فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال هفتم، شماره ۹۱، زمستان ۱۴۰۲، ص ۹۱۶-۹۱۱

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

فناوری بلاک چین و مدیریت کلید

عرفان کائیدی [۱]
نصراله تختائی [۲]

تاریخ دریافت: ۱۴۰۲/۰۹/۰۱ تاریخ چاپ: ۱۴۰۲/۱۲/۲۹

چکیده

بلاک چین[۱] را می توان دنباله ای از بلاک های داده متصل درنظر گرفت که هر یک به بلاک قبلی وابسته است و یک ساختار داده زنجیروار پیوسته را تشکیل می دهد. فناوری بلاک چین در زمینه های مختلفی مانند اینترنت اشیاء، رایانش ابری، مدیریت هویت، ارتباطات و... کاربرد دارد. به طورکلی بلاک چین یک سیستم ثبت اطلاعات و گزارش توزیع شده و به صورت غیرمتمرکز است و بر امنیت داده ها تاکید زیادی دارد. از فناوری بلاک چین، به عنوان یک فناوری انقلابی یاد می شود. از دیدگاه برخی افراد، انقلابی بودن بلاک چین معادل ظهور اینترنت در قرن بیستم است. بلاک چین به دلایلی مانند امکان پذیر بودن سطح بالایی از غیرمتمرکزبودن، حفظ حریم خصوصی و امنیت کاربر محسوب می شود. در این مقاله مروری بر فناوری بلاک چین و مدیریت کلید، چالش ها و روابط بین آن ها انجام شده است.

واژگان کلیدی

فناوری بلاک چین، مدیریت کلید، متادیتا، تایم استمپ، نانس

۱. دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد دزفول، دزفول، ایران.
۲. استادیار حسابداری، دانشگاه آزاد اسلامی واحد دزفول، دزفول، ایران.

[1]-Blockchain

۱-مقدمه

بلاک چین پایه واساس بیت کوین و سایر ارزهای رمزنگاری شده را تشکیل می دهد. بیت کوین، اولین رمزنگاری شده است که در سال ۲۰۰۸ توسط Satoshi Nakamoto پیشنهاد و در سال ۲۰۰۹ پیاده سازی شد. (Silberschats, A, Korth)

بلاک چین را می توان به عنوان یک دفتر عمومی درنظر گرفت که در آن تمام تراکنش ها به اتمام رسیده در یک زنجیره از بلاک ها ذخیره می شود.

بلاک چین، دنباله ای از بلاک های داده متصل است. بلاک یک ظرف ساختار داده با اندازه ثابت است. در مواردی، بلاک ها معمولا شامل هزاران تراکنش هستند و اندازه معمول یک بلاک می تواند به چندین مگابایت هم برسد.

بلاک از دو قسمت تشکیل شده: سرآیند و بدنه اصلی.

پایگاه داده های بلاک چین، ویژگی های خاص بلاک چین نظیر غیرمتمرکز بودن و تغییر ناپذیری و خواص مطلوب و منحصر به فرد پایگاه داده ها نظیر زمان تاخیر کم و توان عملیاتی بالا را دارا هستند.

پایگاه داده های بلاک چین با ویژگی های منحصر به فردشان می توانند در طیف گسترده ای از زمینه ها، از جمله اینترنت اشیاء مورد استفاده قرار می گیرند.

در قسمت بعدی به معرفی فناوری بلاک چین و مدیریت کلید خواهیم پرداخت و رابطه آن ها را با هم بررسی می کنیم و در مورد چالش های مربوط به آن ها صحبت می کنیم.

۲- مبانی نظری

۲-۱، فناوری بلاک چین

بلاک چین نوعی شبکه نظیر به نظیر و دفتر توزیع شده است که با از بین بردن اشخاص ثالث، یک محیط قابل اعتماد برای معاملات بین افراد را فراهم می کند. بلاک چین شبکه ای شفاف و غیرمتمرکز است که از یک زنجیره بلوک شکل گرفته و برای مدیریت معاملات و اطلاعات استفاده می شود.

بلوک ها ساختار اصلی برای ذخیره اظلاعات در زنجیره هستند و توسط کد های خاصی به نام هش شناسایی می شود.

بلوک شامل دو جزء بود: سرآیند و بدنه اصلی.

سرآیند شامل سه مجموعه متادیتا است.

متادیتا: داده ای که اطلاعاتی درباره سایر داده ها ارائه می دهد.

مجموعه اول متادیتا، مرجعی برای اشاره به بلوک قبلی است.

مجموعه دوم متادیتا، مربوط به رقابت در فرآیند ماینینگ یا استخراج است شامل اجزای نانس، تایم استمپ و ان بیتس است.

مجموعه سوم متادیتا: ریشه درخت مرکل است.

تایم استمپ، زمان تقریبی ایجاد یک بلوک است و در ردیابی استفاده می شود.

نانس یک عدد یکبار مصرف است.

ان بیتس[۲]: شکل کد گذاری شده آستانه هدف است.

بدنه بلوک معمولا شامل شمارنده تراکنش و تمام تراکنش ها یا رکورد داده هاست. تعداد تراکنش های یک بلوک به اندازه بلوک و اندازه هر تراکنش بستگی دارد.

در بلاک چین، تراکنش ها به عنوان بخشی ازیک درخت مرکل ذخیره می شوند. در ساختار درخت مرکل، گره های برگ مقدار هش مربوط به هر تراکنش را نشان می دهد.

از مهم ترین اجزای لایه شبکه بلاک چین، شبکه همتا به همتاست.

از ویژگی های مهم بلاک چین، غیرمتمرکز بودن آن است که یک سرور مرکزی برای ذخیره سازی اطلاعات وجود ندارد و اطلاعات در همه سرور ها تکثیر می شود. (محمد پیام الماسیان و همکاران ۱۳۹۹).

هش، یک فرمول ریاضی تصادفی و پیچیده است که در فرآیند تایید بلوک استفاده می شود.

بلاک چین می تواند به عنوان شبکه خصوصی برای گروهی خاص از شرکت کنندگان محدود باشد یا شبکه عمومی که پیوستگی همه آزاد است. (زهرا شریف خطیبی و سید کامیار ایزدی، ۱۳۹۹)

(Xu, Lx) سیستم های بلاک چین سه نوع هستند. بلاک چین عمومی، بلاک چین خصوصی و بلاک چین کنسرسیوم.

در بلاک چین عمومی تمام تراکنش ها برای عموم قابل استفاده است.

در بلاک چین کنسرسیوم، یک سازمان یا کنسرسیوم تصمیم می گیرد که قابلیت مشاهده اطلاعات ذخیره شده، عمومی بوده یا محدود به شرکت کنندگان باشد.

بلاک چین خصوصی کاملا متمرکز است زیرا توسط یک گروه واحد، کنترل می شود.

بلاک چین عمومی با توجه به ویژگی های منحصر به فردش، کاربران زیادی دارد و بلاک چین کنسرسیوم کاربرد تجاری دارد و بلاک چین خصوصی در شرکت ها برای بهره وری و حسابرسی استفاده می شود.

انواع بلاک چین ها دارای ویژگی های زیر هستند:

شفافیت، پایداری، غیرمتمرکز بودن، انکار ناپذیری، ناشناس بودن، قابلیت ردیابی تحمل خطا و مقاومت در برابر حمله. (Magyer)

۲-۲، چالش های مربوط به فناوری بلاک چین:

فناوری بلاک چین با خطرات جدیدی از جمله مفقود شدن یا سرقت کلید های خصوصی، افزایش حملات یا نقض در قرارداد های هوشمند مواجه است.

در این قسمت، دو چالش اصلی که شامل الزامات اجرایی و عملکردی و امنیت است را بررسی می کنیم. در فناوری بلاک چین با رشد مداوم تعداد تراکنش ها، اندازه بلاک چین افزایش می یابد و در نتیجه میزان هزینه های ذخیره سازی زیاد و سرعت توزیع بلاک چین روی شبکه کاهشی می شود. (زهرا شریف خطیبی و سید کامیار ایزدی، ۱۳۹۹).

بلاک چین های عمومی، برای بهره گیری از امنیت مکانیزم توافق، محدودیت هایی روی اندازه بلوک و بازه ی زمانی تراکنش ها ایجاد می کنند که در نهایت باعث کاهش بازده تراکنش ها می شود.

[2]- N Bits

مقیاس پذیری و در دسترس بودن سیستم بلاک چین از مشکلات بالقوه در زمینه عملکردی است.)و همکاران (Hafid با افزایش حجم تراکنش ها، عمومی نمی تواند فعالیت خود را به درستی انجام دهد.

از نظر (Feng و همکاران) دو نوع تهدید اساسی علیه فناوری بلاک چین وجود دارد: حمله اکثریت و ماینینگ خودخواه.

وقتی که مهاجم تعداد زیادی سیستم ایجاد کند که هر کدام یک شرکت کننده هستند و مهاجم آن ها را کنترل می کند، حمله اکثریت رخ داده.

در ماینینگ خودخواه، مهاجم، به جای پخش بلوک ها در شبکه، آن را در یک شعبه خصوصی قرار می دهد.

برخی از مخاطرات بلاک چین: تغییر رفتار، مدت زمان، راه اندازی، قوانین دولتی و ...

۲-۳، مدیریت کلیدی:

مدیریت کارآمد و ایمن کلید یک چالش برای هر سیستم رمزنگاری است. اگر مزاحم بتواند کلیدها را با

مکانیزمی مانند نیروی ضربه، حمله کانال جانبی، دسترسی فیزیکی به سیستم، رمزگذاری ضعیف،

حمله مجدد و غیره کشف کند، در این صورت مهاجم قادر است همه چیز را از سیستم مورد نظر بدزدد.

مدیریت کلیدها یکی از حیاتی ترین اجزای سیستم رمزنگاری است. هیچ زیرساختی امن نیست اگر کلیدهای آن امن نباشد. (Surendra Singh (2021) & Om pal, Bashir Alam, Vinay Thakur)

هیچ زیرساختی امن نیست اگر کلیدهای آن امن نباشد.

زیرساخت کلید عمومی یکی از مکانیسم های مدیریت کلیدها در سیستم های رمزنگاری کلید عمومی است.

زیرساخت کلید عمومی در فناوری بلاک چین برای احراز هویت موجودیت ها و اطمینان از یکپارچگی بلاک چین استفاده می شود. (فرشاد رحیمی اصل، رضا عزمی ۱۳۸۹)

مدیریت کلید[3]، در واقع مدیریت یک کلیدهای رمزنگاری در یک سیستم رمزنگار می باشد و شامل تولید، مبادله، ذخیره، استفاده و جانشانی کلیدها می شود.

رمز گذاری داده ها چالش های فراوانی دارد و از اصلی ترین آن ها مدیریت و توزیع کلید بین اعضای مجاز است. مشکل دیگر انقضا دسترسی و یا ابطال کلید است. (محمد پیام الماسیان و همکاران ۱۳۹۹)

کلید رمزنگاری مجموعه ای از داده هاست که برای رمزگذاری داده ها، رمزگشایی و امضای داده و یا تایید یک امضا مورد استفاده قرار می گیرد.

نمونه هایی از فراهم کنندگان مدیریت کلید:

یونی باند – تچ – لجر

[3]- Key Management

۲-۴، رابطه بین فناوری بلاک چین و مدیریت کلید:

در فناوری بلاک چین اطلاعات زیادی به دلیل وجود افراد بسیار، وجود دارد و حفظ و نگه داشتن این اطلاعات بسیار مهم است و در صورت فاش شدن اطلاعات، اشخاصی ممکن است از آن ها سوء استفاده کنند و در این قسمت مدیریت کلید وارد عمل می شود و از سوء استفاده هکرها از اطلاعات اشخاص جلوگیری می کند.

انواع تهدیدات: ۱- برخط ۲- برون خط

تهدیدات برخط، تهدیداتی که مهاجم برای حمله به سیستم حتما به طور برخط با سیستم و کاربران و منابع اطلاعاتی در ارتباط باشد تا از آن ها استفاده کند.

تهدیدات برون خط، مهاجم نیازی ندارد که که سیستم و کاربران برخط باشند. (فرشاد رحیمی اصل، رضا عزمی ۱۳۸۹)

از دست رفتن کلید و بکارگیری آن توسط مهاجم باعث:

- داده های رمز گذاری شده به شکل اولیه و اصلی خود برمی گردند
- از اسناد و نرم افزار ها سوء استفاده می کند
- ممکن است مهاجم کل زیر ساخت را از بین ببرد

یک مدیریت کلید موفق برای امنیت یک سیستم رمزنگار بسیار حیاتی است.

نتیجه گیری

توسعه فناوری بلاک چین، توجه بسیاری را به کاربرد این فناوری در زمینه های مختلف سوق داده است.

بلاک چین در مواردی مثل مدیریت هویت، قراردادهای هوشمند، زنجیره های تامین، خدمات دولت الکترونیک، انفورماتیک پزشکی و... کاربرد دارد ولی طبق سخنان قبلی که در متن وجود دارد، پیاده سازی بلاک چین با چالش های متعددی روبروست. توجه به این چالش ها در طراحی و برنامه ریزی اهمیت فراوان دارد.

فناوری بلاک چین نیاز شخص ثالث را برای اعتبارسنجی تراکنش های شبکه از بین می برد.

مدیریت کلید مبحث بسیار مهمی در زمینه حفاظت از اطلاعات اشخاص است که اگر فاش شود ممکن است عواقب ناخوشآیندی داشته باشد.

منابع

شریف خطیبی، زهرا و ایزدی، سیدکامیار. (۱۳۹۹). بلاک چین و کاربرد آن در ذخیره اطلاعات به عنوان پایگاه داده توزیع شده امن. فناوری اطلاعات و ارتباطات انتظامی، ۱(۲)، ۸۵-۱۰۶fa/384732/paper/sid.ir/https://SID. .

الماسیان، محمدپیام، شفیعی نژاد، علیرضا و سجادیه، سیدمهدی. (۱۳۹۹). روش کنترل دسترسی مبتنی بر بلاکچین و رمزنگاری ویژگی مبنا. صنایع الکترونیک، ۱۱(۳)، ۱۵-۲۹fa/964254/paper/sid.ir/https://SID. .

رحیمی اصل، فرشاد و عزمی، رضا. (۱۳۸۹). مدلی امن برای مدیریت کلید و کنترل دسترسی رمزنگاری درسیستم فایل رمزنگاری. کنفرانس بین المللی انجمن رمز ایرانfa/813128/paper/sid.ir/https://SID. .

شفیعی، نفیسه و شجری، مهدی. (۱۳۹۴). مدیریت کلید در سیستم های مدیریت حقوق دیجیتال در حالت برون خطی. فناوری اطلاعات و ارتباطات ایران، ۷(۲۳-۲۴)، ۷۹-۸۸fa/171495/https://sid.ir/paper . SID.

Om pal, Bashir Alam, Vinay Thakur & Surendra Singh (2021). Key management for blockchain technology. Journal of The Korean Institue of Communications and Information Sciences, Vol 7, Issue 1, March 2021.