مجله محاسبات نرم، جلد ۹، شماره ۲ (پاییز و زمستان ۱۳۹۹)، صفحه ۱۴ـ۳۳
https://dx.doi.org/10.22052/scj.2021.242836.0

مجله محاسبات نرم
SOFT COMPUTING JOURNAL
تارنمای مجله: scj.kashanu.ac.ir

دانشگاه کاشان
University of Kashan

مروری منظم بر ادبیات رأی‌گیری‌های الکترونیکی مبتنی بر فناوری زنجیره بلوکی ✧

پیام رنجبری[۱]، دانشجوی کارشناسی ارشد، سید امیر شیخ احمدی[۱]*، استادیار
[۱] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد سنندج، سنندج، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت ۰۸ بهمن ماه ۱۳۹۹
پذیرش ۰۹ خرداد ماه ۱۴۰۰

کلمات کلیدی:
رأی‌گیری الکترونیکی
فنّاوری زنجیره بلوکی
پایگاه داده‌های غیرمتمرکز
حریم خصوصی
مرور منظم ادبیات

چکیده

این مقاله باهدف شناسایی، تجزیه‌وتحلیل و سازمان‌دهی ادبیات مربوط به کاربردهای فنّاوری زنجیره بلوکی در رأی‌گیری‌های الکترونیکی/ برخط انجام می‌شود، همچنین چشم‌اندازی برای تحقیقات آینده پیشنهاد می‌دهد. این مطالعه سعی دارد که مهم‌ترین کاربردهای زنجیره بلوکی در رأی‌گیری الکترونیکی را نشان دهد و مهم‌ترین چالش‌های رأی‌گیری الکترونیکی که زنجیره بلوکی راه‌حلی برای آن‌ها ارائه می‌دهد را شناسایی کند. این مطالعه از روش بررسی منظم ادبیات برای تجزیه‌وتحلیل ادبیات موجود در ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی پیروی می‌کند. در این مطالعه، ۳۰ مقاله از کنفرانس‌ها و مجلات بین سال‌های ۲۰۱۷ تا می ۲۰۲۱ موردبررسی قرارگرفته است. به نظر می‌رسد که ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی در مراحل ابتدایی عملیاتی شدن خود قرار دارد و محققان و متخصصان به‌طور کامل از پتانسیل‌های زنجیره بلوکی برای رأی‌گیری الکترونیکی آگاه نیستند. مهم‌ترین نتایج ادغام یا استفاده از زنجیره بلوکی برای رأی‌گیری‌های الکترونیکی، حفظ حریم خصوصی رأی‌دهندگان، ناشناس ماندن، افزایش امنیت و قابلیت اطمینان سامانه‌های رأی‌گیری است. اما از سوی دیگر، ازنظر هزینه‌های کلی و مقیاس‌پذیری سامانه‌های رأی‌گیری مبتنی بر زنجیره بلوکی، اختلاف‌نظرهای جدی در میان محققین وجود دارد. محدودیت‌های این مطالعه عمدتاً در مورد کمیابی مطالعات در مورد کاربردهای زنجیره بلوکی برای رأی‌گیری‌های الکترونیکی (در مقیاس بزرگ) در مجلات و کنفرانس‌های ارائه‌شده است، همچنین اطلاعات در مورد پروژه‌های خصوصی-دانشگاهی که در حال پیاده‌سازی ایده خود هستند در دسترس نبوده است.

۱. مقدمه

امروزه رأی‌گیری یکی از پراستفاده‌ترین ابزار تحقق دموکراسی در جوامع است. حق رأی دادن و ابراز نظر کردن، چه در یک سازمان و یا جامعه کوچک، تا یک جامعه بزرگ مانند رأی‌گیری‌های ریاست جمهوری یا رفراندوم‌ها در مقیاس میلیونی، همیشه از موضوعات موردبحث و نظر کارشناسان، سیاستمداران، محققان و جامعه بوده است. در این میان، شمارش دقیق آراء و تائید صحت نتایج رأی‌گیری و عدالت اجتماعی در رأی‌گیری از الزامات اولیه یک رأی‌گیری است. در راستای چالش‌های متعدد و نگرانی‌های موجود در مورد فرایندهای رأی‌گیری، یکی از فناوری‌های جدید که ویژگی‌های امیدوارکننده‌ای دارد، فنّاوری زنجیره بلوکی است.

✧ نوع مقاله: مروری

* نویسنده مسئول
پست(های) الکترونیک: payam@iausdj.ac.ir **(رنجبر)**
asheikhahmadi@iausdj.ac.ir **(شیخ احمدی)**

نحوه ارجاع به مقاله: رنجبری، پیام، شیخ احمدی، سید امیر، «مروری منظم بر ادبیات رأی‌گیری‌های الکترونیکی مبتنی بر فناوری زنجیره بلوکی»، مجله محاسبات نرم، جلد ۹، شماره ۲، ص۱۴ـ۳۳، پاییز و زمستان ۱۳۹۹.

زنجیره بلوکی برای اولین بار در سال ۲۰۰۸ توسط ساتوشی ناکاموتو ارائه شد [۱, ۲]. بیت کوین[1] یک پول دیجیتالی رمزنگاری‌شده بود که ناکاموتو آن را ارائه داد و زنجیره بلوکی از آن به بعد شناخته شد. زنجیره بلوکی یک شبکه غیرمتمرکز همتا به همتا است که از یک زنجیره‌ی بلوک‌های به هم متصل تشکیل‌شده است [۳]. هر تراکنشی در این شبکه توسط توابعی رمزنگاری‌شده و در بلوک‌های به هم متصل ذخیره می‌شود [۴]. تمام گره‌ها در این شبکه یک نسخه از بلوک‌ها و تراکنش‌ها را دارند [۵]. با این ویژگی، سوابق تراکنش‌ها عملاً تغییرناپذیر هستند. هرچند که اولین بار زنجیره بلوکی در بیت کوین مورداستفاده قرار گرفت، اما در طول این سال‌ها به دلیل ویژگی‌های آن در بسیاری از حوزه‌ها مانند: بانکداری، پول‌های دیجیتالی، اینترنت اشیاء، محیط و سرویس‌های ابری، زنجیره تأمین و رأی‌گیری الکترونیکی/اینترنتی مورداستفاده قرارگرفته است.

بر اساس اصل غیرمتمرکز بودن زنجیره بلوکی که داده‌ها در یک سرور مرکزی ذخیره و نگهداری نمی‌شوند و نیازی به شخص سوم مورد اعتماد نیست، یک سیستم رأی‌گیری غیرمتمرکز اجرا خواهد شد که برای تائید فرایند و صحت نتایج رأی‌گیری نیازی به سازمان مرکزی تائید کننده نیست. در این سیستم، در صورت لزوم، تمام رأی‌دهندگان می‌توانند بر فرایند رأی‌گیری نظارت داشته باشند، درنتیجه، این موضوع اعتماد به فرایند رأی‌گیری و صحت نتایج را بالا می‌برد. باوجود قابلیت‌های زیاد فناوری زنجیره بلوکی برای عملیاتی کردن رأی‌گیری‌های الکترونیکی و حل چالش‌های آن،به نظر می‌رسد ادبیات مربوط به رأی‌گیری‌های (مقیاس بزرگ) مبتنی بر زنجیره بلوکی هنوز در مراحل ابتدایی قرار دارد. برای روشن کردن این موضوع داغ و پرکاربرد، از یک بررسی منظم ادبیات (SLR) [۶, ۷] برای پاسخ به سؤالات زیر استفاده‌شده است:

مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی چیست؟

ویژگی‌های زنجیره بلوکی که می‌تواند راه‌حلی برای چالش‌های یک رأی‌گیری الکترونیکی باشد چیست؟

مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی چیست؟

آینده‌ی رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی چطور است؟

بنابراین، این تحقیق باهدف روشن کردن ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی و موضوع رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی، سهم بسزایی را در ادبیات این موضوع خواهد داشت، همچنین بر سیاستمداران، تصمیم‌گیرندگان و استارت‌آپ ها و محققان علاقه‌مند به درک و شناخت این موضوع تأثیر خواهد داشت.

همانطورکه اشاره شد، زنجیره بلوکی کاربردهای زیادی در حوزه‌های مختلف دارد، این مطالعه در نظر دارد مجلات و کنفرانس‌های فعلی که در ارتباط با این موضوع هستند را نشان دهد. این تحقیق، به تحلیل ادبیات رأی‌گیری الکترونیکی مبتنی بر فناوری زنجیره بلوکی از سال ۲۰۱۷ تا می ۲۰۲۱ می‌پردازد. همچنین SLR شکاف‌ها و محدودیت‌های تحقیقاتی در ادبیات گذشته این موضوع را نشان می‌دهد و یک دستور کار تحقیقاتی قوی را برای آینده نشان خواهد داد. تقسیم‌بندی این مقاله به این شرح است: در بخش ۲، مفاهیم اساسی رأی‌گیری الکترونیکی و فناوری زنجیره بلوکی را ارائه می‌کنیم. در بخش ۳، جنبه‌های اصلی روش‌شناسی مرور منظم ادبیات را بر اساس [۶, ۷] ارائه می‌دهیم. بخش ۴ یافته‌های اصلی تحقیق را ارائه می‌دهد و بخش ۵ بحثی مبتنی بر سؤالات تحقیق ارائه می‌دهد. در بخش ۶، پیامدهای اجرایی و تحقیقاتی مبتنی بر یافته‌ها برجسته شده است. بخش ۷ پیامدهای تحقیق را به‌تفصیل شرح داده و در مورد تحقیقات آینده توضیحاتی را ارائه می‌کند. در بخش ۸ بحثی در مورد یافته‌ها ارائه داده می‌شود. و در آخر، در بخش ۹، نتیجه‌گیری و محدودیت‌های نهایی را ارائه می‌دهیم.

۲. رأی‌گیری الکترونیکی و فناوری زنجیره بلوکی: مفاهیم اساسی

در این بخش ابتدا در نظر داریم که رأی‌گیری‌های الکترونیکی را بیشتر شناخته و سپس با مفاهیم اولیه و ساختار فناوری زنجیره

[1] Bitcoin

بلوکی آشنا شویم و در انتها بحثی کوتاه در ارتباط با ادغام رأی‌گیری الکترونیکی با فناوری زنجیره بلوکی به همراه ارائه یک مدل ساده از رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی خواهیم کرد.

۲,۱. رأی‌گیری‌های الکترونیکی

در این سامانه‌های رأی‌گیری، اغلب رأی‌های کاغذی وجود ندارد (نه همیشه!)، بلکه رأی‌ها به‌صورت دیجیتالی خواهند بود. بنابراین انتظار می‌رود که سرعت فرایند رأی‌گیری (در رأی‌گیری‌های مقیاس بزرگ) بیشتر باشد و زمان اعلام نتایج به نسبت فرایندهای سنتی-کاغذی بهبود یابد، درنتیجه در زمان صرفه‌جویی شود. به‌این‌ترتیب، ایده اصلی الکترونیکی شدن فرایندهای رأی‌گیری شامل صرفه‌جویی در زمان، سهولت فرایند رأی‌گیری (برای معلولین، سربازان خارج از کشور)، در دسترس بودن پورتال رأی‌گیری (به‌عنوان حوزه رأی‌گیری) برای همه رأی‌دهندگان (از طریق بستر ارتباطی اینترنت و غیره)، صرفه-جویی در منابع انسانی و هزینه‌ها بود.

علیرغم این تعریف و ایده‌های اصلی الکترونیکی شدن فرایندهای رأی‌گیری، محققان و کارشناسان زیادی در مورد فرایندهای رأی‌گیری به‌طورکلی (سنتی-کاغذی یا الکترونیکی-اینترنتی) پژوهش‌هایی انجام داده‌اند و اختلاف نظرات جدی در مورد مزایا و معایب الکترونیکی شدن فرایندهای رأی‌گیری وجود دارد. پژوهش [۸] به بررسی قابلیت‌های شبکه‌های اینترنت اشیاء، اینترنت نسل پنجم و بستر شهرهای هوشمند برای ارائه خدمت الکترونیکی کردن رأی‌گیری‌های سنتی پرداخته است. چالش بالقوه اشاره شده در این پژوهش این بود که دستگاه‌های هوشمند چگونه یک رابطه نظام‌مند و قابل‌اعتماد برقرار کنند که توسط دستگاه های مخرب تهدیدی برای نتایج رأی‌گیری به وجود نیاید.

در پژوهش [۹]، نویسندگان معتقد هستند که رأی‌گیری‌های الکترونیکی ازلحاظ ارائه سطح شفافیت به رأی‌دهندگان، مطلوب نیستند و رأی‌دهندگان نمی‌توانند به این سامانه ها اعتماد کامل داشته باشند که آیا واقعاً رأی آن‌ها به‌طور صحیح ثبت و ذخیره خواهد شد. از سوی دیگر [۱۰] بیان می‌کند که رأی‌گیری‌های الکترونیکی موجب افزایش میزان مشارکت و همچنین دقت رأی‌گیری خواهد بود. برای این منظور آن ها یک مدل را مبتنی بر دستگاه‌های اینترنت اشیاء و گوشی‌های موبایل پیشنهاد کرده‌اند که می‌تواند برای فراهم نمودن رأی‌گیری‌های مقیاس بزرگ و درنتیجه به حداکثر رسانی مشارکت عمومی در رأی‌گیری کمک کند. زیرساخت‌های وسیع اینترنتی-ارتباطی برای الکترونیکی بودن فرایند رأی‌گیری، امنیت سرورها و پایگاه داده‌ها در مقابل حملات مهاجمان و هکرها، در دسترس بودن سرورها در صورت خرابی یک یا چند تا از سرورها (ذخیره‌ساز، محاسبه کننده)، جلوگیری از رأی‌گیری دوباره، صحت نتایج رأی‌گیری و جلوگیری از جعل، احراز هویت رأی‌دهندگان و غیره از مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی هستند. این تحقیق همچنین در نظر دارد که مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی را بشناسد، اهمیت و ضرورت این موضوع را درک کند و کاربردهای فنّاوری زنجیره بلوکی برای رأی‌گیری‌های الکترونیکی را برجسته کند. این مطالعه از رویکرد مرور منظم بر ادبیات پیروی می‌کند تا تعاریف کلی رابطه بین رأی‌گیری الکترونیکی و فنّاوری زنجیره بلوکی و چالش‌های احتمالی آن را درک کند.

۲,۲. فناوری زنجیره بلوکی

زنجیره بلوکی به‌عنوان یک فناوری جدید برای پشتیبانی از تراکنش‌ها درزمینه رمزنگاری ظاهر شد [۱]. یک تعریف رسمی از فنّاوری زنجیره بلوکی توسط [۱۱] ارائه‌شده است، و عبارت است از:

"زنجیره بلوکی یک سیستم کاملاً توزیع‌شده است که برای رمزنگاری و ذخیره کردن (به‌صورت تغییرناپذیر و ثابت) تراکنش‌ها بین کاربران (بازیگران) شبکه کاربرد دارد. این عملکرد مانند یک دفترچه توزیع‌شده است که توسط طرفین درگیر در تمام معاملات درون یک شبکه، با یک اجماع نگه‌داشته شده، به‌روز شده و اعتبار سنجی می‌شود. در چنین شبکه‌ای، شفافیت زیادی وجود دارد و اجماع بزرگی از یک

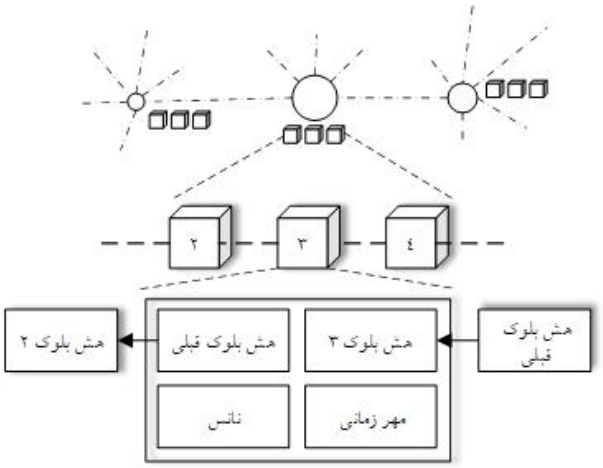
سیستم و کاربران آن، اعتبار تراکنش‌ها را تضمین می‌کنند."

علاوه بر این تعریف رسمی زنجیره بلوکی، برخی دیگر از ویژگی‌های متمایز این فناوری، مانند: امنیت داده‌ها، تراکنش‌های ضد جعل/ دست‌کاری و همچنین اعتبار سنجی اطلاعات در بین اعضای این شبکه وجود دارد. هایپرلدجر[1] (ابتکار بنیاد لینوکس برای زنجیره‌های بلوکی منبع باز) یک دفتر کل توزیع‌شده را به این شرح تعریف کرده است:

"یک بانک اطلاعاتی چند قسمتی (چند حزبی) که هیچ مرجع قابل‌اعتماد مرکزی در آن وجود ندارد (مدیریت غیرمتمرکز). وقتی‌که تراکنش‌ها انجام می‌شوند، در بلوک‌هایی قرار می‌گیرند (ذخیره می‌شوند) که این بلوک‌ها در دفترچه‌های توزیع‌شده، به‌طور هم‌زمان ذخیره می‌شوند که امکان دست‌کاری یا تغییر آن تراکنش‌ها به حداقل ممکن می‌رسد [۱۲]."

فناوری زنجیره بلوکی به‌عنوان یک شبکه‌ای دیجیتالی از تراکنش‌ها کار می‌کند که ویژگی‌های اصلی آن شامل: غیرمتمرکز بودن، غیرقابل دست‌کاری بودن و امنیت زیاد است. پس مفهوم زنجیره بلوکی را می‌توان به‌عنوان یک شبکه‌ای که وابسته به یک مرجع مرکزی برای تائید اعتبار نیست درک کرد [۵]. در رأی‌گیری‌های الکترونیکی، اغلب یک سازمان مرکزی وظیفه اعتبار سنجی رأی‌ها، کاندیداها، رأی‌دهندگان و صحت نتایج رأی‌گیری را بر عهده دارد. در صورت هک شدن یا از دسترس خارج شدن این سازمان مرکزی که به سیستم ارتباطی (اینترنت) متصل است، کل فرایند دچار مشکل شده و اعتبار نتایج قابل‌اعتماد و قابل تائید نخواهد بود.

ازجمله نتایج رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی این است که، چنین سازمان مرکزی وجود ندارد و کل گره‌های (استخراج‌کنندگان، کاربران) شبکه وظیفه اعتبارسنجی رأی‌ها، کاندیداها و رأی‌دهندگان را بر عهده‌دارند، درنتیجه هک کردن و دست‌کاری این شبکه کار آسانی نیست. در شکل (۱)، عناصر اصلی فنّاوری زنجیره بلوکی به‌صورت خلاصه ترسیم‌شده است. بلوک‌ها به‌مانند یک زنجیره به همدیگر متصل هستند که هر بلوک شامل مقدار رمزنگاری‌شده بلوک قبلی (هش بلوک قبلی) است. ازآنجاکه این بلوک دارای یک کپی از همه تراکنش‌ها است و امکان تغییر آن وجود ندارد، زنجیره بلوکی شفافیت و اعتماد به شبکه را تضمین می‌کند [۱۳].



شکل (۱): ساختار بلوک در زنجیره بلوکی

بر اساس این شکل، بلوک شماره ۳، مقدار هش بلوک[2] شماره ۲ را دارد و درنتیجه، این فرایند تا اولین بلوک شبکه ادامه می‌یابد که قابلیت ردیابی و اعتبارسنجی آن را فراهم می‌کند. هر بلوک یک مهر زمانی دارد که بر اساس آن تراکنش‌ها به ترتیب ثبت‌شده، همچنین یک عدد به نام نانس[3] وجود دارد که باید استخراج‌کنندگان[4] سعی کنند با عملیات محاسباتی سنگین بر اساس مقدار هش بلوک و سختی[5] شبکه عددی کوچک‌تر از نانس یافته تا پاداش استخراج بلوک را دریافت کنند.

۲،۳. ادغام رأی‌گیری‌های الکترونیکی با فناوری زنجیره بلوکی

تا به امروز هیچ‌کدام از کشورها فرایند رأی‌گیری مقیاس بزرگ (برای مثال ریاست جمهوری) خود را تماماً به صورت الکترونیکی-اینترنتی برگزار نکرده‌اند، یعنی از فرایند احراز هویت افراد، رأی دادن، ذخیره اطلاعات و رأی‌ها، شمارش آراء، اعلام نتایج و غیره به‌طور کامل الکترونیکی نشده است، بلکه

[1] Hyperledger

[2] Block hash
[3] Nonce
[4] Miners
[5] Difficulty

قسمتی از فرایند الکترونیکی شده است. برای مثال در کشور روسیه، رأی‌دهندگان رأی خود را به‌صورت سنتی در برگه‌های کاغذی رأی نوشته و در صندوق آراء قراردادند و این اسناد به‌صورت اسکن شده در پایگاه داده‌های متفاوت ذخیره و شمارش شدند [۱۴]. شکل (۲)، یک مدل ساده‌ای از رأی‌گیری‌های الکترونیکی مبتنی بر فناوری زنجیره بلوکی با استفاده از قراردادهای هوشمند ارائه می‌دهد. قراردادهای هوشمند یک نوع قرارداد خود اجرا هستند که شرایط توافق‌نامه بین طرفین قرارداد مستقیماً نوشته‌شده (معمولاً کد نویسی است و معروف‌ترین قراردادهای هوشمند در حوزه شبکه‌های غیرمتمرکز مربوط به اتر یوم است که با زبان برنامه‌نویسی سالیدیتی[1] نوشته می‌شود) نوشته‌شده است. این کد و توافق‌نامه‌های موجود در آن در شبکه توزیع‌شده و غیرمتمرکز زنجیره بلوکی اجرا، ثبت و ذخیره خواهد شد [۱۵, ۱۶].

بر اساس این مدل، هر رأی‌دهنده و کاندیدایی دارای یک کلید عمومی و یک کلید خصوصی خواهند بود. رأی‌دهندگان بعد از انتخاب کاندیدای موردنظر، یک قرارداد هوشمند حاوی رأی، کلید خصوصی شخصی و کلید عمومی کاندیدا را امضا کرده و ارسال می‌کنند. این قرارداد هوشمند می‌تواند به‌صورت مستقیم از طرف کاندیدا، شبکه مبتنی بر زنجیره بلوکی یا مجری رأی-گیری تولید و ارسال گردد. سپس این آراء (مبتنی بر قرارداد هوشمند) توسط مجری برگزاری رأی‌گیری در یک پایگاه داده غیرمتمرکز مبتنی بر زنجیره بلوکی ذخیره می‌شود. فرایند شمارش این آراء می‌تواند بعد از اتمام رأی‌گیری انجام شود و کاندیداها با استفاده از کلید خصوصی خود، قراردادهای هوشمندی که درواقع به‌عنوان یک تراکنشی به مقصد آن‌ها بوده است را تائید کرده و از صحت نتایج آراء اطمینان حاصل کنند. به‌این‌ترتیب، ساختار زنجیره بلوکی و قراردادهای هوشمند برای افزایش امنیت، جلوگیری از دوباره رأی دادن و افزایش دقت در ثبت و ذخیره رأی‌های دیجیتال پیشنهاد گردیده است [۱۰].

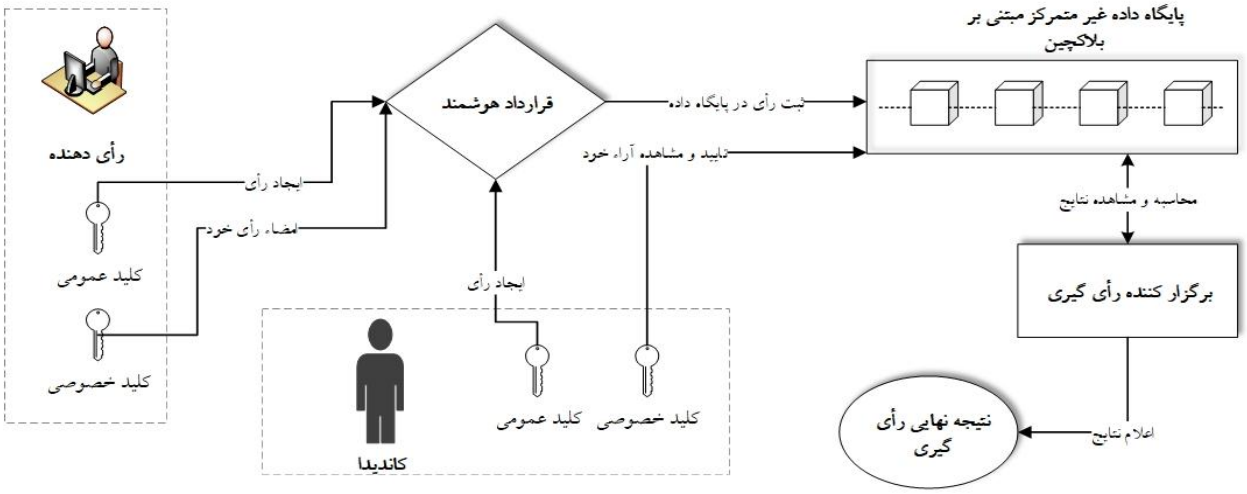
واضح است که به این صورت جعل کردن کلیدهای عمومی یا خصوصی رأی‌دهندگان و کاندیداها و یا تغییر و دست‌کاری رأی‌های ذخیره‌شده (در قالب تراکنش) در پایگاه داده مبتنی بر زنجیره بلوکی به حداقل ممکن می‌رسد. از این‌سو، شفافیت آراء و نتایج برای همگان قابل‌درک است، امنیت فرایند تأمین می‌شود و هیچ‌کسی نمی‌تواند به‌جای کسی دیگر رأی بدهد یا دو بار رأی دهد. علاوه بر این، به دلیل غیرمتمرکز بودن سرورها، از دسترس خارج شدن یک یا چند سرور اختلالی در فرایند رأی‌گیری و نتایج ایجاد نمی‌کند، درنتیجه هزینه‌های نیروی انسانی به نسبت فرایند سنتی رأی‌گیری به دلیل الکترونیکی بودن کاهش می‌یابد. به دلیل اینکه هر گره یا بازیگری در این سیستم مبتنی بر زنجیره بلوکی قادر خواهد بود که یک کپی از رأی‌ها را در قالب تراکنش‌های رمزگذاری شده داشته باشد، اعتماد به نتایج و فرایند رأی‌گیری بسیار بیشتر می‌شود.

یک دیدگاه انتقادی بر اساس تجزیه‌وتحلیل تحقیقات قبلی در مورد خطرات امنیتی رأی‌گیری آنلاین و الکترونیکی توسط [۱۷] ارائه‌شده است. آن‌ها نشان دادند که نه‌تنها این خطرات در سامانه‌های رأی‌گیری مبتنی بر زنجیره بلوکی وجود دارد ، بلکه زنجیره‌های بلوکی می‌توانند مشکلات "اضافی" را برای سامانه‌های رأی‌دهی ایجاد کنند. این پژوهش معتقد است که رأی‌گیری مبتنی بر اینترنت و زنجیره بلوکی خطر شکست‌های غیرقابل‌شناسایی در مقیاس بزرگ را تا حد زیادی افزایش می‌دهد، برای مثال، افزودن فن‌آوری‌های جدید مانند قراردادهای هوشمند، زنجیره بلوکی و غیره به سامانه‌های رأی‌گیری ممکن است پتانسیل‌های جدیدی برای حملات مخرب ایجاد کنند.

۳. روش‌شناسی تحقیق

روش SLR روشی مرجع برای سازمان‌دهی، ترکیب و شناسایی روش‌ها و فرصت‌های در حال ظهور و همچنین درک موضوعات، تضادها و محدودیت‌های مربوطه بر اساس مطالعات قبلی است. SLR روشی کاملاً اثبات‌شده، عمدتاً در تحقیقات پزشکی است [۱۸]. SLR را می‌توان به‌صورت زیر تعریف کرد: "یک روش کارآمد برای آزمایش فرضیه، جمع‌بندی نتایج مطالعات موجود و ارزیابی ثبات در مطالعات قبلی است [۱۹]."

[1] Solidity



شکل (۲): یک مدل ساده ارتباطی رأی‌گیری الکترونیکی و زنجیره بلوکی

رأی‌گیری‌های مبتنی بر زنجیره بلوکی یک زمینه نسبتاً جدیدی است که هنوز در دستور کار محققان و پژوهشگران قرار دارد. همانطورکه [۷] اشاره داشته است، در مباحث نوظهور و رشته-های پیشرفته، مقالات ارائه‌شده در مجلات و اجلاس‌ها می‌توانند کمیاب باشند. با در نظر گرفتن ادبیات قبلی، SLR یک رویکرد مؤثر در توسعه میدانی است و یک رویکرد منظم برای شناسایی موضوعاتی که تحت پوشش قرار نمی‌گیرند، و روش‌های جدیدی برای این زمینه و راه‌های تحقیقاتی جدید ارائه می‌دهد. بنابراین، SLR یک رویکرد مناسب برای درک رأی‌گیری‌های مبتنی بر فناوری زنجیره بلوکی است. این SLR حاضر به دنبال مراحل اصلی SLR که توسط [۷] ارائه‌شده است، است. چهارچوب روش‌شناختی SLR ، یک رویکرد دقیق برای انجام بررسی ادبیات را فراهم می‌کند [۶].

در مرحله اول (برنامه‌ریزی مرور)، دامنه مطالعات تعریف‌شده است. این مرحله بسیار مهم است، زیرا تعریف موضوع و دامنه ادبیات تعریف‌شده است. همانطورکه [۷] توصیه کرده است، این مطالعه آنچه قبلاً به‌طور منظم در مورد زنجیره بلوکی درزمینه رأی‌گیری الکترونیکی موردبحث قرارگرفته است را پوشش می-دهد. درنتیجه همانطورکه قبلاً بیان شد، ۴ سؤال اصلی طرح‌شده است. در مرحله بعدی یک پروتکل تحقیق مدل‌سازی شد [۷]. در مرحله دوم (انجام یک بررسی)، همانطورکه توسط [۷] توصیه‌شده است، مطالعات توسط معیارهای مربوطه مشخص شد (جدول ۱). این مطالعه فقط مقالاتی را شامل می‌شود که معیارهای پروتکل تحقیق این پژوهش را داشته باشد. معیارهای تفصیلی ورود و خروج در جدول (۱) مشخص‌شده است، همچنین در جدول (۲) کلمات کلیدی جستجو شده در پایگاه منابع علمی آورده شده است. طبق گفته [۷]، مرحله استخراج داده‌ها با استفاده از فیلترهایی مانند عنوان، مجله-کنفرانس و کلمات کلیدی، خطا به حداقل رسید و به انتخاب مقالات کمک کرد. در مرحله سوم (گزارش و انتشار)، یافته‌های اصلی ارائه‌شده است. در این مطالعه، یک برنامه تحقیقاتی با سؤالات باز و برخی پیشنهادها برای محققان و کسانی که علاقه‌مند به درک عمیق پتانسیل زنجیره بلوکی در رأی‌گیری‌های الکترونیکی هستند ارائه می‌شود. علاوه بر این، پیامدهای اجرایی و تحقیقاتی در یک نتیجه‌گیری کوتاه آورده شده است. همانطورکه [۷] توصیه کرده است، شکل (۴) مراحل اصلی این پژوهش را نشان می‌دهد. برای انجام SLR، شکل (۳) یک چهارچوبی را نشان می‌دهد که نشان‌دهنده رویه اتخاذشده در این مطالعه است که تعداد مقالات انتخاب‌شده در هر مرحله در آن نمایش داده‌شده است.

۴. یافته‌ها

در این مقاله از روش تجزیه و تحلیل محتوای مقالات برای ترکیب کردن یافته‌ها استفاده شد. جدول (۳) دسته‌های اصلی را برای تجزیه و تحلیل محتوا بکار برده شده را نشان می‌دهد.

جدول (۱): معیارهای انتخاب منابع و مقالات

پروتکل تحقیق	توضیحات
پایگاه منابع علمی	ScienceDirect (Elsevier), Springer Link (Springer), IEEE Xplore Digital Library (IEEE), Taylor & Francis Online (Taylor & Francis), Emerald Insight (Emerald), Google Scholar
بازه زمانی تحقیق	از سال ۲۰۱۷ تا می ۲۰۲۱
زبان جستجو	فقط مقالاتی که به زبان انگلیسی هستند
نوع مقالات ارائه‌شده	کنفرانس‌ها و مجلات
جستجو بر اساس	عنوان، چکیده، کلمات کلیدی
معیارهای انتخاب شدن	مقالاتی که در مورد رأی‌گیری‌های الکترونیکی و قابلیت‌های زنجیره بلوکی برای رفع چالش‌های رأی‌گیری الکترونیکی تحقیق و بحث کرده باشند.
معیارهای انتخاب نشدن	مقالاتی که بر روی بیت کوین، فرایند استخراج بلوک در زنجیره بلوکی، پول‌های دیجیتال، بانکداری، رأی‌گیری سنتی-محلی، سیاست‌ها و قوانین رأی‌گیری تمرکز کرده باشند، همچنین مقالات به زبان غیر انگلیسی و مقالات نامرتبط با موضوع اصلی این مطالعه.
آنالیز و تحلیل	از روش تحلیل محتوا برای پاسخ به سؤالات تحقیق از ادبیات ، برجسته کردن شکاف‌های اصلی و پیشنهاد راه‌هایی برای تحقیقات آینده در موضوعات داغ درون برنامه‌های کاربردی زنجیره بلوکی درزمینه رأی‌گیری‌های الکترونیکی استفاده‌شده است.

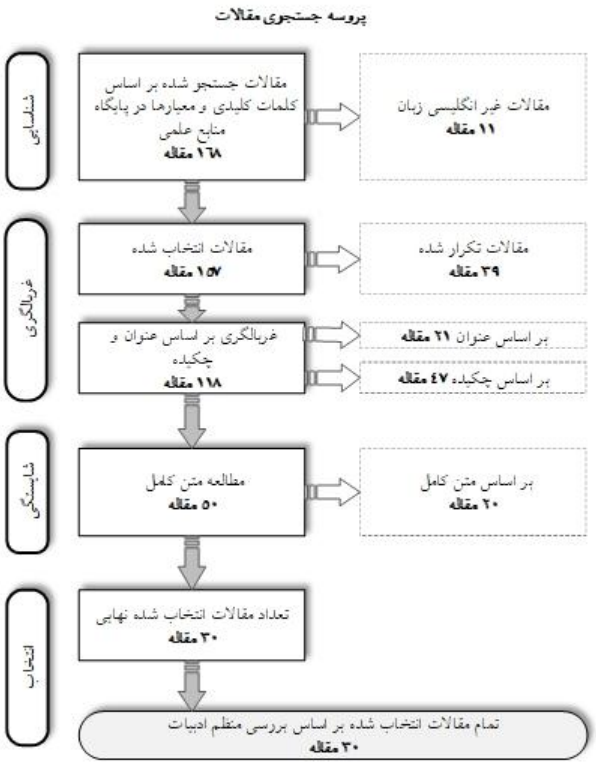
جدول (۲): کلمات کلیدی جستجو شده بر اساس پایگاه منابع علمی

پایگاه منابع علمی	کلمات جستجو شده
ScienceDirect	Blockchain AND Voting, Blockchain AND e-Voting, Blockchain-based AND Voting, Blockchain AND Democracy, Blockchain AND Online-Voting, Decentralize AND Voting, Ethereum AND Voting
IEEE Xplore	(Blockchain) AND (Vote), (Blockchain) AND (e-Voting), (Smart Contract) AND (Voting), (Online) AND (Voting) AND (Systems), (Digital) AND (Election)
Springer	Blockchain AND Voting, Blockchain AND Digital AND Vote, Blockchain AND e-Voting
Emerald Insight	(Blockchain) AND (Vote), (Blockchain) AND (e-Voting), (Smart Contract) AND (Voting), (Online) AND (Voting) AND (Systems), (Digital) AND (Election), (Decentralize) AND (Election)
Taylor & Francis Online	[All: Blockchain] AND [All: Voting], [All: Blockchain] AND [Election], [All: e-Voting], [All: Online-Voting]
Google Scholar	Blockchain + e-Voting, Blockchain-based + Election, Online + Voting, Digital + Voting + Process

جدول (۳): دسته‌بندی برای تجزیه‌وتحلیل محتوای مقالات

دسته‌بندی	توضیح / مثال
تعداد کل مقالات منتشرشده بین سال‌های ۲۰۱۷ و می ۲۰۲۱	تعداد مقالات بر اساس سال
مجله	مقالات منتشرشده توسط مجلات
کنفرانس	مقالات منتشرشده توسط کنفرانس‌ها
تمرکز بر حوزه اصلی	فناوری زنجیره بلوکی، رأی‌گیری الکترونیکی، حریم خصوصی، یکپارچه‌سازی اطلاعات، مقیاس‌پذیری، بیت کوین، اتریم، قراردادهای هوشمند، رأی‌گیری مبتنی بر زنجیره بلوکی، رأی‌گیری آنلاین
کار اصلی و نظریه ارائه‌شده	ارائه مدل، ارائه متد، ارائه یک سیستم، ارائه پروتکل، آنالیز منظم، مرور کوتاه، ارائه طرح، شبیه‌سازی، پیاده‌سازی یک اپلیکیشن، طراحی یک معماری
موضوعات مهم و چالش‌های رأی‌گیری الکترونیکی	عدالت و انصاف در اعلام نتایج، واجد شرایط بودن و احراز هویت افراد، حریم خصوصی رأی‌دهندگان و کاندیداها، قابل‌اطمینان بودن سیستم رأی‌گیری و فرایند، ناشناس بودن رأی‌دهندگان، سازگاری داده‌ها و یکپارچگی در سرورهای مختلف، منحصربه‌فرد بودن هویت‌ها و شناسه‌ها، صحت نتایج نهایی و موضوع تقلب، شفافیت فرایند رأی‌گیری، کارایی سیستم ازنظر زمان و هزینه، مقیاس‌پذیری رأی‌گیری و امنیت فرایند و سرورها در مقابل حمله هکرها و خراب شدن
قابلیت‌های زنجیره بلوکی	غیرمتمرکز بودن، تغییرناپذیری و غیرقابل دست‌کاری بودن، مقیاس‌پذیری، شفافیت، الگوریتم‌های اجماع و پروتکل‌های اثبات و رمزنگاری

شکل (۳): مراحل اصلی اجرای پژوهش



شکل (۴): پروسه انتخاب مقالات بر اساس بررسی منظم ادبیات

۴،۱. انتشار مقالات بر اساس کشور

شکل (۵) تعداد مقالات منتشرشده بر اساس کشور را نشان می‌دهد (کشور نویسندگان اصلی مقاله). علی‌رغم اینکه زنجیره بلوکی از سال ۲۰۰۸ معرفی‌شده است، اما مقالات بسیار کمی در بازه ۲۰۰۸ تا ۲۰۱۶ وجود داشت، بنابراین برای استخراج یافته-های مهم و پاسخ سؤالات تحقیق، دامنه زمانی این پژوهش به سال ۲۰۱۷ تا می ۲۰۲۱ محدود می‌شود. این موضوع نشان می‌دهد که شناخت قابلیت‌های اصلی و کاربردهای زنجیره بلوکی برای رأی‌گیری‌های الکترونیکی در بازه ۲۰۰۸ تا ۲۰۱۶ به نسبت جذابیت و اهمیت موضوع کم بوده است. در شکل (۵) محققان از ۲۰ کشور حضور دارند و مشاهده می‌شود که محققان کشور آمریکا، هند و بریتانیا به‌تنهایی حدود ۴۵ درصد از مقالات منتشرشده در حوزه رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی را دارا می‌باشند. این امر نشان می‌دهد که اهمیت رأی‌گیری‌های الکترونیکی بر جوامع آن‌ها احتمالاً تأثیر بیشتری دارد.

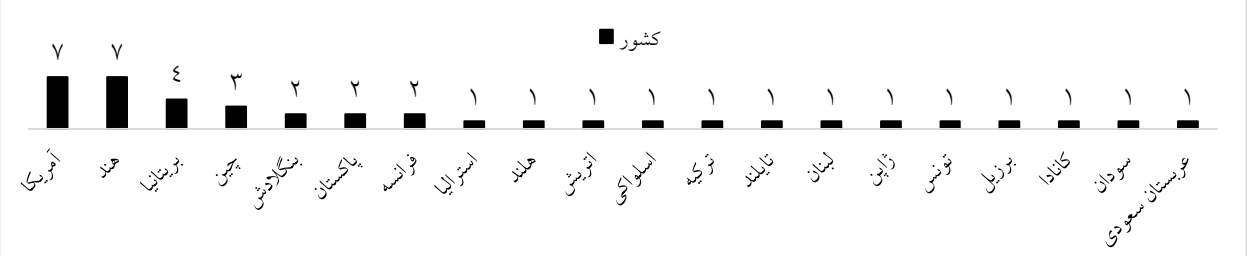
انتظار می‌رفت که پژوهشگران زیادی در کشورهای آلمان، ایتالیا و اسپانیا را شاهد باشیم، اما در این جدول موردی مشاهده نمی‌شود، هرچند که آن کشورها در ارتباط با دموکراسی، شفافیت و اقتصاد جزو کشورهای مطرح هستند. در رده‌های بعدی پژوهشگران چین، بنگلادش،پاکستان و فرانسه حضور دارند که باهم حدود ۲۲ درصد را شامل می‌شوند. اگر بر اساس قاره در نظر بگیریم، قاره آسیا حدوداً ۴۷ درصد از سهم مقالات را در اختیاردارند و قاره اروپا (با در نظر گرفتن بریتانیا) حدوداً ۲۲ درصد و قاره آمریکا ۲۰ درصد، قاره آفریقا ۵ درصد و نهایتاً قاره استرالیا ۲ درصد. انتظار می‌رود که در سال‌های آتی تعداد مقالات و پراکندگی جغرافیایی پژوهشگران علاقه‌مند به حوزه ادغام زنجیره بلوکی با رأی‌گیری‌های الکترونیکی رو به افزایش باشد.

۴،۲. انتشار مقالات بر اساس مجلات

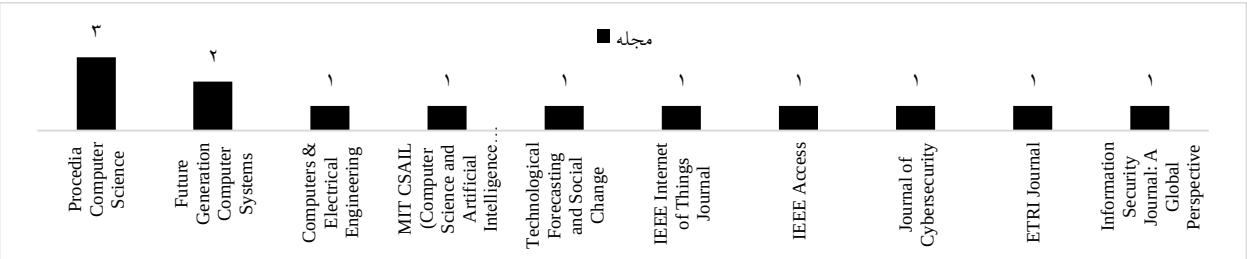
شکل (۶) مقالات را با توجه به مجله سازمان‌دهی می‌کند. مجله Procedia Computer Science از انتشارات ScienceDirect به‌تنهایی مسئول ۲۳ درصد از مقالات منتشرشده در مجلات است. پس از آن مجله Future Generation Computer Systems که حوزه تخصصی کامپیوتر، زیرساخت و سامانه‌های آن را پوشش می‌دهد مسئول ۱۵درصد از مقالات منتشرشده است. دو مجله Computers & Electrical Engineering از انتشارات ScienceDirect و MIT CSAIL مرتبط با دانشگاه MIT در ماساچوست آمریکا، هرکدام ۷ درصد از انتشار مقاله در این گروه را دارا می‌باشند. نشریه IEEE با دو مجله Internet of Thongs Journal و Access هرکدام با یک مقاله سهم ۱۴ درصدی کل مقالات را دارد. دیگر مجلات هرکدام از یک مقاله برخوردار هستند که در شکل (۶) نشان داده‌شده‌اند.

۴،۳. انتشار مقالات بر اساس کنفرانس‌ها

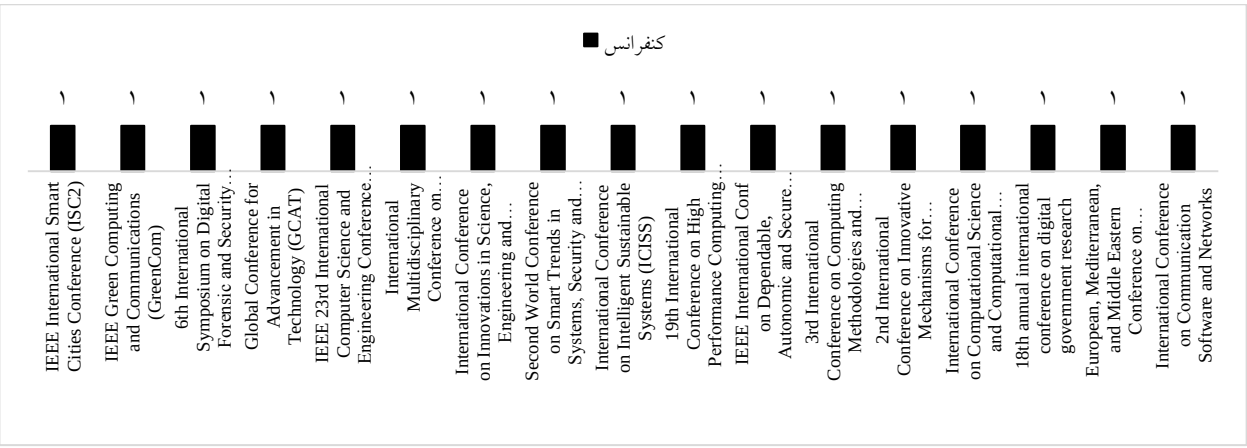
در شکل (۷) مقالات بر اساس کنفرانس‌های مربوطه ارائه‌شده است. بر اساس این شکل ۱۷ کنفرانس مختلف وجود دارند که هرکدام حدوداً سهم ۵ درصدی از مقالات این دسته رادارند. از مهم‌ترین حوزه‌های اصلی این کنفرانس‌ها می‌توان به شهرهای هوشمند، محاسبات و ارتباطات، صنعت کامپیوتر، امنیت و شبکه‌های غیرمتمرکز اشاره کرد.



شکل (۵): انتشار مقالات بر اساس کشور



شکل (۶): مقالات منتشرشده بر اساس مجله.



شکل (۷): تعداد مقالات منتشرشده در کنفرانس ها

۴،۴. طبقه‌بندی مطالعات رأی‌گیری‌های الکترونیکی مبتنی بر فناوری زنجیره بلوکی

برای درک عمیق کاربردهای زنجیره بلوکی در رأی‌گیری‌های الکترونیکی ، جدول (۴) آنالیز و تحلیل مقالات بررسی‌شده را بر اساس تمرکز بر حوزه اصلی، کار اصلی و نظریه ارائه‌شده، موضوعات مهم و چالش‌های موردبحث رأی‌گیری‌های الکترونیکی، همچنین قابلیت‌های زنجیره بلوکی برای ادغام با رأی‌گیری الکترونیکی را نشان می‌دهد. در جدول (۴)، بر اساس تحقیقات انجام‌شده و منابع مورداستفاده تعداد ۱۲ الزام مهم و چالش رأی‌گیری الکترونیکی به دست آورده شده سپس بررسی شد که هرکدام از این ۲۱ مقاله کدام‌یک از آن‌ها را بررسی و ذکر کرده‌اند. دوازده الزام و چالش به این شرح است: عدالت و انصاف[1] در اعلام نتایج مربوط به کاندیداها (چ۱)، واجد شرایط بودن[2] و احراز هویت افراد (چ۲)، حریم خصوصی رأی‌دهندگان و کاندیداها (چ۳)، قابل‌اطمینان بودن سیستم رأی‌گیری و فرایند (چ۴)، ناشناس بودن رأی‌دهندگان (چ۵)، سازگاری داده‌ها و یکپارچگی[3] در سرورهای مختلف (چ۶)، منحصربه‌فرد[4] بودن هویت‌ها و شناسه‌ها (چ۷)، تقلب و صحت نتایج نهایی (چ۸)، شفافیت[5] فرایند رأی‌گیری (چ۹)، کارایی سیستم ازنظر زمان و هزینه (چ۱۰)، مقیاس‌پذیری رأی‌گیری (چ۱۱) و امنیت فرایند، سرورها در مقابل حمله هکرها و خرابی سیستم (چ۱۲).

همانطورکه انتظار می‌رود، بر اساس نتایج به‌دست‌آمده ۲۹ پژوهش به مهم‌ترین چالش رأی‌گیری الکترونیکی یعنی امنیت سامانه‌ها و فرایند رأی‌گیری اشاره کردند. موضوع مهم بعدی ازنظر این پژوهش‌ها حفظ شدن حریم خصوصی رأی‌دهندگان و کاندیداها، قابل‌اطمینان بودن سامانه‌های رأی‌گیری که مرتبط به امنیت و در دسترس بودن است، یکپارچگی سامانه‌های رأی‌گیری و سازگاری اطلاعات سرورهای مختلف با همدیگر از دیگر چالش‌های موردنظر است که هرکدام در ۲۱ پژوهش موردبحث و بررسی. همچنین قرارگرفته‌اند شفافیت سامانه‌های رأی‌گیری است که تعداد ۱۹ پژوهش به آن پرداخته‌اند. هرچند که عدالت و انصاف در اعلام نتایج به‌موقع، مقیاس‌پذیری سیستم رأی‌گیری ازنظر زمانی و تعداد رأی ثبت‌شده در بازه زمانی مشخص و کار آیی سیستم مهم است ولی هرکدام به ترتیب در ۱۰، ۱۲ و ۱۳ پژوهش موردتوجه قرارگرفته است که نشان‌دهنده این است که این موضوعات در اولویت‌های اولیه ارائه و پیاده‌سازی یک سیستم رأی‌گیری مبتنی بر فناوری زنجیره بلوکی نیستند.

به همین ترتیب ۶ قابلیت و ویژگی اصلی زنجیره بلوکی که در رأی‌گیری‌های الکترونیکی مورداستفاده قرارگرفته بود از منابع مطالعاتی استخراج شد که به این شرح است: غیرمتمرکز بودن (و۱)، تغییرناپذیری و غیرقابل دست‌کاری بودن (و۲) ، مقیاس‌پذیری (و۳)، شفافیت (و۴)، الگوریتم‌های اجماع و پروتکل‌های اثبات[6] (و۵) و رمزنگاری (و۶).

طبق بررسی‌های انجام‌شده قابلیت غیرمتمرکز بودن شبکه زنجیره بلوکی بارزترین ویژگی کاربردی زنجیره بلوکی است برای یک سیستم رأی‌گیری الکترونیکی، که مشخصاً ۲۴ پژوهش به این موضوع اشاره داشته‌اند. الگوریتم‌های اجماع و پروتکل‌های اثبات که برای شفافیت بیشتر، قابل‌اطمینان بودن و امنیت بیشتر شبکه در زنجیره بلوکی ارائه‌شده است در ۱۹ پژوهش بررسی‌شده موردتوجه قرارگرفته. یکی دیگر از ویژگی‌های زنجیره بلوکی، یعنی شفافیت شبکه بسیار به یک سیستم رأی‌گیری کمک خواهد کرد که اعتماد عمومی و رأی‌دهندگان را جلب کند، و این امر در ۲۰ مقاله اشاره‌شده ***است***. دیگر ویژگی‌های کلیدی زنجیره بلوکی اعم از فن رمزنگاری اطلاعات و بلوک‌ها، مقیاس‌پذیری شبکه و تغییرناپذیری و غیرقابل دست‌کاری بودن به ترتیب هرکدام در ۱۹، ۱۱ و ۱۱ مقاله موردتوجه قرارگرفته است. آنچه دریافت می‌شود نشان می‌دهد که اساساً زنجیره بلوکی برای افزایش امنیت سامانه‌های رأی‌گیری از طریق غیرمتمرکز بودن شبکه و فن‌های رمزنگاری اطلاعات پیشنهاد می‌شود.

[1] Fairness and justice
[2] Eligibility
[3] Data consistency and integrity
[4] Uniqueness
[5] Transparency
[6] Consensus algorithms and proofs protocols

جدول (۴): آنالیز و تحلیل مقالات بررسی‌شده

منابع	تمرکز بر حوزه اصلی	کار اصلی و نظریه ارائه‌شده	موضوعات مهم و چالش‌های رأی‌گیری الکترونیکی														قابلیت‌های زنجیره بلوکی					
			۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱	۲	۳	۴	۵	۶
[۱۵]	اتریم، رأی‌گیری الکترونیکی	آنالیز بر اساس چندین معیار	✓	✓	✓	✓				✓				✓	✓	✓	✓	✓				✓
[۲۰]	امضای حلقه، رأی‌گیری	ارائه یک متد					✓	✓	✓			✓	✓	✓	✓		✓	✓		✓		✓
[۲۱]	زنجیره بلوکی، رأی‌گیری الکترونیکی، رمزنگاری	ارائه یک پروتکل	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓		✓		✓		✓	✓
[۲۲]	زنجیره بلوکی، بیت کوین	شبیه‌سازی		✓		✓			✓		✓		✓		✓		✓					
[۲۳]	زنجیره بلوکی، رأی‌گیری الکترونیکی، مقیاس‌پذیری	ارائه یک مدل	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	
[۲۴]	زنجیره بلوکی، رأی‌گیری الکترونیکی، هوشمند سازی	ارائه یک طرح		✓	✓		✓		✓	✓	✓	✓	✓				✓		✓	✓		
[۲۵]	رأی‌گیری آنلاین، رأی‌گیری مبتنی بر زنجیره بلوکی	آنالیز منظم	✓	✓		✓			✓	✓	✓							✓	✓	✓	✓	✓
[۱۶]	زنجیره بلوکی، قرارداد هوشمند، رأی‌گیری	مطالعه موردی		✓			✓			✓		✓	✓				✓	✓	✓	✓	✓	✓
[۲۶]	رأی‌گیری، حریم خصوصی، زنجیره بلوکی	ارائه پروتکل	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓		
[۲۷]	اتریم	پیاده‌سازی یک اپلیکیشن		✓			✓	✓		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
[۲۸]	زنجیره بلوکی، رأی‌گیری	ارائه یک سیستم		✓			✓	✓	✓					✓	✓		✓		✓	✓	✓	✓
[۲۹]	زنجیره بلوکی، رأی‌گیری الکترونیکی	طراحی یک معماری						✓									✓		✓			✓
[۳۰]	اتریم، رأی‌گیری، اعتماد، یکپارچه‌سازی	ارائه یک سیستم	✓	✓			✓	✓		✓	✓		✓		✓	✓	✓		✓	✓	✓	✓
[۳۱]	زنجیره بلوکی، رأی‌گیری الکترونیکی، حریم خصوصی	ارائه یک مدل		✓	✓			✓	✓			✓	✓	✓			✓		✓	✓	✓	✓
[۳۲]	زنجیره بلوکی، رأی‌گیری الکترونیکی، اعتبارسنجی	ارائه یک سیستم	✓		✓	✓			✓		✓	✓	✓			✓	✓		✓		✓	✓
[۳۳]	زنجیره بلوکی، رأی‌گیری الکترونیکی	مرور کوتاه		✓	✓	✓			✓			✓	✓				✓		✓			
[۳۴]	الگوریتم‌های اجماع، رأی‌گیری، زنجیره بلوکی کنسرسیوم	ارائه یک پروتکل اجماع	✓				✓			✓	✓		✓		✓		✓	✓				✓
[۳۵]	رأی‌گیری، حریم خصوصی، زنجیره بلوکی	ارائه یک سیستم	✓		✓	✓			✓	✓	✓	✓	✓				✓		✓			
[۳۶]	زنجیره بلوکی، رایانش ابری، رأی‌گیری	ارائه یک طرح									✓											
[۳۷]	رأی‌گیری الکترونیکی، شناسه‌های مجازی، زنجیره بلوکی	ارائه یک طرح									✓	✓	✓				✓					
[۳۸]	رأی‌گیری اینترنتی، بیت کوین	ارائه یک طرح				✓	✓			✓	✓			✓	✓		✓		✓	✓		✓
[۹]	رأی‌گیری الکترونیکی، اعتماد، زنجیره بلوکی	یک بررسی کوتاه				✓				✓				✓	✓		✓		✓		✓	
[۳۹]	رمزنگاری، رأی‌گیری الکترونیکی، زنجیره بلوکی	طراحی یک پروتکل	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓	✓
[۴۰]	رأی‌گیری، تقلب انتخاباتی، زنجیره بلوکی	بررسی یک ایده	✓	✓	✓		✓	✓	✓		✓	✓				✓	✓		✓		✓	✓
[۱۰]	رأی‌گیری از راه دور، ناشناس ماندن رأی‌دهندگان	ارائه یک مدل	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
[۸]	رأی‌گیری الکترونیکی، شهرهای هوشمند، زنجیره بلوکی	ارائه یک طرح	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓			✓
[۱۷]	امنیت رأی‌گیری، رأی‌گیری مبتنی بر فناوری زنجیره بلوکی	تحلیل و بررسی		✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓		✓	✓	✓	✓
[۴۱]	زنجیره بلوکی، سامانه‌های رأی‌گیری، قراردادهای هوشمند	ارائه یک مدل		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
[۴۲]	اینترنت اشیا، زنجیره بلوکی	طراحی یک الگوریتم				✓			✓	✓	✓			✓	✓		✓		✓	✓	✓	✓
[۴۳]	رأی‌گیری آنلاین، زنجیره بلوکی	ارائه یک مدل									✓			✓	✓		✓					✓
		نتایج نهایی	۱۰	۱۴	۲۱	۱۶	۱۳	۲۰	۱۱	۲۰	۱۹	۱۳	۱۳	۲۹	۱۲	۱۳	۲۴	۱۱	۱۱	۲۰	۱۹	۱۹

۵. بررسی نتایج و پاسخ به سؤالات تحقیق

در این بخش سعی شده است که به سؤالات تحقیق بر اساس مقالات بررسی‌شده پاسخ داده شود. ابتدا بر اساس روش بررسی منظم ادبیات مهم‌ترین چالش‌های رأی‌گیری الکترونیکی را همانطورکه در جدول (۴) اشاره شد شرح داده می‌شود. سپس، با درک و شناخت مهم‌ترین قابلیت‌های زنجیره بلوکی و ارتباط دادن آن ویژگی‌ها با چالش‌های رأی‌گیری الکترونیکی، نتایج حاصل از ادغام فناوری زنجیره بلوکی با رأی‌گیری الکترونیکی ارائه می‌شود. بر اساس یافته‌های به‌دست‌آمده از بررسی منظم ادبیات، چالش‌های جدیدی پیش روی سامانه‌های رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی وجود دارد، مانند مقیاس‌پذیری و موضوع هزینه‌های استخراج بلوک، که در این بخش آن‌ها را شرح خواهیم داد. در انتهای این بخش هم بحثی

پیرامون آینده رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی ارائه شده است.

۵,۱. مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی چیست؟

در جدول (۴)، به ۱۲ موضوع مهم و چالش اصلی در ارتباط با رأی‌گیری‌های الکترونیکی اشاره شد. مهم‌ترین چالش برجسته که محققان در نظر دارند امنیت یک سیستم رأی‌گیری است، و این مهم به دلیل اینترنتی بودن ارتباطات سرورهای رأی‌گیری، دیجیتالی بودن برگه‌های رأی و احراز هویت الکترونیکی افراد شرکت‌کننده است [۲۱]. معمولاً نتایج رأی‌گیری بعد از اتمام ثبت آخرین رأی و شمارش آن‌ها اعلام خواهد شد. اگر رأی‌ها به‌درستی ثبت‌نشده باشند و یا سرور اصلی رأی‌گیری از دسترس خارج شود یا هک شود، نتایج به‌دست‌آمده با ابهاماتی روبرو خواهد بود که آن را قابل‌اطمینان و تائید نخواهد کرد [۲۳]. این ریسک در سامانه‌هایی بیشتر موضوعیت پیدا می‌کند که در آن سرورهای مرکزی وظیفه اجرای فرایند رأی‌گیری و ذخیره‌سازی اطلاعات و رأی‌ها هستند [۳۲].

بدین ترتیب یکپارچه‌سازی اطلاعات برخط حوزه‌های رأی‌گیری شامل داده‌های تائید شده هویتی و رأی‌های اخذشده و سازگاری آن‌ها با همدیگر از چالش‌هایی است که ممکن است با قطع شدن ارتباط این مراکز با همدیگر به وجود بیاید [۳۰]. نهایتاً یک فرد به دلیل اینکه رأی ثبت‌شده او در یک حوزه به دلیل قطعی ارتباط (اینترنت یا خراب شدن سخت‌افزار سرورها) هنوز به دیگر حوزه‌ها و سرورها ارائه نشده، می‌تواند دوباره رأی بدهد و یا اینکه اصلاً رأی او ثبت نشود.

در اولویت‌های بعدی دسته‌بندی چالش‌ها، حفظ حریم خصوصی رأی‌دهندگان و کاندیداها در عین اینکه سیستم شفاف و قابل‌اطمینان باشد، است. برای ایجاد اعتماد و اطمینان به سیستم رأی‌گیری مهم است که مراحل ثبت، نحوه ذخیره‌سازی و مکانیسم شمارش آراء شفاف و قابل‌درک باشد، اما نیاز است که نتایج تا بعد از اخذ آخرین رأی محرمانه بماند تا اینکه بر روند رأی‌گیری تأثیر نداشته باشد. اغلب رأی‌دهندگان تمایل دارند که مشارکتشان در رأی‌گیری آشکار نشود و اطلاعات هویتی و رأی آن‌ها باید کاملاً محرمانه باشد همچنین در مکانیسم رأی‌گیری مشخص نباشد که چه شخصی به چه کاندیدی رأی داده است تا از این موضوع سوء استفاده نشود [۲۶, ۳۵].

از دیگر چالش‌های موردبحث می‌توان به واجد شرایط بودن رأی‌دهندگان و اجرا نمودن قوانین به همراه مکانیسم احراز هویت قوی برای جلوگیری از جعل هویت و سوءاستفاده از حق رأی افراد واجد شرایط، همچنین به مقیاس‌پذیری سیستم رأی‌گیری اشاره نمود. مقیاس‌پذیری یک سیستم رأی‌گیری الکترونیکی به دلیل استفاده از دستگاه‌های شخصی مانند کامپیوتر شخصی و تلفن همراه هوشمند متصل به پورتال یا نرم‌افزار رأی‌گیری این امکان را فراهم می‌کند که افراد در منزل، محل کار و حتی در مسافرت در رأی‌گیری شرکت کنند. اما مدیریت محاسباتی و ذخیره‌سازی اطلاعات یک سیستم رأی‌گیری در مقیاس میلیونی می‌تواند چالش‌هایی جدی همراه با الزامات و ریسک‌های امنیتی به همراه داشته باشد.

۵,۲. ویژگی‌های زنجیره بلوکی که می‌تواند راه‌حلی برای چالش‌های یک رأی‌گیری الکترونیکی باشد، چیست؟

همانطورکه پیش‌تر اشاره‌شده، زنجیره بلوکی یک شبکه‌ای از گره‌های غیرمتمرکز است که در آن اطلاعات در قالب تراکنش‌های رمزنگاری‌شده در بلوک‌ها ثبت‌شده و به‌طور یکسان در کل شبکه ثبت و ذخیره می‌گردد. آنچه پژوهشگران را متقاعد کرد که زنجیره بلوکی گزینه مناسبی برای ادغام با رأی‌گیری‌های الکترونیکی است شامل مجموعه‌ای از ویژگی‌های ساختاری و فن‌های در نظر گرفته‌شده در این شبکه یا به تعبیری پایگاه داده غیرمتمرکز است که مستقیماً برای افزایش امنیت یک سیستم رأی‌گیری الکترونیکی قابل‌استفاده است. به دلیل غیرمتمرکز بودن گره‌های ذخیره‌سازی و محاسباتی در شبکه زنجیره بلوکی، این ایده توسط پژوهشگران ارائه‌شده است که سرورهای محاسباتی و ذخیره‌سازی مرکزی یک سیستم رأی‌گیری

الکترونیکی مبتنی بر زنجیره بلوکی طراحی و بهره‌برداری شود. این ایده برای افزایش امنیت سرورها در مقابل خرابی و هک شدن آن‌ها، همچنین ثبت نسخه‌های پشتیبان در سرتاسر شبکه باعث اطمینان از اطلاعات ذخیره‌شده می‌شود [۱۵, ۲۵].

در صورت خرابی یا از دسترس خارج شدن تعدادی از گره‌ها و سرورها در شبکه زنجیره بلوکی، همچنان شبکه به‌طور قابل‌اطمینان می‌تواند به کار خود یعنی ثبت و ذخیره‌سازی رأی‌ها ادامه دهد. در زنجیره بلوکی، بر اساس نوع کاربرد تعداد زیادی مکانیسم اجماع و پروتکل اثبات ارائه‌شده است. وقتی از سازوکار اجماع برای تائید فرایند رأی‌گیری استفاده شود، تمام شبکه به فرایند ثبت و ذخیره‌سازی آراء نظارت خواهند داشت و این اعتماد به نتایج و سیستم را بسیار افزایش می‌دهد و این حاصل شفافیت سیستم خواهد بود. در مقاله [۳۴] اشاره شده است که بیت کوین برای اولین بار سازوکار اجماع غیرمتمرکز را معرفی کرد. بااین‌حال، سازوکارهای اجماع بیت کوین برای اعمال در یک سیستم رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی کنسرسیوم مناسب نیست، به همین دلیل آن‌ها یک سازوکار اجماع جدید، اثبات رأی (POV) را پیشنهاد دادند. این سازوکار اجماع ارائه‌شده توسط گره‌های توزیع‌شده در زنجیره بلوکی کنسرسیوم هماهنگ می‌شود که با رأی‌گیری به یک داوری و نظارت غیرمتمرکز می‌رسند.

ایده اصلی ایجاد هویت امنیتی متفاوت برای شرکت‌کنندگان در شبکه است به‌طوری‌که ارسال و تأیید بلوک‌ها با یک فرایند رأی‌گیری گره‌ها که بدون وابستگی به یک واسطه شخص ثالث است، تصمیم‌گیری می‌شود. از دیگر ویژگی‌های مهم زنجیره بلوکی می‌توان به رمزنگاری تراکنش‌ها و بلوک‌ها اشاره کرد که در این سیستم هیچ داده‌ای اعم از رأی‌ها و اطلاعات هویتی تائید شده به‌صورت اصلی وجود ندارد بلکه توسط توابع مختلف برای افزایش امنیت رمزنگاری خواهند شد. هر رأی که در قالب یک تراکنش در زنجیره بلوکی ثبت خواهد شد به دلیل اینکه توسط سازوکار اجماع به‌صورت کاملاً شفاف تائید شده و در سرتاسر شبکه ذخیره می‌شود، امکان تغییر و دست‌کاری آن وجود ندارد، یعنی عملاً برای تغییر یا تحریف یک رأی باید کل داده ذخیره‌شده در شبکه زنجیره بلوکی تغییر داده شود که این موضوع به دلیل ویژگی تغییرناپذیری زنجیره بلوکی، ناممکن است [۳۵].

۵،۳. مهم‌ترین چالش‌های رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی چیست؟

هرچند که پژوهش‌های انجام‌شده مناسبی در ارتباط با ادغام رأی‌گیری الکترونیکی با زنجیره بلوکی در چند سال اخیر انجام‌شده است، اما در بعد عملیاتی در مراحل اولیه خود هستند، بااین‌وجود محققان انتظار دارند که چالش‌هایی پیش روی سامانه‌های رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی باشد. بر اساس بررسی ادبیات تحقیق، مطالعات نشان می‌دهد که ۳ چالش اصلی در سامانه‌های رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی وجود خواهد داشت، که به مقیاس‌پذیری، هزینه استخراج بلوک‌ها و حمله انعطاف‌پذیری تقسیم می‌گردد. باوجوداینکه چالش‌هایی در ارتباط با رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی وجود دارد، اما از بین مطالعات انجام‌شده تعداد بسیار کمی از آن‌ها به این موضوع پرداخته بودند.

یکی از ویژگی‌های شبکه‌های زنجیره بلوکی این بود که به دلیل پراکندگی جغرافیای گره‌ها و کاربران این امکان وجود دارد که چند صد هزار یا میلیون گره به شبکه ملحق شوند (همانطورکه در بیت کوین شاهد هستیم) اما در حقیقت به دلیل سازوکار در نظر گرفته‌شده در سامانه‌های زنجیره بلوکی تعداد تراکنش یا رأی که امکان ثبت شدن را در بازه مشخص (مثلاً دقیقه یا ساعت) دارند بسیار کم است. این موضوع باعث می‌شود که استفاده از معروف‌ترین پلتفرم‌های زنجیره بلوکی یعنی، بیت کوین و اتریم در رأی‌گیری‌های مقیاس کوچک استفاده شود و مدل متناسب آن ارائه شود [۱۵, ۲۲, ۲۷, ۳۸].

در بیت کوین و اتریم به ازای هر تراکنش یک مقدار مشخص به‌عنوان هزینه اجرای تراکنش که به آن کمیسیون گفته می‌شود اخذ می‌شود [۴۴]. اینجا است که باید تعیین کرد که آیا رأی‌دهندگان این هزینه را بپردازند، دولت یا مجری رأی‌گیری و یا توسط سازمان‌های نظارتی–حمایتی پرداخت شود. در این

مورد هنوز پژوهشگران بـه راهکـاری عملیـاتی و موردتوافـق نرسیده‌اند.

در مقالــه [۲۲]، تمرکــز اصــلی نویســندگان بــر حمــلات انعطاف‌پذیری تراکنش‌های زنجیره بلوکی است کـه مـی‌توانـد به‌عنوان یک حمله مبتنی بر طراحی نرم‌افزار در نظر گرفته شود که می‌تواند منجـر بـه هزینـه مضـاعف شـود. در یـک حملـه انعطاف‌پذیری تراکنش، شناسه تـراکنش قبـل از اسـتخراج در شبکه زنجیره بلوکی تغییر می‌کند. مشخصاً، هدف استفاده از این تراکنش انعطاف‌پذیر تأییدشده، تکرار تراکنش اصلی است کـه امکان استخراج آن در ابتدا وجود ندارد (یعنی دو بار تراکنش را در شبکه اجرا کردن و این هزینه مضـاعف دارد). همانطورکـه توسط [۴۵] نشان داده‌شده است، در یک حمله موفقیـت‌آمیـز، گیرنده تراکنش معمولاً معتقد است که تراکنش آن‌ها تأیید شده است درحالی‌که در همین حین تلاش می‌شود تـراکنش مشـابه دیگری در شبکه اجرا شود و مورد تأیید شبکه قرار بگیرد. اگر این حمله موفق آمیز باشد، به ازای یک شناسه معتبر رأی، می‌توان دو رأی را در شبکه بلاک چین ذخیره و ثبت نمود و به این صورت نتیجه آراء قابل اعتبار نخواهد بود.

۵,۴. آینده‌ی رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی چگونه خواهد بود؟

آنچه امروزه مشاهده می‌شود اهمیت روزافزون تأثیر رأی‌گیری بر مسائل سیاسـی و اجتمـاعی اسـت. نـه‌تنهـا در کشـورهای توسعه‌یافته و مدرن که ابعاد تحقق دموکراسی اجتماعی و حفظ آن از طریق رأی‌گیری مهم است، بلکـه دیگـر کشـورها بـرای ارتقاء سطح اعتماد و شفافیت در جامعه باید فرایند رأی‌گیری را جدی گرفته و چالش‌های آن‌ها تشریح و موردتوجه قرار دهند. در این میان چالش‌های موجود رأی‌گیری‌های سنتی-کاغذی و رأی‌گیری‌های الکترونیکی واضح و قابل‌درک است. در سال‌های اخیر با الکترونیکی/اینترنتی شدن خدمات و فرایندهای دولتی و سازمانی، نیاز به الکترونیکی/اینترنتی شدن رأی‌گیری‌های سنتی به‌موازات این تغییرات، بسیار احساس می‌گردد [۴۰]. در مقاله [۴۰] تأثیر تقلب در رأی‌گیری‌های الکترونیکی بررسی‌شده است و فناوری زنجیره بلوکی به‌عنوان فناوری کاربردی امـا پیچیـده پیشنهاد گردیده است. امنیت سیستم رأی‌گیری و مسائل پیرامون حریم خصوصی رأی‌دهندگان به همراه جلـوگیری از تقلـب و نتایج قابل‌اطمینان از اصولی‌ترین مباحث مرتبط بـا رأی‌گیـری الکترونیکی است. باوجوداینکه چندین چالش در ارتباط با ادغام رأی‌گیری الکترونیکی با زنجیره بلوکی وجود دارد، اما محققان بر این اصل اتفاق‌نظر دارند که قابلیت‌های زنجیره بلوکی برای رفع چالش‌های موجود این سامانه‌های رأی‌گیری بسیار مناسب و مؤثر خواهد بود.

لازمه ارائه یک سیستم شفاف برای رأی‌گیری به همـراه حفـظ حریم خصوصی شرکت‌کنندگان با توجـه بـه شـفافیت شـبکه زنجیره بلوکی و ناشناس ماندن افراد در زنجیره بلـوکی امـری است که محققان به آن اشاره داشته و در آینده برای تحقق آن، زنجیره بلوکی گزینه عملیاتی متناسب آن خواهد بود. امروزه در کشورهای پیشرفته که سطح آشنایی مردم با رسانه‌های شنیداری و اجتمـاعی بـه نسـبت دیگـر کشـورها زیـاد اسـت و ارکـان الکترونیکی شدن خدمات دولتی در آن‌ها سال‌ها است ارائه‌شده، مردم با الکترونیکی بودن رأی‌گیـری‌هـا و مزایـا و معایـب آن آشنایی دارند. اما آنچه این مطالعه نشان می‌دهـد پژوهشـگران علاقه‌مند به این حوزه و مقالات ارائه‌شـده سـابقه‌ای چندسـاله دارد و ارائه و اجرایی کردن سامانه‌های رأی‌گیری الکترونیکـی مبتنی بر زنجیره بلوکی نیازمند تحقیق بیشـتر و آشـنا سـاختن عموم جامعه با این موضوع و جلب اعتماد مردم دارد.

چند سالی است که اتریم یکی از پلتفرم‌های معـروف زنجیـره بلوکی، فنّاوری جدیدی به نام قراردادهای هوشمند ارائه کـرده است. همانطورکه قبلاً به‌طور مختصر اشاره شـد، قراردادهـای هوشمند که نوعی عملیـات کـامپیوتری و ریاضـی اسـت کـه به‌صورت خودکار اجرا خواهد شد، نیازی به اعتمـاد مـابین دو طرف قرارداد نیست. زنجیره بلوکی به‌واسطه فناوری قراردادهای هوشمند این امکان را فراهم می‌کند که رأی‌ها به‌صورت خودکار شـمارش‌شـده و بلافاصـله بعـد از اخـذ آخـرین رأی نتـایج قابل‌استخراج باشد [۱۶]. می‌توان نتیجه گرفت که رأی‌گیری‌های الکترونیکی بـه‌واسـطه قابلیـت تغییرناپـذیری زنجیـره بلـوکی

دستخوش تغییر و ادغام با این فناوری جدید خواهد شد. اما پروتکل‌های اجماع قدیمی، به‌عنوان رکن و ابزار اساسی ایجاد امنیت و اعتماد در شبکه، مانند آنچه در بیت کوین استفاده‌شده است، باعث هدر رفت و مصرف بیش از اندازه انرژی خواهد بود [۴۱].

۶. پیامدهای اجرایی و تحقیقاتی

این مطالعه برای سیاست‌گذاران دولتی، پژوهشگران، گروه‌های استارت‌آپ و تصمیم‌گیرندگان کلان علاقه‌مند به درک عمیق‌تر کاربردهای زنجیره بلوکی در حوزه رأی‌گیری الکترونیکی پیامدهای مهمی دارد. در این زمینه، اعلام نتایج به‌موقع و دقیق و حفظ حریم خصوصی رأی‌دهندگان بسیار حائز اهمیت است. به‌عنوان‌مثال، در انتخابات ریاست جمهوری آمریکا در سال ۲۰۲۰ تأخیر در اعلام نتایج، ادعای تقلب و تحریف نتایج و غیرقابل اطمینان بودن سامانه‌های رأی‌گیری الکترونیکی همچنین سوءاستفاده از اطلاعات رأی‌دهندگان از مهم‌ترین چالش‌های پیش‌آمده بود. یکی از نامزدها، آقای دونالد ترامپ، اسنادی را ارائه کردند که به نظر می‌رسید فرایند ثبت و شمارش آراء به‌طور دقیق انجام نگرفته است و نتایج اعلام‌شده را مغایر با واقعیات و اسناد می‌دانست.

به نظر می‌رسد در اینجا مشخصاً ویژگی غیرمتمرکز بودن سامانه‌های رأی‌گیری مبتنی بر الگوریتم‌های اجماع زنجیره بلوکی و فن‌های رمزنگاری اطلاعات، به‌خوبی می‌تواند این چالش‌ها را برطرف نماید. آنچه یک سیستم رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی به همراه دارد شامل شمارش خودکار آراء، امنیت بسیار زیاد سیستم و جلوگیری از هک شدن، ذخیره‌سازی ایمن و قابل‌اطمینان بودن نتایج است. این امر سیاست‌گذاران و مدیران عملیاتی را ترغیب خواهد کرد که برای جلوگیری از ریسک‌ها و چالش‌های به وجود آمده رأی‌گیری‌های الکترونیکی و اینترنتی بیش‌ازپیش به فناوری زنجیره بلوکی توجه داشته باشند و مهم‌ترین قابلیت‌های زنجیره بلوکی را درک کنند و در فرایندهای مدیریتی، تصمیمی و عملیاتی خود به آن اهمیت دهند. همچنین یکی از پیامدهای این پژوهش انجام‌شده این است که اهمیت نتایج و پیامدهای رأی‌گیری بر جوامع، سیاست‌ها، افکار عمومی و دموکراسی، پژوهشگران را به مطالعه و بررسی این حوزه ترغیب کند و در عمل خلأهای تحقیقاتی را پیدا کنند و پژوهش‌های متناسبی در این حوزه در آینده انجام گیرد.

۷. پیامدهای تحقیق و تحقیقات آینده

از نظر دانشگاهی، این مطالعه دیدگاه‌های اساسی را به پژوهشگران علاقه‌مند به پیشرفت و توسعه این موضوعات داغ ارائه می‌دهد. قابلیت‌های زنجیره بلوکی می‌تواند در اکثر حوزه‌ها و برای حل چالش‌های رأی‌گیری الکترونیکی استفاده شوند. بنابراین، همانطورکه در شکل‌های (۵)، (۶) و (۷) برجسته شده است، انتظار داریم روند رو به رشدی در انتشار تحقیقات را در این زمینه در چند سال پیش رو داشته باشیم. درنتیجه، این یک حوزه تحقیقاتی جذاب برای تحقیقات آینده است.

به‌عنوان یک دستاورد مهم، این مقاله یک دستور کار مفصل و مداوم را برای تحقیقات آینده پیشنهاد می‌دهد. جدول (۵) دستور کار تحقیقاتی پیشنهادی در مورد ادغام زنجیره بلوکی با رأی‌گیری‌های الکترونیکی را ارائه می‌دهد. مطالعه صورت گرفته برای این مقاله نشان داد که کمبود مطالعات تجربی گزارش‌شده و طرح‌های ارائه‌شده برای رأی‌گیری‌های مقیاس بزرگ همچنین بررسی چالش‌های اصلی رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی وجود دارد. همچنین شکل (۵) نشان می‌دهد، پژوهش‌های منتشرشده از اقتصادهای در حال ظهور و کشورهای کمتر توسعه‌یافته در مقایسه با کشورهای پیشرفته، از نظر انتشار کم است. برای غلبه بر این موضوع، این مقاله تحقیقاتی را برای درک سطح فعلی موضوع رأی‌گیری‌های الکترونیکی و چالش‌های اصلی آن به‌علاوه زنجیره بلوکی و قابلیت‌های آن برای ترسیم و شناخت بیشتر این مشکلات اصلی پیشنهاد می‌دهد. علاوه بر این، مطالعات بررسی‌شده گزارش دهنده دیدگاه‌های مختلف از کاربردهای زنجیره بلوکی درزمینه رأی‌گیری الکترونیکی و کمک به تحقق دموکراسی در جوامع هستند، و این‌یک موضوع بالقوه است.

جدول (۵): دستور کاری برای تحقیقات آینده در حوزه رأی‌گیری‌های الکترونیکی مبتنی بر زنجیره بلوکی

نواقص در مطالعات	فرصت‌های مطالعاتی در آینده
مطالعات تجربی و تحلیل معیارهای پیاده‌سازی مدل در مقیاس واقعی	برای بررسی بهترین روش‌های کارآمد مرتبط با اجرای زنجیره بلوکی در رأی‌گیری‌های مقیاس بزرگ
مطالعات تجربی و تحلیل چالش‌های اجرایی	بررسی چالش‌های اصلی مرتبط با اجرا و شناسایی راه‌حل‌های اصلی مؤثر برای غلبه بر چالش‌ها
حملات ۵۱٪	بررسی اجرایی تأثیر حملات ۵۱٪ در نتایج نهایی رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی
بررسی دقیق‌تر قابلیت‌های زنجیره بلوکی	برای بررسی توانایی‌های موردنیاز دولت‌ها برای پیاده‌سازی و استفاده از زنجیره بلوکی در رأی‌گیری الکترونیکی
قراردادهای هوشمند	برای بررسی قابلیت‌های جدید با استفاده از قراردادهای هوشمند در رأی‌گیری‌های الکترونیکی
هزینه تراکنش‌ها	برای بررسی هزینه‌ها در مدل‌هایی که زنجیره بلوکی و قراردادهای هوشمند را در رأی‌گیری الکترونیکی اجرا کرده‌اند
تعامل و ارتباط رأی‌دهنده و کاندیدا	درزمانی که از قرارداد هوشمند استفاده شود، اعتماد مابین رأی‌دهنده و کاندیدا چطور خواهد بود؟ اطمینان از ثبت رأی چگونه خواهد بود؟
امنیت زنجیره بلوکی	برای شناسایی سطح امنیت ارائه‌شده توسط زنجیره بلوکی در رأی‌گیری‌های الکترونیکی. مزایای اصلی آن چیست؟
ادغام اینترنت اشیا با رأی‌گیری الکترونیکی	بررسی قابلیت‌های اینترنت اشیا در رأی‌گیری الکترونیکی
احراز هویت غیرمتمرکز	بررسی چالش‌های سامانه‌های احراز هویت و ذخیره‌سازی اطلاعات هویتی تائید شده
زنجیره بلوکی ترکیبی	بررسی قابلیت‌های زنجیره‌های بلوکی ترکیبی برای رأی‌گیری الکترونیکی در مقابل زنجیره بلوکی عمومی و خصوصی

۸. بحثی در مورد یافته‌ها

مطالعات نشان می‌دهد که موضوع ارائه و اجرایی کردن یک سیستم رأی‌گیری الکترونیکی به‌صورت واقع‌گرایانه و در مقیاس بزرگ، موردتوجه قرار خواهد گرفت و این‌یک نیاز عملیاتی و تحقیقاتی است که حوزه جذابی برای پژوهشگران خواهد بود. در این پژوهش ۳۰ مقاله علمی را بر اساس کلمات کلیدی در پایگاه داده‌های علمی-تخصصی جستجو شده انتخاب گردید. ذکر این نکته مهم است که تعداد مقالات موجود همانطورکه در شکل (۴) نشان داده‌شده است بیشتر از ۳۰ عدد است، اما به دلیل محدودیت حجم مطالب و دسترسی به جدیدترین پژوهش‌های انجام‌شده و نتایج آن‌ها، و همچنین با توجه به معیارهای انتخاب مقالات درنهایت این تعداد انتخاب گردید. در این ۳۰ مقاله انتخاب‌شده، ۱۲ چالش و الزام مهم مربوط به رأی-گیری الکترونیکی استخراج شد (جدول ۴).

بیشترین حساسیت موجود مربوط به امنیت یک سیستم رأی-گیری مبتنی بر بستر ارتباطی اینترنت با دستگاه‌های الکترونیکی و داده‌های دیجیتالی، است. حفظ امنیت در مقابل تهدیدات هکرها، خرابی سرورها، حملات DDos[1]، امنیت دستگاه‌های شخصی و پورتال یا نرم‌افزار رأی‌گیری بسیار مهم است. این موضوع باعث شده که عموم جامعه به نتایج حاصله از این سامانه‌های رأی‌گیری الکترونیکی اعتماد کمی داشته باشند، باوجوداینکه مزایای بسیاری به نسبت رأی‌گیری‌های سنتی-کاغذی دارد. زنجیره بلوکی به‌عنوان یک شبکه غیرمتمرکز از گره‌های متعدد با استفاده از فن‌های رمزنگاری، الگوریتم‌های اجماع و دیگر قابلیت‌ها (جدول ۴)، سطح رضایت خوبی برای رفع چالش‌های رأی‌گیری‌های الکترونیکی ایجاد کرده است. یافته‌ها نشان می‌دهد که هرچند عملیاتی کردن یک سیستم رأی-گیری الکترونیکی در مقیاس بزرگ مهم است اما آخرین چالش موردنظر محققان این موضوع مقیاس‌پذیری بوده است.

به دلیل اینکه در سال‌های اخیر کاربردهای فناوری زنجیره بلوکی در حوزه‌های مختلف بسیار زیاد شده، پلتفرم‌های متعددی مبتنی بر زنجیره بلوکی ارائه‌شده، و قابلیت جدیدی از فناوری زنجیره بلوکی به اثبات رسیده، و شاهد هستیم که پژوهشگران به دنبال ارائه مدل و سامانه‌های رأی‌گیری الکترونیکی در مقیاس کوچک برای ارزیابی اولیه این موضوع هستند. از دیگر یافته‌های این مطالعه این است که، ادغام زنجیره بلوکی با رأی‌گیری‌های الکترونیکی دستخوش چالش‌هایی خواهد بود مانند ۳ چالش مقیاس‌پذیری، موضوع هزینه و کمیسیون تراکنش‌ها و حملات انعطاف‌پذیری که از مقالات

[1] Distributed Denial-of-Service

بررسی‌شده استخراج شد. اما به‌طور واضح انتظار می‌رفت که بحث در مورد چالش‌های حملات ۵۱٪ و مشکلات انشعاب مرتبط با فناوری زنجیره بلوکی و تأثیر آن در نتایج نهایی یک سیستم رأی‌گیری الکترونیکی مبتنی بر زنجیره بلوکی در مطالعات بررسی‌شده مشاهده شود، ولی متأسفانه به آن پرداخته نشده بود.

در مورد آینده ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی انتظار درک بیشتر از قابلیت‌های زنجیره بلوکی و چالش‌های عملیاتی شدن این ادغام می‌رود، زیرا اکثر مقالات مطالعه شده طرح‌های تحقیقاتی بسیار خوبی از منظر توسعه مدل خود و پوشش دادن منسجم‌تر چالش‌های رأی‌گیری الکترونیکی برای آینده ارائه نمودند. همچنین، در عصر دیجیتالی امروز با توسعه زیرساخت‌های اینترنت و هوشمند شدن محیط و بهبود امنیت دستگاه‌های الکترونیکی و دستگاه‌های شخصی ارتباطی، انتظار می‌رود که به‌سرعت کشورهای مختلف که با چالش‌ها و هزینه-های فرایندهای رأی‌گیری سنتی-کاغذی خود روبرو هستند همچنین بر اساس انتظارات این جوامع از دولت‌های خود، واقعیت الکترونیکی شدن رأی‌گیری‌ها بیشتر اهمیت پیدا کند. بنابراین اینجا است که ۶ قابلیت زنجیره بلوکی که در جدول (۴) به آن اشاره‌شده موردتوجه قرار خواهد گرفت.

۹. نتیجه‌گیری و محدودیت‌های نهایی

این مطالعه وضعیت فعلی کاربردهای زنجیره بلوکی را درزمینه رأی‌گیری الکترونیکی بررسی کرد. در بررسی ادبیات از یک رویکرد منظم برای کشف کاربردهای زنجیره بلوکی درزمینه رأی‌گیری الکترونیکی استفاده شد. یافته‌ها نشان داد اگرچه پیاده‌سازی و عملیاتی کردن ادغام زنجیره بلوکی در رأی‌گیری الکترونیکی و تحقیقات کامل مرتبط هنوز در مراحل ابتدایی قرار دارند، برخی از کشورها (بین سال‌های ۲۰۱۷ تا ۲۰۲۱) سهم بیشتری از ادبیات مربوطه در ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی دارند. به‌عنوان‌مثال پژوهشگران آمریکا، هند و بریتانیا حدوداً ۴۵ درصد از مطالعات را انجام داده‌اند.

به‌طور قابل‌توجهی، بررسی‌های انجام‌گرفته نشان داد که کشورهای مختلف، شناخت و اطلاعات مرتبط در مورد فناوری زنجیره بلوکی و رأی‌گیری‌های الکترونیکی را درک کرده‌اند و از آن برخوردار هستند. بااین‌حال، بین سال‌های ۲۰۱۷ تا ۲۰۲۱ تعداد کمی مقاله از آمریکای لاتین یا آفریقا بررسی‌شده است. این پیامدهای مهمی برای محققان و تصمیم‌گیرندگان دارد. اول، یک فرصت تحقیقاتی وجود دارد تا از طریق مطالعات تجربی سطح بلوغ علمی و توانایی‌های عملیاتی را در این کشورها درک کنند. دوم، برای تصمیم‌گیرندگان اجرایی و سیاست‌گذاران، این فرصتی است برای درک عمیق ادغام زنجیره بلوکی با رأی-گیری‌های الکترونیکی و شروع پروژه‌های عملی و فراهم نمودن امکانات زیرساختی برای اجرا نمودن رأی‌گیری‌ها به‌صورت الکترونیکی در بستر اینترنت.

برای پژوهشگران علاقه‌مند به ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی، لیست مجلات و کنفرانس‌های استخراج‌شده ما (شکل (۶) و (۷)) به‌عنوان یک منبع تحقیقاتی مهم برای آن‌ها است. SLR انجام‌شده نشان داد که اصلی‌ترین رویکردهای نظری مورداستفاده در مقاله‌ها مفهومی و چارچوبی است. این زمینه‌هایی را برای پژوهشگران برای استفاده از روش‌های دیگر ارزیابی، ادغام و ضرورت توسعه مطالعات تجربی نزدیک به مقیاس واقعی رأی‌گیری‌های مهم را نشان می‌دهد. به همین دلیل، ما معتقدیم که این مطالعه کمک اساسی به ادبیات ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی می‌کند.

اولین مورد، ارائه درک پیشرفته ادبیات ادغام زنجیره بلوکی با رأی‌گیری الکترونیکی است. مورد دوم توجه به لزوم توسعه مطالعات بیشتر در کشورهای نوظهور را جلب می‌کند. سومین واقعیت این است که ادغام زنجیره بلوکی و رأی‌گیری الکترونیکی یک موضوع داغ است و باید مجلات و کنفرانس-های تخصصی بیشتری به آن بپردازند. سرانجام، این مقاله دستور کار مفصل را برای پژوهشگران علاقه‌مند به مطالعه این موضوع ارائه کرد (جدول ۵).

این مطالعه محدودیت‌هایی دارد که عمدتاً مربوط به کمبود ادبیات منسجم مربوط به زنجیره بلوکی و رأی‌گیری‌های الکترونیکی در مجلات تحقیقاتی و پایگاه‌های اطلاعاتی است،

احتمالاً به دلیل تازگی موضوع است، اگرچه در این مطالعه از لیست گسترده‌ای از کلمات کلیدی برای جستجو در پایگاه داده‌های تحقیقاتی مختلف استفاده شده است. محدودیت دیگر مربوط به این واقعیت است که این مطالعه "ادبیات خاکستری"، یعنی ادبیات عمومی غیردانشگاهی (به‌عنوان مثال گزارش‌های فنی، روزنامه‌ها و اطلاعات موجود در صفحات وب، داده‌ها و کدهای پروژه‌های موجود در گیت‌هاب و پروژه‌های گروهی دانشگاهی) را در نظر نگرفته است. بنابراین، دستور کار پیشنهادی برای تحقیقات آینده نمایانگر تلاشی مهم برای غلبه بر این محدودیت‌ها و پیشبرد ادبیات است.

توضیح: برای دسترسی به ۱۱۸ مقاله مرتبط با موضوع رأی‌گیری‌های الکترونیکی مبتنی بر فناوری زنجیره بلوکی که در بازه زمانی ۲۰۱۷ تا می ۲۰۲۱ ارائه شده‌اند (مرحله غربالگری شکل (۴)) می‌توانید به آدرس زیر مراجعه کنید.

https://github.com/prichain/Blockchain-integration-with-e_Voting-system/blob/main/1.docx

تعارض منافع: نویسندگان اعلام می‌کنند که هیچ تعارض منافعی ندارند.

مراجع

[1] Nakamoto S., "Bitcoin: a peer-to-peer electronic cash system ", ed, 2008.

[۲] برنگی ح.، راجی ف.، خاصه، ع.، «تحلیل تحقیقات امنیت و حریم خصوصی حوزه بلاکچین: یک مطالعه علم سنجی»، مجله محاسبات نرم، جلد ۹، شماره ۱، ص ۴۰-۵۵، ۱۳۹۹.

[3] Christidis K. and Devetsikiotis M., "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[4] Marsal-Llacuna M.-L., "Future living framework: Is blockchain the next enabling network?," Technological Forecasting and Social Change, vol. 128, pp. 226-234, 2018, doi: 10.1016/j.techfore.2017.12.005.

[5] Al-Saqaf W. and Seidler N., "Blockchain technology for social impact: opportunities and challenges ahead," Journal of Cyber Policy, vol. 2, no. 3, pp. 338-354, 2017, doi: 10.1080/23738871.2017.1400084.

[6] Denyer D. and Tranfield D., "Producing a systematic review," in The Sage handbook of organizational research methods. Thousand Oaks, CA: Sage Publications Ltd, 2009, pp. 671-689.

[7] Tranfield D., Denyer D., and Smart P., "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," British journal of management, vol. 14, no. 3, pp. 207-222, 2003.

[8] Rathee G., Iqbal R., Waqar O., and Bashir A. K., "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[9] Moura T. and Gomes A., "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th annual international conference on digital government research, 2017, pp. 574-575, doi: 10.1145/3085228.3085263.

[10] Zaghloul E., Li T., and Ren J., "d-BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting," IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3074877.

[11] Risius M. and Spohrer K., "A blockchain research framework," Business & Information Systems Engineering, vol. 59, no. 6, pp. 385-409, 2017, doi: 10.1007/s12599-017-0506-0.

[12] Hyperledger, "The hyperledger vision: blockchain 101, introducing hyperledger, industry cases," ed: Hyperledger 2018.

[13] Khan M. A. and Salah K., "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018, doi: 10.1016/j.future.2017.11.022.

[14] Babenko L., Pisarev I., and Makarevich O., "A model of a secure electronic voting system based on blind intermediaries using Russian cryptographic algorithms," in Proceedings of the 10th International Conference on Security of Information and Networks, 2017, pp. 45-50, doi: 10.1145/3136825.3136876.

[15] Dhulavvagol P. M., Bhajantri V. H., and Totad S., "Blockchain Ethereum Clients Performance

Analysis Considering E-Voting Application," Procedia Computer Science, vol. 167, pp. 2506-2515, 2020, doi: 10.1016/j.procs.2020.03.303.

[16] Cooley R., Wolf S., and Borowczak M., "Blockchain-based election infrastructures," in IEEE International Smart Cities Conference (ISC2), 2018: IEEE, pp. 1-4, doi: 10.1109/ISC2.2018.8656988.

[17] Park S., Specter M., Narula N., and Rivest R. L., "Going from bad to worse: from internet voting to blockchain voting," Journal of Cybersecurity, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyaa025.

[18] Library C., "Cochrane Database Of Systematic Review."https://www.cochranelibrary.com/cdsr/about-cdsr.

[19] Petticrew M., "Systematic reviews from astronomy to zoology: myths and misconceptions," Bmj, vol. 322, no. 7278, pp. 98-101, 2001.

[20] Wang B., Sun J., He Y., Pang D., and Lu N., "Large-scale election based on blockchain," Procedia Computer Science, vol. 129, pp. 234-237, 2018, doi: 10.1016/j.procs.2018.03.063.

[21] Yang X., Yi X., Nepal S., Kelarev A., and Han F., "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," Future Generation Computer Systems, 2020, doi: 10.1016/j.future.2020.06.051.

[22] Khan K. M., Arshad J., and Khan M. M., "Simulation of transaction malleability attack for blockchain-based e-Voting," Computers & Electrical Engineering, vol. 83, p. 106583, 2020, doi: 10.1016/j.compeleceng.2020.106583.

[23] Khan K. M., Arshad J., and Khan M. M., "Investigating performance constraints for blockchain based secure e-voting system," Future Generation Computer Systems, vol. 105, pp. 13-26, 2020, doi: 10.1016/j.future.2019.11.005.

[24] Pawlak M., Poniszewska-Marańda A., and Kryvinska N., "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018, doi: 10.1016/j.procs.2018.10.177.

[25] Park S., Specter M., Narula N., and Rivest R. L., "Going from bad to worse: from internet voting to blockchain voting," ed: MIT CSAIL (Computer Science and Artificial Intelligence Laboratory), 2020.

[26] Hardwick F. S., Gioulis A., Akram R. N., and Markantonakis K., "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy," in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018: IEEE, pp. 1561-1567, doi: 10.1109/Cybermatics_2018.2018.00262.

[27] Yavuz E., Koç A. K., Çabuk U. C., and Dalkılıç G., "Towards secure e-voting using ethereum blockchain," in IEEE 6th International Symposium on Digital Forensic and Security (ISDFS), 2018: IEEE, pp. 1-7, doi: 10.1109/ISDFS.2018.8355340.

[28] Pandey A., Bhasi M., and Chandrasekaran K., "VoteChain: A Blockchain Based E-Voting System," in IEEE Global Conference for Advancement in Technology (GCAT), 2019: IEEE, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978295.

[29] Angsuchotmetee C., Setthawong P., and Udomviriyalanon S., "BlockVOTE: An Architecture of a Blockchain-based Electronic Voting System," in IEEE 23rd International Computer Science and Engineering Conference (ICSEC), 2019: IEEE, pp. 110-116, doi: 10.1109/ICSEC47112.2019.8974826.

[30] Khoury D., Kfoury E. F., Kassem A., and Harb H., "Decentralized voting platform based on ethereum blockchain," in IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018: IEEE, pp. 1-6, doi: 10.1109/IMCET.2018.8603050.

[31] Alam A., Rashid S. Z. U., Salam M. A., and Islam A., "Towards Blockchain-Based E-voting System," in IEEE International Conference on Innovations in Science, Engineering and Technology (ICISET), 2018: IEEE, pp. 351-354, doi: 10.1109/ICISET.2018.8745613.

[32] Adiputra C. K., Hjort R., and Sato H., "A proposal of blockchain-based electronic voting system," in IEEE Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2018: IEEE, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.

[33] Khandelwal A., "Blockchain implimentation on E-voting System," in IEEE International Conference on Intelligent Sustainable Systems (ICISS), 2019: IEEE, pp. 385-388, doi: 10.1109/ISS1.2019.8907951.

[34] Li K., Li H., Hou H., Li K., and Chen Y., "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City;

IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2017: IEEE, pp. 466-473, doi: 10.1109/HPCC-SmartCity-DSS.2017.61.

[35] Bosri R., Uzzal A. R., Al Omar A., Hasan A. T., and Bhuiyan M. Z. A., "Towards a Privacy-Preserving Voting System Through Blockchain Technologies," in 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2019: IEEE, pp. 602-608, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00116.

[36] Sathya V., Sarkar A., Paul A., and Mishra S., "Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting," in IEEE 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019: IEEE, pp. 1075-1079, doi: 10.1109/ICCMC.2019.8819649.

[37] Roopak T. and Sumathi R., "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," in IEEE 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020: IEEE, pp. 71-75, doi: 10.1109/ICIMIA48430.2020.9074942.

[38] Akbari E., Wu Q., Zhao W., Arabnia H. R., and Yang M. Q., "From blockchain to internet-based Voting," in IEEE International Conference on Computational Science and Computational Intelligence (CSCI), 2017: IEEE, pp. 218-221, doi: 10.1109/CSCI.2017.34.

[39] Chaieb M., Yousfi S., Lafourcade P., and Robbana R., "Verify-your-vote: A verifiable blockchain-based online voting protocol," in European, Mediterranean, and Middle Eastern Conference on Information Systems, 2018: Springer, pp. 16-30, doi: 10.1007/978-3-030-11395-7_2.

[40] Baudier P., Kondrateva G., Ammi C., and Seulliet E., "Peace engineering: The contribution of blockchain systems to the e-voting process," Technological Forecasting and Social Change, vol. 162, p. 120397, 2021, doi: 10.1016/j.techfore.2020.120397.

[41] Abuidris Y., Kumar R., Yang T., and Onginjo J., "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," ETRI Journal, vol. 43, no. 2, pp. 357-370, 2021, doi: 10.4218/etrij.2019-0362.

[42] Alhejazi M. M. and Mohammad R. M. A., "Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA)," Information Security Journal: A Global Perspective, pp. 1-19, 2021, doi: 10.1080/19393555.2020.1869356.

[43] Prajapati A. and Reddy V., "Online Voting System Using Blockchain," presented at the Communication Software and Networks, 2021.

[44] Vo-Cao-Thuy L., Cao-Minh K., Dang-Le-Bao C., and Nguyen T. A., "Votereum: An Ethereum-Based E-Voting System," in 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), 2019: IEEE, pp. 1-6, doi: 10.1109/RIVF.2019.8713661.

[45] Rosenfeld M., "Analysis of hashrate-based double spending," arXiv preprint arXiv:1402.2009, 2014.