دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۴، جلد ۲۳، شماره ۱ (۶۴-۹۶)
https://monadi.isc.org.ir

مرور روشمند ادبیات امنیت و حفظ حریم‌خصوصی و بهبود گمنامی در شبکه زنجیره قطعات

فاطمه چارلنک بختیاری* و عباس قائمی بافقی

گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی، مشهد، ایران

اطلاعات مقاله

کلمات کلیدی:
امنیت
حریم‌خصوصی
گمنامی
زنجیره قطعات

نوع مقاله: مروری

چکیده

فن‌آوری زنجیره قطعات به عنوان یک دفتر کل توزیع شده به دلیل عمومی بودن، شفافیت، تمرکززدایی و ثبات در امنیت و حفظ حریم‌خصوصی تراکنش‌های کاربران بسیار مورد توجه قرار گرفته است. با این وجود، در این روش ممکن است حریم‌خصوصی کاربران در مبدا، مقصد و گردش تراکنش‌های ارزهای دیجیتال به خطر بیفتد. از این رو قابلیت گمنامی در تراکنش‌های زنجیره قطعات و حفاظت از حریم‌خصوصی کاربران در این روش اهمیت زیادی دارد. هدف این مقاله براساس روش‌های علمی، مروری بر امنیت و حفظ حریم خصوصی و نیز گمنامی تراکنش و هویت کاربران زنجیره قطعات است. همچنین ویژگی‌های امنیتی زنجیره قطعات، طبقه‌بندی، چالش‌ها و عملکرد آن‌ها مورد بحث قرار می‌گیرد. به منظور رسیدن به این هدف، چهار سوال تحقیقاتی مهم در هر زمینه تحقیقاتی مطرح شده و سپس در پاسخ به این سوالات و پیدا کردن راه‌کارهای مناسب، مقالات موجود مرور و دسته بندی می‌شود. سوال اول: ویژگی‌های انواع مختلف زنجیره قطعات چیست؟ و مزایا و معایب هریک کدام است؟ سوال دوم: مفهوم گمنامی، شبه گمنامی، حریم خصوصی و محرمانگی چیست و شیوه‌های حفظ حریم‌خصوصی کدام است؟ سوال سوم: آسیب پذیری‌ها و تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟ سوال تحقیق چهارم: شیوه‌های مقابله با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟ در پاسخ به سوال اول و براساس مقالات موجود، زنجیره قطعات به سه دسته عمومی (بدون مجوز)، خصوصی (مجوزدار) و کنسرسیوم طبقه‌بندی می‌شود که ویژگی‌های آن را می‌توان به پارامترهایی مانند کارایی، مشارکت و اجماع، شبکه، امنیت و شفافیت و دسترسی و اجازه خواندن طبقه‌بندی کرد. در پاسخ به سوال دوم، مفهوم گمنامی، شبه گمنامی و حریم‌خصوصی به دلیل اهمیت بسزایی که در میان تراکنش‌ها و کاربران زنجیره قطعات دارد مورد بررسی قرار می‌گیرد و در نهایت به مهم‌ترین ویژگی‌های شیوه‌های حفظ حریم‌خصوصی اشاره شده است. سوال سوم، حملات را براساس نوع حمله به ۹ گروه دسته‌بندی کرده است و مقالات مطالعه شده میزان توجه جامعه علمی به جنبه‌های حمله و تهدید را نشان می‌دهد. سوال چهارم، طبق مقالات مطالعه شده اقدامات متقابل با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی را براساس نوع حمله دسته بندی کرده است.

© ۱۴۰۴ انجمن رمز ایران

۱ مقدمه

زنجیره قطعات به دلیل ویژگی‌های غیرمتمرکز بودن، تغییر ناپذیری داده‌ها و اعتماد، کاربرد گسترده‌ای در زمینه‌های مختلف از جمله امنیت، اینترنت اشیاء، بهداشت و ... دارد. با این‌حال، شفافیت و غیرمتمرکز بودن،

*نویسنده مسئول
آدرس‌های رایانامه: fatemeh.bakhtiari1126@gmail.com (فاطمه چارلنک بختیاری)، ghaemib@um.ac.ir (عباس قائمی بافقی)
© ۱۴۰۴ تمامی حقوق متعلق به انجمن رمز ایران است.

حفاظت مؤثر از حریم‌خصوصی کاربر را با مشکل مواجه ساخته است. از این رو مسئله حفاظت از حریم‌خصوصی در زنجیره قطعات، خصوصا زنجیره قطعات عمومی (بدون مجوز) تبدیل به یک موضوع تحقیقاتی مهم شده است. زنجیره قطعات را می‌توان به دو نوع مجوزدار و بدون مجوز تقسیم کرد، که در زنجیره قطعات مجوزدار، اجماع و دسترسی به داده‌ها تنها برای نهادهای خصوصی و دارای صلاحیت فراهم شده است، اما زنجیره قطعات بدون مجوز به هر نهادی اجازه می‌دهد که آزادانه به زنجیره قطعات ملحق شده یا آن را ترک کند [۱]. علاوه بر این، داده‌های موجود در زنجیره قطعات بدون مجوز، جهت تأیید عمومی برای تمام نهادها شفاف است و تضمین حریم‌خصوصی با کنترل دسترسی آسان‌تر است. اما برای زنجیره قطعات بدون مجوز افشای محتوای تراکنش ممکن است منجر به افشای حریم‌خصوصی و مخصوصا اطلاعات حساس کاربران شود. زنجیره قطعات بدون مجوز، یک سیستم باز و غیرمتمرکز است که فاقد یک حاکمیت قوی برای حفظ سیستم و تضمین حریم‌خصوصی است، در نتیجه حفاظت از حریم‌خصوصی در زنجیره قطعات بدون مجوز بسیار اهمیت دارد [۲]. اما راه‌حل‌های حریم‌خصوصی سنتی در زنجیره قطعات قابل استفاده نیست و دستیابی به حفاظت حریم‌خصوصی واقعی در سیستم‌های زنجیره قطعات بدون مجوز مشکل و چالش برانگیز است.

شش ویژگی مهم امنیتی زنجیره قطعات شامل یکپارچگی، شفافیت، قابلیت ردیابی، پاسخگویی، گمنامی و جعل ناپذیری در کارهای مرتبط با زنجیره قطعات مشاهده می‌شود.

- یکپارچگی خاصیتی است که مطمئن می‌شود داده‌های ارسالی بدون هیچ تغییری در مقصد دریافت می‌شود [۶]. یکپارچگی می‌تواند در دسترس بودن خدمات را فعال کند. دقت، اصالت و مقاومت در برابر دستکاری از ویژگی‌های مربوط به یکپارچگی است [۷، ۸]. ویژگی یکپارچگی زنجیره قطعات تضمین می‌کند که داده‌ها پس از ثبت نمی‌تواند تغییر یابد. این ویژگی در بسیاری از رویکردها مورد بحث و بررسی قرار گرفته است [۹-۱۲].
- شفافیت زنجیره قطعات توسط نوع ساختار داده‌های زنجیره‌ای درهم‌سازی توالی اضافه می‌شود [۱۳، ۱۴]. شفافیت زمانی حاصل می‌شود که چیزی به صورت عمومی در زنجیره قطعات بارگذاری شود و در دسترس همه باشد. شفافیت یک عنصر تعیین کننده ایجاد اعتماد برای زنجیره قطعات است که می‌توان در زمینه‌های مختلف اعمال کرد [۷، ۱۵، ۱۶].
- قابلیت ردیابی داده‌ها عموماً با ثبت داده‌ها در زنجیره‌های قطعات و ارجاع به آن‌ها با استفاده از یک هویت خاص مانند یک مقدار درهم‌ساز به دست می‌آید [۱۸] و [۱۹]. که در آن هویت امضاکنندگان می‌تواند زمانی که برخی از اعضای گروه با هم کار می‌کندکشف شود[۲۰]. علاوه بر این، یکپارچگی و شفافیت با خاصیت ردیابی ارتباط دارد [۱۵]. این ویژگی زنجیره قطعات رایج‌تر شده و به عنوان یک راه‌حل امنیتی در بسیاری از کارها استفاده می‌شود [۷، ۲۱، ۲۲].
- صداقت و عدم انکار از ویژگی‌های مهم است [۲۳] و پاسخگویی مشابه عدم انکار است که در آن کنشگر نمی‌تواند یک معامله متعهد را انکار کند [۱۰، ۲۴].
- گمنامی کاربران تهدید اصلی است که در [۲۵] مورد بحث قرار گرفته و در بخش‌های مختلف اعمال می‌شود [۷، ۲۶، ۲۷]. در اینجا، گمنامی را می‌توان به عنوان شیوه حفاظت از حریم خصوصی در نظر گرفت که در آن هویت و اطلاعات شخصی کاربران حفظ می‌شود. علاوه بر این، آدرس زنجیره قطعات که نشان دهنده مقصدی برای پرداخت ارز دیجیتال است، می‌تواند به عنوان نام مستعار استفاده شود.
- جعل ناپذیری زنجیره قطعات تضمین می‌کند که دشمن نتواند خود را به عنوان کاربر نشان دهد یا شبکه را فاسد کند. برای این منظور، جعل ناپذیری در زنجیره قطعات از یکپارچگی داده‌ها ناشی می‌شود و همراه با تراکنش‌های امضا شده دیجیتالی در چندین کار مورد استفاده قرار گرفته است [۱۱، ۲۸، ۲۹].

برای بررسی حجم وسیع کارهای پژوهشی، نیاز به یک روش تحقیق پیشرفته است. این روش باید بتواند تمام کارهای تحقیقاتی انجام شده در حوزه را پوشش دهد و همچنین باید قابل اعتماد و دقیق با نتایج قابل ردیابی باشد. یکی از قابل اعتمادترین روش‌ها مهندسی نرم افزار مبتنی بر شواهد است که روش تحقیق معروف، مرور روشمند ادبیات را معرفی می‌کند. مرور روشمند ادبیات توسط کیچنهام و چارترز در زمینه مهندسی نرم‌افزار در [۵] شرح داده شده مبنای تحقیق ما می‌باشد که شامل سه مرحله زیر است و ساختار مقاله برآن اساس سازماندهی شده است:

(۱) برنامه‌ریزی: در طول این مرحله، سوالات تحقیق و اهداف مرور روشمند استخراج می‌شود. همچنین، پایگاه‌های اطلاعاتی برای بازیابی مقالات مورد نظر انتخاب شده و معیارهای شمول و عدم شمول ارائه می‌شود.

(۲) اجرا: مرور روشمند طبق طرحی که قبلاً طراحی شده بود انجام می‌شود. مطالعات استخراج و سپس پالایش می‌شود و مقالات باقی مانده خوانده می‌شود. از یک چارچوب تحلیلی برای استخراج داده‌های لازم برای پاسخ به سوالات تحقیق استفاده می‌شود.

(۳) گزارش: نتایج مرور روشمند به طور واقعی ارائه می‌شود و همچنین ارزیابی کیفیت از مطالعات استخراج شده انجام می‌شود.

سپس، آن‌ها در بخش خود مورد بحث قرار می‌گیرد.

در مرحله اول با جستجوی کلمه Blockchain در منابع، ۹۲۲ نشریه شامل مجلات علمی و مقالات کنفرانس بدست آمد. دسترسی به ۱۱۰ مورد فراهم نشد و سوال اول و دوم تحقیق مبتنی بر ۸۱۲ نشریه حاصل پاسخ داده شد. از میان ۸۱۲ نشریه مرحله یک، ۱۷۹ مورد مربوط به Privacy، Anonymity و Security برای ورود به مرحله دوم انتخاب شده و بعد از بررسی مراجع آن‌ها ۶۰ نشریه دیگر هم اضافه شد. در مرحله دوم با جستجوی کلمات کلیدی Blockchain، Privacy، Anonymity، Security در منابع ۳۱۱ نشریه بدست آمد که بعد از پالایش ۱۳۵ مورد برای استخراج داده‌ها انتخاب شده و ۳۰ نشریه هم از بررسی مراجع آن‌ها بدست آمده است. مجموع ۲۳۹ نشریه مرحله اول و ۱۶۵ نشریه مرحله

دوم برای پاسخ به بقیه سوالات تحقیق مورد استفاده قرار گرفت.

در بخش ۲ اهداف و انگیزه تحقیق بیان شده و برنامه‌ریزی انجام می‌شود. در بخش ۳ روند اجرا بیان شده و منابع گردآوری شده ارائه می‌شود. در بخش ۴ نتایج تجزیه و تحلیل مطالعات انتخاب شده بیان می‌شود و یافته‌های تحقیق مورد بحث و بررسی قرار می‌گیرد و پاسخ به سوالات تحقیق ارائه می‌شود. بخش ۵ شامل جمع‌بندی و نتیجه‌گیری است و پیشنهادهایی برای تحقیقات بیشتر ارائه می‌دهد.

۲ برنامه‌ریزی روش تحقیق مرور روشمند

در این روش تحقیقی، که به طور گسترده در زمینه‌های مختلف از جمله علوم کامپیوتر استفاده می‌شود، بطور روشمند پروژه‌ها یا انتشارات تحقیقاتی جمع‌آوری و بررسی انتقادی می‌شود. این یک رویکرد جامع برای بررسی و ارزیابی کلیه مقالات و مطالعات دانشگاهی مرتبط در مورد یک سوال یا موضوع پژوهشی خاص است [۴].

۱.۲ بررسی مرورهای پیشین و انگیزه تحقیق

در سالهای اخیر مرورهای مختلف برروی حریم خصوصی در زنجیره قطعات انجام شده است [۲، ۵۳، ۶۱، ۶۴، ۶۶، ۶۹، ۷۸، ۸۰، ۱۱۰، ۱۷۷، ۲۰۲، ۲۰۴، ۲۱۴، ۲۲۲، ۲۳۱]. با این حال، پیشرفت خود زنجیره قطعات و فناوری‌های مربوط به حفظ حریم خصوصی در آن کاملا سریع است، و این پیشرفت در حدی سریع بوده که این بررسی‌ها نمی‌تواند به خوبی آخرین وضعیت تحقیقاتی را نشان دهد و قادر به بررسی تحقیقات با یک دسته بندی کلی نیست. که از جمله می توان به موارد زیر اشاره کرد:

(۱) در مرورهای پیشین ویژگی انواع زنجیره قطعات بصورت خلاصه آمده است و به مزایا و معایب آن‌ها اشاره‌ای نشده است.
(۲) بیشتر مطالعات تنها به چند مورد مهم از شیوه‌های حفظ حریم خصوصی پرداخته است.
(۳) مطالعات مروری یا بر شیوه‌های حفظ حریم خصوصی و یا بر حملات و تهدیدات تاکید دارد.

جدا از مطالعات بالا، این مرور روشمند یک مقایسه و بررسی جامع از ویژگی‌های انواع زنجیره قطعات را ارائه می‌دهد. مزایا و معایب هر تحقیق را خلاصه کرده و در زمینه شیوه‌های حفظ حریم خصوصی زنجیره قطعات و حملات و تهدیدات منتشر شده در مجلات و کنفرانس‌های سطح بالا بررسی‌هایی انجام شده است که براساس آن می‌تواند برای ایجاد مسائل باز و ایجاد مسیرهای تحقیقاتی مهم درآینده مورد مطالعه قرار گیرد.

۲.۲ اهداف و سؤالات تحقیق

هر کار پژوهشی مروری از تعدادی سؤالات تحقیقی سرچشمه می‌گیرد. به عبارت دیگر، پژوهشگران برای پاسخ به پرسش‌های اساسی، مطالعات مربوط به یک حوزه پژوهشی را مطالعه و بررسی می‌کند. بنابراین یکی از مهم‌ترین قسمت‌های مرور روشمند، مشخص کردن سوالاتی است که در فرآیند بررسی به آن‌ها پاسخ داده شده است. در واقع این سوالات تعیین‌کننده اهداف است و روند بررسی با پاسخگویی به این موضوعات پیش خواهد رفت. در این تحقیق، هدف تجزیه و تحلیل کارهای موجود، یافتن و خلاصه کردن تحقیقات انجام شده در مورد حفظ حریم‌خصوصی و بهبود گمنامی زنجیره قطعات است. برای این منظور چهار سوال تحقیق زیر تعیین شده که به آن‌ها پاسخ داده خواهد شد:

- سوال اول: ویژگی‌های انواع مختلف زنجیره قطعات چیست؟ و مزایا و معایب هریک کدام است؟
- سوال دوم: مفهوم گمنامی، شبه گمنامی، حریم خصوصی و محرمانگی چیست و شیوه‌های حفظ حریم‌خصوصی کدام است؟
- سوال سوم: آسیب پذیری‌ها و تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟
- سوال چهارم: شیوه‌های مقابله با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟

۳.۲ برنامه‌ریزی فرآیند جست‌وجو

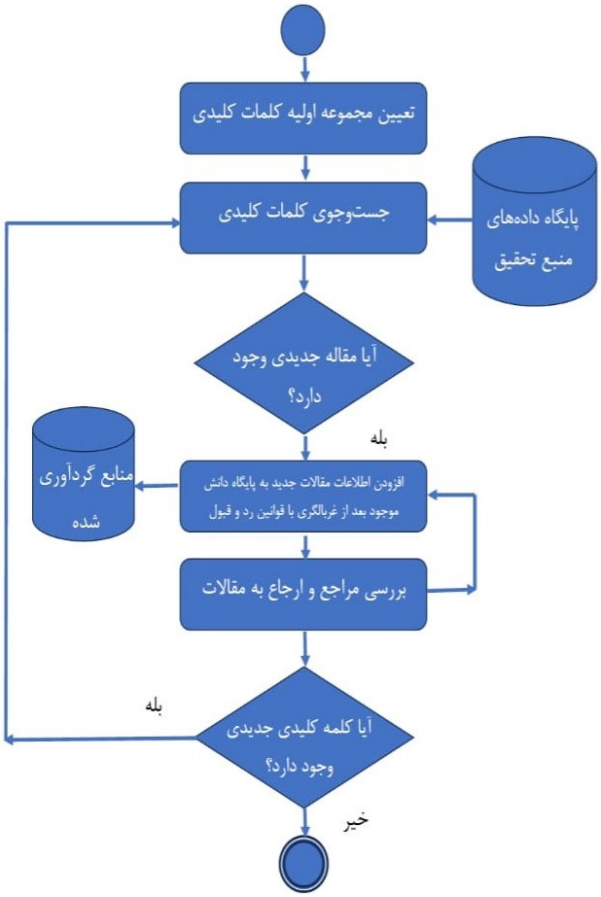
مرحله بعدی طراحی یک روندنمای انجام جست‌وجوهای مختلف در جهت یافتن کارهای پژوهشی است که تضمین می‌نماید پایگاه دانش از پوشش حداکثری از اطلاعات موجود برخوردار خواهد بود. این برنامه‌ریزی شامل تعیین تمامی قواعد و تصمیماتی است که به انجام فرآیند جست‌وجو مربوط می‌شود. این مرحله شامل سه گام تعیین استراتژی جست‌وجو ، تعیین فضای جست‌وجو و تعیین رشته جست‌وجو است.

۱.۳.۲ تعیین استراتژی جست‌وجو

برای مدیریت فرآیند جست‌وجو ، نیاز به یک استراتژی جست‌وجوی مشخص و واضح است. این اولین نیاز برای انجام جست‌وجو است. در این مقاله، نحوه جمع‌آوری و تکمیل اطلاعات در قالب یک استراتژی جست‌وجوی مطابق شکل ۱ طراحی شده و جزئیات آن در طول گام‌های مختلف جست‌وجو ارائه و توصیف می‌گردد. بعد از انجام این مراحل به کلمات کلیدی جدیدی رسیده و ابعاد مرور روشمند را برای این کلمات کلیدی تکرار کرده تا آنجا که هیچ مقاله و کلمه کلیدی جدیدی یافت نشود.

۲.۳.۲ تعیین رشته‌های جست‌وجو

در این مقاله، با توجه به بررسی همه مطالعات در زمینه حریم‌خصوصی و گمنامی زنجیره قطعات، رشته‌های جست‌وجوی پویا (به نام مجموعه کلمات کلیدی) وجود دارد. در ابتدا، جست‌وجو با استفاده از عبارت کلیدی «blockchain» انجام می‌شود و به تعداد زیادی مقالات در زمینه‌های مختلف دست پیدا شده است. مجموعه کلمات کلیدی در طول پیشرفت فرآیند جست‌وجو تکمیل می‌شود و سپس کلمات کلیدی Blockchain، Privacy، Anonymity، Security مورد جست‌وجو قرار گرفته است.



شکل ۱. استراتژی جست‌وجو در مرور روشمند

۴.۲ قوانین شمول و عدم شمول

از دیگر موارد مهم در حین افزودن اطلاعات به پایگاه دانش حوزه، وضع قوانین شمول و عدم شمول مناسب جهت پالایش کارهای پژوهشی و در ادامه شناسایی و اضافه کردن موارد با کیفیت می‌باشد. این قوانین می‌تواند برای منابع و نیز خود مقالات پژوهشی تعریف شود که در جدول ۱ نشان داده شده است.

برای این کار از پایگاه داده‌های IEEE Xplore Digital Library، ACM، ScienceDirect، Springer و Google Scholar برای جست‌وجو استفاده شده و مقالات منتشر شده به زبان انگلیسی در نظر گرفته شده است. مطالعات تکراری حذف شد، سپس نتایج از طریق قوانین شمول و عدم شمول پالایش شد.

۳ گردآوری منابع

روند جست‌وجوی روشمند انتشارات از طریق موتورهای جست‌وجوی مختلف انجام شده و سپس به انتخاب مطالعات اولیه پرداخته شده است. در مرحله اول کلمه کلیدی "Blockchain" مورد جست‌وجو قرار گرفت و به تعداد زیادی مقالات در حوزه‌های کاربردی مختلف مانند

جدول ۱. قوانین شمول و عدم شمول

قوانین شمول
مقاله باید مربوط به حفظ حریم‌خصوصی و گمنامی زنجیره قطعات باشد. (کلمات کلیدی در مراحل جست‌وجو کامل می‌شود)
پایگاه داده‌های IEEE Xplore Digital Library، ACM، ScienceDirect، Springer و Google Scholar
مقاله در مجموعه مقالات کنفرانس یا مجله معتبر منتشر شده است.
انتشار مقاله باید بین سال‌های ۲۰۱۸ تا ۲۰۲۳ باشد.

قوانین عدم شمول
مقالاتی که نسخه کامل آن‌ها در دسترس نیست.
نتایج جست‌وجوی بعد از صفحه پنجم
مقالات خاکستری یا غیر انگلیسی زبان
مقالات پژوهشی کوتاه کمتر از ۵ صفحه

اینترنت اشیاء، مراقبت‌های بهداشتی، قرارداد هوشمند، بانک‌داری و مالی، کسب و کار و صنعت و سایر حوزه‌ها دست پیدا شد. پس از آن، با خواندن عناوین، کلمات کلیدی و چکیده‌های آن‌ها، بررسی شد که یکی از چالش‌های مهم و مورد بحث در این حوزه‌ها، حریم‌خصوصی تراکنش‌ها و هویت کاربران زنجیره قطعات می‌باشد. بنابراین در مرحله دوم کلمات کلیدی "Blockchain، Privacy، Anonymity، Security" مورد جست‌وجو قرار گرفت.

برای پاسخگویی به سؤالات تحقیق، یک فراتحلیل از مطالعات انتخابی نهایی شده و فرآیند استخراج داده‌ها انجام شد. در هر مقاله، هم چکیده و هم متن کامل مطالعه و اطلاعات مربوط به حفظ حریم خصوصی و گمنامی استخراج شد. همچنین اطلاعاتی در مورد معایب موجود در هر مقاله و مطالعات آتی پیشنهادی استخراج شده است.

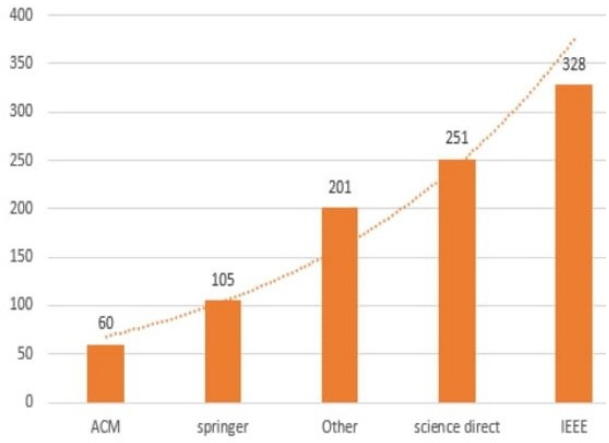
در فرآیند پالایش سه مرحله وجود دارد. در مرحله اول عناوین و کلید واژه‌های ۱۲۳۳ مقاله مورد بررسی قرار گرفت که منجر به باقی ماندن ۹۴۷ مقاله شد. مرحله دوم بعد از بررسی چکیده مقالات به منظور تعیین ارتباط آن‌ها با این تحقیق تنها ۴۰۴ مقاله مرتبط شناسایی شد. در مرحله سوم پس از مطالعه روزنامه‌ای متن کامل مقالات باقی مانده، تنها ۴۰۴ مقاله به عنوان مرتبط انتخاب شد. برای پاسخ به سؤالات پژوهش، این ۴۰۴ مقاله به‌طور کامل برای استخراج اطلاعات دقیق‌تر مطالعه شده است.

۱.۳ توزیع آماری منابع

در این بخش توزیع آماری مقالات از سه منظر سال انتشار، نشریه و انتشارات گزارش شده است.

الف) تعداد مقالات مطالعه شده در هر سال همانطور که در شکل ۲ مشاهده می‌شود، یک روند صعودی در استفاده از زنجیره قطعات در زمینه امنیت سایبری وجود دارد. اصطلاح "حریم‌خصوصی" و "گمنامی" طی چند سال گذشته به حداکثر خود رسیده است. قابل پیش‌بینی است که در آینده شاهد تعداد قابل توجهی از مطالعات تحقیقاتی در رابطه با پذیرش

شکل ۲. تعداد مقالات مطالعه شده در هر سال

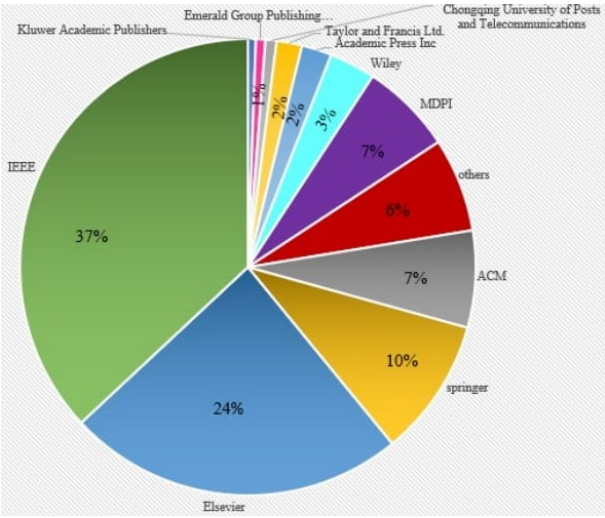


شکل ۳. تعداد مقالات مطالعه شده در هر نشریه

زنجیره قطعات در برنامه‌های کاربردی دنیای واقعی باشیم. از آنجایی که این مطالعه در ابتدای سال ۲۰۲۳ انجام شده، هنوز اطلاعات زیادی منتشر نشده است.

ب) تعداد مقالات مطالعه شده در هر نشریه همان‌طور که در شکل ۳ نشان داده شده است کلمات Blockchain، Privacy، Anonymity، Security در ۴ نشریه شامل ACM، Springer، Science direct، IEEE جست‌وجو شد و Other هم شامل مقالاتی است که کلمه مورد جست‌وجو در Google scholar انجام شده است.

ج) تعداد مقالات مطالعه شده در هر انتشارات همان‌طور که می‌دانید نشریات در انتشارات چاپ می‌شود و ۴ نشریه‌ای که در بخش ب وجود داشت، در این بخش انتشارات مربوط به هر کدام مورد جست‌وجو قرار گرفته است. شکل ۴ تعداد مقالات را نشان می‌دهد.



شکل ۴. تعداد مقالات مطالعه شده در هر انتشارات

۲.۳ توجه جامعه علمی به موضوعات مختلف

در ادبیات بررسی شده، حوزه‌ها یا زمینه‌های مختلفی یافت شد. که در آن فن‌آوری زنجیره قطعات برای پاسخ به تغییرات موقعیتی و چالش‌های جدید ناشی از پیشرفت مستمر و همچنین نیازهای جدید در مورد حفظ حریم‌خصوصی و امنیت اطلاعات، اجرا می‌شود. توزیع آماری زمینه‌های کاری در شکل ۵ آمده است که در ادامه تشریح می‌شود.

زمینه سلامت: از آنجایی که برای تبادل موفقیت آمیز داده در مقیاس بزرگ، چالش‌های جدید، الزامات امنیتی و حریم خصوصی[۳۲] باید مورد توجه قرار گیرد. بنابراین اطلاعات بهداشتی باید از حریم‌خصوصی کافی برخوردار باشد. هنگامی که زنجیره قطعات برای ذخیره داده‌های سلامت استفاده می‌شود، یک کلید عمومی به هویت فرد مرتبط می‌شود تا از طریق یک نام مستعار از هویت واقعی او محافظت شود. یک مشکل جدی این است که خطر شناسایی مجدد از طریق داده‌های عمومی در زنجیره قطعات وجود دارد که باعث می‌شود هویت واقعی فرد شناخته شود. علاوه بر این، این احتمال وجود دارد که سوابق مختلف ممکن است برای متخصصان مختلف سلامت در دسترس باشد، که دستیابی به آن از طریق زنجیره قطعات دشوار است و باید پیاده‌سازی شود.

اینترنت اشیا: فن‌آوری زنجیره قطعات با کارایی و مقیاس پذیری خود، اینترنت اشیاء [۳۶، ۳۸] را متحول کرده است و سعی می‌کند راه‌حلی را برای نحوه ارتباط دستگاه‌های مختلف مداخله کننده ارائه دهد و محیطی قابل اطمینان و امن و همچنین روشی قابل اعتماد برای انتقال اطلاعات بین دستگاه‌ها را ایجاد کند. با این حال، محدودیت‌های حل نشده‌ای برای بهبود مقیاس‌پذیری دستگاه‌های اینترنت اشیا وجود دارد [۳۹]. این از دیدگاه جدیدی از دفتر کل توزیع شده تحت پروژه IoTA مورد بررسی قرار گرفته است. یکی از مهم‌ترین مشکلاتی که باید حل شود، جعل هویت دستگاه، احراز هویت نادرست یا غیرقابل اعتماد بودن است که می‌تواند در تبادل داده رخ دهد. این می‌تواند یک نقض امنیتی باشد که پیش نیاز

اجرای حریم‌خصوصی است.

داده بزرگ: رویکرد اتخاذ شده در این زمینه [۳۴، ۴۰، ۴۱] با استفاده از فن‌آوری زنجیره قطعات، سطح محرمانه بودن اطلاعات به اشتراک گذاشته شده را افزایش می‌دهد. ذخیره سازی مقادیر زیادی از اطلاعات و ترکیب آن با فن‌آوری زنجیره قطعات، نقطه ضعف ظرفیتی است که می‌تواند هر تراکنش را پشتیبانی کند. بنابراین ذخیره‌سازی خارج از زنجیره به عنوان یک راه‌حل ظاهر می‌شود که به نوبه خود مسائلی مانند امنیت و حفظ حریم خصوصی داده‌ها را ایجاد می‌کند.

ذخیره‌سازی اطلاعات: نویسندگان در [۴۲] با انتخاب ویژگی تغییرناپذیری ارائه شده توسط فن‌آوری زنجیره قطعات، مقاومت در برابر اصلاح یا حذف داده‌های ذخیره شده را تضمین می‌کند و هدف آن افزایش سطح حریم‌خصوصی است. در آینده این امکان را برای یک زنجیره قطعات ایجاد می‌کند که می‌تواند تراکنش‌ها را به روشی ایمن اصلاح یا حذف کند و گمنامی هویت‌های درگیر را حفظ کند. برای این کار یک حافظه بهینه و انعطاف پذیر در زنجیره قطعات پیشنهاد می‌کند.

شبکه وسایل نقلیه موقت: از آنجایی که تمرکز بر اعتماد و حریم‌خصوصی است، وسایل نقلیه به عنوان گره در یک شبکه استفاده می‌شود [۴۳]. اما مسائل باز باقی می‌ماند و جلوگیری از ارسال پیام‌های نادرست توسط وسایل نقلیه و در عین حال حفظ حریم‌خصوصی از انواع مختلف حملات احتمالی بسیار مهم است. محققان در [۴۴]، توجه خود را بر روی ارتباط بین وسایل نقلیه و دستگاه‌های محیطی، شهر هوشمند، اینترنت وسایل نقلیه (IoV) متمرکز می‌کند. ارتباطات باید گمنام باشد تا حریم‌خصوصی وسایل نقلیه حفظ شود، اما از سوی دیگر، گمنامی برای اطمینان از اینکه مقامات قادر به دریافت اطلاعات از آن‌ها در صورت بروز اختلاف هست، مورد نیاز است. برای رسیدن به این هدف، یک سیستم گمنام معروف مبتنی بر زنجیره قطعات (BARS) پیشنهاد شده است که در آن یک مرجع صدور گواهی (CA)، مقام اجرای قانون (LEA)، واحد کنار جاده (RSU) و همچنین وسایل نقلیه به عنوان اجزای مدل تعریف می‌شود. در این مدل، CA و LEA مسئول راه‌اندازی سیستم، به‌روزرسانی گواهی‌ها و باطل کردن کلیدهای عمومی است. در این حالت کلیدهای عمومی به عنوان یک نام مستعار برای حفظ هویت وسایل نقلیه عمل می‌کند.

کسب و کار: در این زمینه، چندین شرکت پیاده‌سازی فن‌آوری زنجیره قطعات [۴۵] را به عنوان راه‌حلی برای مشکلاتی مانند قابلیت ردیابی، شفافیت، حسابرسی و سایر کاربردهای احتمالی که هنوز مورد بررسی قرار نگرفته، انتخاب کرده است. استفاده از زنجیره قطعات در محیط کسب و کار هنوز در مراحل اولیه است و نیاز به بررسی کامل دارد. قراردادهای هوشمند، همراه با پروتکل‌های اجماع، راه جدیدی برای توسعه فرآیندهای تجاری ارائه می‌دهد.

صنعت 4.0: در زمینه صنعت [۳۹، ۴۶]، زنجیره قطعات به عنوان راهی برای ارائه تضمین حریم‌خصوصی و امنیت، احراز هویت گمنام دستگاه‌ها، ظرفیت ممیزی فرآیندهای صنعتی و محرمانه بودن داده‌های پردازش شده انتخاب شده است. یکی از ویژگی‌های قابل توجه فن‌آوری زنجیره قطعات در این حوزه، امکان مقیاس پذیری آن است. در فرآیندهای درگیر در صنعت، طیف گسترده‌ای از دستگاه‌ها و حسگرها با جمع‌آوری انواع داده‌ها مانند دما، فاصله، اندازه، رطوبت، درخشندگی یا حرکت تعامل دارد و ذخیره و پردازش ایمن آن‌ها را ضروری می‌سازد. بین سنسورها و دستگاه‌ها ارتباطی وجود دارد که باید ردیابی و در صورت لزوم ممیزی شود.

ارزهای رمزنگاری شده: ا گرچه در این تحقیق از ورود به ارزهای رمزنگاری مختلف که توسط فن‌آوری زنجیره قطعات پشتیبانی می‌شود، اجتناب شده است، اما قابل توجه است که یکی از کاربردهای مهم این فن‌آوری، مدیریت ارزهای دیجیتال است. در حال حاضر انواع مختلفی از ارزهای رمزنگاری شده وجود دارد و باید توجه داشت که پروژه‌های خاصی مانند ALASTRIA [۴۷] وجود دارد که هدف آن‌ها ادغام بانک‌های مختلف و ارائه قابلیت همکاری بانکی از طریق زنجیره قطعات است. از سوی دیگر، ETHEREUM [۴۸] کاربردهای دیگری را برای فن‌آوری زنجیره قطعات ارائه می‌کند. فن‌آوری ارزهای دیجیتال برای اهداف دیگری مانند قراردادهای هوشمند [۴۰] و ارائه حریم‌خصوصی و گمنامی استفاده می‌شود.

۴ پاسخ به سوالات تحقیق

زنجیره قطعات یک ساختار داده پیوندی مبتنی بر درهم‌ساز است که توسط هر گره در شبکه همتا به همتا نگهداری می‌شود. با توجه به ماهیت آن، زنجیره قطعات می‌تواند امنیت، حریم خصوصی، عدم تمرکز، گمنامی و تغییرناپذیری را فراهم کند. پس از بررسی ادبیات انتخاب شده برای استخراج اطلاعات، به سوالات مختلف مطرح شده در این مرور پاسخ داده می‌شود.

۱.۴ پاسخ به سوال اول تحقیق

ویژگی‌های انواع زنجیره قطعات چیست؟ مزایا و معایب هریک کدام است؟

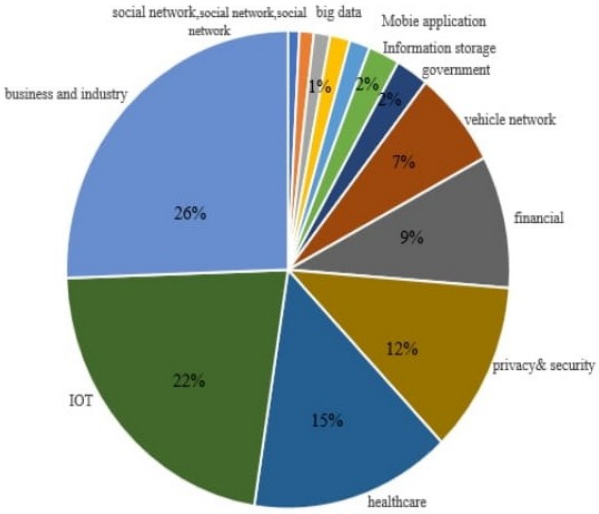
زنجیره قطعات به سه دسته عمومی (بدون مجوز)، خصوصی (مجوزدار) و کنسرسیوم طبقه‌بندی می‌شود که ویژگی‌های آن‌ها در جدول ۲ مقایسه شده و در جدول‌های ۳ و ۴ به ترتیب مزایا و معایب آن‌ها آمده است.

۲.۴ پاسخ به سوال دوم تحقیق

مفهوم گمنامی، شبه گمنامی، حریم خصوصی و محرمانگی را تعریف کنید و شیوه‌های حفظ حریم خصوصی کدام است؟

توجه به مفهوم کلمات حریم خصوصی، گمنامی و شبه گمنامی و رابطه بین آنها بسیار مهم و ضروری می‌باشد. اگرچه در برخی از مقالات تعریف صریحی از هریک از این مفاهیم امنیتی ارائه شده است اما در برخی از

جدول ۲. مقایسه طبقه‌بندی انواع زنجیره قطعات



جدول ۳. مزایای انواع زنجیره قطعات

مراجع	پارامترها	زنجیره قطعات عمومی	زنجیره قطعات کنسرسیوم	زنجیره قطعات خصوصی
[۱,۳۷,۶۰,۶۱,۷۵]	توان عملیاتی	پایین	بالا	بالا
	سرعت	پایین	پایین	بالا
	ظرفیت تراکنش	پایین	بالا	بالا
	سرعت پردازش تراکنش	آهسته	سریع	
	مقیاس پذیری	پایین	بالا	بالا
[۱,۳۷,۶۰,۶۱,۷۵]	احراز هویت	لازم نیست	لازم است	لازم است
	فرآیند اجماع	بدون مجوز	مجوزدار	مجوزدار
	شیوه‌های اجماع	PoW, PoS	BFT	BFT
	مرجع اعتماد (TA)	۰	۱≤	۱
[۱,۳۷,۶۰,۶۱,۶۲,۷۵]	نوع مدیریت(شبکه)	غیرمتمرکز	تاحدودی متمرکز	کاملاً متمرکز
	اندازه شبکه	عظیم	محدود	محدود
	همگام سازی شبکه	ناهمزمان	کاملاً همزمان	کاملاً همزمان
	اتصال به شبکه	متصل جزئی	کاملا متصل	کاملا متصل
	مشارکت کنندگان در اجماع (اعضای‌اجماع)	اجماع عمومی	زیر مجموعه‌ای از اعضا	دارای مالک واحد
	دارایی	دارایی بومی	هر دارایی	هر دارایی
[۱,۶۰,۶۱,۷۵]	دستکاری	تقریبا غیرممکن	قابل دستکاری	قابل دستکاری
	امنیت	اثبات کار	اثبات سهام	پیش تایید
	هویت	گمنام	شبه گمنام	قابل شناسایی برای شرکت کنندگان
	احراز هویت بلاک	تمام ماینرها	گره‌های انتخاب شده	سازمان خاص
	شفافیت	باز	باز / بسته	باز / بسته
[۱,۶۰,۶۱,۷۵]	قابل خواندن	عمومی	مجوز سازمان	مجوز سازمان
	دسترسی‌خواندن/نوشتن	همه	چندین سازمان منتخب	یک سازمان واحد
	تعداد خوانندگان	بالا	بالا	بالا
	تعداد نویسندگان	بالا	پایین	پایین
	تعداد نویسندگان غیرقابل اعتماد	بالا	پایین	پایین

مقالات این مفاهیم با یکدیگر خلط شده است بطوریکه یکی وابسته به دیگری تعریف شده است. در این بخش بعد از بیان تعاریف مختلف، شیوه های ارائه آنها بیان و با هم مقایسه می شود.

۱.۲.۴ تعاریف گمنامی

گمنامی در مقالات به شکل های مختلف تعریف شده است، که در ادامه برخی از آنها را می آوریم:

هر موجودی در زنجیره قطعات در یک آدرس تولید شده با دیگران ارتباط برقرار می‌کند. گمنامی به این معنی است که این آدرس‌ها هویت

جدول ۴. معایب انواع زنجیره قطعات

	مزایا	نوع زنجیره قطعات
امکان دسترسی	امکان دسترسی همه به اینترنت	عمومی [۷۵-۶۱]
	دسترس بودن اطلاعات تراکنش و تأیید آن به صورت عمومی	عمومی [۷۱,۷۵, ۶۸,۶۹, ۶۴,۶۵,۶۶, ۶۲,۶۱,۵۳,۱]
	عدم دسترسی همه به اطلاعات تراکنش	خصوصی [۷۰,۶۶,۶۴,۶۲,۶۱,۱]
	برای دسترسی کاربران نیازمند شناسایی به صورت دیجیتالی	خصوصی [۶۲]
	فراهم کردن دسترسی بهتری نسبت به دسترسی خصوصی	کنسرسیوم [۶۸]
اجماع	امکان شرکت کاربران در فرایند اجماع	عمومی [۷۲, ۶۶, ۶۵, ۳۷, ۵۳, ۱]
	دارای سرعت اجماع آهسته	عمومی [۳۷]
	دارای سرعت اجماع سریع	خصوصی [۳۷]
	دارای سرعت اجماع اندکی سریع	کنسرسیوم [۳۷]
	روند اجماع در مقایسه با زنجیره‌های قطعات خصوصی نسبتا کند،اما سریعتر از زنجیره‌های قطعات عمومی	کنسرسیوم [۶۶]
	تحمل خطا عملی برای بهبود کارایی اجماع	کنسرسیوم [۷۳]
	اجرای مکانیسم اجماع کنسرسیوم زنجیره‌قطعات توسط گره‌های خاصی	کنسرسیوم [۷۴, ۷۰, ۵۳, ۱]
	تحمل خطا عملی برای بهبود کارایی اجماع	کنسرسیوم [۷۳]
	پردازش سریعتر	کنسرسیوم [۶۲]
	قادر ساختن سازمان ها برای یافتن راه‌حل‌هایی و صرفه جویی در زمان و هزینه توسعه	کنسرسیوم [۶۲]
مرجع مرکزی	کاملا غیرمتمرکز	عمومی [۷۵,۷۴,۷۳,۶۸,۶۶,۶۲,۵۳]
	عدم نیاز به کنترل کننده داده ای (مرجع مرکزی)	عمومی [۷۵,۶۸,۶۳]
	امکان کنترل به صورت توزیع شده بین اعضای ممتاز و گره های مشترک	کنسرسیوم [۶۲,۶۱]
امنیت و شفافیت	امنیت بالایی با استفاده از رمزنگاری و پروتکل اجماع	عمومی [۷۴,۷۲,۷۰,۶۳,۵۳]
	شفاف بودن کامل تراکنش (سطح شفافیت بالا)	عمومی [۷۲,۷۳,۶۹,۶۸, ۵۳]
	محافظت از دستکاری محتویات قطعه‌ها با درهم‌سازها و اجماع غیرمتمرکز	عمومی [۷۰,۶۶]
	امکان گمنامی تعداد زیادی از گره‌ها برای محافظت از حریم خصوصی	عمومی [۶۶]
	پشتیبانی از تغییر ناپذیری و یکپارچگی اطلاعات	عمومی [۶۸]
	استفاده شرکت‌کنندگان از گمنامی یا شبه‌گمنامی	عمومی [۷۲,۷۰]
	امنیت بالا	خصوصی [۶۸,۶۵,۶۲,۶۱]
	نظارت مجوزهای نوشتن بلاک‌ها توسط مقامات خاصی	خصوصی [۷۵,۷۳,۷۱,۶۹,۶۸,۶۶,۶۵]
	امکان محافظت از دستکاری با درهم‌سازها و اجماع شرکت‌کنندگان	خصوصی [۶۶]
	ایجاد سطح بیشتری از حریم خصوصی با فراهم نمودن مجوزهای خواندن محدود	خصوصی [۶۹, ۶۸, ۶۵, ۵۳]
	فراهم کردن پلت فرم قابل ردیابی و تغییر ناپذیر برای جلوگیری از حملات داخلی و خارجی	خصوصی [۷۳]
	کارایی و امنیت بیشتر	کنسرسیوم [۶۶,۶۲]
	فقط شرکت کنندگان دعوت شده و مورد اعتماد مجاز به پیوستن و حفظ شبکه هستند	کنسرسیوم [۷۵,۷۳,۷۲,۷۱,۶۶,۳۷]
	حق خواندن می‌توانند عمومی یا محدود به گره‌های انتخاب شده در شبکه باشند	کنسرسیوم [۷۴,۶۸,۵۳]
	حریم خصوصی بهتری نسبت به عمومی دارد	کنسرسیوم [۶۸]
	به سیستم‌ها اجازه می‌دهد تا با شفافیت بدون نیاز به کاهش حریم خصوصی سیستم عمل کنند	کنسرسیوم [۶۸]

واقعی کاربران درگیر را فاش نکند [۷۶].

گمنامی فرستند در صورتی حاصل می‌شود که دشمن نتواند تعیین کند که فرستندگان صادق وجوه را برای چه کسی ارسال می‌کند، با این فرض که سپرده‌های فرستنده صادق غیرقابل تشخیص است. گمنامی گیرنده در صورتی حاصل می‌شود که تراکنش‌های برداشت گیرندگان صادق غیرقابل تشخیص باشد [۸۲].

گمنامی اشاره به عدم شناسایی هویت واقعی یک کاربر دارد. در حالت گمنامی، کاربران می‌تواند بدون افشای نام، آدرس یا هر گونه اطلاعات شناسایی شخصی، اقدام به تراکنش کند. گمنامی معمولاً با استفاده از شیوه‌های خاصی مانند پروتکل‌های زیربنایی که هویت را پنهان می‌کند، فراهم می‌شود [۶۱].

مفهوم کلیدی گمنامی این است که یک فرد غیرقابل شناسایی، غیرقابل دسترس یا غیرقابل ردیابی باقی می‌ماند [۶۴]. گمنامی اغلب با فعالیت‌های آنلاین مرتبط است که در آن افراد ممکن است بدون افشای هویت واقعی خود در بحث‌ها، انجمن‌ها یا تراکنش‌ها شرکت کند.

گمنامی اغلب یک انتخاب عمدی توسط افراد برای محافظت از هویت خود یا ابراز عقاید بدون ترس از مجازات است.

در زمینه زنجیره قطعات، گمنامی را می توان با استفاده از آدرس‌های مستعار، که رشته‌های منحصر به فردی از کاراکترها نشان دهنده هویت کاربر در زنجیره قطعات است، به دست آورد. این آدرس‌ها از طریق یک فرآیند رمزنگاری ایجاد می‌شود و مستقیماً به هویت دنیای واقعی شخص مرتبط نیست. در نتیجه، ردیابی فعالیت‌های یک کاربر خاص در زنجیره قطعات دشوار است [۲۵۵].

برای دستیابی به اعتبار یک شیوه گمنام سازی، باید از تکنیک تک هویتی، پیوند داده‌های مرتبط و استنتاج اطلاعات مربوط به یک هویت معین اجتناب شود [۲۵۳].

۲.۲.۴ تعاریف شبه گمنامی (نام مستعار)

شبه گمنامی به حالتی از هویت پنهان اشاره دارد. آدرس‌ها در زنجیره قطعات، درهم سازهای کلیدهای عمومی یک گره (کاربر) در شبکه است. کاربران می‌تواند با استفاده از درهم ساز کلید عمومی خود به عنوان شبه هویت با سیستم تعامل داشته باشد بدون اینکه نام واقعی خود را فاش کند. بنابراین، آدرسی که کاربر استفاده می‌کند را می‌توان به عنوان یک شبه هویت مشاهده کرد. علاوه بر این، کاربران می‌تواند هر تعداد جفت کلید (آدرس های چندگانه) را که می‌خواهد تولید کند، به روشی مشابه که یک شخص می‌تواند چندین حساب بانکی را به دلخواه خود ایجاد کند. اگرچه شبه گمنامی می‌تواند با استفاده از کلیدهای عمومی به شکل ضعیفی از گمنامی دست یابد، اما هنوز خطراتی برای افشای اطلاعات هویتی کاربران وجود دارد [۳۸].

منظور از شبه گمنامی این است که در آن فرستنده و گیرنده مشخص نیست ولی آدرس مبدا و مقصد تراکنش مشخص است و مواردی از قبیل کد ثبتی تراکنش، ID درهم ساز آن تراکنش و مسیر ارتباطی در شبکه زنجیره قطعات ثبت می‌شود که از کدام آدرس کیف پول یعنی آدرس خروجی به کدام آدرس ورودی رفته است. چون آن تراکنش دیده می‌شود به همین دلیل گمنامی کامل را ایجاد نمی‌کند و از آنجایی که فقط فرستنده و گیرنده مشخص نیست، شبه گمنامی به وجود می‌آید.

با این حال، این گمنامی کامل برای کاربران زنجیره قطعات فراهم نمی‌کند زیرا هر تراکنش با آدرس فرستنده و گیرنده در دفتر ثبت می‌شود و توسط هر کسی که از آدرس‌های مرتبط فرستنده و گیرنده آن استفاده می‌کند، آزادانه قابل ردیابی است. بنابراین، هر کسی می‌تواند تراکنش کاربر را با سایر تراکنش‌های مربوط به حساب‌های او با یک تحلیل آماری ساده از آدرس‌های مورد استفاده در تراکنش‌ها مرتبط کند [۸۴].

شبه گمنامی در شبکه‌های زنجیره قطعات به حالتی اشاره دارد که در آن هویت کاربران به طور کامل گمنام نیست، اما به گونه‌ای طراحی شده است که مشخصات و جزئیات هویتی آن‌ها به راحتی شناسایی نمی‌شود. این نوع گمنامی در زنجیره قطعات عمومی معمولاً به وسیله استفاده از آدرس‌های عمومی و کلیدهای رمزنگاری شده حاصل می‌شود. در زیر به برخی از ویژگی‌ها و ابعاد این مفهوم پرداخته می‌شود:

(۱) در اکثر زنجیره قطعات، کاربران برای ارسال یا دریافت ارز دیجیتال نیاز به استفاده از آدرس‌های عمومی دارد. اگر اطلاعات دیگری در دسترس باشد، این آدرس‌ها می‌تواند به طور غیرمستقیم به هویت واقعی کاربر متصل شود.
(۲) با تجزیه و تحلیل اطلاعات موجود در زنجیره قطعات، می‌توان تراکنش‌ها را ردیابی کرد و به تدریج به هویت واقعی کاربران پی برد. این می‌تواند با ترکیب اطلاعات عمومی و داده‌های موجود در زنجیره قطعات صورت گیرد.
(۳) در حالی که اطلاعات کاربر به طور کامل گمنام نیست، اما کاربران می‌تواند در شرایطی مشخص بدون افشای هویت خود اقدام کند. این ویژگی به کاربران اجازه می‌دهد تا از حریم خصوصی نسبی برخوردار باشد.

در اغلب زنجیره قطعات، کاربران به‌طور مستقیم با آدرس‌های عمومی خود شناسایی می‌شود. این بدان معناست که در حالی که هویت واقعی کاربر در ابتدا ناشناخته است، با تحلیل داده‌ها و تراکنش‌ها می‌توان به هویت واقعی کاربران پی برد. این موضوع به «شبه گمنامی» معروف است [۷۱].

نام مستعار تقریباً حالتی از گمنامی است که در آن کاربر یک شناسه ثابت دارد که بجای نام واقعی او یک نام مستعار است. این به افراد اجازه می‌دهد تا در هنگام استفاده از یک شناسه ثابت اما نه لزوما قابل ردیابی، در فعالیت‌ها شرکت کند. یک مفهوم مرتبط، نام مستعار است، که یک روش مدیریت داده و شناسایی هویت است که توسط آن فیلدهای اطلاعات شناسایی شخصی در یک رکورد داده با یک یا چند شناسه مصنوعی یا نام مستعار جایگزین می‌شود.

- نام مستعار شامل استفاده از یک نام مستعار یا شناسه ثابت است که به افراد این امکان را می‌دهد تا حضور یا شهرت قابل تشخیصی را در طول زمان ایجاد کند.
- نام مستعار نیز می‌تواند آزادی بیان را ارتقا دهد، زیرا افراد ممکن است احساس راحتی بیشتری داشته باشد بدون اینکه هویت واقعی

خود را آشکار کند.

- در زمینه‌های قانونی، مقامات ممکن است ابزاری برای ردیابی هویت پشت نام مستعار تحت شرایط خاص داشته باشد.
- با نام مستعار، می‌توان یک شخصیت خیالی برای نشان دادن خود ساخت و از آن استفاده کرد و این امکان را می‌دهد که بدون افشای هویت واقعی خود با دیگران تعامل داشت. در دنیای زنجیره قطعات، این مفهوم اهمیت بیشتری پیدا می‌کند، زیرا نام مستعار می‌تواند برای محافظت از هویت مورد استفاده قرار گیرد و در عین حال این امکان را می‌دهد که تراکنش‌ها را انجام داد و در فعالیت‌های دیگر روی زنجیره قطعات شرکت کرد. با استفاده از یک هویت مستعار منحصر به فرد برای نشان دادن خود، می‌توان اطلاعات شخصی را فاش نشده نگه داشت.
- قابل توجه است که در حالی که نام مستعار می‌تواند درجه بالایی از حریم خصوصی را ارائه دهد اما با گمنامی یکسان نیست. همه تراکنش‌هایی که با هویت مستعار انجام می‌شود همچنان می‌تواند به آن هویت مرتبط شود. در نتیجه، گمنامی نسبت به نام مستعار نسخه قدرتمندتری از حریم خصوصی است [۲۵۷].

۳.۲.۴ تعاریف حریم خصوصی

حریم خصوصی به معنای حفاظت از اطلاعات شخصی و معاملاتی کاربران است. در یک شبکه زنجیره قطعات، حریم خصوصی به این معناست که کاربران بتواند کنترل کند که چه اطلاعاتی را به اشتراک بگذارد و چه اطلاعاتی را مخفی نگه دارد. به عنوان مثال، در برخی زنجیره قطعات، اطلاعات مربوط به تراکنش‌ها به صورت رمزگذاری شده یا به صورت خصوصی انجام می‌شود [۶۱].

حریم خصوصی در زنجیره قطعات به بررسی چگونگی محافظت از اطلاعات شخصی و تراکنش‌های کاربران در یک شبکه غیرمتمرکز می‌پردازد. در حالی که زنجیره قطعات عمومی (که در آن‌ها اطلاعات به صورت شفاف و در دسترس برای همه است) می‌تواند گمنامی را فراهم کند، حریم خصوصی به معنای محافظت از هویت و جزئیات تراکنش‌های کاربران است.

حریم خصوصی دربرگیرنده ظرفیت یک فرد یا یک گروه برای محافظت از خود یا اطلاعات است. این حوزه از حریم خصوصی، زمینه مشترکی با امنیت دارد، که شامل اطمینان از استفاده مناسب و حفاظت از اطلاعات است [۶۲].

حریم خصوصی تراکنش در زنجیره قطعات به معنای حفاظت از اطلاعات شخصی و جزئیات تراکنش‌ها است. به عبارت دیگر، حریم خصوصی به این موضوع اشاره دارد که اطلاعات درباره فرستنده، گیرنده و مقدار تراکنش به گونه‌ای حفظ شود که برای عموم قابل مشاهده نباشد. اما باید توجه داشت که مفهوم حریم خصوصی با مفهوم محرمانگی متفاوت است. محرمانگی به معنای مخفی نگه‌داشتن اطلاعات از تصمیم‌گیرندگان یا افراد غیرمجاز است، در حالی که حریم خصوصی عمدتاً به حفاظت از اطلاعات شخصی مربوط می‌شود. در زنجیره قطعات عمومی اطلاعات تراکنش‌ها در دسترس عموم قرار دارد، به این معنی که هرکسی می‌تواند تاریخچه تراکنش‌ها را مشاهده کند. اما آدرس‌های فرستنده و گیرنده گمنام است، مگر اینکه این آدرس‌ها به هویت واقعی افرادی مرتبط شود [۲۵۷].

۴.۲.۴ رابطه بین گمنامی و حریم خصوصی

گمنامی و حریم خصوصی دو مفهومی است که گفتن تفاوت بین آن‌ها ممکن است کمی دشوار باشد، حریم خصوصی متن را پنهان می‌کند و گمنامی به معنای پنهان کردن صاحب آن است. در زندگی روزمره، حریم خصوصی کاربر بیشتر از گمنامی جستجو می‌شود، زیرا داده‌های شخصی برای استفاده مناسب باید محافظت شود. در تراکنش‌های آنلاین، کاربران معمولاً تمایل دارد که اطلاعات حساب و تراکنش خود را حداقل نمایش دهد. بنابراین، امنیت، محرمانگی، و حفظ حریم خصوصی در این تراکنش‌ها بسیار مهم است و باید به دقت رعایت شود. گمنامی و حفظ حریم خصوصی معمولاً هزینه دارد. از یک طرف، به طور کلی، سیستم‌هایی که هدفشان گمنامی و حفظ حریم خصوصی است، به منابع بیشتری در فضا، زمان یا قدرت محاسباتی نیاز دارد، زیرا کار اضافی انجام می‌شود. از طرف دیگر، کاربران برای گمنام ماندن و خصوصی شدن نیاز به پرداخت بیشتر دارد [۸۱].

یک سیستم مبتنی بر زنجیره قطعات در صورتی از قابلیت گمنامی پشتیبانی می‌کند که بتواند حریم‌خصوصی هویت و حریم خصوصی تراکنش را فراهم کرده و در عین حال، امکان تأیید با هر استخراج کننده احتمالی مورد نیاز برای بروز رسانی زنجیره قطعات باشد [۷۹].

- حریم خصوصی هویت به این معناست: (الف) نباید هیچ ارتباطی بین هویت‌های رمزنگاری و هویت دنیای واقعی کاربر برقرار باشد. (ب) نباید هیچ ارتباطی بین فرستنده و گیرندهٔ یک تراکنش وجود داشته باشد (ج) نباید هیچ تراکنشی بین دو تراکنش از یک کاربر وجود داشته باشد.
- حریم‌خصوصی تراکنش به این معناست که محتوای تراکنش را باید تنها در دسترس افرادی قرار داد که در تراکنش شرکت دارد. و نباید در دسترس سایر اعضای زنجیره قطعات قرار گیرد.

همان طور که در مطالعهٔ [۷۰] شرح داده شد، گمنامی به این معناست که فرد در بین مجموعه‌ای از افراد (مجموعهٔ گمنام) قابل شناسایی نباشد. در زنجیره قطعات گمنامی به وضعیتی نسبت داده می‌شود که در آن دشمن نتواند یک فرد خاص را از یک مجموعه هویت‌های واقعی تشخیص دهد که اندازهٔ آن بستگی به روش حفاظت از حریم خصوصی دارد. گمنامی یک شرط اساسی برای حفاظت از حریم خصوصی هویت است. گمنامی در شبکه زنجیره قطعات به معنای حفظ حریم خصوصی و عدم شناسایی هویت کاربران در فرآیندهای تراکنش و تعاملات در این شبکه‌ها است. در حالی که زنجیره قطعات به‌طور ذاتی شفاف است و همه تراکنش‌ها بر روی آن قابل مشاهده است. برخی از پروژه‌ها و پروتکل‌ها راه‌کارهایی را برای دستیابی به گمنامی ارائه می‌دهد [۶۲].

حریم خصوصی مربوط به اشتراک گذاری کنترل شده اطلاعات است و می‌تواند در یک طیف وجود داشته باشد و سطوح مختلف افشا را امکان پذیر می‌کند. از سوی دیگر، گمنامی نشان دهنده انتهای شدید طیف حریم خصوصی است، جایی که هیچ اطلاعات هویتی فاش نمی‌شود و فرد کاملاً پنهان می‌ماند. گمنامی و حریم خصوصی چالش‌های موروثی در سیستم زنجیره قطعات است. گمنامی به این معنی است که فرستنده اصلی بی نام باقی می‌ماند. از سوی دیگر، حریم خصوصی بیشتر به تراکنش و محتوای پیام اشاره دارد که با چالش دشمنانی که سیستم را هک می‌کند، روبرو می‌شود [۲۵۵].

۵.۲.۴ شیوه‌های ایجاد گمنامی و حفظ حریم خصوصی

فناوری‌های مختلفی مانند Zero-Knowledge Proofs می‌تواند به ایجاد حریم خصوصی و گمنامی در زنجیره قطعات کمک کند. این شیوه‌ها به کاربران این امکان را می‌دهد بدون اینکه اطلاعات خاصی را افشا کند، اطلاعات را تأیید کند.

در برخی موارد، کاربران ممکن است بخواهد که حریم خصوصی بیشتری داشته باشد اما هویت خود را افشا کند، یا برعکس. به عنوان مثال، یک کاربر ممکن است بخواهد اطلاعات مالی خود را مخفی کند اما هویت خود را در یک قرارداد هوشمند افشا کند. به طور کلی، حریم خصوصی و گمنامی در زنجیره قطعات نیازمند تعادل است تا کاربران بتواند به طور امن و راحت از این فناوری استفاده کند [۶۱].

روش‌های حفظ حریم خصوصی: برای افزایش محرمانگی در زنجیره قطعات، شیوه‌ها و پروتکل‌های مختلفی توسعه یافته است:

- ترکیب کننده‌ها (Mixers): این ابزارها تراکنش‌ها را ترکیب می‌کند تا ردیابی منابع و مقاصد آن‌ها دشوار شود.
- زنجیره‌های حریم خصوصی: برخی از زنجیره قطعات مانند مونرو و زکی‌کش (Zcash) به‌طور خاص برای حفظ حریم خصوصی طراحی شده است. این زنجیره‌ها از شیوه‌های رمزنگاری پیشرفته برای پنهان‌سازی اطلاعات تراکنش‌ها و هویت کاربران استفاده می‌کند.
- آدرس‌های یک‌بار مصرف: استفاده از آدرس‌های جدید برای هر تراکنش می‌تواند به کاهش ریسک ردیابی کاربر کمک کند.

در شکل ۶ آخرین مقالات مورد توجه به شیوه‌های مختلف امنیت و حفظ حریم‌خصوصی و گمنامی هویت و تراکنش آورده شده است. همان‌طور که در شکل ۶ مشاهده می‌شود، روش‌های ایجاد حریم‌خصوصی هویت کاربر شامل رویکردهای به هم زدن آدرس صریح، به هم زدن آدرس پنهان، به هم زدن مالکیت، رمزگذاری و تجزیه داده و روش‌های ایجاد حریم‌خصوصی تراکنش‌ها به هم زدن آدرس پنهان، به هم زدن مالکیت، رمزگذاری و تجزیه داده می‌باشد. روش‌های تأمین حریم خصوصی هویت سرویس‌های ترکیب کننده، امضای گروهی، امضای کور (پنهان شده) و اثبات با صفر دانش غیرتعاملی است. در زنجیره قطعات سرویس‌های ترکیب‌کننده به دو نوع ترکیب‌کننده متمرکز و ترکیب‌کننده غیرمتمرکز تقسیم می‌شود، که پروتکل‌های زیادی براساس سرویس‌های ترکیب‌کننده موجود است. امضای گروهی شامل امضای حلقه‌ای و امضای ترکیبی است. اثبات با صفر دانش هم به دو بخش اثبات صفر-دانش تعاملی و اثبات صفر-دانش غیرتعاملی تقسیم می‌گردد. روش‌های تأمین تراکنش اثبات صفر-دانش، تعهدات هم شکل، ذخیره‌سازی خارج از زنجیره و امضای حلقه‌ای می‌باشد، که شامل پروتکل‌های SNARK و تراکنش محرمانه است. در شکل ۶ همچنین پیامدهای هر کدام از روش‌ها و پروتکل‌ها آمده است که شامل شکستن پیوندهای بین آدرس ورودی و خروجی در یک تراکنش، مخفی کردن مقادیر و شکستن پیوندهای بین تراکنش می‌باشد و ممکن است بعضی از روش‌ها و پروتکل‌ها هر دو پیامد را شامل شود.

در جدول ۵ ویژگی‌های شیوه‌های حفظ حریم‌خصوصی آمده است. که در واقع این جدول پروتکل‌های موجود در شکل ۶ را همراه با جزئیات بیشتر شامل مشخصات و محدودیت‌ها تشریح می‌کند.

۳.۴ پاسخ به سوال سوم

آسیب‌پذیری‌ها و تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟

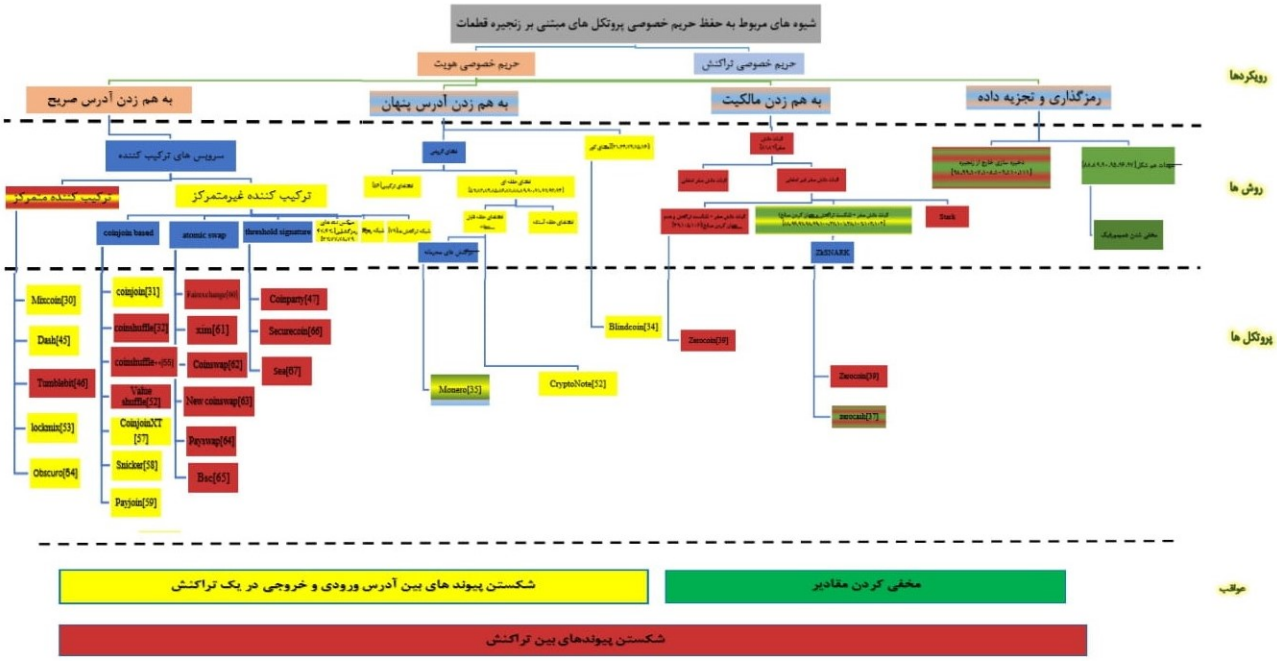
مطابق مقالات مطالعه شده، حملات براساس نوع حمله به ۹ گروه با عناوین زیر دسته‌بندی است. براساس مقالاتی که جمع آوری شده توجه جامعه علمی به جنبه‌های حمله و تهدید در شکل ؟؟ آمده است. همان‌طور که در شکل ؟؟ مشاهده می‌شود بیشترین مورد مربوط به حملات شبکه می‌باشد.

۱.۳.۴ حملات کاربردی

چالش‌های امنیتی این لایه نشان دهنده مسائل امنیتی مربوط به گره‌های متمرکز در تراکنش‌های ارزهای دیجیتال است. از آنجایی که این لایه ترکیبی از زنجیره قطعات مختلف است، مؤلفه‌ها و فن‌آوری‌های شخص ثالث برای توسعه یک برنامه کاربردی در برابر طیف گسترده‌ای از حملات قرار دارد. مهاجمان معمولاً با نگاهی به لایه کاربردی شروع به دنبال کردن آسیب‌پذیری‌های برنامه نوشته شده در کد هستند.

اگرچه حملات، زبان‌های برنامه‌نویسی خاصی را بیشتر از سایرین هدف قرار می‌دهد، طیف وسیعی از برنامه‌های کاربردی که نشان دهنده زبان‌های مختلف هستند، حملات را دریافت می‌کند. آسیب‌پذیری‌ها هم در کدهای سفارشی و هم در چارچوب‌ها و کتابخانه‌های منبع باز یافت می‌شود. در این مرور منابع مختلفی برای حملات کاربردی بدست آمده است که در ادامه تنها به ذکر نام و مراجع مرتبط اکتفا می‌شود.

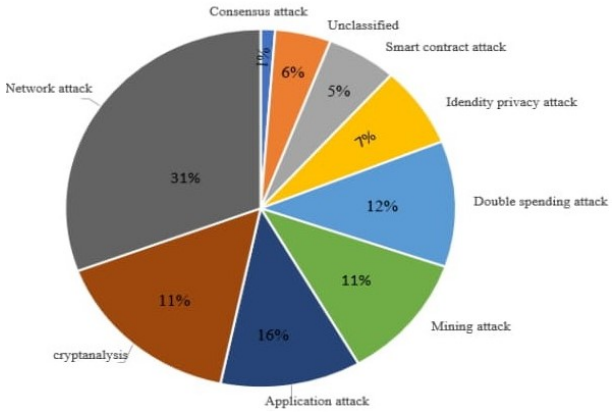
حمله الحاق و شکستن فاصله زمانی [۲۰۰]، خطای کدگذاری [۲۰۲]، حمله تبانی [۷۰، ۱۹۵-۱۹۷]، فاصله زمانی تخریب [۱۹۸، ۱۹۹]، حمله شکست اجرا [۲۱۰]، حملات بددهنی و ارتقایافته [۷۰]، حمله تحقیرآمیز [۲۴۴، ۲۴۵]، حمله آلودگی [۲۴۵]، حمله تزریق داده‌های نادرست [۱۹۲، ۱۹۷]، حمله تزریقی [۱۹۷]، قابلیت پیوند [۲۱۲]، حمله پیوند [۷۰، ۱۹۸-۲۰۰، ۲۰۷، ۲۰۸]، حمله مخرب [۷۱، ۱۹۱-



شکل ۵. شیوه‌های حصول حریم‌خصوصی

جدول ۵. ویژگی‌های شیوه‌های حفظ حریم خصوصی

| نام طرح (روش‌ها) | مشخصات / ویژگی‌ها | | |



شکل ۶. حملات امنیت و حریم‌خصوصی زنجیره قطعات

۱۹۳، ۱۹۳، ۱۹۴]، فعالیت‌های بدخواهانه کاربران مخرب [۲۱۱]، افشای اطلاعات [۲۴۶]، حملات بدافزار [۲۰۲، ۲۰۵]، حمله مسمومیت [۷۱، ۲۰۶]، حمله انکار [۲۴۵، ۲۴۶]، حمله مبتنی بر شهرت [۱۹۷، ۲۰۱، ۲۰۲]، حملات نرم‌افزاری [۲۰۹]، نشت حریم خصوصی تراکنش [۲۰۳، ۲۰۴]، حمله استنتاج عضویت [۲۴۷].

۲.۳.۴ حملات اجماع

حملات اجماع یک مشاجره بین استخراج کننده‌ها برای استخراج قطعه بعدی است. در این صورت گروهی که از نظر قدرت درهم‌ساز قوی‌تر است برنده می‌شود. هنگامی که یک استخراج کننده یا گروهی از استخراج کننده‌ها با قدرت محاسباتی زیادی در سیستم ظاهر می‌شود، می‌تواند با حمله به شیوه اجماع به هدف تضعیف امنیت و قابلیت اطمینان شبکه دست یابد. شایان ذکر است که حملات اجماع تنها می‌تواند بر اجماع آینده کل زنجیره قطعات یا حداکثر بر اجماع چند قطعه در گذشته نزدیک (تا ۱۰ قطعه در گذشته) تأثیر بگذارد. و با گذشت زمان، احتمال کمتری دارد که کل زنجیره قطعات دستکاری شود. به لحاظ نظری، پراکندگی، چند شاخگی، شاخه به شاخه شدن زنجیره قطعات می‌تواند بسیار طولانی شود. یک حمله اجماع نمی‌تواند رمزارزها را از کیف پول‌های دیگر بدزدد، تنها تاثیری که یک حمله اجماع می‌تواند داشته باشد این است که بر آخرین قطعات (تا قطعه۱۰) تأثیر بگذارد و بر تولید قطعات آینده از طریق انکار سرویس تأثیر بگذارد. با گذشت زمان و افزایش همتایان در یک زنجیره قطعات پایگاه داده بین همتایان خود توزیع می‌شود و هر چه بیشتر این اتفاق بیفتد تغییر ناپذیرتر می‌شود. حملات اجماع بر امنیت کلیدهای خصوصی و الگوریتم امضا تأثیر نمی‌گذارد، همچنین قادر به سرقت رمزارز یا خرج کردن آن‌ها بدون امضای نیست. علاوه بر این حملات اجماع نمی‌تواند تراکنش‌های ثبت شده در دفتر کل و یا مالکیت آن‌ها را تغییر دهد . در عوض، آن‌ها فقط می‌تواند بر آخرین قطعات استخراج شده تأثیر بگذارد و در نتیجه باعث انکار سرویس شوند و ایجاد هر قطعه دیگری را غیرممکن کند.

حمله چرخه اجماع [۱۹۹]، حمله دوره اجماع [۲۰۰]، تأخیر اجماع [۲۱۳]، حمله دوربرد و حمله انباشت سکه [۱۹۴].

۳.۳.۴ حملات تحلیل رمزی

تحلیل رمزی فرآیندی برای یافتن نقاط ضعف در الگوریتم‌های رمزنگاری و استفاده از این نقاط ضعف برای رمزگشایی متن رمز بدون دانستن کلید مخفی است. گاهی اوقات ضعف در خود الگوریتم رمزنگاری نیست، بلکه در نحوه استفاده از آن است که باعث موفقیت تحلیل رمزنگاری می‌شود. یک مهاجم ممکن است اهداف دیگری نیز داشته باشد، مانند: پیدا کردن کلید مخفی، یافتن یک الگوریتم عملکردی معادل برای رمزگذاری و رمزگشایی که نیازی به دانش کلید مخفی ندارد وبه دست آوردن اطلاعاتی در مورد متون ساده یا متون رمزی که قبلاً شناخته شده نبود. هدف مهاجم از انجام تحلیل رمز به نیازهای خاص مهاجم در یک زمینه حمله مشخص بستگی دارد. در بیشتر موارد، اگر تحلیل رمزی موفقیت آمیز باشد، مهاجم نمی‌تواند از استنباط برخی اطلاعات در مورد متن ساده عبور کند. با این حال، بسته به زمینه، ممکن است برای یک مهاجم کافی باشد.

حمله ذهنی دولتی، حمله پیش محاسباتی [۲۴۶]، حمله عملیات درهم‌ساز [۲۰۲]، حمله مرد در میانه [۷۰، ۱۹۷، ۲۰۵، ۲۱۴–۲۱۸]، حمله تغییر پیام [۷۰، ۷۱، ۱۹۸–۲۰۰، ۲۲۰؟]، حمله جعل پیام [۲۱۲]، حمله زمان‌بند [۲۴۸]، پول‌شویی، حمله به خطر افتادن کلید خصوصی، حمله متن رمزی انتخاب شده [۷۰]، حمله جریان ساعت، حمله پیش تصویر [۱۹۵]، حملات همتا به همتا [۲۱۳]، فعالیت‌های جنایی [۲۰۳، ۲۰۴]، حمله عملیات رمزنگاری، حمله تبادلات، حملات‌اخیر [۲۰۲]، حمله تاخیر زمانی، مدل‌سازی آماری [۷۱]، حمله داده [۱۹۲، ۲۰۹، ۲۱۹]، احراز هویت، اجرای سیاست، حملات کانال جانبی [۱۹۲]، شهرت کاذب [۲۰۰]، حملات سرریز [۲۱۳]، حمله همپوشانی [۱۹۷]، حملات فیزیکی [۲۰۹]، حملات عملی [۲۲۱]، افشای حریم خصوصی و پرداخت‌های غیرقابل اعتماد [۱۹۱]، امنیت کلید خصوصی [۱۹۶، ۲۰۳، ۲۰۴]، اصلاح قطعه عمومی [۱۹۹]، آسیب‌پذیری کوانتومی [۷۰، ۱۹۷، ۲۰۲، ۲۱۴]، باج‌افزار [۲۰۴]، حملات اختلاف زمانی [۲۱۰]، ابطال کاربر ثبت مجدد، حمله ورود/به‌روزرسانی رمز عبور اشتباه، امنیت کلید جلسه شناخته‌شده [۲۱۸]، حمله رمزارزی [۷۰، ۲۱۳]، حمله ذخیره‌ساز [۲۴۹، ۲۵۰]، حمله سرریز عدد صحیح [۷۰، ۱۷۷]، حمله روز صفر، حمله رمزعبور ضعیف، حمله جعل قدرت درهم‌ساز [۱۹۴]، رمزنگاری ناسازگار [۱۹۶].

۴.۳.۴ حملات دو بار خرج کردن

در رمزارزهای پایه مبتنی بر زنجیره قطعات، یک مهاجم با تبانی در شبکه سعی می‌کند با ارسال مقداری ارز دیجیتال مصرف شده به دیگران، یک تراکنش تازه ایجاد کند. در این صورت، مهاجم می‌تواند از ارز دیجیتال مضاعف برای تبانی با شخصی در شبکه استفاده کرده و آن را خرج کند. این مشکل زمانی ایجاد می‌شود که یک تراکنش موفق با همان وجوه تکرار شود. این نشان دهنده یک نقص بالقوه در پول نقد دیجیتال است، زیرا در صورت وقوع چنین حمله‌ای، رمز دیجیتالی مشابه را می‌توان دو بار خرج

کرد. این نوع آسیب‌پذیری تنها در ارزهای دیجیتال به دلیل محدودیت توانایی‌های استخراج کننده‌ها در طول فرآیند تأیید یافت می‌شود. بنابراین، ارزهای دیجیتال پیشنهادی اخیر و سیستم‌های مختلف زنجیره قطعات در تلاش هستند تا با استفاده از آخرین پروتکل‌های اجماع و شیوه‌های رمزنگاری، مانند امضای دیجیتال، بر حمله دوبار خرج کردن غلبه کنند.

حمله جستجوی فراگیر [۲۲۳–۲۲۵]، حمله ظریف،حمله بردار ۷۶ [۱۹۷، ۲۰۲، ۲۲۲–۲۲۵]، حمله چکش خواری [۷۰، ۷۱، ۲۰۲، ۲۲۵، ۲۲۶]، حمله بیش از حد خرج کردن [۲۱۲]، حمله دسترسی غیرمجاز [۱۹۴]، حمله مسابقه [۱۹۵، ۱۹۷، ۲۰۲، ۲۲۲، ۲۲۴، ۲۲۵]، حمله حدسی [۷۰، ۱۹۷، ۲۰۲، ۲۲۲–۲۲۵].

۵.۳.۴ حملات حریم‌خصوصی هویت

در حمله به حریم‌خصوصی هویت، مهاجم اطلاعات حریم‌خصوصی کاربر را با استفاده از ارتباط بین آدرس معامله‌گر در زنجیره و هویت واقعی کاربر به دست می‌آورد. مهاجم با نظارت بر داده‌های عمومی در دفتر کل جهانی و تجزیه و تحلیل تراکنش‌های مرتبط بین آدرس‌ها، هویت کاربر را استنباط می‌کند. در حال حاضر، حمله به حریم‌خصوصی هویت مشترک عمدتاً شامل حملات کلید، پخش مجدد و جعل هویت است. هنگام استفاده از زنجیره قطعات، کلید خصوصی کاربر که توسط او تولید و نگهداری شده به عنوان هویت و اعتبار امنیتی در نظر گرفته می‌شود. هنگامی که کلید خصوصی کاربر گم شود، قابل بازیابی نخواهد بود. اگر کلید خصوصی توسط مجرمان دزدیده شود، حساب زنجیره قطعات کاربر با خطر دستکاری دیگران مواجه خواهد شد. از آن‌جایی که زنجیره قطعات به هیچ مؤسسه مورد اعتماد شخص ثالث متمرکزی وابسته نیست، اگر کلید خصوصی کاربر به سرقت رفته باشد، ردیابی رفتارهای مجرم و بازیابی اطلاعات زنجیره قطعات اصلاح شده دشوار است.

حمله گمنام [۲۱۲]، بی‌نام‌سازی [؟]، حمله همگن، حمله دانش پس‌زمینه، حمله اریبی و حمله شباهت [۷۱]، سرقت حریم خصوصی هویت [۷۳، ۲۱۴]، حمله جعل هویت [۷۰، ۱۹۷، ۲۰۲، ۲۱۸، ۲۲۰، ۲۳۰]، حدس زدن رمز عبور آفلاین [۲۲۷]، حمله پاسخ [۷۰، ۱۹۲، ۱۹۷، ۲۰۲، ۲۱۳–۲۱۸، ۲۲۰، ۲۲۷–۲۲۹]، اثر انگشت تراکنش [۲۳۱، ۲۳۲]، نشت حریم خصوصی کیف پول [۲۰۸]، حمله سفید [۱۹۷]، نشت شناسه در HTLC [۱۹۶].

۶.۳.۴ حملات شبکه

حملات شبکه و در نتیجه امنیت شبکه از ابتدای محاسبات توزیع شده به صورت تاریخی وجود داشته است. امنیت شبکه معمولاً به عنوان زیرمجموعه‌ای از امنیت تعریف می‌شود و به این ترتیب حملات امنیتی شبکه و اقدامات متقابل برای پیاده‌سازی زنجیره قطعات نیز اعمال می‌شود. اقدامات متقابل معمولی شامل طراحی پروتکل‌های ایمن، اعمال رمزگذاری متقارن/نامتقارن، فیلتر کردن و نظارت بر شبکه‌ها است. حملات شبکه از طراحی و ویژگی‌های شبکه استفاده می‌کند. آن‌ها را می‌توان به عنوان فعال، جایی که کاربر مخرب اطلاعات را تغییر می‌دهد یا حذف می‌کند، و غیرفعال، جایی که کاربر مخرب به داده‌های ارسال شده در شبکه گوش می‌دهد، طبقه‌بندی کرد. هدف مهاجم جداسازی کاربران و استخراج کننده‌ها از شبکه واقعی، محدود کردن دسترسی آن‌ها به منابع شبکه، یا ایجاد بخش‌بندی در شبکه و اجرای قوانین متناقض در بین همتایان است.

استفاده مجدد آدرس، جعل پیام [۲۰۸]، حمله ربودن [۷۰، ۷۱، ۱۹۴، ۲۰۳، ۲۰۴، ۲۱۳، ۲۱۴، ۲۲۴]، فریب داده‌ها، حملات متفرقه [۲۴۲]، حملات مبتنی بر سرویس [۱۹۷]، حملات فروچاله [۱۹۲]، حمله سیبل [۷۰، ۷۱، ۷۳، ۱۹۴–۱۹۷، ۲۰۱، ۲۰۳، ۲۰۸، ۲۱۴، ۲۱۷، ۲۲۲، ۲۲۴، ۲۲۵، ۲۲۹، ۲۳۱، ۲۳۲، ۲۳۴، ۲۳۷، ۲۳۸]، حمله انکار سرویس توزیع‌شده [۷۱، ۲۰۲، ۲۱۳، ۲۱۴، ۲۲۵، ۲۲۷، ۲۲۹، ۲۳۹]، ربودن نام دامنه سیستم [۲۱۳]، حملات انکار سرویس [۷۳، ۱۹۶، ۱۹۸–۲۰۰، ۲۰۵، ۲۱۳، ۲۱۴، ۲۲۶، ۲۲۸، ۲۳۱–۲۳۳، ۲۳۶، ۲۳۷]، حملات کسوف [۷۰، ۷۱، ۷۳، ۱۹۶، ۱۹۷، ۲۰۲، ۲۰۴، ۲۱۳، ۲۲۲، ۲۲۴، ۲۲۵، ۲۲۹، ۲۳۲]، حمله جعل [۱۹۲، ۱۹۸، ۲۱۴، ۲۱۸، ۲۱۹]، حمله جعل دروازه [۲۴۱]، دشمن منفعل جهانی، خیانت دشمن داخلی، فریب دشمن داخلی، دشمن منفعل محلی [۲۴۰]، حمله رهگیری [۲۱۵]، نشت آدرس IP [۱۹۱]، حمله زنده بودن [۷۰، ۷۱، ۲۰۳، ۲۰۴، ۲۲۴، ۲۳۳]، حمله مبتنی بر دستکاری [۱۹۴، ۱۹۷، ۲۱۴، ۲۱۷، ۲۲۵]، حملات ضبط گره [۱۹۲]، حملات فریب [۷۰، ۱۹۲، ۱۹۴]، حملات مسیریابی [۷۰، ۲۲۵]، حمله جعل سرور [۲۱۸]، ربودن زمان [۷۰، ۱۹۷، ۲۰۲، ۲۱۳، ۲۲۵]، حمله قابلیت ردیابی [۲۱۲]، حمله تجزیه و تحلیل ترافیک [۷۱، ۲۱۷]، تاخیر انتشار [۷۶]، حمله تقلب موقعیت مکانی [۷۰]، حمله انکار خواب [۲۵۲]، حمله سقوط [۱۹۹، ۲۰۰]، استراق سمع [۷۱، ۱۹۲، ۲۱۹].

۷.۳.۴ حملات قرارداد هوشمند

زمانی که یک برنامه در یک زنجیره قطعات اجرا می‌شود، یک قرارداد هوشمند می‌تواند آسیب‌پذیری‌های امنیتی ناشی از نقص در آن برنامه داشته باشد. به عنوان مثال، نویسندگان یک مطالعه دریافت که « قرارداد هوشمند اتریوم در برابر حملاتی مانند وابستگی به سفارش تراکنش، وابستگی به مهر زمانی، استثنائات نادرست مدیریت شده، و حمله ورود مجدد آسیب‌پذیر است. » این آسیب‌پذیری باعث مشکلات قراردادی در زمینه کدگذاری، امنیت، حریم‌خصوصی و عملکرد سیستم، از جمله مقیاس‌پذیری زنجیره قطعات می‌شود.

کیف پول چند امضایی [۲۲۶]، خوشه‌بندی آدرس [۲۳۱]، حمله DAO [۷۱، ۲۰۳، ۲۰۴، ۲۱۳، ۲۲۳، ۲۲۶]، انتقال اجباری تعادل [۲۱۳]، حمله ورود مجدد [۷۳، ۱۹۴، ۲۰۴، ۲۱۴، ۲۲۳، ۲۳۳]، حملات بازپرداخت [۷۰، ۲۲۵]، حملات آدرس کوتاه [۷۰، ۲۱۳]، وابستگی مهر زمانی، وابستگی تراکنش–سفارش [۲۰۴].

۸.۳.۴ حملات دسته‌بندی نشده

حمله رها شده [۱۹۸]، سوءاستفاده از حافظه پنهان [۲۴۲]، بالارفتن از تپه [۲۴۳]، حملات مهاری [۲۰۱]، مولد اعداد تصادفی، توقف معاملات خاص [۱۹۵]، حمله امتناع از امضا [۱۹۷]، حمله اثبات تقلب [۱۹۶]، حمله بلع زنجیره قطعات [۷۰]، مدیریت اعتماد [۱۹۲]، سرقت کیف پول [۷۰، ۱۹۵، ۲۱۳، ۲۲۶، ۲۳۷].

۴.۴ پاسخ به سوال چهارم تحقیق

شیوه‌های مقابله با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی چیست؟

طبق مقالات مطالعه شده، جدول ۶ اقدامات متقابل با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی را نشان می‌دهد که براساس نوع حمله دسته‌بندی شده است.

جدول ۶. اقدامات متقابل با تهدیدات علیه حفظ حریم‌خصوصی و گمنامی

نوع حمله	اقدامات متقابل
کاربردی	نگاشت خود سازماندهی [۱۵۵] رویکردهای شبه تصادفی [۱۵۶، ۱۵۷] لایه پیوند یا رمزگذاری لایه شبکه، کنترل دسترسی [۱۵۸] هر بار داده‌ها را با یک جفت کلید جدید رمزگذاری کنید [۷۰]
اجماع	اعتبار معامله چشم انداز [۱۵۹]
تحلیل رمزی	تجزیه و تحلیل ترافیک شبکه، رویکردهای تحلیل و آزمایش کد، تجزیه و تحلیل و آزمایش کد مناسب، طرح‌های احراز هویت [۷۰] پروتکل BGPsec [۱۶۰] رمزگذاری حفظ نظم [۱۶۱] ارتباطات گروهی ایمن، توزیع کلید تصادفی، رمزگذاری کلید عمومی [۱۵۸] الگوریتم‌های اجماع [۱۶۲،۱۶۳،۴۶] شیوه‌های رمزنگاری [۱۶۴] طرح کوانتومی پس از امضا [۱۶۵]
دوبار خرج کردن	اصلاح مشخصات [۱۶۶] رویکردهای تعهد زمانی [۱۶۶] تعهد زمان بندی شده [۱۶۷]
حریم خصوصی هویت	شیوه‌های تأیید [۱۶۸،۵۰] اضافه کردن nonce در همه تراکنش‌ها، شیوه‌های ترکیب، امضای دیجیتال [۱۶۹]
استخراج	انتخاب تصادفی استخراج کننده‌ها [۱۷۰] محدود کردن تعداد استخراج کننده‌ها با تراز شبکه بیشتر [۱۷۱] مهرهای زمانی بی صدا [۱۷۲] روش‌های تعیین‌کننده صفر [۱۷۳] مشارکت استخرهای کوچکتر [۱۷۴] مدل‌های نظریه بازی و تعادل نش [۱۷۵] الگوریتم بلوک صفر [۱۷۶] رویکرد پاو [۱۷۷] تعریف مقیاس و ارتفاع برای تشخیص استخراج کننده [۱۷۸]
شبکه	طرح‌های مبتنی بر هزینه و سن [۱۷۹] یادگیری نش، [۱۸۰] تشخیص نفوذ، مسیریابی اضافی، بررسی سازگاری و لغو گره، ضد دستکاری، پروتکل مسیریابی امنیتی، نوشتن یک تابع درهم‌ساز ایمن [۱۵۸] راه اندازی یک شبکه خصوصی، محدود کردن اتصالات ورودی/خروجی [۱۸۱،۱۸۲] زمان رفت و برگشت، پروتکل‌های حسابرسی و تأیید، ایجاد هویت شبکه محدود، اعتبار کاربران، سیستم‌های سخت‌افزار گرا [۷۰] هر بار مکان جدید را از مکان های ذخیره شده محاسبه کنید [۱۸۳] نرم افزار ضد جاسوس افزار، ارتقاء دیواره آتش‌ها [۱۸۴] شیوه‌های رمزنگاری [۱۸۵] پروتکل زمان شبکه [۱۸۶،۱۹۰] محدودیت دامنه تحمل [۱۸۶]
قرارداد هوشمند	فازبندی پویا جریان داده قرارداد هوشمند [۱۸۷] با نام سرنوم [۱۸۷] یک روش درخواست پرداخت با شواهد کافی [۱۸۸] داوران [۱۸۸] اعتبار سنجی و ترکیب کد [۷۰] اسکوپ هوشمند [۱۸۹]

۵ جمع‌بندی و کارهای آینده

در این مقاله، هدف بررسی رویکرد زنجیره قطعات با در نظر گرفتن دیدگاه امنیت، حریم‌خصوصی و گمنامی در زمینه‌های مختلف و پاسخ به سوالات مطرح شده است. زنجیره قطعات امکان اجرای گمنامی تراکنش‌های درگیر را فراهم می‌کند. اما همچنین خطرات خاصی در مورد قابلیت ردیابی وجود دارد که می‌تواند هویت واقعی اعضای زنجیره قطعات درگیر در تراکنش را آشکار و اطلاعات آن‌ها را در معرض خطر قرار دهد. زنجیره‌های قطعات عمومی بیشتر در معرض غیرگمنام سازی است. برخی ناسازگاری‌ها بوجود آمده می‌تواند حریم‌خصوصی و گمنامی نهادهای شرکت‌کننده در زنجیره قطعات و حتی اطلاعات درگیر در یک تراکنش خاص را به خطر بیندازد. این تحقیق بر روی مطالعاتی متمرکز شده است که از انواع شیوه‌های حفظ حریم‌خصوصی برای ایجاد امنیت و کارایی بیشتر و گمنامی تراکنش و هویت کاربران استفاده می‌کند.

اطلاعات شبکه های معمولی و ابرداده می‌تواند برای استنباط اطلاعات اضافی در مورد کاربران شرکت کننده در تراکنش استفاده شود، که این اطلاعات ممکن است شامل هویت کاربران نیز باشد. این افشای هویت می‌تواند تمام تراکنش‌های مربوط به کاربران را نشان دهد. به عبارت دیگر، این ابرداده حتی با قوی‌ترین شیوه‌های حفظ حریم خصوصی همچنان در شبکه جریان دارد. این یکی از بزرگترین چالش‌ها برای هر رویکرد حفاظت از حریم خصوصی است که ممکن است در شبکه‌های زنجیره قطعات عمومی بدون مجوز استفاده شود.

به نظر می‌رسد تحقیقات در مورد محدودیت‌ها و چالش‌های امنیتی مربوط به اندازه قطعات و انتشار آن و این‌که چگونه این تصمیم‌ها بر تأخیر و توان عملیاتی شبکه تأثیر می‌گذارد، به اندازه کافی انجام نشده است. توان عملیاتی شبکه زنجیره قطعات باید بهبود یابد تا در محیط‌های تولید فعلی قابل استفاده باشد. در حال حاضر، در اکثر فن آوری‌های زنجیره قطعات، تایید یک تراکنش چند دقیقه طول می کشد. بنابراین بهبود تأخیر با حفظ امنیت یک چالش کلیدی است.

۱.۵ چالش‌های زنجیره قطعات و مسیرهای آینده

جدای از طیف وسیعی از مزایایی که فناوری زنجیره قطعات ارائه می‌کند، چالش‌های کمی وجود دارد که عملی بودن آن را برای کاربردهای امنیتی متعددی محدود می‌کند. مزیت و ویژگی اصلی استفاده از فناوری زنجیره قطعات این است که گمنامی شبه کاربران را فراهم می‌کند که بسیار مورد نیاز است. زیرا زنجیره قطعات عمومی به دلیل ماهیت باز آن مستعد حملات مختلف است. یک زنجیره قطعات مجاز، تعامل ایمن را بین نهادهایی که برای یک هدف مشترک کار می‌کنند، امکان پذیر می‌کند. محدودیت‌های متعددی در زنجیره قطعات مجاز وجود دارد، مانند ناتوانی آن در انجام حجم عظیمی از تراکنش‌ها، نیاز به نوشتن قرارداد هوشمند به زبان خاص دامنه، ناتوانی در پشتیبانی از تراکنش‌های غیرقطعی و عملکرد محدود به دلیل اجرای متوالی تراکنش‌ها. اکثر طرح‌های موجود فقط می‌تواند سطحی از گمنامی را فراهم کند، بنابراین تحقیقات بیشتری برای توسعه یک رویکرد کاملاً گمنام که نیاز برنامه‌های امنیتی مختلف را برآورده می‌کند، مورد نیاز است. برخی از این چالش‌ها در بخش‌های زیر به تفصیل آمده است.

گره‌های محاسبه و استخراج: خدمات امنیتی به کار گرفته شده و فرآیند استخراج مرتبط با فناوری زنجیره قطعات نیازمند محاسبات بزرگ در تولید امضا، رمزگذاری و فرآیند رمزگشایی است. برای این منظور، چندین کار تحقیقاتی به راهبرد تخصیص منابع در فرآیند استخراج قطعات اختصاص داده شده است. همچنین، به منظور کاهش نیازهای محاسباتی برای رمزگذاری و امضای داده‌ها، توسعه یک طرح رمزنگاری ساده نیاز به بررسی بیشتر دارد.

سازگاری: برای الزامات و سناریوهای کاربردی مختلف، ساختارهای تراکنش‌های متعددی مانند معماری ACCOUNT اتریوم و معماری UTXO (خروجی تراکنش‌های خرج نشده) بیت کوین وجود دارد. UTXO بیت‌کوین یک جزء ارز دیجیتال یکپارچه است که توسط یک زنجیره امضای دیجیتال به هم مرتبط شده است. عملکرد معماری ACCOUNT اتریوم شبیه دنیای بانکداری سنتی است که در آن یک دولت جهانی حساب را نگهداری می‌کند و تراکنش‌ها به طور مستقل بر وضعیت این حساب‌ها تأثیر می‌گذارد. با این حال، هیچ یک از طرح‌های پیشنهادی شیوه موثر حفظ حریم خصوصی را تحت این ساختار تراکنش در نظر نمی‌گیرد. اتریوم به دلیل داشتن سیستم قابل برنامه ریزی پذیرفته شده‌ترین راهبرد برای برنامه‌های غیرمتمرکز است. اما، سازگاری طرح‌های حفظ حریم خصوصی با معماری ACCOUNT یک چالش است و نیاز به بررسی بیشتر دارد.

سربار ارتباط و ذخیره‌سازی: به دلیل ماهیت بسیار پویا برنامه‌های فعلی، به طور مکرر نیاز به تغییر در داده‌های مبدا و لیست‌های دسترسی وجود دارد. بنابراین، گره مجبور به پخش تراکنش‌های مکرر به منظور اصلاح اطلاعات مبدا یا به روز رسانی ACL است. در مقابل، فناوری زنجیره قطعات از نظر قابلیت‌های پردازش سیستم و ترافیک شبکه، هزینه‌های زیادی را متحمل می‌شود، زیرا یک شبکه همتا به همتا است. این سربار پردازش و ذخیره‌سازی چالش‌های بیشتری را در پذیرش زنجیره قطعات برای برنامه‌های امنیتی مختلف ایجاد می‌کند. این موضوع زمانی که زنجیره قطعات در زنجیره تامین یا هر برنامه کاربردی مشابه دیگری که دارای داده فشرده است، بدتر می‌شود. چندین راه‌حل پیشنهادی بر تخلیه فعالیت تراکنش‌های زنجیره قطعات اصلی با استفاده از شبکه‌های کانال پرداخت تکیه دارد. با این حال، این شفافیت داده‌ها را پنهان می‌کند و حریم خصوصی را به خطر می‌اندازد. این امر نیاز به ارائه راه‌حل های موثرتر در این زمینه را مطرح می‌کند.

پرس‌وجو بر روی داده‌های ذخیره شده در قطعات: برنامه‌های کاربردی مبتنی بر زنجیره قطعات بر کاهش تقلب، افزایش مقاومت در برابر دستکاری، کاهش هزینه‌های عملیاتی و اجرای قراردادها تمرکز دارد. با این حال، زنجیره قطعات از توانایی جستجوی محدود پشتیبانی می‌کند و می‌تواند به عنوان پایگاه داده غیرقابل جعل و توزیع شده که بر روی ذخیره‌سازی داده تمرکز دارد، برچسب‌گذاری شود. زنجیره قطعات یکپارچگی داده‌ها را با کمک پروتکل‌های اجماع و روش زنجیره درهم‌ساز تضمین می‌کند. با افزایش تصاعدی در پذیرش فناوری زنجیره قطعات برای برنامه‌های کاربردی داده فشرده مانند مدیریت حقوق مالکیت معنوی، زنجیره تامین و امور مالی، درخواست کاربران برای پرس‌وجو از داده‌های ذخیره شده افزایش یافته است. برای اجرای چنین پرس‌وجوهایی، سیستم از تمام گره‌های همتا می‌خواهد که از تمام رکوردها عبور کرده و نتیجه نهایی پرس‌وجو را ایجاد کند. این فرآیند بازیابی تصادفی رکورد، پردازش پرس‌وجو را بسیار وقت گیر می‌کند. اگرچه زنجیره قطعات مزایای امنیتی متعددی را به همراه دارد، ولیکن جستجوی کارآمد رکورد و ردیابی تراکنش‌های داده در سیستم‌های زنجیره قطعات فعلی هنوز حل نشده است.

بنابراین نقاط باز پژوهشی در مورد عملکرد، امنیت، مقیاس‌پذیری، گمنامی و اعتماد وجود دارد. ضرورت اصلاح و عملکرد ضعیف به دلیل افزایش عناصر رمزنگاری، مواردی است که پذیرش پیشنهادات را دشوار می‌کند و هنوز فرصت‌هایی برای پیشرفت بیشتر وجود دارد. لازم به ذکر است که روش‌هایی که گمنامی و حفظ حریم‌خصوصی را بهبود می‌بخشد، امکان بررسی یکپارچگی سیستم را به طور کلی کاهش می‌دهد و در نتیجه اعتماد مورد نیاز به سیستم افزایش می‌یابد. واضح است که نیاز به حرکت به سمت قوانین جهانی در خصوص حریم‌خصوصی و گمنامی بودن نیز یک نیاز ضروری محسوب می‌شود. با توجه به داده‌هایی که محرمانه‌تر است، مانند داده‌های سلامت، مکانیسم‌های امن‌تری باید برای تضمین حریم‌خصوصی و گمنامی در برابر خطرات یا حملات امنیتی احتمالی فراهم شود. همچنین پروتکل‌های مختلف قابلیت گمنامی را برای کاربران و تراکنش‌ها پوشش می‌دهد، با این حال، باید شیوه‌های سبک وزنی برای شبکات و دستگاه‌های محدود به منابع تکامل یابد.

مراجع

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, H.Wang, An overvie of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress),IEEE,pp.557-564,2017. 10.1109/BigDataCongress.2017.85

[2] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges., IJ Network Security19(5)653–659,2017. http://dio.org/10.6633/IJNS.201709.19(5).01

[3] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008.

[4] Okoli, C., & Schabram, K. (2015). A guide to conducting a systematic literature review of information systems research. . http://sprouts.aisnet.org/10-26

[5] J.2010 . http://dx.doi.org/10.2139/ssrn.1954824.

[6] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering. Engineering 1051(2), 1051,2017. https://doi.org/10.1145/2372233.2372235

[7] Z. Li, A. V. Barenji, G. Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robotics andComputer-Integrated Manufacturing, Vol. 54, pp.133-144,December,2018. https://doi.org/10.1016/j.rcim.2018.05.011

[8] D. Kumar, D. Chandini, B. Reddy, D. Bhattacharyya, T.-h.Kim, Secure Electronic Voting System using Blockchain Technology, International Journal of Advanced Science and Technology, Vol. 118, pp. 13-22, 2018. 10.21742/IJSH.2020.14.2.04

[9] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu,Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data, IEEE Internet of Things Journal,Vol. 6, No. 5, pp. 87708781,October,2019. 10.1109/JIOT.2019.2923525

[10] B. Zhao, P. Fan, M. Ni, Mchain: A Blockchain-Based VM Measurements Secure Storage Approach in IaaS Cloud with Enhanced Integrity and Controllability, IEEE Access, Vol. 6, pp. 43758-43769, August, 2018. 10.1109/ACCESS.2018.2861944

[11] H. R. Hasan, K. Salah, Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters,IEEE Access, Vol. 6, pp. 4678146793,August,2018. 10.1109/ACCESS.2018.2866512

[12] X. Li, J. Niu, J. Gao, Y. Han, Secure Electronic Ticketing System based on Consortium Blockchain, KSII Transactions on Internet and Information Systems, Vol. 13, No. 10 pp.5219-5243,October,2019. https://doi.org/10.3837/tiis.2019.10.022

[13] F. Luo, Z. Y. Dong, G. Liang, J. Murata, Z. Xu, A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain, IEEE Transactions on Power Systems, Vol. 34, No. 5, pp.4097-4108,September,2019. 10.1109/TPWRS.2018.2876612

[14] Q. Xing, B. Wang, X. Wang, BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution, Symmetry, Vol.10,No.9,ArticleNo.408,September,2018. https://doi.org/10.3390/sym10090408

[15] E. Bertino, A. Kundu, Z. Sura, Data Transparency with Blockchain and AI Ethics, Journal of Data and Information Quality, Vol. 11, No. 4, pp. 1-8, September, 2019. https://doi.org/10.1145/3312750

[16] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks, IEEE Internet of Things Journal, Vol. 6,No.5,pp.7992-8004,October,2019 . 10.1109/JIOT.2019.2904303

[17] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs, IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, Vol. 27, No. 12, pp.2792-2801,Decemer,2019. 10.1109/TVLSI.2019.2929420

[18] S. Figueroa, J. Anorga, S. Arrizabalaga, An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments,Computers, Vol. 8, No. 3, ArticleNo.57, September, 2019. https://doi.org/10.3390/computers8030057

[19] H. Wang, Y. Song, Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and

2018.2827163

[28] J. M. Kang, B. Kim, S.-j. Kim, A Study on Privacy Protection Method Applying Blockchain Technology for Big DataUtilization, Journal of Engineering and Applied Sciences, Vol.13, No. 3,pp.691695,2018. https://doi.org/jeasci.2018.691.695

[29] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain,Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains, IEEE Transactions on Industrial Informatics,Vol. 13, No. 6, pp. 3154-3164, December,2017. 10.1109/TII.2017.2709784

[30] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, Vol.14, No.8,pp.3690-3700,August,2018. 10.1109/TII.2017.2786307

[31] Manoj Kumar, N.; Kumar Mallick, P. Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci.132, 1815–1823, 2018. 10.1109/CSMIS60634.2023.00108

[32] Lai, R.; Kuo, L.E.E.; Chuen, D. Handbook of Blockchain, Digital Finance, and Inclusion; Singapore University of Social Sciences: Singapore,Volume2,pp.145–177,2018. https://doi.org/10.1016/C2015-0-04334-9

[33] Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.

[34] Comput. Struct. Biotechnol. J. 16, 224–230,2018. https://doi.org/10.1016/j.csbj.2018.06.003

[35] Efanov, D.; Roschin, P. The All-Pervasiveness of the Blockchain Technology. Procedia Comput. Sci.123,116–121,2018. https://doi.org/10.1016/j.procs.2018.01.019

[36] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput.Syst.88,173–190,2018. https://doi.org/10.1016/j.future.2018.05.046

[37] Yang, J.; Lu, Z.; Wu, J. Smart-toy-edge-computing-oriented data exchange based on blockchain. J. Syst. Archit.87, 36–48,2018. https://doi.org/10.1016/

Blockchain, Journal of Medical Systems, Vol. 42, No.8,ArticleNo.152,August,2018. https://doi.org/10.1007/s10916-018-0994-6

[20] A. Nakadaira, S. Ohashi, H. Watanabe, S. Fujimura, S.Sakuma, S. Kinoshita, Initiatives concerning development of applications utilizing blockchains, NTT Technical Review,Vol. 15, No.12,pp.1-7,December, 2017. 10.53829/ntr201712ra1

[21] L. Huang, G. Zhang, A. Fu, Privacy-Preserving Public Auditing for Non-manager Group Shared Data, Wireless Personal Communications, Vol. 100,pp.4, pp. 1277-1294, June, 2018. https://doi.org/10.1007/s11277-018-5634-4

[22] M. A. Ferrag, L. Maglaras, DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services, Computers, Vol. 8,No.3,ArticleNo.58, September ,2019 . https://doi.org/10.3390/computers8030058

[23] R.-Y. Chen, A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain,Future Generation Computer Systems, Vol. 80, pp. 198-210,March,2018. https://doi.org/10.1016/j.future.2017.09.077

[24] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S.Efraimidis, E. Kaldoudi, A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval, Computational and Structural Biotechnology Journal, Vol. 16, pp. 288297,2018. https://doi.org/10.1016/j.csbj.2018.08.002

[25] N. Kshetri, Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy, Telecommunications Policy, Vol. 41, No. 10, pp. 1027-1038,November,2017. https://doi.org/10.1016/j.telpol.2017.09.003

[26] Y. Zhao, Y. Li, Q. Mu, B. Yang, Y. Yu, Secure Pub-Sub:Blockchain-Based Fair Payment With Reputation for Reliable Cyber Physical Systems, IEEE Access, Vol. 6, pp. 12295-12303,January,2018. 10.1109/ACCESS.2018.2799205

[27] Y. Liu, X. Liu, C. Tang, J. Wang, L. Zhang, Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin, IEEE Access, Vol.6,pp.23261-23270,April,2018. 10.1109/ACCESS.

K.; Vasilakos, A.V. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Netw. Comput.Appl,116,42–52,2018. https://doi.org/10.1016/j.jnca.2018.05.005

[49] ALASTRIA. Available online: https://alastria.io (accessed on 15 September 2020).

[50] ETHEREUM.Availableonline: https://www.Ethereum.org/ (accessed on 15 September 2020).

[51] Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur.78, 126–142, 2018. https://doi.or10.1016/j.cose.2018.06.004

[52] Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.;Wang, C. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. IEEE Access,6,17545–17556, 2018. 10.1109/ACCESS.2018.2805837

[53] García, M.; Dubey, A.; Botti, V. Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges. J. Syst.Archit.91,83–102,2018. https://doi.org/10.1016/j.sysarc.2018.05.007

[54] Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale Election Based On Blockchain. Procedia Comput.Sci.129,234–237,2018. https://doi.org/10.1016/j.procs.2018.03.063

[55] Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl, 126, 4558,2019. https://doi.org/10.1016/j.jnca.2018.10.020

[56] Li, X.; Mei, Y.; Gong, J.; Xiang, F.; Sun, Z. A Blockchain Privacy Protection Scheme Based on Ring Signature. IEEE Access, 8, 76765–76772, 2020. 10.1109/ACCESS.2020.2987831

[57] Wang, Q.; Huang, J.; Wang, S.; Chen, Y.; Zhang, P.; He, L. A Comparative Study of Blockchain Consensus Algorithms. J. Phys. Conf. Ser.1437, 012007,2020.DOI 10.1088/1742-6596/1437/1/012007

[58] Joo, L.Y.; Myung, L.K. Blockchain-based Multi-Purpose Authentication Method for Anonymity and Privacy. Int. J. Recent Technol. Eng. (IJRTE),8,409–414,2019.doi 10.j.sysarc.2018.05.001

[38] Eddine Kouicem, D.; Bouabdallah, A.; Hicham, L. Internet of things security: A top-down survey. Comput. Netw.141,199–221,2018. https://doi.org/10.1016/j.comnet.2018.03.012

[39] Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. ACM Comput. Surv.52, 1–34, 2019. https://doi.org/10.1145/3316481

[40] Sultan, A.; Mushtaq, M.A.; Abubakar, M. IOT Security Issues Via Blockchain: A Review Paper. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu,HI,USA,pp.60–65,2019. https://doi.org/10.1145/3320154.3320163

[41] Rathore, H.; Mohamed, A.; Guizani, M. A Survey of Blockchain Enabled Cyber-Physical Systems. Sensors,20,282,2020. https://doi.org/10.3390/s20010282

[42] Wu, Y.; Tang, S.; Zhao, B.; Peng, Z. BPTM: Blockchain-Based Privacy-Preserving Task Matching in Crowdsourcing. IEEE Access,7, 45605–45617,2019. 10.1109/ACCESS.2019.2908265

[43] Jo, H.J.; Choi, W. BPRF: Blockchain-based privacy-preserving reputation framework for participatory sensing systems. PLoS ONE,14, e0225688,2019. https://doi.org/10.1371/journal.pone.0225688

[44] Dorri, A.; Kanhere, S.; Jurdak, R. MOF-BC: A memory optimized and flexible blockchain for large scale networks. Future Gener. Comput. Syst.92,357–373,2017. https://doi.org/10.1016/j.future.2018.10.002

[45] Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. IEEE Access,6, 4565–45664,2018. 10.1109/ACCESS.2018.2864189

[46] Xu, C.; Liu, H.; Li, P.; Wang, P. A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X. IEEE Access, 6, 67809–67818,2018. 10.1109/ACCESS.2018.2878995

[47] Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. J. Ind. Inf. Integr.13,32–39,2019. https://doi.org/10.1016/j.jii.2018.07.004

[48] Lin, C.; He, D.; Huang, X.; Raymond Choo,

puter Science and Applications (IJACSA), 11(9),130-139,2020. 10.14569/IJACSA.2020.0110915

[67] Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S.Blockchain security threats, attacks and countermeasures. In Ambient Communications and Computer Systems: RACCCS (pp. 51-62). SpringerSingapore,2019 . https://doi.org/10.1007/978-981-15-1518-7_5

[68] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9,61048-61073,2021. 10.1109/ACCESS.2021.3072849

[69] Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. IEEE Communications Surveys & Tutorials, 23(1), 341-390,2020. 10.1109/COMST.2020.3033665

[70] Ahmadjee, S., Mera-Gómez, C., Bahsoon, R., & Kazman, R.A study on blockchain architecture design decisions and their security attacks and threats. ACM Transactions on Software Engineering and Methodology (TOSEM), 31(2), 1-45,2022. https://doi.org/10.1145/3502740

[71] Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S.Privacy preservation in permissionless blockchain: A survey. Digital Communications and Networks, 7(3), 295-307, 2021. https://doi.org/10.1016/j.dcan.2020.05.008

[72] Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration, 26,100312,2022. https://doi.org/10.1016/j.jii.2021.100312

[73] Aslam, S., Tošić, A., & Mrissa, M.Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions. Journal of Cybersecurity and Privacy, 1(1), 164-194, 2021. https://doi.org/10.3390/jcp1010009

[74] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. 35940/ijrte.b1077.0782s619

[59] Lee, Y.; Myung Lee, K. Blockchain-based RBAC for user authentication with anonymity. In Proceedings of the Conference on Research in Adaptive and Convergent Systems (RACS '19); Chongqing, China,Association for Computing Machinery: New York, NY, USA; pp. 289–294,2019. https://doi.org/10.1145/3338840.3355673

[60] Noh, J.; Jeon, S.; Cho, S. Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles. Electronics,9,74, 2020. https://doi.org/10.3390/electronics9010074

[61] Zou, S.; Xi, J.;Wang, S.; Lu, Y.; Xu, G. Reportcoin: A Novel Blockchain-Based Incentive Anonymous Reporting System. IEEE Access,7,65544–65559,2019. 10.1109/ACCESS.2019.2915956

[62] Soni, S., & Bhushan, B. (2020, July). A comprehensive survey on blockchain: Working, security analysis, privacy threats and potential applications. In 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT) (Vol. 1, pp. 922-926).IEEE,2020. 10.1109/ICICICT46008.2019.8993210

[63] Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Computers & Electrical Engineering, 90,106897,2021. https://doi.org/10.1016/j.compeleceng.2020.106897

[64] AlFaw, A., Elmedany, W., & Sharif, M. S. (2022, October). Blockchain Vulnerabilities and Recent Security Challenges: A Review Paper. In International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 780-786). IEEE, 2022. 10.1109/ICDABI56818.2022.10041611

[65] Khanum, S., & Mustafa, K. A systematic literature review on sensitive data protection in blockchain applications. Concurrency and Computation: Practice and Experience, 35(1), e7422,2023. https://doi.org/10.1002/cpe.7422

[66] Junejo, A. Z., Hashmani, M. A., & Alabdulatif, A. A. A survey on privacy vulnerabilities in permissionless blockchains. International Journal of Advanced Com-

//ia.cr/2019/341

[84] Kausar, F., Senan, F. M., Asif, H. M., & Raahemifar, K. 6G technology and taxonomy of attacks on blockchain technology. Alexandria Engineering Journal, 61(6), 4295-4306, 2022. https://doi.org/10.1016/j.aej.2021.09.051

[85] Gao, W., Hatcher, W. G., & Yu, W. A survey of blockchain: Techniques, applications, and challenges. In 2018 27th international conference on computer communication and networks (ICCCN) (pp.1-11).IEEE,2018. 10.1109/ICCCN.2018.8487348

[86] Stockinger, J. Analysis of Decentralized Mixing Services in the Greater Bitcoin Ecosystem (Doctoral dissertation, Wien), 2021. www.tuwien.at

[87] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll, E.W. Felten, Mixcoin: Anonymity for bitcoin with accountable mixes, in: International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, pp. 486–504, 2014. https://doi.org/10.1007/978-3-662-45472-5_31

[88] G. Maxwell, CoinJoin: Bitcoin privacy for the real world, in: Post on Bitcoin Forum, 2013. https://bitcointalk.org/index.php?topic=279249.0

[89] T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: Practical decentralized coin mixing for bitcoin, in: European Symposium on Research in Computer Security, Springer, Cham, pp. 345–364, 2014. https://doi.org/10.1007/978-3-319-11212-1_20

[90] L. Valenta, B. Rowan, Blindcoin: Blinded, accountable mixes for bitcoin, in: International Conference on Financial Cryptography and Data Security,Springer, Berlin, Heidelberg, pp. 112–126, 2015. https://doi.org/10.1007/978-3-662-48051-9_9

[91] S. Noether, Ring signature confidential transactions for monero, IACR Cryptol. ePrint Arch. 1098, 2015. https://ia.cr/2015/1098

[92] E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza,Zerocash: Decentralized anonymous payments from bitcoin, in: 2014 IEEE Symposium on Security and Privacy, IEEE, pp. 459–474, 2014. 10.1109/SP.2014.36

[93] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox, Zcash

L., Moreno, R. T., & Skarmeta, A. Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908-164940,2020. 10.1109/ACCESS.2019.2950872

[75] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z.A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence Computing, 2(2), 100048,2022. https://doi.org/10.1016/j.hcc.2021.100048

[76] V. Buterin, "On public and private blockchains," 2015.[Online].Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains

[77] Hedayati, A., & Hosseini, H. A.A Survey on Blockchain: Challenges, Attacks, Security, and Privacy. International Journal of Smart Electrical Engineering, 10(03),141-168,(2021). http://dx.doi.org/10.30495/ijsee.2021.684027

[78] Cheng, J., Xie, L., Tang, X., Xiong, N., & Liu, B. A survey of security threats and defense on Blockchain. Multimedia Tools and Applications, 80,30623-30652,2021. https://doi.org/10.1007/s11042-020-09368-6

[79] Bansod, S., & Ragha, L. Challenges in making blockchain privacy compliant for the digital world: some measures. Sādhanā, 47(3), 168, 2022. https://doi.org/10.1007/s12046-022-01931-1

[80] Andola, N., Yadav, V. K., Venkatesan, S., & Verma, S. Anonymity on blockchain based e-cash protocols—A survey. Computer Science Review, 40,100394,2021. https://doi.org/10.1016/j.cosrev.2021.100394

[81] Ghesmati, S., Fdhila, W., & Weippl, E. Sok: How private is bitcoin? classification and evaluation of bitcoin mixing techniques. Cryptology ePrint Archive, 2021. 10.1145/3538969.3538971

[82] Khalilov, M. C. K., & Levi, A.A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials, 20(3),2543-2585,2019. 10.1109/COMST.2018.2818623

[83] Seres, I. A., Nagy, D. A., Buckland, C., & Burcsi, P. Mixeth: efficient, trustless coin mixing service for ethereum. Cryptology ePrint Archive, 2019. https:

Protocol Specification,Tech. Rep. 2016–1.10, Zerocoin Electric Coin Compan , 2016.

[94] I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: Anonymous distributed e-cash from bitcoin, in: 2013 IEEE Symposium on Security and Privacy, IEEE, pp. 397–411, 2013. 10.1109/SP.2013.34

[95] J.H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, K. Wehrle, Secure and anonymous decentralized bitcoin mixing, Future Gener. Comput.Syst.80,448–466,2018. https://doi.org/10.1016/j.future.2016.05.018

[96] E. Duffield, D. Diaz, Dash: A privacycentric cryptocurrency, No Publisher, 2015.

[97] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg, Tumblebit:An untrusted bitcoin-compatible anonymous payment hub, in: Network and Distributed System Security Symposium,2017. 10.14722/NDSS.2017.23086

[98] J.H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, K. Wehrle, Coinparty: Secure multi-party mixing of bitcoins, in: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, pp.75–86, 2015. https://doi.org/10.1145/2699026.269910

[99] Bin, W., Bao, Z., Zhang, Y., Wang, Q., & Shi, W. Lockcoin: a secure and privacy-preserving mix service for bitcoin anonymity,2018. https://doi.org/10.48550/arXiv.1811.04349

[100] Tran, M., Luu, L., Kang, M. S., Bentov, I., & Saxena, P.(Obscuro: A bitcoin mixer using trusted execution environments. In Proceedings of the 34th Annual Computer Security Applications Conference (pp. 692-701), 2018. https://doi.org/10.1145/3274694.3274750

[101] Ruffing, T., & Moreno-Sanchez, P. Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin, 2017. https://ia.cr/2017/238

[102] T. Ruffing, P. Moreno-Sanchez, A. Kate, P2p mixing and unlinkable bitcoin transactions., in: NDSS, pp. 511–532, 2017. https://ia.cr/2016/824

[103] Gibson, A.,Coinjoinxt – a more flexible, extended approach to coinjoin. https://joinmarket.me/blog/blog/coinjoinxt/, 2018.

[104] Gibson, A.(Last accessed 31 August 2020). Snicker -simple non-interactive coinjoin with keys for encryption reused. https://joinmarket.me/blog/blog/snicker/, 2017.

[105] Gibson, A.(Last accessed 23 August 2020)b. Payjoin. https://joinmarket.me/blog/blog/payjoin/, 2018.

[106] Ray, I., Ray, I., & Natarajan, N. An anonymous and failure resilient fair-exchange e-commerce protocol. Decision Support Systems, 39(3), 267-292, 2005. 10.1016/j.dss.2003.10.011

[107] Bissias, G. D., Ozisik, A. P., Levine, B. N., & Liberatore, M. D. Xim: Distributed Match-and-Mix for Bitcoin.

[108] Maxwell, G.,Coinswap: transaction graph disjoint trustless trading ,URL: https://bitcointalk.org/index.php , 2013.

[109] Gibson, A.(Last accessed 23 August 2020). New coinswap. https://joinmarket.me/blog/blog/coinswaps/, 2017.

[110] Belcher, C.,Design for a coinswap implementation for massively improving bitcoin privacy and fungibility. https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964 ,2020.

[111] Heilman, E., Baldimtsi, F., Goldberg, S., Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions, 2016. https://doi.org/10.1007/978-3-662-53357-4_4

[112] Ibrahim, M.H., Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem. IJ Network Security 19, 295–312, 2017. 10.6633/IJNS.201703.19(2).14

[113] Wang, D., Zhao, J., & Wang, Y. A survey on privacy protection of blockchain: the technology and application. IEEE Access, 8, 108766-108781,2020. 10.1109/ACCESS.2020.2994294

[114] O. Coutu, "Privacy in Bitcoin through decentralized mixers," Master's Thesis, Université de Montréal, Apr. 2014.[Online].Available: https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11498/Coutu_Olivier_2014_memoire.pdf. Accessed: 28-Dec-2016

[115] M. Florian, J. Walter, and I. Baumgart, "Sybil-Resistant Pseudonymization and Pseudonym Change without Trusted Third Parties," in Proceedings of the

14th ACM Workshop on Privacy in the Electronic Society (WPES '15), ACM, New York, NY, USA, pp. 65-74, 2015. https://doi.org/10.1145/2808138.280814

[116] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in Bitcoin," Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 8976, pp. 127–141, 2015. https://doi.org/10.1007/978-3-662-48051-9_10

[117] N. van Saberhagen, "CryptoNote.v2.0 Whitepaper," Oct. 2013. [Online]. Available: https://cryptonote.org/whitepaper.pdf. Accessed: 2017.

[118] Bytecoin Team, "Aggregate Addresses in CryptoNote: Towards Efficient Privacy," Sep. 2015.[Online].Available: https://bytecoin.org/static/files/docs/aggregate-addresses.pdf. Accessed: 04-Jan-2017.

[119] "DigitalNote, XDN-project", DigitalNote whitepaper, Jun. 2015. [Online]. Available: http://digitalnote.org/whitepaper.pdf. Accessed: 25- 2017.

[120] "The Anonymity of DarkNetSpace", DarkNetSpace Whitepaper, Oct. 2014. [Online]. Available: http://www.darknetspace.org/files/whitepaper.pdf. Accessed: 20-Jan-2017.

[121] aeon: [ANN] AEON [2017-03-04: important update to 0.9.8.0], Bitcoin Forum, Jun. 2014. [Online].Available: https://bitcointalk.org/index.php?topic=641696.0. Accessed: 27-Jan2017.

[122] monero: [XMR] Monero - A secure, private, untraceable cryptocurrency, Bitcoin Forum, Aug. 2014.[Online].Available: https://bitcointalk.org/index.php?topic=583449.0. Accessed: 13-Nov2016.

[123] G. Maxwell, "Confidential Transactions". [Online].Available: https://people.xiph.org/~greg/confidential_values.txt. Accessed: 25-Nov2016.

[124] S. Noether, "Ring Confidential Transactions," IACR Cryptology ePrint Archive, 2015:1098, 2015.

[125] S. Noether, A. Mackenzie and Monero Core Team, "Ring Confidential Transactions," Feb. 2016.[Online].Available: https://lab.getmonero.org/pubs/MRL-0005.pdf. Accessed: 16-Nov-2016.

[126] Boolberry.[Online].Available: http://boolberry.com/. Accessed: 23-Jan2017.

[127] Rynomster and Tecnovert, "ShadowCash: Zero-knowledge Anonymous Distributed E-Cash via Traceable Ring Signatures". [Online]. Available: http://bravenewcoin.com/assets/Whitepapers/ShadowCashZeroknowledge-Anonymous-Distributed-ECash.pdf. Accessed: 17-Jan2017

[128] Hondo | stealthcoin, "Stealthsend Whitepaper Brief," Sep. 2014. [Online]. Available: https://www.stealth-coin.com/wpcontent/uploads/Stealthsend_Whitepaper_brief0914.pdf. Accessed: 21- Jan-2017.

[129] R. Mercer, "Privacy on the Blockchain: Unique Ring Signatures," arXiv: 1612.01188, Dec. 2016. https://doi.org/10.48550/arXiv.1612.01188

[130] C. Garman, M. Green, I. Miers, and A. D. Rubin, "Rational Zero: Economic security for Zerocoin with everlasting anonymity," Financial Cryptography and Data Security, Lecture Notes in Computer Science, Springer, vol. 8438, pp. 140–155, 2014. https://doi.org/10.1007/978-3-662-44774-1_10

[131] G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno, "Pinocchio coin: building zerocoin from a succinct pairing-based proof system," in Proceedings of the First ACM workshop on Language support for privacy-enhancing technologies (PETShop '13), ACM, New York, NY,USA,pp.27-30,2013. https://doi.org/10.1145/2517872.2517878

[132] F. Schuh, and D. Larimer, "Bitshares 2.0: General Overview," 2015. [Online]. Available: http://docs.bitshares.org/_downloads/bitsharesgeneral.pdf. Accessed: 15-Jan-2017.

[133] D. Lukianov, "Compact Confidential Transactions for Bitcoin," 2015. [Online]. Available: http://voxelsoft.com/dev/cct.pdf. Accessed: 19-Dec2016

[134] gmaxwell: Really Really ultimate blockchain compression: CoinWitness, Bitcoin Forum, Aug. 2013.[Online].Available: https://bitcointalk.org/index.php?topic=277389.0. Accessed: 22-

[135] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in Proceedings of the IEEE Symposium on Security and Privacy (SP), pp. 839-858, 2016. 10.1109/SP.2016.55

[136] E. Androulaki and G. O. Karame, "Hiding transaction amounts and balances in Bitcoin," Trust and Trustworthy Computing, Lecture Notes in Computer Science, Springer, vol. 8564, pp. 161–178, 2014. https://doi.org/10.1007/978-3-319-08593-7_11

[137] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in Proceedings of the 2014 IEEE Symposium on Security and Privacy, 2014. 10.1109/SP.2014.36

[138] Zcash - All coins are created equal. [Online]. Available: https://z.cash/. Accessed: 15-Jan-2017.

[139] Komodo Platform – Making Bitcoin more Anonymous, Secure and Green. [Online]. Available: https://komodoplatform.com.Accessed:27-Jan-2017

[140] jl777: [ANN][KMD][dPoW] Komodo - Zcash Zero Knowledge Privacy Secured by Bitcoin, Bitcoin Forum, Sep. 2016. [Available]. Online: https://bitcointalk.org/index.php?topic=1605144.0.Accessed:27-Jan2017

[141] extrabyte: [ANN] Ebitz - 237 BTC in 8 days - POS - Zero Knowledge Proof - Deep Web, Bitcoin Forum, Nov. 2016. [Online]. Available: https://bitcointalk.org/index.php?topic=1681965.0. Accessed: 27-Jan2017.

[142] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly Signed Contracts Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions," IACR Cryptology ePrint Archive, 2016:056, 2016.

[143] tonych: Hiding entire content of on-chain transactions, Bitcoin Forum, Aug. 2016. [Online]. Available: https://bitcointalk.org/index.php?topic=1574508.0.Accessed:28-Dec-2016

[144] A. Churyumov, "Byteball: A Decentralized System for Storage and Transfer of Value". [Online]. Available: https://byteball.org/Byteball.pdf. Accessed:27-Dec-2016

[145] tonych: BYTEBALL: Totally new consensus algorithm + private untraceable payments, Bitcoin Forum, Sep. 2016. [Online]. Available: https://bitcointalk.org/index.php?topic=1608859.0.Accessed:27-Dec2016

[146] J.Jogenfors, "Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics," arXiv:1604.01383, Apr. 2016. https://doi.org/10.1109/BLOC.2019.8751473

[147] D. Lukianov, "Compact Confidential Transactions for Bitcoin," 2015. [Online]. Available: http://voxelsoft.com/dev/cct.pdf.Accessed: 19-Dec2016.

[148] adam3us: bitcoins with homomorphic value (validatable but encrypted), Bitcoin Forum, Oct. 2013.[Online].Available: https://bitcointalk.org/index.php?topic=305791.0.Accessed:25-Nov2016.

[149] "Onionbc." http://6fgd4togcynxyclb.onion/

[150] "Bitblender." https://bitblender.io/

[151] "Dash is digital cash." https://www.dash.org//

[152] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybilresistant mixing for bitcoin," in The Workshop on Privacy in the Electronic Society,pp.149–158,2014. http://dx.doi.org/10.1145/2665943.2665955.

[153] A. Mackenzie, S. Noether, and M. C. Team, "Improving obfuscation in the CryptoNote protocol," Tech. Rep. MRL-0004, Jan. 2015. [Online]. Available: https://www.docin.com/p-2122152949.html

[154] N. Van Saberhagen, Cryptonote v 2.0, 2013

[155] S.-F. Sun, M. H. Au, J. K. Liu, T. H. Yuen, Ringct 2.0:A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero, in: European Symposium on Research in Computer Security, pp. 456–474,2017. https://ia.cr/2017/921

[156] T. H. Yuen, S.-f. Sun, J. K. Liu, M. H. Au, M. F. Esgin,Q. Zhang, D. Gu, Ringct 3.0 for blockchain confidential transaction: shorter size and stronger security, Tech.rep., Cryptology ePrint Archive, Report 2019/508,2019. https://doi.org/10.1007/978-3-030-51280-4_25

and Computer Applications 127 43–58,2019. https://doi.org/10.1016/j.jnca.2018.11.03

[167] A. M. Khalifa, A. M. Bahaa-Eldin, M. A. Sobh, Quantum attacks and defenses for proof-of-stake, in: 2019 14th International Conference on Computer Engineering and Systems (ICCES), IEEE,pp.112–117,2019. 10.1109/ICCES48960.2019.9068181

[168] M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek, Fair two-party computations via bitcoin deposits, in: International Conference on Financial Cryptography and Data Security, pp.105–121.105–121, 2014. https://doi.org/10.1007/978-3-662-44774-1_8

[169] M. Andrychowicz, S. Dziembowski, D. Malinowski, L. Mazurek, How to deal with malleability of bitcoin transactions, CoRR abs/1312.3230 arXiv: 1312.3230, 2013. https://doi.org/10.48550/arXiv.1312.3230

[170] N. Malik, P. Nanda, A. Arora, X. He, D. Puthal, Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, in: 2018 17th IEEE International Conference On Trust, Security And PrivacyIn Computing And Communications/12th IEEE International Conference On Big Data ScienceAndEngineering (TrustCom/BigDataSE) ,IEEE,pp.674–679,2018. 10.1109/TrustCom/BigDataSE.2018.00099

[171] E. Androulaki, A. De Caro, T. Kramp, D. W. Kravitz, A. Sorniotti,M. Vukolic,Resisting replay attacks efficiently in a permissioned and privacy-preserving blockchain network, uS Patent 10,230,756,2019.

[172] M. Bastiaan, Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin, in: Availab le at http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin.pdf, 2015.

[173] C. Natoli, V. Gramoli, The balance attack against proof-ofwork blockchains: The r3 testbed as an example, arXiv preprint arXiv:1612.09426 ,2016. https://doi.org/10.48550/arXiv.1612.09426

[174] S.-Y. Chang, Y. Park, Silent timestamping for

[157] Z. Bankovi´c, J. C. Vallejo, D. Fraga, J. M. Moya, Detecting badmouthing attacks on reputation systems using self-organizing maps,in: Computational Intelligence in Security for Information Systems,Springer, pp. 9–16, 2011.

[158] E. Owiyo, Y. Wang, E. Asamoah, D. Kamenyi, I. Obiri, Decentralized privacy preserving reputation system, 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)665–672,2018. 10.1109/DSC.2018.00106

[159] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 ,11676–11686, 2018. 10.1109/ACCESS.2018.2801266

[160] Ren, Y., Leng, Y., Zhu, F., Wang, J., & Kim, H. J. Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors, 19(10), 2395.2019. https://doi.org/10.3390/s19102395

[161] P. Ga˘zi, A. Kiayias, A. Russell, Stake-bleeding attacks on proof-of-stake blockchains, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 85–92,2018. 10.1109/CVCBT.2018.00015

[162] M. Lepinski, K. Sriram, Bgpsec protocol specification,RFC8205, 2017. https://www.rfc-editor.org/info/rfc8205.

[163] Y. Ji, J. Zhang, J.Ma, C. Yang, X. Yao, Bmpls: Blockchain-based multilevel privacy-preserving location sharing scheme for telecare medical information systems, Journal of medical systems 42(8)147, 2018. https://doi.org/10.1007/s10916-018-0998-2

[164] T.-T. Kuo, L. Ohno-Machado, Modelchain: Decentralized privacy preserving healthcare predictive modeling framework on private blockchain networks, arXiv preprint arXiv:1802.01746,2018. https://doi.org/10.48550/arXiv.1802.01746

[165] G. Zyskind, O. Nathan, A. Pentland, Enigma: Decentralized computation platform with guaranteed privacy, ArXiv abs/1506.03471, 2015. https://doi.org/10.48550/arXiv.1506.03471

[166] L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains, Journal of Network

[183] A. Singh, et al., Eclipse attacks on overlay networks: Threats and defenses,in: In IEEE INFOCOM,Citeseer,2006. 10.1109/INFOCOM.2006.231

[184] E. A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin's peer -to-peer network, in: 24th USENIX Security Symposium (USENIX Security15).,2015. https://www.usenix.org/conference/

[185] B. Li, Y. Wang, P. Shi, H. Chen, L. Cheng, Fppb: a fast and privacy preserving method based on the permissioned blockchain for fair transactions in sharing economy, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications /12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, pp. 1368–1373,2018. 10.1109/TrustCom/BigDataSE.2018.00189

[186] J. Hong, The state of phishing attacks, Communications of the ACM 55 (1) ,74–81, 2012. https://doi.org/10.1145/2063176.2063197

[187] A. P. Joshi, M. Han, Y.Wang, A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing1(2),121–147,2018. 10.3934/mfc.2018007

[188] G. Ma, C. Ge, L. Zhou, Achieving reliable timestamp in the bitcoin platform, Peer-to-Peer Networking and Applications 13 ,2251–2259, 2020. https://doi.org/10.1007/s12083-020-00905-6

[189] M. Rodler, W. Li, G. O. Karame, L. Davi, Sereum: Protecting existing smart contracts against re-entrancy attacks, arXiv preprint arXiv:1812.05934,2018. https://doi.org/10.48550/arXiv.1812.05934

[190] P.McCorry, S. F. Shahandashti, F. Hao, Refund attacks on bitcoin's payment protocol, in: International Conference on Financial Cryptography and Data Security, pp. 581–599, 2016. https://doi.org/10.1007/978-3-662-54970-4_34

[191] Y. Feng, E. Torlak, R. Bodik, Precise attack synthesis for smart contracts,arXiv preprint arXiv:1902.06067,2019. https://doi.org/10.48550/arXiv.1902.06067

[192] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, A.H. Sarower, T. Bhuiyan, Blockchain Attacks, Analysis and a Model to Solve Double SpendingAttack,2019. 10.

blockchain mining pool security, in: 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE, pp.1–5,2019. 10.1109/ICCNC.2019.8685563

[175] Q. Hu, S. Wang, X. Cheng, A game theoretic analysis on block withholding attacks using the zero-determinant strategy, in: Proceedings of the International Symposium on Quality of Service, pp.1–10,2019. https://doi.org/10.1145/3326285.3329076

[176] S. Elliott, Nash equilibrium of multiple, non-uniform bitcoin block withholding attackers, in: 2019 2nd International Conference on Data Intelligence and Security (ICDIS), IEEE, pp. 144–151,2019. 10.1109/ICDIS.2019.00029

[177] W. Li, M. Cao, Y. Wang, C. Tang, F. Lin, Mining pool game model and nash equilibrium analysis for pow-based blockchain networks, IEEEAccess8,101049–101060,2020. 10.1109/ACCESS.2020.2997996

[178] S. Solat, M. Potop-Butucaru, ZeroBlock: Preventing selfish mining in bitcoin, CoRR abs/1605.02435arXiv:1605.02435,2016. https://doi.org/10.1145/3326285.3329076

[179] Wen, Y., Lu, F., Liu, Y., & Huang, X. Attacks and countermeasures on blockchains: A survey from layering perspective. Computer Networks, 191,107978,2021. https://doi.org/10.1016/j.comnet.2021.107978

[180] M. Saad, L. Njilla, C. Kamhoua, A. Mohaisen, Countering selfish mining in blockchains, in: 2019 International Conference on Computing,Networking and Communications (ICNC),IEEE,pp.360–364,2019. 10.1109/ICCNC.2019.8685577

[181] M. Saad, M.T. Thai, A. Mohaisen, POSTER: Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization, in: Proceedings of the 2018 on Asia Conference on Computer and Communications Security, ASIACCS '18, ACM, New York, NY, USA, pp. 809–811,2018. https://doi.org/10.1145/3196494.3201584

[182] S. Wu, Y. Chen, M. Li, X. Luo, Z. Liu, L. Liu, Survive and thrive: A stochastic game for DDoS attacks in bitcoin mining pools, IEEE/ACM Trans.Netw.28(2),874–887,2020. 10.1109/TNET.2020.2973410

18178/ijmlc.2020.10.2.942

[193] Zhang, Q., Lv, H., Ma, J., Li, J., & Zhang, J. Overview of Blockchain Data Privacy Protection. In Proceedings of the 2021 3rd Blockchain and Internet of Things Conference,pp. 53-58, 2021. https://doi.org/10.1145/3475992.3476000

[194] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal,8(2),881-888,2020. 10.1109/JIOT.2020.3008906

[195] Jiang, W., Li, H., Xu, G., Wen, M., Dong, G., & Lin, X. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI. Future Generation Computer Systems, 96, 185-195,2019. https://doi.org/10.1016/j.future.2019.01.026

[196] Wang, H., Wang, Y., Cao, Z., Li, Z., & Xiong, G. An overview of blockchain security analysis. In Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers 15,pp.55-72,2019. http://www.springer.com/series/7899

[197] Yaji, S., Bangera, K., & Neelima, B. Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications. In 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW),pp. 81-85, IEEE,2018. 10.1109/HiPCW.2018.8634280

[198] Haugum, T., Hoff, B., Alsadi, M., & Li, J. Security and Privacy Challenges in Blockchain Interoperability-A Multivocal Literature Review. In Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering,pp. 347-356,2022. https://doi.org/10.1145/3530019.353134

[199] Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 103633, 2023. https://doi.org/10.1016/j.jnca.2023.103633

[200] Da Xu, L., Lu, Y., & Li, L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473,2021. 10.1109/JIOT.2021.3060508

[201] Si, H., Sun, C., Li, Y., Qiao, H., & Shi, L. IoT information sharing security mechanism based on blockchain technology. Future generation computer systems, 101, 1028-1040, 2019. https://doi.org/10.1016/j.future.2019.07.036

[202] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 134,180-197,2019. https://doi.org/10.1016/j.jpdc.2019.08.005

[203] Zou, R., Lv, X., & Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing & Management, 58(4), 102604, 2021. https://doi.org/10.1016/j.ipm.2021.102604

[204] Dasgupta, D., Shrein, J. M., & Gupta, K. D. A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3,1-17,2019. https://doi.org/10.1007/s42786-018-00002-6

[205] Singh, S., Hosen, A. S., & Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, 13938-13959,2021. 10.1109/ACCESS.2021.3051602

[206] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. A survey on the security of blockchain systems. Future generation computer systems, 107,841-853,2020. https://doi.org/10.1016/j.future.2017.08.020

[207] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys(CSUR), 53(6),1-37,2020. https://doi.org/10.1145/3417987

[208] Shayan, M., Fung, C., Yoon, C. J., & Beschastnikh, I. Biscotti: A blockchain system for private and secure federated learning. IEEE Transactions on Parallel and Distributed Systems, 32(7),1513-1525,2020. 10.1109/TPDS.2020.3044223

[209] Al Amiri, W., Baza, M., Banawan, K., Mahmoud, M., Alasmary, W., & Akkaya, K. Privacy-preserving smart parking system using blockchain and private information retrieval. In 2019 international conference on smart applications, communications and networking (Smart Nets)

(pp. 1-6). IEEE,2019. 10.1109/SmartNets48225.2019.9069783

[210] Hassan, M. U., Rehmani, M. H., & Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512-529,2019. https://doi.org/10.1016/j.future.2019.02.060

[211] Sengupta, J., Ruj, S., & Bit, S. D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149,102481,2020. https://doi.org/10.1016/j.jnca.2019.102481

[212] Wan, J., Li, J., Imran, M., & Li, D.A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Transactions on Industrial Informatics, 15(6), 3652-3660, 2019. 10.1109/TII.2019.2894573

[213] Tian, Y., Wang, Z., Xiong, J., & Ma, J. A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics, 16(9), 6193-6202,2020. 10.1109/TII.2020.29659_75

[214] Luo, M., Zhou, J., & Yang, P. RATS: A regulatory anonymous transaction system based on blockchain. Journal of Parallel and Distributed Computing, 182,104751,2023. https://doi.org/10.1016/j.jpdc.2023.104751

[215] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. arXiv preprint arXiv:1904.03487,2019. https://doi.org/10.48550/arXiv.1904.03487

[216] Iqbal, M., & Matulevičius, R.Blockchain-based application security risks: a systematic literature review. In Advanced Information Systems Engineering Workshops: CAiSE 2019 International Workshops, Rome, Italy, Proceedings 31 (pp. 176-188). Springer InternationalPublishing,2019. https://doi.org/10.1007/978-3-030-20948-3_16

[217] Karbasi, A. H., & Shahpasand, S. A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks. Peer-to-peer networking and applications, 13, 1423-1441, 2020. https://doi.org/10.1007/s12083-020-00901-w

[218] Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. Journal of Network and Computer Applications, 176,102917,2021. https://doi.org/10.1016/j.jnca.2020.102917

[219] Pal, K.Privacy, security and policies: a review of problems and solutions with blockchain-based internet of things applications in manufacturing industry. Procedia Computer Science, 191, 176-183,2021. https://doi.org/10.1016/j.procs.2021.07.022

[220] Xiong, L., Li, F., Zeng, S., Peng, T., & Liu, Z. A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures. IEEE Access, 7, 125840-125853,2019. DOI: 10.1109/ACCESS.2019.2939368

[221] Li, W., Guo, H., Nejad, M., & Shen, C. C. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. IEEE access, 8, 181733-181743, 2020. DOI: 10.1109/ACCESS.2020.3028189

[222] Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M. K., Thomas, R., ... & Kim, T. H. Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things. IEEE Internet of Things Journal, 9(16), 14203-14215, 2020. DOI: 10.1109/JIOT.2020.3019074

[223] Mangla, S. K., Kazançoğlu, Y., Yıldızbaşı, A., Öztürk, C., & Çalık, A. A conceptual framework for blockchain-based sustainable supply chain and evaluating implementation barriers: A case of the tea supply chain. Business Strategy and the Environment, 31(8), 3693-3716,2022. https://doi.org/10.1002/bse.3027

[224] Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Computers & ElectricalEngineering , 90,106897,2021. https://doi.org/10.1016/j.compeleceng.2020.106897

[225] Ghosh, A., Gupta, S., Dua, A., & Kumar, N. Security of Cryptocurrencies in blockchain technology: State-of-

blockchain: Working, security analysis, privacy threats and potential applications. In 2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT) (Vol. 1, pp. 922-926). IEEE,2019. DOI: 10.1109/ICICICT46008.2019.8993210

[235] Sayadi, S., Rejeb, S. B., & Choukair, Z. Blockchain challenges and security schemes: a survey. In 2018 Seventh International Conference on Communications and Networking (ComNet) (pp.1-7).IEEE,2018. DOI: 10.1109/COMNET.2018.8621944

[236] Wang, Q., Ji, T., Guo, Y., Yu, L., Chen, X., & Li, P. TrafficChain: A blockchain-based secure and privacy-preserving traffic map. IEEE Access, 8,60598-60612,2020. DOI: 10.1109/ACCESS.2020.2980298

[237] Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In 2018 IEEE international conference on big data (big data) (pp. 1178-1187). IEEE,2018. DOI: 10.1109/BigData.2018.8622598

[238] Matzutt, R., Pennekamp, J., Buchholz, E., & Wehrle, K. Utilizing public blockchains for the sybil-resistant bootstrapping of distributed anonymity services. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security,pp. 531-542,2020. https://doi.org/10.1145/3320269.3384729

[239] Ghesmati, S., Fdhila, W., & Weippl, E. SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Privacy Techniques. In Proceedings of the 17th International Conference on Availability, Reliability and Security pp.1-14,2022. https://doi.org/10.1145/3538969.3538971

[240] Chen, X., Shen, J., Cao, Z., & Dong, X. A blockchain-based privacy-preserving scheme for smart grids. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology,pp.120-124,2020. https://doi.org/10.1145/3390566.3391667

[241] Li, B., & Wang, Y. RZKPB: a privacy-preserving blockchain-based fair transaction method for sharing economy. In 2018 17th IEEE international conference on trust, security and privacy in computing and com-

art, challenges and future prospects. Journal of Network and Computer Applications, 163,102635,2020. https://doi.org/10.1016/j.jnca.2020.102635

[226] Alizadeh, M., Andersson, K., & Schelen, O.A survey of secure internet of things in relation to blockchain. Journal of Internet Services and Information Security (JISIS), 10(3), 47-75, 2020. DOI: 10.22667/JISIS.2020.08.31.047

[227] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. A survey on security and privacy issues of bitcoin. IEEE communications surveys & tutorials, 20(4),3416-3452,2018. DOI: 10.1109/COMST.2018.2842460

[228] Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060, 2019. https://doi.org/10.1002/nem.2060

[229] Feng, Q., He, D., Zeadally, S., & Liang, K. BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Transactions on Industrial Informatics, 16(6), 4146-4155, 2019. DOI: 10.1109/TII.2019.2948053

[230] Zhou, B., Li, H., & Xu, L. An authentication scheme using identity-based encryption & blockchain. In 2018 IEEE Symposium on computers and communications (ISCC) (pp. 00556-00561).IEEE,2018. DOI: 10.1109/ISCC.2018.8538446

[231] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal, 6(5), 8114-8154,2019. DOI: 10.1109/JIOT.2019.2922538

[232] Wang, J., Li, M., He, Y., Li, H., Xiao, K., & Wang, C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. Ieee Access, 6, 17545-17556, 2018. DOI: 10.1109/ACCESS.2018.2805837

[233] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. A survey on privacy protection in blockchain system. Journal of network and computer applications, 126, 45-58, 2019. https://doi.org/10.1016/j.jnca.2018.10.020

[234] Soni, S., & Bhushan, B. A comprehensive survey on

100192, 2023. https://doi.org/10.1016/j.health.2023.100192

[250] Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Transactions on Industrial Informatics, 15(6), 3548-3558,2019.DOI: 10.1109/TII.2019.2893433

[251] Nasr Esfahani, M., Ghahfarokhi, B. S., & Etemadi Borujeni, S. Blockchain-based end-to-end privacy-preserving scheme for IoT-based healthcare systems. The Journal of Supercomputing, 1-61, 2023. https://doi.org/10.1007/s11227-023-05522-7

[252] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326, 2019. https://doi.org/10.3390/s19020326

[253] Pal, K. Securing the Internet of Things Applications Using Blockchain Technology in the Manufacturing Industry. In IoT Protocols and Applications for Improving Industry, Environment, and Society (pp. 234-273). IGI Global, 2021. DOI: 10.4018/978-1-7998-6463-9.ch011

[254] de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. Sensors, 20(24), 7171. https://doi.org/10.3390/s20247171

[255] Oksuz, O. (2024). A System For Storing Anonymous Patient Healthcare Data Using Blockchain And Its Applications. The Computer Journal, 67(1),18-30 https://doi.org/10.1093/comjnl/bxac155

[256] Saad, M., Bhutta, M. R., Kim, J., & Chung, T. S. (2024). A Framework for Enhancing Privacy and Anonymity in Blockchain-Enabled IoT Devices. Computers, Materials & Continua, 78(3). DOI: 10.32604/cmc.2024.0471_32

[257] Bhushan, B., & Sharma, N. (2021). Transaction privacy preservations for blockchain technology. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 2 (pp. 377-393). Springer Singapore. https://doi.org/10.1007/978-981-15-5148-2_34

[258] https://www.immunebytes.com/blog/munications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 11641169).IEEE,2018.DOI:10.1109/TrustCom/BigDataSE.2018.00161

[242] Bao, S., Cao, Y., Lei, A., Asuquo, P., Cruickshank, H., Sun, Z., & Huth, M. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. IEEE Access, 7, 80390-80403, 2019. DOI: 10.1109/ACCESS.2019.2921605

[243] Rahmadika, S., & Rhee, K. H. Toward privacy-preserving shared storage in untrusted blockchain P2P networks. Wireless communications and mobile computing, 2019. https://doi.org/10.1155/2019/6219868

[244] Zhu, K., Chen, Z., Yan, W., & Zhang, L. Security attacks in named data networking of things and a blockchain solution. IEEE Internet of Things Journal, 6(3), 4733-4741,2018. DOI: 10.1109/JIOT.2018.2877647

[245] Sarier, N. D. (2018). Privacy preserving biometric identification on the bitcoin blockchain. In Cyberspace Safety and Security: 10th International Symposium, CSS 2018, Amalfi, Italy, Proceedings 10 (pp. 254-269). Springer International Publishing, ,2018. https://doi.org/10.1007/978-3-030-01689-0_20

[246] Whig, P., Velu, A., & Nadikattu, R. R. Blockchain platform to resolve security issues in IoT and smart networks. In AI-Enabled Agile Internet of Things for Sustainable FinTech Ecosystems (pp. 46-65). IGI Global, 2022. DOI: 10.4018/978-1-6684-4176-3.ch003

[247] Attarian, R., & Hashemi, S. An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. Computer Networks, 190, 107976, 2021. https://doi.org/10.1016/j.comnet.2021.107976

[248] Chen, H., Pendleton, M., Njilla, L., & Xu, S. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR), 53(3), 1-43, 2020. https://doi.org/10.1145/3391195

[249] Hiwale, M., Walambe, R., Potdar, V., & Kotecha, K. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. Healthcare Analytics,

pseudonymity-and-anonymity-be-
untraceable-in-the-blockchain-world/

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2025, Volume 23, Number 1 (pp. 64–96)
https://monadi.isc.org.ir

A systematic review of the literature on security and privacy and improving anonymity in the blockchain network

Fatemeh Charlank Bakhtiari * and Abbas Ghaemi Bafghi

Department of Computer Science, Faculty of Engineering, Ferdowsi University, Mashhad, Iran

ARTICLE INFO.

Keywords:
Blockchain, Privacy, Anonymity, Security

Type: Review paper

With the rapid development of digital technologies, the need for new solutions to protect privacy and data security has increased. One technology that has attracted much attention is blockchain, a distributed ledger known for its features like transparency, decentralization, and security, particularly regarding privacy. However, this technology can pose a threat to users' privacy, especially concerning the origin, destination, and flow of cryptocurrency transactions. Therefore, anonymity in blockchain transactions and the protection of users' privacy are key aspects of this technology. In this paper, we review the security features of blockchain, which include integrity, transparency, traceability, honesty, anonymity, and immutability. Each feature plays a fundamental role in maintaining the security and integrity of blockchain-based systems. Also, the problems in protecting privacy in permissionless blockchains have been examined. For this purpose, a systematic review of the existing articles and research in this field has been reviewed and categorized. A systematic literature review is an efficient research tool. It includes three main stages: planning, implementation, and reporting. In the planning phase, research questions are extracted and appropriate databases are selected for searching. In the implementation phase, data is extracted from various articles and publications, and in the reporting phase, the results are presented in detail. Finally, this research method answers fundamental questions in various blockchain fields, including privacy, anonymity, and threats. The four main research questions are: 1) What are the characteristics, advantages, and disadvantages of different types of blockchains? 2) What are the concepts of anonymity, pseudo-anonymity, privacy, and confidentiality, and how are privacy practices implemented? 3) What are the vulnerabilities and threats to privacy and anonymity? 4) What methods can address threats to privacy and anonymity?

To carry out this research, a detailed plan was developed to search for and collect scientific articles and resources from reputable databases, including IEEE Xplore, ACM, ScienceDirect, Springer, and Google Scholar. The searches were conducted using keywords like "blockchain," "privacy," "anonymity," and "security." A review was conducted of articles published between 2018 and 2023. Based on the established inclusion and exclusion criteria, duplicate studies were eliminated, refining the final results.

The initial stage of searching using the keyword "Blockchain" in various databases identified numerous articles from diverse fields such as the Internet of Things, healthcare, smart contracts, banking and finance, and other fields. After reviewing the titles, keywords, and abstracts, it was determined that a significant challenge in this field is ensuring the privacy and security of users' identities in the blockchain. In the next stage, the keywords "Blockchain," "Privacy," "Anonymity," and "Security" were used to search and identify more articles. The article filtering process was divided into three stages. In the first stage, the initial review of titles and keywords reduced the number

* Corresponding author
Email addresses: fatemeh.bakhtiari1126@gmail.com (Fatemeh Charlank Bakhtiari), ghaemib@um.ac.ir (Abbas Ghaemi Bafghi)
© 2025 ISC. All rights reserved.

of articles from 1,233 to 947. In the second stage, after reviewing the abstracts, 404 relevant articles were identified. Finally, in the third stage, the full texts of the remaining articles were read, and the same number of articles was selected for more accurate information extraction.

The distribution of articles was analyzed in three ways: year of publication, source of publication, and topic. This survey indicates that the scientific community's attention has fluctuated, increasing and then decreasing until 2019. IEEE and ScienceDirect have contributed the most to this topic, with 328 and 251 papers, respectively, while ACM has contributed the least. Figures 1, 2, and 3 demonstrate an increasing use of blockchain technology across various fields, including cybersecurity, privacy, and anonymity.

Answer to the first research question: Blockchains can be classified into three categories: public (permissionless), private (permissioned), and consortium. Public chains like Bitcoin and Ethereum offer high transparency and decentralized security, enabling participation from everyone. The need for widespread consensus leads to decreased efficiency and increased energy consumption. In contrast, private chains allow access only to specific individuals or organizations and are suitable for corporate applications with high efficiency, faster processing, and greater control over data, but may lead to centralization and are vulnerable to changes. Consortium chains blend elements of both public and private blockchains. They maintain a balance between transparency and privacy by being managed by a group of trusted organizations. Nonetheless, this management approach can complicate processes because it necessitates coordination among the various network members.

Answer to the second research question: Anonymity, pseudo-anonymity, privacy, and confidentiality are key concepts in blockchain security. Anonymity refers to the concealment of users' identities, while pseudo-anonymity refers to the use of pseudonymous addresses that still allow indirect identification of users. Privacy gives users control over their personal information and transactions, while confidentiality protects against unauthorized disclosure of that information. Although these concepts are related, they have distinct differences. Anonymity can improve user security but may also foster abuse, while privacy mainly focuses on the management of user data. To preserve privacy on the blockchain, methods such as one-time addresses (generating a new address for each transaction), group signatures (allowing an individual's identity to remain hidden among a group of users), zero-knowledge proofs (which allow a claim to be verified without revealing information), and transaction mixers (which combine transaction data to prevent tracking) are used, each of which offers different levels of security and efficiency. The following is a comparison of various privacy methods and their key features, including security level, efficiency, level of anonymity, and implementation challenges. Some methods, such as zero-knowledge proofs, are highly secure but computationally expensive, while methods such as one-time addresses are simpler but provide a lower level of anonymity. This table helps you decide which method is best for your needs.

Answer to the third research question: Blockchain threats and vulnerabilities are categorized into nine main groups: application attacks, consensus attacks, cryptanalysis, double spending, identity privacy, network attacks, smart contracts, mining attacks, and unclassified attacks, each of which threatens user security and privacy differently. Network attacks such as sibyl attacks, denial of service, and data interception are the most common threats that can expose user information and reduce network performance. Consensus and cryptanalysis attacks can disrupt transaction security and put user data at risk. On the other hand, double spending attacks and smart contract vulnerabilities (such as the DAO attack) may lead to financial fraud and asset theft. Also, identity privacy attacks such as impersonation and wallet information leakage can reveal user identities. Addressing these threats necessitates the use of stronger cryptography, enhanced consensus mechanisms, and the application of privacy-preserving methods. Additionally, the focus of the scientific community highlights that network attacks are particularly critical due to their direct impact on the security and performance of blockchain technology. To address the fourth research question, various security solutions have been evaluated to counter threats to the chain of custody, tailored to the specific type of attack. Self-organizing maps, access control layer encryption, and rigorous transaction validation are employed to combat application and consensus attacks. Network attacks and cryptanalysis can be mitigated through data encryption, traffic analysis, security protocols like BGPsec, and strong digital signatures. To prevent double spending, techniques such as utilizing nonces in transactions and combining digital signatures are employed. Smart contracts are secured through dynamic rules, secure payment methods, and smart contracts. Also, to prevent user identity extraction and general threats, techniques such as zero-knowledge proofs, zero-blocks, anonymity, and intrusion detection are implemented in the network, which plays an important role in maintaining user security and privacy.

This study can be used as a research basis to identify open issues and create new research directions in the future. The statistical data presented in tables and graphs indicate the positive impact of

the blockchain on improving the performance of information systems and reducing costs. The findings of this study can guide the development of secure blockchain-based systems in the future and provide new directions for further research.