JCWR2020

کنفرانس بین المللی وب پژوهی
ایران، تهران، ۲۷ خرداد ۱۳۹۹

# A Servey on Applications and Challenges of Blockchain for Internet of Things

Fatemeh Motie Shirazi[*1], Reza Bakhtiari Shohani[1], Seyed Akbar Mostafavi[2]

[1] Master of Computer Engineering, Yazd University, Yazd, Iran
motie@stu.yazd.ac.ir, rezabakhtiari@yazd.ac.ir

[2] PhD Student of Computer Engineering, Yazd University, Yazd, Iran
a.mostafavi@yazd.ac.ir

## Abstract

This article provides a comprehensive literature review of blockchain protocols for IoT. First, we describe the blockchain and summarize the research involved with blockchain technologies. Then, we provide an overview of the application areas of blockchain technologies in IoT, for example, the Internet of Vehicles, Energy Internet, Cloud Internet, Edge Computing and more In addition, we provide a categorization of threat models that are divided into five categories by blockchain protocols in IoT networks, namely: identity-based attacks, manipulation-based attacks, coding attacks, Credit-based and service-based attacks. In addition, we provide a peer-to-peer classification and comparison of modern methods for securing and protecting the privacy of blockchain technologies with respect to blockchain model, specific security objectives, performance, constraints, computational complexity, communications. Based on current research, we highlight emerging research challenges and discuss possible future research directions in blockchain technologies for IoT.

**Keywords:** Internet of Things (IoT), security, blockchain.

JCWR2020

کنفرانس بین المللی وب پژوهی
ایران، تهران، ۲۷ خرداد ۱۳۹۹

# مروری بر کاربردها و چالش‌های بلاک چین در اینترنت اشیاء

فاطمه مطیع شیرازی[۱]، رضا بختیاری شوهانی[۲]، سید اکبر مصطفوی[۳]

[۱] دانشجوی کارشناسی ارشد مهندسی کامپیوتر، گروه مهندسی کامپیوتر، دانشگاه یزد، یزد،
motie@stu.yazd.ac.ir

[۲] دانشجوی کارشناسی ارشد مهندسی کامپیوتر، گروه مهندسی کامپیوتر، دانشگاه یزد، یزد،
rezabakhtiari@yazd.ac.ir

[۳] استادیار، گروه مهندسی کامپیوتر، دانشگاه یزد، یزد
a.mostafavi@yazd.ac.ir

## چکیده

**این مقاله، یک مرور ادبی جامع در مورد پروتکل‌های بلاک چین موجود برای شبکه‌های اینترنت اشیاء (IoT)، ارائه می‌دهد. ابتدا به توصیف بلاک چین‌ها و خلاصه کردن پژوهش‌های انجام‌شده که با فن‌آوری‌های بلاک چین سروکار داشته‌اند، می‌پردازیم. سپس، یک توضیح کلی در مورد حوزه‌های کاربردی فن‌آوری‌های بلاک چین در IoT ارائه می‌دهیم، برای مثال، می‌توان اینترنت وسایل نقلیه، اینترنت انرژی، اینترنت ابری، رایانش لبه‌ای و غیره را نام برد. علاوه بر آن، یک دسته‌بندی در مورد مدل‌های تهدید ارائه می‌دهیم که توسط پروتکل‌های بلاک چین در شبکه‌های IoT، به پنج دسته تقسیم‌شده‌اند، یعنی: حمله‌های برپایه هویت، حمله‌های برپایه دستکاری، حمله‌های تحلیل رمزی، حمله‌های برپایه اعتبار و حمله‌های برپایه خدمات. علاوه بر آن، یک رده‌بندی و مقایسه نظیر به نظیر روش‌های نوین برای امنیت و حفظ محرمانگی فن‌آوری‌های بلاک چین با توجه به مدل بلاک چین، اهداف امنیتی خاص، عملکرد، محدودیت‌ها، پیچیدگی محاسبات، ارتباطات، ارائه می‌دهیم. بر اساس پژوهش فعلی، چالش‌های پژوهشی هنوز مطرح را خاطرنشان می‌کنیم و در مورد جهت‌های پژوهشی آتی احتمالی در فن‌آوری‌های بلاک چین برای IoT، بحث می‌کنیم.**

## کلمات کلیدی

**اینترنت اشیاء، امنیت، بلاک چین**

## ۱- مقدمه

در چند سال اخیر، شاهد ظرفیت و پتانسیل اینترنت اشیاء در ارائه خدمات مهیج در چندین بخش، از رسانه‌های اجتماعی، کسب‌وکار، حمل‌ونقل هوشمند و شهرهای هوشمند تا صنایع بوده‌ایم [۱]. IoT همیشه و به‌صورت یکپارچه ادوات و وسایل ناهمگن را با کارکردهای مختلف در شبکه‌های انسان‌محور و ماشین محور به هم متصل می‌کند تا الزامات نوظهور بخش‌های ذکرشده در قبل را برآورده کند. بااین‌حال، تعداد قابل‌توجهی از ادوات متصل شده به هم و ترافیک داده هنگفت، در برآورده کردن نیازهای «کیفیت خدمات» (QoS) به خاطر محدودیت‌های محاسباتی، ذخیره‌ای و پهنای باند دستگاه‌های IoT به یک تنگنا تبدیل‌شده است. همین اواخر ، بلاک چین [۲]، که یک تغییر الگو بوده است، همه کاربردهای عمده IoT را با ممکن ساختن یک محیط غیرمتمرکز با تراکنش‌های ناشناس و مطمئن، متحول کرده است. سیستم‌های IoT در ترکیب با فن‌آوری بلاک چین از هزینه عملکردی کمتر، مدیریت منابع غیرمتمرکز، مقاومت در برابر تهدیدات و حمله‌ها و غیره، سود برده است. بنابراین همگرایی IoT و فن‌آوری بلاک چین، هدفش غلبه بر چالش‌های قابل‌توجه محقق سازی بستر IoT در آینده نزدیک است[۳].

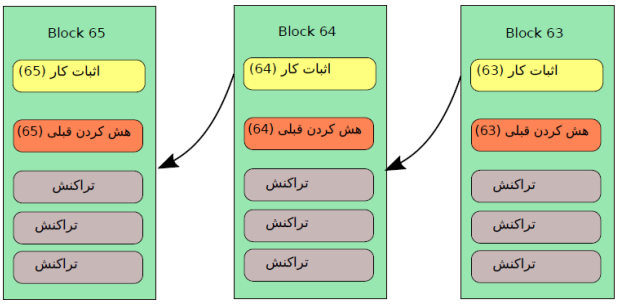
بلاک چین، که یک فن‌آوری دفتر حساب عمومی فقط الحاقی توزیع‌شده است، در ابتدا برای ارزهای رمزی برای مثال Bitcoin در نظر گرفته‌شده بود. در سال ۲۰۰۸، ساتوشی ناکاموتو [۴]، مفهوم بلاک چین را معرفی کرد که در چند سال اخیر به‌عنوان یک فن‌آوری نظیر به نظیر نوظهور (P2P) برای رایانش توزیع‌شده و اشتراک داده غیرمتمرکز، توجه زیادی را به خود جلب کرد. به خاطر به‌کارگیری فن‌آوری رمزنگاری و بدون یک کنترل متمرکز بازیگر یا یک ذخیره داده متمرکز، بلاک چین می‌تواند از حمله‌هایی که می‌خواهند بر سیستم کنترل وارد کنند، جلوگیری کند. بعداً، در سال ۲۰۱۳،

Ethereum، که یک حالت ماشین برپایه تراکنش بود، برای برنامه‌ریزی و برنامه‌نویسی فن‌آوری‌های بلاک چین، ارائه شد. جالب اینکه، به خاطر ویژگی‌های منحصربه‌فرد و جذابش مانند: محرمانگی تراکنشی، امنیت، غیرقابل تقلید بودن داده‌ها، قابلیت حسابرسی، یکپارچگی، تصدیق، شفافیت سیستم و تحمل خطا، بلاک چین در چندین بخش فراتر از ارز رمزی، بکار گرفته‌شده است[۵].

همان‌گونه که در شکل (۱) نشان داده‌شده، ساختار بلاک چین از یک دنباله یا سلسله بلوک تشکیل‌شده که باهم به‌وسیله مقادیر هش خود، متصل شده‌اند. در شبکه بلاک چین، یک دفتر حساب عمومی، تراکنش‌های امضای دیجیتالی شده کاربران در یک شبکه P2P را نگهداری می‌کند. به‌طورکلی، یک کاربر دو کلید دارد: یک کلید عمومی برای کاربران دیگر جهت رمزگذاری و یک کلید خصوصی برای قرائت یک پیام رمزگذاری شده. از جنبه بلاک چین، کلید خصوصی برای امضای تراکنش بلاک چین استفاده می‌شود و کلید عمومی، آدرس یکتا را نشان می‌دهد. رمزنگاری نامتقارن برای رمزگشایی پیام رمزنگاری‌شده توسط کلید عمومی متناظر، استفاده می‌شود. در مرحله اول، یک کاربر یک تراکنش را با استفاده از کلید خصوصی خود امضا می‌کند و آن را به همتایان خود منتشر می‌کند. بعدازاینکه همتایان تراکنش امضاشده را دریافت کردند، تراکنش را تأیید اعتبار می‌کنند و آن را بر روی شبکه منتشر می‌کنند. همه طرف‌هایی که در تراکنش دخیل هستند، به‌صورت متقابل و دوبه‌دو، تراکنش را اعتبار یابی می‌کنند تا به یک توافق اجماع برسند. بعدازاینکه یک اجتماع توزیع‌شده حاصل شد، گره ویژه، که کاوشگر نامیده می‌شود، آن تراکنش معتبر را در یک بلوک دارای برچسب زمانی، شامل می‌کند. این بلوک که به‌وسیله کاوشگر شامل شده است، دوباره به شبکه منتشر می‌شود. بعد از اعتبارسنجی بلوک منتشرشده، که حاوی تراکنش است و همچنین مطابقت دهی هش آن با بلوک قبلی در بلاک چین، بلوک انتشار شده به بلاک چین، اضافه می‌شود[۶].

بار اساس مدیریت داده‌ها و نوع کاربردها، بلاک چین را می‌توان به خصوصی (اجازه‌ای) یا عمومی (بدون مجوز)، تقسیم کرد. هر دودسته، غیرمتمرکز هستند و یک سطح معین از ایمنی در برابر کاربران خطادار یا بدخواه برای دفتر حساب ، فراهم می‌کند. تفاوت‌های اصلی بین بلاک چین‌های خصوصی و عمومی در اجرای پروتکل اجتماع، حفظ دفتر حساب و احراز هویت برای پیوستن به شبکه P2P می‌باشند. مثال‌های تفصیلی این کلاس‌ها در [۷] نشان داده‌شده‌اند. درزمینهٔ IoT، بلاک چین‌ها را می‌توان بر اساس احراز هویت و تأیید، دسته‌بندی کرد. در یک بلاک چین خصوصی، مقام معتمد مرکزی که احراز هویت و تأیید را مدیریت می‌کند، کاوشگران را انتخاب می‌کند. از سوی دیگر، در یک بلاک چین عمومی (به‌طورکلی، بدون مجوز)، مداخله هیچ شخص ثالث برای انتخاب کاوشگر و الحاق یک کاربر جدید به شبکه بلاک چین وجود ندارد.

اخیراً حجم هنگفتی سرمایه‌گذاری از جانبه صنایع صورت گرفته است [۸] و همچنین یک توجه قابل‌ملاحظه‌ای از جانب دانشگاهیان برای حل چالش‌های پژوهشی عمده در فن‌آوری‌های بلاک چین صورت گرفته است.




**شکل (۱).ساختار بلاک چین**

برای مثال، پروتکل‌های اجماع، بلوک‌های سازنده اصلی فن‌آوری‌های بلاک چین می‌باشند، بنابراین تعهدی‌هایی که پروتکل‌های اجتماع را هدف قرار می‌دهند، یک مسئله پژوهشی قابل‌توجه درزمینهٔ بلاک چین است. علاوه بر آن، چنگال‌های بلاک چین تهدیداتی برای پروتکل‌های اجماع بلاک چین به وجود می‌آورند. علاوه بر آن، مشاهده می‌شود که آسیب‌پذیری برای یک بلاک چین جدید، حدود ۵۱٪ است [۹]. درعین‌حال، نگهداری چندین بلاک چین نیاز به حجم هنگفتی مصرف برق و انرژی دارد.

چندین مقاله مروری مرتبط که جنبه‌های مختلف فن‌آوری بلاک چین را پوشش داده‌اند، انجام‌شده است. برای مثال، یک نمای کلی مختصر از بلاک چین برای بیت کوین در[۱۱] به بحث گذاشته‌شده است. اما، این مطالعات با توجه به بحث تفصیلی در مورد چالش‌های پژوهشی در بلاک چین، بسیار محدود هستند. علاوه بر آن، سانکار و همکاران [۱۰]، به‌اختصار، امکان‌پذیری پروتکل‌های اجماع مختلف در بلاک چین را ارائه داده‌اند. نگرش‌های تفصیلی در مورد بیت کوئین در ارائه‌شده‌اند. اخیراً، مطالعات مروری [۷]، نمایی کلی از کاربردهای IoT برپایه بلاک چین (BIoT)، را ارائه داده‌اند. جنبه‌های امنیت و حریم خصوصی در [۱۲، ۱۳] برای بیت کوئین که یکی از کاربردهای بلاک چین است، ارائه‌شده‌اند.

## ۲- مطالب اصلی

در این بخش ابتدا پس‌زمینه مختصری در رابطه با حیطه‌های کاربردی فن‌آوری بلاک چین در IoT و سپس مسائل حل‌نشده و چالش‌های پژوهشی ارائه می‌شود.

### ۲-۱- کاربردهای بلاک چین برای IoT

فن‌آوری بلاک چین را می‌توان به‌طور مؤثر در تقریباً همه حیطه‌های IoT بکار گرفت. توجه داشته باشید که لزوماً نیاز نیست از بلاک چین در زمینه‌های خاص استفاده کرد (برای مثال، هنگامی‌که نهادهای IoT به یک شخص ثالث اطمینان دارند).

مسائل مقیاس‌پذیری که ممکن است به خاطر افزایش تعداد گره‌های شرکت‌کننده به وجود بیاید و بنابراین اندازه بلوک، بخصوص برای G۵ و اینترنت وسایل نقلیه، که می‌توانند بر مصرف توان ، انتشار شبکه و ازدحام

شبکه تأثیر بگذارند باید هنگام پیشنهاد فن‌آوری بلاک چین برای چنین سیستم‌هایی مورد ملاحظه قرار گیرد.

**اینترنت اشیاء مراقبت سلامت:** استفاده از IoT در مراقبت سلامت، بازخورد دادن و تغذیه سیستم‌های مراقبت سلامت با داده‌های بالینی مرتبط با بیماران، خانواده‌هایشان، دوستانشان و همچنین فراهم‌کنندگان مراقبت سلامت را اجازه داده است. داده‌ها، که به رکوردهای پزشکی الکترونیکی (EMR ها) معروف هستند، به‌وسیله ارائه‌دهنده مراقبت سلامت مسئول، ذخیره می‌شود. برای تسهیل قابل‌حمل بودن داده‌های بیمار، رکوردهای سلامت الکترونیکی (EHR ها) وجود دارند که ساختار داده‌ای غنی‌تری نسبت به EMR ها دارند. بر اساس ایده پایگاه داده آنلاین توزیع‌شده، اسپوسیتو و همکاران [۱۴] ، طراحی رح برپایه بلاک چین برای IoT در مراقبت سلامت را پیشنهاد کردند. در یک مدل از بلاک چین کنسرسیومی، یک بلوک جدید ایجاد می‌شود و توزیع می‌شود هنگامی‌که داده‌های مراقبت سلامت جدید خلق می‌شوند. برای حفظ حریم خصوصی بیماران و حفظ تقلیدناپذیری EHR ها، گائو و همکاران [۱۵] یک طرح امضای برپایه صفات به نام MA-ABS ارائه دادند که از چندین مقام یا اختیار استفاده می‌کند. طرح MA-ABS از فن‌آوری بلاک چین استفاده می‌کند و می‌تواند در برابر N-1 حمله‌های مقامات فاسد، مقاومت کند. علاوه بر آن، MA-ABS، در قرار گرفتن در برابر حمله اعلام گزینشی، غیرقابل تقلب است. بنابراین، لیانگ و همکاران [۱۶] از شبکه بلاک چین در کاربردهای مراقبت سلامت موبایل برای حفاظت از یکپارچگی ، حسابرسی در ادامه یا بررسی، استفاده کرده‌اند.

**اینترنت اشیاء در عصر 5G:** در عصر IoT، G۵ ، یک جامعه کاملاً متحرک و متصل‌به‌هم را برای میلیاردها اشیاء متصل، فراهم می‌کند. برای حل مسائل حریم خصوصی در محیط ارتباطات ناهمگن G۵، فان و همکاران [۱۷] یک طرح حفظ‌کننده حریم خصوصی و اشتراک داده برپایه بلاک چین پیشنهاد دادند. بر اساس ایده افزودن بلوک‌ها به بلاک چین، هر بلوک جدید به‌وسیله مقدار هش خود به بلاک چین متصل می‌شود. توجه داشته باشید که مقدار هش قبلی را می تونان از هدر بلوک فهمید.

**اینترنت وسایل نقلیه:** اینترنت وسایل نقلیه (IoV)یک مفهوم نوظهور است که تلفیق و تجمیع وسایل نقلیه و تبدیل به عصر جدید IoT را جهت برقراری ارتباطات هوشمند بین وسایل نقلیه و شبکه‌های ناهمگن مانند ماشین به ماشین، خودرو به جاده، خودرو به انسان، خودرو به حسگر و خودرو به همه‌چیز، ممکن می‌سازد. اما، تعدادی مقاله جدید، تلاش کرده‌اند از فن‌آوری بلاک چین برای IoV استفاده کنند. بر اساس مدل امنیت غیرمتمرکز، هوانگ و همکاران [۵] یک مدل اکوسیستم بلاک چین، به نام LNSC را برای مدیریت وسایل نقلیه الکتریکی و مجموعه شارژ کنندگی، پیشنهاد کردند. مدل LNSC از رمزنگاری منحنی بیضوی (ECC) برای محاسبه توابع هش در خودروهای الکتریکی و ایستگاه‌های شارژ استفاده می‌کند. برای اجتناب و جلوگیری از ردیابی مکان در IoV، دوری و همکاران [۱۸] یک معماری حفظ‌کننده حریم خصوصی غیرمتمرکز را پیشنهاد داد که در آن گره‌های لایه اصلی، بلاک چین را مدیریت می‌کنند. علاوه بر آن، هش ذخیره پشتیبان، در بلاک چین ذخیره می‌شود. لی و همکاران، [۱۹] بدون مدیریت از جانب مدیر مرکزی، یک مدیریت کلید دینامیک برپایه بلاک چین برای سیستم‌های ارتباطاتی خودرویی، پیشنهاد کردند. بر اساس یک ساختار بلاک چین غیرمتمرکز، مقامات شخص ثالث، حذف می‌شوند و فرآیندهای انتقال کلید، توسط شبکه مدیر امنیتی، تأیید و احراز هویت می‌شوند. علاوه بر آن، کانگ و همکاران [۲۰] یک سیستم معامله برق P2P به نام PETCON معرفی کردند تا عملیات‌های تفصیلی معامله برق P2P محلی را نشان دهند. با استفاده از روش بلاک چین کنرسیومی، سیستم PETCON می‌تواند به‌صورت عام، رکوردهای تراکنش را بدون اتکا به یک شخص ثالث معتمد، حسابرسی و اشتراک‌گذاری کند. برای حل مسائل انتقال اعلام‌های معتبر بدون آشکارسازی هویت کاربران، لی و همکاران [۲۱] یک طرح حفظ‌کننده حریم خصوصی، به نام CreditCoin ، برای ارسال اعلام‌ها به‌صورت گمنام در IoV پیشنهاد کردند. طرح CreditCoin از بلاک چین از طریق یک پروتکل تجمیع اعلام وسایل نقلیه ناشناس برای اعتمادسازی در ارتباطات IoV، استفاده می‌کردن. برای ارزیابی قابل‌اطمینان بودن داده‌ها در IoV، یانگ و همکاران [۲۲] یک سیستم اعتبار برپایه بلاک چین پیشنهاد کردند که می‌تواند در مورد پیام‌های دریافتی به صورت واقعی یا دروغین بر اساس مقادیر اعتبار فرستنده، قضاوت کند.

**اینترنت انرژی:** اینترنت انرژی (IoE)، یک مفهوم نوین برای افزایش قابل‌مشاهده بودن مصرف انرژی در شبکه هوشمند (اسمارت گرید)، ارائه می‌دهد. بر اساس این فن‌آوری بلاک چین نوظهور، گائو و همکاران [۱۵]، یک سیستم نظارت بر شبکه هوشمند به نام GridMonitoring را برای تضمین شفافیت، اثبات و تقلیدناپذیری، معرفی کردند. سیستم GridMonitoring بر اساس چهار لایه است، یعنی ۱) لایه ثبت و تصدیق، ۲) کنتور هوشمند ۳) گره‌های پردازش و اجتماع و ۴) پردازش داده‌ها بر روی شبکه هوشمند. در سیستم‌های قدرت مدرن، لیانگ و همکاران [۱۶] یک چارچوب حفاظت از داده‌ها بر اساس بلاک چین توزیع‌شده پیشنهاد کردند که می‌تواند در برابر دستکاری داده‌ها، از جانب مهاجمان سایبری (برای مثال، حمله‌های تزریق داده‌های کاذب) مقاومت کند. برای تضمین دقت و صحت داده‌ها، چارچوب لیانگ از مکانیزم اجماع استفاده می‌کند، که این مکانیزم به‌صورت خودکار توسط هر گره پیاده‌سازی می‌شود و مشخصات نماینده دارد یعنی ۱) تنظیم فرکانس یا تعداد دفعات بروز رسانی کلید خصوصی/عمومی ۲) تولید بلوک ۳) انتخاب کاوشگر و ۴) آزادسازی حافظه کنتور (سنجشگر) به‌صورت دوره‌ای. برای تجارت انرژی ایمن در «اینترنت اشیاء صنعتی» (IIoT)، لی و همکاران [۱۹]، بلاک چین انرژی را معرفی کردند که بر اساس فن‌آوری بلوک چین کنسرسیومی و بازی استاکلبرگ است. آیتشان و سوتینوویچ [۲۳] یک سیستم معامله انرژی غیرمتمرکز خصوصی برپایه توکن برای انرژی شبکه هوشمند غیرمتمرکز شده، که برای IoE قابل پیاده‌سازی است، ارائه کردند.

**ادوات اینترنت اشیاء:** در ادوات اینترنت اشیاء، مهاجمان به دنبال واردکردن داده‌های ادوات IoT با استفاده از کدهای بدخواه در بدافزار بخصوص بر روی پلتفرم منبع باز آندروید هستند. با بهره‌گیری از روش تحلیل آماری، گائو و همکاران [۱۵] یک سیستم آشکارسازی بدافزار بر اساس مکانیزم کنسرسیومی، به نام CB-MDEE معرفی کردند که از آشکارسازی زنجیره کنسرسیوم به‌وسیله اعضای آزمایشی و زنجیره عمومی به‌وسیله کاربران، استفاده می‌کند. سیستم CB-MDEE از یک روش مقایسه فازی و چندین کارکرد علامت‌گذاری (مارکینگ) استفاده می‌کند تا نرخ مثبت کاذب را کاهش دهد و توانایی آشکارسازی انواع بدافزارها را بهبود بخشد. برای حفاظت از ادوات گنجانده‌شده در IoT، لی و همکاران [۱۹] از یک طرح به‌روز سازی میان‌افزار بر اساس فن‌آوری بلاک چین، استفاده کردند که در آن ادوات تعبیه‌شده دو حالت عملکردی مختلف دارند، یعنی ۱) پاسخ از یک گره تأیید تا یک گره درخواست و ۲) پاسخ از یک گره پاسخ به یک گره درخواست.

**مدیریت دسترسی در IoT:** برای مدیریت ادوات IoT، نووو [۲۴] یک سیستم کنترل دسترسی توزیع‌شده با استفاده از فن‌آوری بلاک چین را پیشنهاد کرد. معماری این سیستم از ۶ جزء تشکیل‌شده، یعنی ۱) شبکه‌های حسگر بی‌سیم ۲) مدیران، ۳) گره کارگزار ۴) قرارداد هوشمند ۵) شبکه بلاک چین و ۶) هاب ها یا مراکز مدیریت. این سیستم، مزیت‌هایی برای کنترل دسترسی در IoT فراهم می‌کند، مانند ۱) تحرک، که در سیستم‌های مدیریتی ایزوله قابل‌استفاده است ۲)، قابلیت دسترسی که تضمین می‌کند که قوانین کنترل دسترسی همیشه مهیا هستند ۳) همزمانی، که اجازه می‌دهد سیاست‌های کنترل دسترسی به‌صورت همزمان اصلاح شوند؛ ۴) سبک‌وزن، که بدان معناست که ادوات IoT، نیاز به هرگونه اصلاح برای بکار گیری این سیستم دارد ۵) مقیاس‌پذیری، زیرا ادوات IoT بتوانند از طریق شبکه‌های محدود مختلف، متصل شوند ، ۶) شفافیت، به‌گونه‌ای که سیستم بتواند حریم خصوصی مکانی را حفظ کند.

**تحویل مشارکتی ویدئو:** گسیل محتوای کیفیت بالا در IoT امروزه تعدادی از ارائه‌دهندگان خدمات اینترنت را به چالش می‌کشد. اما، هرباوت و نگرو [۲۵]، یک مکانیزم واسطه‌گری غیرمتمرکز برای تحویل ویدئوی برپایه بلاک چین مشارکتی، ارائه دادند که بر زنجیره‌های خدمات شبکه پیشرفته متکی است. بخصوص این، مکانیزم مدیریتی از سه بلاک چین تشکیل‌شده است، یعنی) بلاک چین واسطه‌گری محتوا ۲) بلاک چین نظارت بر تحویل و ۳) ارائه خدمات بلاک چین. علاوه بر آن، این مکانیزم مدیریت با پروژه منبع باز (اوپن سورس) Hyperledger-Fabric پیاده‌سازی شد که در آن نتایج نشان می‌دهند که تعداد گره‌ها به‌صورت جزئی زمان همگرایی را افزایش می‌دهد.

**اینترنت ابری:** در اینترنت ابری (IoC)، میلیون‌ها دستگاه IoT، داده‌های خود را از طریق اتصال اینترنت با بهره‌گیری از فن‌آوری مجازی‌سازی، به ابر آپلود می‌کنند. شو و همکاران [۲۶]، یک مدیریت منابع هوشمند برای دیتاسنترهای ابری بر اساس فن‌آوری بلاک چین، معرفی کردند تا هزینه کل مصرف انرژی را کاهش دهند. مخصوصاً اینکه، کاربران از کلیدهای خصوصی فردی خود برای امضای یک تراکنش استفاده می‌کنند، درحالی‌که کاربران همسایه یا مجاور، تراکنش انتشاریافته را تأیید می‌کنند. این بلوک حذف می‌شود هنگامی‌که از مرحله تأیید نگذرد. بنابراین، شارما و همکاران [۲۷] یک معماری ابری توزیع‌شده پیشنهاد کردند که از سه فن‌آوری نوظهور، یعنی شبکه‌سازی تعریف‌شده با نرم‌افزار (SDN)، رایانش مه ای ، و فن‌آوری بلاک چین استفاده می‌کند. کنترلرهای SDN گره مه، برای فراهم کردن رابطهای برنامه‌نویسی برای بهره‌برداران مدیریت شبکه، استفاده می‌شوند. فن‌آوری بلاک چین برای فراهم کردن خدمات مقیاس‌پذیر، مطمئن و بسیار مهیا، استفاده می‌شود. علاوه بر آن، شیا و همکاران [۲۸] یک سیستم اشتراک داده برپایه بلاک چین، به نام MeDShare برای ارائه‌دهندگان خدمات ابری ارائه می‌دهند. این سیستم از چهار لایه استفاده می‌کند، یعنی ۱) لایه کاربر ، ۲) لایه کوئری داده‌ها ۳) لایه ساختاربندی و حاکمیت داده‌ها و ۴) لایه زیرساخت موجود.

**آشکارسازی نفوذ:** فنون بسیاری برای پیاده‌سازی سیستم‌های آشکارسازی نفوذ (IDS) در محیط IoT پیشنهادشده‌اند که بر اساس یادگیری ماشینی هستند. برای بهبود سیستم‌های آشکارسازی نفوذ مشارکتی (CIDS ها)، آلکسوپولوس و همکاران [۲۹] ایده بهره‌گیری از فن‌آوری بلاک چین برای ایمن‌سازی مبادله هشدارها بین گروه‌های مشارکت‌کننده را معرفی کردند. منگ و همکاران [۳۰] در مورد کاربردی بودن فن‌آوری بلاک چین در یک سیستم آشکارسازی نفوذ بحث کردند. سیستم‌های آشکارسازی نفوذ مدرن باید بر اساس ارتباطات مشارکتی بین IDS های توزیع‌شده باشند که نیاز به اشتراک‌گذاری داده‌های گسترده میان نهادها و محاسبات اعتماد دارند. برای سروکار داشتن با نگرانی‌های حریم خصوصی که به‌وسیله تبادل داده به وجود می‌آیند و برای سرکوب هرگونه حمله خودی‌ها، فن‌آوری بلاک چین بکار گرفته می‌شود. به این روش، استفاده از طرف ثالث مورد اعتماد، که همچنین یک نقطه خرابی است، که در IDS های مشارکتی سنتی نیاز است، دیگر موردنیاز نیست.

**شبکه‌سازی تعریف‌شده با نرم‌افزار:** برای افزایش پهنای باند IoT، محققان، فن‌آوری شبکه‌سازی تعریف‌شده توسط نرم‌افزار (SDN) را پیشنهاد کرده‌اند، که این کار مسیریابی هوشمند را فراهم می‌کند و فرآیندهای تصمیم‌گیری را به‌وسیله کنترلر SDN، ساده‌سازی می‌کند. اخیراً، شارما و همکاران [۲۷] یک معماری شبکه IoT توزیع‌شده، به نام DistBlockNet را پیشنهاد کرده‌اند. بر اساس فن‌آوری بلاک چین، معماری DistBlockNet می‌تواند مقیاس‌پذیری و انعطاف‌پذیری را بدون نیاز به یک کنترلر مرکزی، فراهم کند. این شبکه بلاک چین توزیع‌شده از دو نوع گره استفاده می‌کند، یعنی ۱)، گره کنترلر/تأیید گره، که اطلاعات جدولی قوانین جریان بروز شده را حفظ می‌کند و ۲)، گره درخواست/پاسخ که جدول قوانین جریان خود را در یک شبکه بلاک چین، بروز رسانی می‌کند.

**رایانش لبه‌ای:** رایانش لبه‌ای، یک بستر بسیار مجازی‌سازی شده است که رایانش و ذخیره بین کاربران انتهایی و دیتاسنتر رایانش ابری سنتری را ممکن می‌سازد. بدون طرف‌های ثالث، ادوات مه ای می‌توانند با همدیگر تبادل داده داشته باشند. اما، روش بلاک چین را می‌توان برای تسهیل ارتباطات میان گره‌های مه و ادوات IoT مورداستفاده قرارداد. هوانگ و همکاران [۳۱] یک طرح پرداخت عادلانه برای برون‌سپاری محاسبات ادوات مه پیشنهاد کرده‌اند. بر اساس بیت کوین، این طرح، خواص امنیتی زیر، یعنی کامل بودن، عادلانه بودن و پاسخگو بودن را مورد ملاحظه قرار می‌دهد.

**کاربردهای P2P توزیع‌شده:** در کاربردهای نظیر به نظیر (P2P) توزیع‌شده، برای IoT، ادوات IoT، برای یک نسل جدید از کاربردها، مانند فیلم‌های مشارکتی، ارسال فایل‌ها، تحویل پیام‌ها، تجارت الکترونیک و بارگذاری داده‌ها با استفاده از شبکه‌های حسگری، خود را سازمان‌دهی و هماهنگ می‌کند. برای انگیزش دادن به کاربران جهت همکاری، هی و همکاران [۳۲] یک مکانیزم مشوق مورد اعتماد بر اساس روش بلاک چین برای محیط‌های P2P دینامیک و توزیع‌شده پیشنهاد کردند. برای جلوگیری از کاربران خودخواه برای دفاع در برابر حمله‌های تصادمی، این طرح یک استراتژی قیمت‌گذاری پیشنهاد کرده است که به گره‌های میانی و وسط اجازه به دست آوردن پاداش از تراکنش‌های بلاک چین به خاطر مشارکتشان در تحویل موفق را می‌دهند.

**کاربردهای سنجش تجمع:** الگوی سنجش تجمع یا ازدحام موبایل نوظهور، یک دسته نوین از کاربردهای IoT موبایل (متحرک) (برای مثال، کاربردهای حسگری جغرافیایی) است. وانگ و همکاران [۳۳] یک مکانیزم مشوق جالب برای حفظ حریم خصوصی در کاربردهای سنجش ازدحام بر اساس ارزهای رمزی بلاک چین می‌باشد. بخصوص اینکه، این مکانیزم می‌تواند مسائل امنیتی و حریم خصوصی را با استفاده از ارزیابی کیفیت داده‌های قابل‌تأیید کاوشگران حذف کند تا با حمله‌های شخصی‌سازی در بلاک چین باز و شفاف مقابله کند. علاوه بر آن، برای دستیابی به حفاظت از حریم خصوصی k–ناشناسی، این مکانیزم از یک روش همکاری گره برای کاربران شرکت‌کننده استفاده می‌کند.

**ذخیره داده:** ذخیره‌سازی داده‌ها می‌تواند با منابع داده ناهمگن برای سیستم‌های ذخیره داده برپایه IoT، سروکار داشته باشد. نحوه اشتراک‌گذاری و حفاظت از این داده‌های حساس، چالش‌های اصلی در ذخیره داده IoT می‌باشند. بر اساس فن‌آوری بلاک چین، جیانگ و همکاران [۳۴] یک جستجوی کلمه کلیدی خصوصی، به نام Searchain را برای ذخیره‌سازی غیرمتمرکز پیشنهاد کردند. معماری Searchain شامل دو مؤلفه است، ۱) گره‌های تراکنش در یک ساختار نظیر به نظیر و ۲) یک بلاک چین از همه بلوک‌های مرتب‌شده. علاوه بر آن، معماری Searchain می‌تواند حریم خصوصی کاربر، غیرقابل‌تمایز بودن و پاسخگویی ، فراهم کند.

**بیت کوین:** بیت کوین که در سال ۲۰۰۹، عرضه شد، یک شبکه پرداخت نظیر به نظیر (P2P) است که نیاز به هیچ مقام مرکزی ندارد. بر اساس روش هسته بلاک چین، کاربران بیت کوئین از نام واقعی استفاده نمی‌کنند؛ بجایش نام‌های مستعار استفاده می‌شوند. بنابراین، بیت کوین بر اساس سه مؤلفه فنی اصلی است: تراکنش‌ها، پروتکل اجتماع و شبکه ارتباطاتی.

خلیلوف و لوی [۳۵] یک بررسی جالب در مورد گمنامی و حریم خصوصی در سیستم‌های پرداخت دیجیتال شبیه به بیت کوین انجام دادند. بخصوص، این مطالعه روش‌های تحلیل گمنامی و حریم خصوصی در بیت کوین را به چهار دسته تقسیم کرده است، یعنی ۱) تعامل و تراکنش ۲) بهره‌گیری اطلاعات خارج از شبکه ۳) بکار گیری شبکه و ۴) تحلیل داده‌های بلاک چین.

همان‌گونه که توسط وانگ و همکاران [۳۳] بحث شد، بیت کوئین در عمل کار می‌کند، اما در تئوری، ن، مسئله اصلی نحوه حفاظت از حریم خصوصی خریداران بالقوه در بیت کوین با استفاده از زیرساخت کلید عمومی است. وانگ و همکاران [۳۳]، اثبات تأییدکننده اختصاصی دارایی‌ها برای مبادله بیت کوین با استفاده از رمزنگاری منحنی بیضوی را مطالعه کردند. مخصوصاً اینکه، نویسندگان یک طرح حفظ حریم خصوصی به نام DV-PoA پیشنهاد کردند که می‌تواند عدم تقلب را برآورده کند. توجه داشته باشید که طرح DV-PoA از مسئله الگوریتم گسسته منحنی بیضوی، مسئله دیفی–هلمن محاسباتی منحنی بیضوی و مقاومت در برابر تصادم تابع هش رمزنگاری را استفاده می‌کند. علاوه بر آن، برای حفاظت از حریم خصوصی مشتریان تأیید پرداخت ساده (SPV)، کانمورا و همکاران [۳۶]، یک طراحی فیلتر Bloom حفظ‌کننده حریم خصوصی برای یک مشتری SPV بر اساس γ– انکارپذیری، ارائه دادند.

با حذف شخص ثالث معتمد، کین و همکاران [۳۷]، یک PKI برپایه بلاک چین توزیع برای سیستم بیت کوئین، یعنی Cecoin ارائه کردند. برای تضمین هماهنگی و سازگاری، Cecoin از مکانیزم مشوق و یک پروتکل اجماع توزیع‌شده استفاده می‌کند. برای فراهم کردن خدمات چند مجوزی و انتساب هویت، Cecoin، یک سه‌تایی (آدرس، حیطه (دامین)، مجوز) را به یک سه‌تایی (کلید، آدرس، مجوز)، تبدیل می‌کند و کلید نشان‌دهنده مسیر مجوز (cert) در درخت است. بنابراین، برای حفاظت از حریم خصوصی تراکنش در بیت کوین، وانگ و همکاران [۳۳] یک چارچوب را با افزودن سیستم رمزگذاری Paillier هم‌ریخت برای پوشش دادن مقادیر متن ساده در تراکنش‌ها پیشنهاد کردند. برای حل مسئله اعتماد در بیت کوئین، هوانگ و همکاران [۳۱] یک طرح نمونه‌گیری برپایه تعهد بجای رینگر پیشنهاد کردند که برای محاسبات عمومی در برون‌سپاری رایانش قابل‌استفاده است.

## ۲-۲- مسائل حل‌نشده و چالش‌های پژوهشی

جهت تکمیل مرور ادبی خودمان، دو مسئله حل‌نشده و چالش پژوهشی را تشریح می‌کنیم که می‌توانند قابلیت‌ها و اثربخشی‌های بلاک چین برای IoT را بهبود بخشند، که این‌ها در توصیه‌های زیر خلاصه‌شده‌اند:

**چابکی در برابر حمله‌های ترکیبی:** همان‌گونه که در این مقاله مروری بیان شد، راهکارهای امنیتی بسیاری برای IoT برپایه بلاک چین در این

پژوهش‌ها پیشنهادشده است که هرکدام برای رفع و مقابله با مسائل امنیتی و مدل‌های تهدید مختلف، طراحی‌شده‌اند. حمله‌هایی که در این مطالعه مروری به بحث گذاشته‌شده‌اند به دو دسته تقسیم می‌شوند: وابسته به کاربرد و بدون کاربرد. حمله‌های وابسته به کاربرد، مخصوص کاربرد خاص هستند، بنابراین، به‌آسانی برای ایمن‌سازی کاربرد، مدنظر قرار می‌گیرند. علاوه بر آن، برای حمله‌های بدون کاربرد، هر پروتکل به یک زیرمجموعه از حمله‌ها می‌پردازد و هر حمله بدون کاربرد، با استفاده از یک راهکار امنیتی متفاوت، مقابله می‌شود. پرسش اصلی که ممکن است به ذهن بیاید این است که چگونه یک راهکار امنیتی طراحی کنیم که بتواند در برابر حمله‌های بدون کاربرد ترکیبی مقاوم باشد و در عین حاصل امکان‌پذیری پیاده‌سازی راهکار ، بخصوص در مورد ادوات IoT مقید به منابع کم، را مدنظر بگیریم.

**چهارچوب ایمنی دینامیک و وفق پذیر:** دستگاه‌ها و ادوات ناهمگن در شبکه IoT وجود دارند که از ادوات توان پایین تا سرورهای فوق پیشرفته، متنوع هستند. بنابراین، یک راهکار امنیتی منفرد را نمی‌توان برای همه معماری‌های IoT برپایه بلاک چین بکار گرفت که این به خاطر مقدار منابع متفاوتی است که فراهم می‌شود. بنابراین، راهکار امنیتی باید در ابتدا خود را با منابع موجود وفق دهد و تصمیم بگیرد که کدام خدمات امنیتی را ارائه دهد، تا حداقل الزامات ایمنی کاربران نهایی را برآورده کند. بنابراین، یکی از چالش‌هایی که قطعاً باید بیشتر در آینده موردتوجه قرار گیرد، این است که چگونه چنین چهارچوب امنیتی دینامیک و وفق پذیر را برای معماری‌های IoT برپایه بلاک چین طراحی کنیم.

**کاوش کم‌مصرف:** کاوش شامل اجرای الگوریتم‌های اجماع بلاک چین مانند Proof of Work (اثبات کار، PoW) می‌باشد. علاوه بر آن، بلاک چین رشد می‌کند هنگامی‌که کاربران تراکنش‌های خود را ذخیره کنند. بنابراین، کاوشگران قدرتمندی برای مدیریت پروتکل‌های اجتماع در بلاک چین لازم است. چندین الگوریتم اجماع کارآمد، مانند «اثبات فضا»، «اثبات فضای اختصاصی» و «اثبات سهم» و مینی بلاک چین برای ذخیره تنها تراکنش‌های بلاک چین جدید، پیشنهادشده‌اند. اما ادوات IoT محدود به منابع و محدود به توان همیشه قادر به برآورده تأمین مصرف محاسباتی و قدرت اساسی در پردازش اجماع بلاک چین و ذخیره بلاک چین‌ها، نیستند. بنابراین، طراحی پروتکل‌های اجتماع کم‌مصرف، یکی از چالش‌های پژوهشی قابل‌توجه در فن‌آوری‌های بلاک چین برای IoT می‌باشد.

**شبکه‌های اجتماعی و مدیریت اعتماد:** هنگامی‌که در مورد امنیت صحبت به میان می‌آید، باید همچنین در نظر داشته باشیم که اخبار جعلی نیز می‌توانند قسمتی از یک حمله سایبری باشند. شایعه‌پراکنی مقیاس بزرگ، می‌تواند آسیب‌های اجتماعی و اقتصادی شدیدی به یک سازمان یا کشور بزند بخصوص با استفاده از شبکه‌های اجتماعی آنلاین. بلاک چین‌ها می‌توانند وسیله‌ای برای محدود کردن شایعه‌پراکنی باشند همان‌گونه که در [۲۲] بیان‌شده، و در آن مرجع، شبکه اجتماعی فعال‌شده با بلاک چین ارائه‌شده است.

**زیرساخت مخصوص بلاک چین:** ادوات IoT ذخیره محدود ممکن است قادر به ذخیره بلاک چین مقیاس بزرگ که با اضافه شدن بلوک‌ها در بلاک چین رشد می‌کنند، نیستند. علاوه بر آن، معمولاً مشاهده می‌شود که ادوات IoT، داده‌های بلاک چین که حتی برای تراکنش‌های خودشان مفید نیستند را ذخیره می‌کنند. بنابراین، تجهیزات مخصوص بلاک چین که از ذخیره غیرمتمرکز بلاک چین مقیاس بزرگ پشتیبانی می‌کند به یک مسئله چالش‌برانگیز تبدیل می‌شود. علاوه بر آن، پروتکل‌های مدیریت آدرس و ارتباطات ضمنی، نقش قابل‌توجهی در زیرساخت بلاک چین ایفا می‌کنند. علاوه بر آن، اعتمادپذیری در میان ادوات غنی از منابع محاسباتی باید در زیرساخت بلاک چین، برقرار شود. علاوه بر آن، «رابط برنامه‌نویسی کاربردی» (API ها) باید تا آنجا که ممکن است کاربرپسند باشند.

**انتشار تبلیغ ابری در وسایل نقلیه:** همان‌گونه که در این مطالعه مروری بیان شد، بر اساس یک ساختار بلاک چین غیرمتمرکز، طرح‌های گمنامی مختلفی برای مخفی سازی هویت‌های واقعی در IoV، پیشنهادشده‌اند. بنابراین، ازآنجاکه هویت واقعی وسیله نقلیه، مکان واقعی خودرو و تراکنش را می‌توان در انتشار تبلیغ ابری خودرویی افشا کرد ، مسائل امنیتی اساسی به‌صورت زیر به وجود می‌آیند:

- چگونه یک پروتکل کنترل دسترسی تک ویژگی بر اساس فن‌آوری بلاک چین برای حفظ حریم خصوصی تراکنش در انتشار تبلیغ ابری خودرویی، طراحی کنیم؟
- چگونه یک طرح اشتراک‌گذاری رمز حفظ‌کننده حریم خصوصی بر اساس فن‌آوری بلاک چین تدوین شود تا از مشارکت خودروهای انتخاب‌شده در وسایل نقلیه، اطلاع حاصل شود؟ برای مثال، با استفاده از سیستم رمزگذاری Paillier همریخت (همشکل).
- نحوه طراحی یک احراز هویت دارای پیچیدگی کم با استفاده از فن‌آوری بلاک چین بین RSU ها و خودروهای شرکت کننده در طی فرآیند انتشار تبلیغ؟

**پردازش کوئری اسکای لاین:** کوئری اسکای لاین، به یک مسئله مهم در جستجوی پایگاه داده، برای مثال، پایگاه داده متمرکز، پایگاه داده توزیع‌شده (پراکنده) و جستجوی شباهت تبدیل‌شده است. طرح‌های بررسی‌شده، امکان استفاده از کوئری اسکای لاین با بلاک چین را موردمطالعه قرار نداده‌اند. اخیراً، محققان یک چارچوب تشخیص بیماری اولیه پزشکی آنلاین حفظ‌کننده حریم خصوصی، به نام CINEMA را پیشنهاد کرده‌اند که از کوئری اسکای لاین استفاده می‌کند. مخصوصاً، چارچوب CINEMA می‌تواند از حریم خصوصی داده‌های پزشکی کاربران حفاظت کند و محرمانه بودن مدل تشخیص بر اساس مدل تشخیص اسکای لاین را تضمین کند. بنابراین، نحوه مدیریت مسائل ایمنی و حریم خصوصی هنگامی‌که یک مدل تشخیص اسکایلاین به‌وسیله تعداد زیادی بلاک چین ساخته می‌شود، چگونه است؟ بنابراین، طرح‌های حفظ‌کننده حریم خصوصی بر اساس بلاک چین با

کوئری اسکای لاین، چالش‌های عمده می‌باشند و باید در آینده موردبررسی قرار گیرند.

## ۳- نتیجه‌گیری

در این مقاله، پیشرفت‌ها در پروتکل‌های بلاک چین موجود که برای شبکه‌های اینترنت اشیاء (IoT) طراحی‌شده‌اند را مرور کردیم. یک طرح کلی از حوضه‌های کاربردی فن‌آوری‌های بلاک چین در IoT، برای مثال، «اینترنت وسایل نقلیه»، «اینترنت انرژی»، «اینترنت ابری»، و رایانش ابری، ارائه کردیم. از طریق پژوهش و تحلیل گسترده که انجام شد، توانستیم مدل‌های تهدید مورد ملاحظه به‌وسیله پروتکل‌های بلاک چین در شبکه‌های IoT، را به پنج طبقه اصلی، یعنی حمله‌های برپایه هویت، حمله‌های برپایه دستکاری، حمل‌های تحلیل رمزی، حمله‌های برپایه اعتبار و حمله‌های برپایه خدمات تقسیم کردیم. چندین زمینه پژوهشی چالش‌برانگیز وجود دارد، که برای مثال، چابکی در برابر حمله‌های ترکیبی، چارچوب امنیتی دینامیک و وفق پذیر، کاوش کم‌مصرف، مدیریت شبکه‌های اجتماعی و اعتماد، زیرساخت مخصوص بلاک چین، انتشار تبلیغ ابری خودرویی و پردازش کوئری اسکای لاین، می‌باشند که این‌ها را در آینده نزدیک بیشتر می‌توان موردبررسی قرارداد.

## ٤- مراجع

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das,“Everything you wanted to know about the blockchain: Its promise,components, processes, and problems,” IEEE Consumer Electronics Mag., vol. 7, no. 4, pp. 6–14, July 2018.

[2] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, “Security and privacy in fog computing: Challenges,”IEEE Access, vol. 5, pp. 19 293–19 304, 2017.

[3] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury,and V. Kumar, “Security and privacy in fog computing: Challenges,”IEEE Access, vol. 5, pp. 19 293–19 304, 2017.

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

[5] X. Huang, C. Xu, P. Wang, and H. Liu, “LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem,” IEEE Access, vol. 6, pp. 13 565–13 574, 2018.

[6] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang,“CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles,” IEEE Trans. Intell. Transp. Syst., pp. 1–17, 2018.

[7] T. M. Fernández-Caramés and P. Fraga-Lamas, “A review on the use of blockchain for the internet of things,” IEEE Access, pp. 1–23, May 2018.

[8] Blockchain technology report to the US federal advisory committee on insurance,” accessed on 15 June, 2018.

[9] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Proc. Annual Technical Conference (USENIX ATC), June 2016, pp. 181–194.

[10] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in Proc. IEEE 4th Int. Conf. on Advanced Comput. and Commun. Syst. (ICACCS), Jan. 2017.

[11] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram,“Blockchain-literature survey,” in Proc. IEEE 2nd Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2017.

[12] M. C. K. Khalilov and A. Levi, “A survey on anonymity and privacy in Bitcoin-like digital cash systems,” IEEE Commun. Surveys & Tut., pp. 1–1, Mar. 2018.

[13] M. Conti, S. K. E, C. Lal, and S. Ruj, “A survey on security and privacy issues of Bitcoin,” IEEE Commun. Surveys & Tut., pp. 1–39, May 2018.

[14] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo,“Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?” IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, Jan. 2018.

[15] R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems,” IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[16] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, pp. 1–5, oct 2017.

[17] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, “When Intrusion Detection Meets Blockchain Technology: A Review,” IEEE Access, vol. 6, pp. 10 179–10 188, 2018.

[18] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, dec 2017.

[19] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” IEEE Internet Things J., vol. 4, no. 6, pp. 1832–1843, dec 2017.

[20] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains,” IEEE Trans. Ind. Informatics, vol. 13, no. 6, pp. 3154–3164, dec 2017.

[21] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, “CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles,” IEEE Trans. Intell. Transp. Syst., pp. 1–17, 2018

[22] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, “A blockchain-based reputation system for data credibility assessment in vehicular networks,” in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, pp. 1–5, oct 2017.

[23] N. Zhumabekuly Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging

Streams," IEEE Trans. Dependable Secur. Comput., pp. 1–1, 2016.
[24] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[25] N. Herbaut and N. Negru, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains," IEEE Commun. Mag., vol. 55, no. 9, pp. 70–76, 2017.
[26] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," IEEE Cloud Comput., vol. 4, no. 6, pp. 50–59, nov 2017.
[27] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.
[28] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.
[29] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivanko, and M. Muhlhauser, "Towards blockchain-based collaborative intrusion detection systems," in Proc. Int. Conf. Critical Inf. Infrastruct. Secur, 2017, pp. 1 12.
[30] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," IEEE Access, vol. 6, pp. 10 179–10 188, 2018.
[31] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," Futur. Gener. Comput. Syst., vol. 78, pp. 850–858, jan 2018.
[32] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, and M. E. Ylianttila, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain," jan 2018.
[33] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," IEEE Access, vol. 6, pp. 17 545–17 556, 2018.
[34] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchainbased private keyword search in decentralized storage," Futur. Gener. Comput. Syst., sep 2017.
[35] M. C. K. Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems," IEEE Commun. Surv. Tutorials, pp. 1–1, 2018.
[36] K. Kanemura, K. Toyoda, and T. Ohtsuki, "Design of privacy-preserving mobile Bitcoin client based on -deniability enabled bloom filter," in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, pp. 1–6, oct 2017.
[37] Y. Chen, Q. Li, and H. Wang, "Towards trusted social networks with blockchain technology," arXiv preprint arXiv:1801.02796, 2018.