌تر برای استقرار گسترده ارائه شده‌اند. اقدامات امنیتی و فناوری‌های مکمل نظیر شبکه‌های خصوصی، الگوریتم‌های اجماع پیشرفته و ابزارهای تحلیل آسیب‌پذیری، در راستای افزایش امنیت و مقیاس‌پذیری بلاکچین نقش مهمی دارند. اهمیت توجه به این چالش‌ها همراه با بهره‌گیری از فناوری‌های نوظهور، کلید موفقیت در توسعه پایدار و گسترده این فناوری است. این مقاله می‌تواند مرجعی ارزشمند برای پژوهش‌های آینده در زمینه امنیت بلاکچین و توسعه فناوری‌های مرتبط باشد.

تعارض منافع

نویسندگان این مقاله اعلام می دارند که هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

مراجع

1. Rezae M, Mohammadpur A. Exploring the Security Aspects of Blockchain Technology: Challenges and Prospects. Arman Process Journal. 2025;6(2):49-59.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
3. Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Applied Innovation. 2016;2(6-10):71.
4. Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data. 2017:557-564.
5. Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303.
6. Gervais A, Karame G, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the Security and Performance of Proof of Work Blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016:3-16.
7. Kshetri N. Blockchain’s roles in meeting key supply chain management objectives. International Journal of Information Management. 2018;39:80-89.
8. Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303.
9. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE. 2016;11(10):e0163477.
10. Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology. IEEE International Congress on Big Data. 2017:557-564.
11. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. 2014.
12. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy. 2015:104-121.
13. Conti M, Dehghantanha A, Franke K, Watson S. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems. 2018;78:544-546.
14. Dinh T, Wang J, Chen D, Liu R, Ooi BC, Wang J. BLOCKBENCH: A Framework for Analyzing Private Blockchains. Proceedings of the 2017 ACM International Conference on Management of Data. 2017:1085-1100.
15. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
16. Saleh F. Blockchain Without Waste: Proof-of-Stake. The Review of Financial Studies. 2020;33(7):3428-3470.
17. Popov S. The Tangle. 2018. Available from: https://iota.org/IOTA_Whitepaper.pdf.
18. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. ACM SIGMETRICS Performance Evaluation Review. 2014;42(3):34-37.
19. Szabo N. Smart Contracts: Building Blocks for Digital Markets. EXTROPY. 1996;16.
20. Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303.
21. Gai K, Qiu M, Sun X. A Survey on FinTech. Journal of Network and Computer Applications. 2018;103:262-273.
22. Atzei N, Bartoletti M, Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Proceedings of the 6th International Conference on Principles of Security and Trust. 2017:164-186.
23. Bonneau J, Felten E. The Twin Challenges of Privacy and Transparency in Generic Blockchain Designs. IEEE Security & Privacy. 2020;18(4):16-26.

24. Merkle RC. A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology — CRYPTO '87. 1988;pp:369-378.
25. Li X, Jiang P, Chen T, Luo X, Wen Q. A Survey on the Security of Blockchain Systems. Future Generation Computer Systems. 2020;107:841-853.
26. Luu L, Chu D, Olickel H, Saxena P, Hobor A. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016:254-269.
27. Chen T, Li X, Luo X, Wen Q. A Review on Security Privacy Challenges and Attacks of Blockchain. IEEE International Congress on Big Data. 2018:557–564.
28. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang F. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019;49(11):2266-2277.