بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۷۱

خرداد ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

تحول نظام‌های رای‌گیری غیرحضوری با استفاده از فناوری بلاک‌چین

تهیه شده در پژوهشگاه فضای مجازی
(گروه علوم و فناوری‌های نوین)

تهیه‌کننده: محمد مهدی رضاپور
حمیده قراخانی‌بنی (کارشناسی ارشد مهندسی کامپیوتر دانشگاه اصفهان)

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

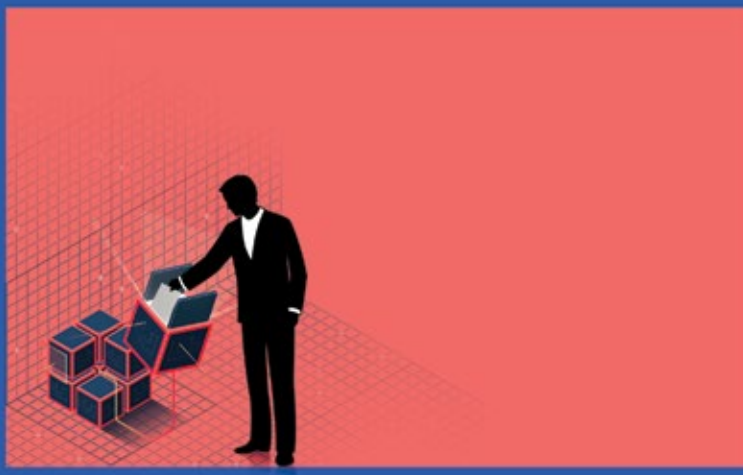
چکیده

چکیده

بلاک‌چین سازوکاری توزیع‌شده، دیجیتال و ایمن برای ذخیره‌سازی اطلاعات است که بر تأیید جمعی مبتنی است. گزارش حاضر، نمایی کلی از سیستم‌های رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین را ارائه می‌کند. هدف اصلی این گزارش این است که وضعیت فعلی رأی‌گیری مبتنی بر بلاک‌چین و چالش‌های احتمالی مرتبط را بررسی کرده و چشم‌اندازی از آینده‌ی آن ارائه کند. پژوهش‌ها نشان می‌دهند که سیستم‌های رأی‌گیری الکترونیکی که از بلاک‌چین استفاده می‌کنند می‌توانند راه‌کارهایی را برای برخی مشکلات رایج در سیستم‌های رأی‌گیری کنونی ارائه کنند. از طرفی محافظت از حریم خصوصی و سرعت تراکنش از مشکلات موجود در برنامه‌های بلاک‌چین هستند که اغلب مورد تأکید قرار می‌گیرند. به‌منظور دستیابی به رأی‌گیری الکترونیکی پایدار، امنیت مشارکت از راه دور و مقیاس‌پذیری باید بهبود پیدا کنند. با توجه به این ملاحظات، چارچوب‌های موجود باید ارتقا داده شوند تا بتوان از آن‌ها در سیستم‌های رأی‌گیری استفاده کرد.

واژگان کلیدی: رای‌گیری برخط، بلاک‌چین، رای‌گیری الکترونیکی، رای‌گیری از راه دور

مقدمه



مقدمه

یکپارچگی انتخابات برای کشورهایی که تحت دموکراسی اداره می‌شوند ضروری است. این امر در افزایش اطمینان و مسئولیت رأی‌دهندگان اثرگذار است. در این راستا، سیستم‌های رأی‌گیری حائز اهمیت هستند. سیستم‌های رأی‌گیری الکترونیکی می‌توانند میزان مشارکت رأی‌دهندگان و اطمینان آن‌ها را افزایش داده و افراد را دوباره به سیستم رأی‌گیری علاقه‌مند کنند. تحقیقات گسترده نشان می‌دهد که پیاده‌سازی سیستم‌های رأی‌گیری الکترونیکی می‌تواند امنیت را افزایش دهد. هنگام استفاده از سیستم رأی‌گیری الکترونیکی، باید سؤال شود که چرا سیستم رأی‌گیری الکترونیکی گزینه‌ی بهتری نسبت به سیستم رأی‌گیری سنتی و کاغذی محسوب می‌شود؟ این سیستم اثربخشی و کارایی دموکراسی را بهبود می‌بخشد و انتظار می‌رود به راهکاری برای برخی از مسائل مشکل‌ساز تبدیل شود و بهبود دسترسی به انتخابات، امکان رأی دادن برای معلولین و سالمندان، افزایش مشارکت در انتخابات و سهولت و سرعت استفاده را به همراه بیاورد. اما استفاده از سیستم‌های رأی‌گیری الکترونیکی نیازمند دستورالعمل‌های امنیتی سخت‌گیرانه‌ای است، مخصوصاً زمانی که به

استفاده از تکنیک‌های رمزنگاری پیشرفته تکیه می‌کنیم.[۱]

در ابتدا قرار بر این بود که رأی‌گیری الکترونیکی راهکاری برای برطرف کردن چالش‌های رأی‌گیری کاغذی باشد تا بتوان از انتخابات دقیق و بدون تقلب اطمینان حاصل کرد[۲]. مباحث امنیتی مرتبط با سیستم‌های رأی‌گیری الکترونیکی ازجمله مباحثی است که به‌طور گسترده در ادبیات مسئله مورد مطالعه قرارگرفته است. مطالعات نشان می‌دهد که استفاده از رأی‌گیری الکترونیکی ممکن است چالش‌های زیر را متضمن شود: یکپارچگی داده‌ها، پایایی، شفافیت، محرمانه ماندن رأی، پیامدهای تفکیک آرا، بی‌سوادی رأی‌دهندگان، مهارت‌های تخصصی حوزه‌ی IT، نگهداری تجهیزات، امنیت و پیامدهای تقلب و فروش رأی[۳]. بلاک‌چین اخیراً به‌عنوان راهکاری برای پیشرفت سیستم‌های مورد استفاده در حوزه‌های مختلف پدید آمده است. کاربرد اصلی و اولیه‌ی فناوری بلاک‌چین، نظارت بر تراکنش رمزارزها بود. بااین‌حال، ظرف چند سال گذشته مصارف و کاربردهای دیگری برای آن به وجود آمده است. اخیراً، سیستم رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین به گزینه‌ی مهمی برای غلبه بر چالش‌های خاص مرتبط با رأی‌گیری الکترونیکی تبدیل‌شده است. سیستم‌های رأی‌گیری مبتنی بر بلاک‌چین، نسل بعدی سیستم‌های رأی‌گیری الکترونیکی مدرن به‌حساب می‌آیند زیرا تغییرناپذیر بودن بلاک‌چین آن را به یک صندوق رأی‌گیری غیرمتمرکز تبدیل کرده است.

در سیستم‌های مبتنی بر بلاک‌چین، رأی‌دهندگان از قبل ثبت‌نام می‌کنند و سپس می‌توانند از سنسورهای بیومتریک تلفن همراه هوشمند (مانند سنسور اثر انگشت یا فناوری تشخیص چهره) برای

ورود به سیستم و رأی‌دادن استفاده کنند.

بااینکه سیستم‌های آزمایشی رو به رشد هستند، اما تعدادشان زیاد نیست و عمدتاً برای رأی‌گیری نیابتی سهام‌داران و رأی‌گیری انجمن‌های دانشجویی استفاده می‌شوند اما دولت‌های محلی و ایالتی طی سال گذشته رأی‌گیری مبتنی بر بلاک‌چین را مورد آزمایش قرار داده‌اند.

پژوهش‌های جدید دانشگاه شیکاگو نشان می‌دهد که فراهم کردن امکان رأی با استفاده از تلفن همراه برای نظامیانی که در خارج از این کشور هستند، میزان مشارکت را در بین افراد واجد شرایط استفاده از این سیستم در انتخابات ۲۰۱۸ ویرجینیا غربی از ۳ درصد به ۵ درصد افزایش داده است.

آنتونی فولر[1] استاد دانشگاه شیکاگو می‌گوید که امکان رأی دادن آنلاین با استفاده از تلفن هوشمند یا سایر دستگاه‌های همراه می‌تواند به‌طور چشمگیری هزینه‌های انتخابات را کاهش دهد (به‌ویژه برای گروه‌هایی که کمتر به آن‌ها توجه شده است) و تأثیرات قابل‌توجهی روی اندازه و ترکیب جمعیت رأی‌دهندگان داشته باشد.

فولر می‌نویسد: «به احتمال زیاد، به‌زودی شاهد آزمایش‌های بیشتری خواهیم بود، بنابراین زمان مناسبی است که پیامدهای این اصلاحات را مطالعه کنیم. داده‌های حاصل از پیمایش‌های جدید نشان می‌دهد که بسیاری از مردم آمریکا نسبت به رأی‌گیری آنلاین باملاحظه رفتار می‌کنند».

جاسلین بوکارو[2] معاون حوزه انتخاباتی دنور در ویریجینیای غربی می‌گوید: «ما به آینده‌ی این فناوری امیدوار هستیم. هدف ما این

1. Anthony Fowler
2. Jocelyn Bucaro

بـود کـه روش راحت‌تـر و ایمن‌تـری را بـرای رأی دادن نظامیـان و شـهروندان خـارج از کشـور فراهـم کنیـم. ایـن آزمایـش مـا موفقیت‌آمیـز بـود. در ایـن دوره، تـا حـدودی بـه لطـف سـهولت رأی دادن، رأی‌دهنـدگان بیشـتری در انتخابـات شـرکت کردنـد و رأی‌دهندگانـی کـه بـا اسـتفاده از برنامـه رأی دادنـد ترجیـح می‌دهنـد در رأی‌گیری‌هـای بعـدی هـم از همیـن روش اسـتفاده کننـد».

جاناتـان جانسـون[1]، از اعضـای هیئت‌مدیـره‌ی Overstock.com و مدیـر[2] Medici Ventures ، عقیـده دارد رأی‌گیـری از راه دور بـا اسـتفاده از دسـتگاه‌های الکترونیکـی در آینـده بیشـتر رواج پیـدا می‌کنـد.

جانسـون می‌گویـد: «بعـد از آزمایـش موفقیت‌آمیـزی کـه بـا برنامـه‌ی رأی‌گیـری دیجیتـال Voatz در ویرجینیـای غربـی داشـتیم، ایالت‌هـای بیشـتری بـه دنبـال ایـن خواهنـد بـود کـه بـه رأی‌دهنـدگان خـارج از کشـور حـق رأی بدهنـد. ایـالات دیگـر ممکـن اسـت از آن بـرای کمـک بـه رأی‌دهنـدگان دارای معلولیـت اسـتفاده کننـد. امـا بـا پذیـرش بیشـتر ایـن روش، رأی‌دهنـدگان داخلـی بـه ایـن موضـوع اعتـراض خواهنـد کـرد کـه اگـر می‌تـوان از خـارج از کشـور بـا اسـتفاده از ایـن برنامـه رأی داد، پـس چـرا مـن کـه داخـل کشـور هسـتم نتوانـم از آن اسـتفاده کنـم؟»

بااین‌حـال، چنـد کشـور اروپایـی پس‌ازاینکـه مشـاهده کردنـد افزایـش میـزان مشـارکت در حـد انتظارشـان نبـوده اسـت، رأی‌گیـری اینترنتـی را رهـا کردنـد. امـا مطالعـه‌ای کـه در دانشـگاه شـیکاگو صـورت گرفتـه اسـت، نشـان می‌دهـد ایـن افزایـش مشـارکتِ کمتـر از حـد انتظـار، ممکـن اسـت بـه دلیـل کاهـش میـزان رأی‌دهنـدگان دیگـر در ایـن کشـورها باشـد[۲۸].

فنـاوری بلاک‌چیـن دولت‌ها را تشـویق می‌کند به سیسـتم‌های رأی‌گیری

1. Jonathan Johnson

۲. بخش فرعی شرکت Overstock که مسئولیت توسعه فناوری بلاک‌چین را بر عهده دارد

پایدار و هوشمند روی بیاورند و در سیستم‌های رأی‌گیری از اطلاعات پایدار استفاده کنند. به‌این‌ترتیب می‌توان اطمینان حاصل کرد همه‌ی شرکت‌کنندگان اطلاعات موثقی برای انتخاب درست در اختیار دارند. گرچه استفاده از بلاک‌چین به‌منظور افزایش امنیت سیستم رأی‌گیری الکترونیکی رو به افزایش است، اما هنوز هم مشکلاتی به‌جای خود باقی‌مانده‌اند.

به‌این‌ترتیب، تعیین اینکه چه موضوعاتی باید در طراحی سیستم رأی‌گیری مبتنی بر بلاک‌چین مورد توجه قرار بگیرد، حائز اهمیت است. مطالعات نشان می‌دهد بااینکه سیستم‌های رأی‌گیری مبتنی بر بلاک‌چین می‌توانند از دست‌کاری داده‌ها و مشکلات مربوط به یکپارچگی جلوگیری کنند، اما محافظت از حریم خصوصی و سرعت تراکنش هنوز هم از مسائلی هستند که زیاد مورد تأکید قرار می‌گیرند. این موارد باید در سیستم رأی‌گیری پایدار بهبود پیدا کنند.

اینترنت و دستگاه‌های رأی‌گیری هنوز نقطه‌ضعف‌های امنیتی زیادی دارند. انجام رأی‌گیری الکترونیکی از طریق اینترنت ایمن و مطمئن به پیشرفت‌های امنیتی قابل‌توجهی نیاز دارد. بااینکه سیستم بلاک‌چین یک راهکار کامل به نظر می‌رسد، نتایج نشان می‌دهد که به دلیل نقطه‌ضعف‌هایی که دارد نمی‌تواند مشکلات موجود در سیستم رأی‌دهی را به‌کلی حل کند. این مطالعه نشان داده است که سیستم‌های بلاک‌چین مسائلی را به وجود آورده‌اند که باید بیشتر به آن‌ها توجه شود و هنوز مشکلات فنی زیادی به‌جای خود باقی است. به همین دلیل، لازم است توجه داشته باشیم که راهکارهای رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین هنوز در مراحل اولیه خود هستند.

بخش اول

مفهوم بلاک چین

بخش اول

مفهوم بلاک‌چین

در این بخش مروری بر مفهوم بلاک‌چین ارائه شده است. اولین سیستم مبتنی بر بلاک‌چین در سال ۲۰۰۸ توسط ساتوشی ناکاموتو[1] ساخته شده است[۴]. شواهد نشان می‌دهد که بیت‌کوین اولین مورد استفاده‌ی گسترده از فناوری بلاک‌چین است. مفهوم بلاک‌چین را می‌توان مشابه یک کتاب داده باز و ایمن دانست که در سراسر جهان توزیع‌شده است[۵]. درنتیجه می‌توان از این مفهوم هم در رمزارزها و حوزه‌ی مالی و هم در حوزه‌های مختلفی که با تراکنش‌ها درگیر هستند، استفاده کرد. بنابراین، معمولاً این مفهوم را یکی از مؤلفه‌های اساسی کاربردهای صنعت ۵,۰ در سال‌های آینده در نظر می‌گیرند. بلاک‌چین در حوزه رمزارزها کاملاً شناخته‌شده است، ولی می‌توان گفت پتانسیل آن می‌تواند از حوزه پول دیجیتال فراتر برود. شرکت‌های خصوصی و سازمان‌های دولتی نیز مطالعه و آزمایش روی بلاک‌چین را شروع کرده‌اند.

بلاک‌چین را می‌توان زنجیره‌ای از بلاک‌ها تعریف کرد، هش‌هایی[2] که برچسب زمان خورده و با رمزنگاری به یکدیگر متصل شده‌اند. این زنجیره دائماً با افزودن بلاک‌های جدید بزرگ‌تر می‌شود

1. Satoshi Nakamoto
2. Hashes

به‌گونه‌ای که هر بلاک جدید، هشِ اطلاعات بلاک قبلی را در خود حفظ می‌کند. در واقع، بلاک‌چین به محافظت از اطلاعات خصوصی و عمومی در برابر تغییر و دست‌کاری کمک می‌کند. بلاک‌چین اساساً یک کیف پول توزیع‌شده برای کلیه‌ی تراکنش‌هایی است که در سیستم به شکل مستقیم بین مصرف‌کنندگان و ارائه‌کنندگان انجام می‌شوند. شبکه‌ای توزیع‌شده از گره‌ها[1] که منبعی مشترک از تراکنش‌ها را در خود نگه می‌دارد. این گره‌ها، وظیفه‌ی تایید تراکنش‌ها را به عهده دارند. بنابراین بلاک‌چین اعتمادسازی بدون نیاز به یک مرجع مرکزی را امکان‌پذیر می‌کند. سیستم بلاک‌چین به رمزنگاری نامتقارن متکی است که از رمزنگاری متقارن کندتر است.

۱-۱- پروتکل‌های تأیید جمعی

برای گنجاندن بلاکی از تراکنش‌ها در کیف پول توزیع‌شده همتا به همتا، سازوکار تأیید جمعی در میان گره‌ها برقرار می‌شود. الگوریتم تأیید جمعی در بلاک‌چین تضمین می‌کند که تمام تراکنش‌ها صحیح و معتبر هستند، علاوه بر این همه‌ی گره‌های شبکه نسخه‌ی یکسانی از کیف پول عمومی را در اختیار دارند. الگوریتم‌های متعدد و متنوعی برای تأیید جمعی وجود دارد. گواه اثبات کار[2] (PoW) و گواه اثبات سهام[3] (PoS) اغلب به‌عنوان سازوکار تأیید جمعی در زیرساخت‌های بلاک‌چین مورد استفاده قرار می‌گیرند. PoW روشی است که امکان بررسی منحصربه‌فرد بودن و قابل‌اطمینان بودنِ تراکنش‌ها را فراهم می‌کند. طرفین تراکنش می‌توانند کارمزدی را به کاربران بپردازند تا تراکنش را با موفقیت بررسی و تأیید کنند

1. Nodes
2. Proof-of-Work
3. Proof-of-Stake

البته این کار اختیاری است. اما برای مثال در بیت‌کوین و در بعضی برنامه‌های خاص، این کار اجباری است. علاوه بر کارمزد تراکنش، شبکه پس از تأیید موفقیت‌آمیز یک بلاک از تراکنش‌ها، تعداد مشخصی سکه را به تاییدکنندگان پاداش می‌دهد. این فرایند «استخراج»[1] نامیده می‌شود، که در اصل تراکنش برای حل مسئله‌ای است که یک کاربر آن را ایجاد کرده است. بررسی نتایج این فرایند کار آسانی است اما تولید مجدد آن‌ها بسیار دشوار است. بااین‌وجود، از معایب PoW می‌توان به پرهزینه و زمان‌بر بودن آن اشاره کرد. عیب دیگر آن مصرف زیاد انرژی است[۶]

از طرفی، PoS پروتکلی است که از استخراج برای تأیید اعتبار بلاک‌های جدید استفاده می‌کند؛ زنجیره‌های PoS از طریق استیکینگ[2] بلاک‌های جدیدی را تولید و تأیید می‌کنند. تاییدکنندگان PoS بر اساس تعداد سکه‌هایشان انتخاب می‌شوند نه بر اساس رقابت برای پیدا کردن بلاک بعدی از طریق محاسبات کامپیوتری دشوار. رمزارزهای موجود در این شبکه از قبل ایجاد شده‌اند و برخلاف PoW هیچ‌گونه فرآیند استخراجی وجود ندارد. به‌این‌ترتیب، هزینه‌ای که باید برای انرژی پرداخت شود کمتر است زیرا نیازی به حل مسئله‌ی پیچیده نیست و پردازش آن بسیار سریع‌تر از PoW انجام می‌شود[۷]. علاوه بر این، پروتکل‌های تأیید جمعی دیگری نیز وجود دارد که بر مفاهیمی مانند گواه اهمیت، ظرفیت و وزن تمرکز می‌کنند[۸].

۲-۱- انواع شبکه‌ی بلاک‌چین

از منظر حفظ حریم خصوصی، بلاک‌چین را می‌توان به سه روش مختلف

1. Mining
2. Staking

طراحی کرد. بسته به نیازها، می‌توان آن را به شکل بلاک‌چین عمومی، خصوصی یا کنسرسیوم طراحی کرد. در جدول ۱، دسته‌بندی انواع بلاک‌چین بر اساس مدیریت، نوع شرکت‌کنندگان، تمرکز، تأیید جمعی و مدت‌زمان تراکنش ارائه شده که باید در طراحی سیستم در نظر گرفته شوند. در بلاک‌چین خصوصی که مجوزمحور نیز نامیده می‌شود، فقط عده‌ی مخصوصی که دارای حقوق خاص هستند می‌توانند در بلاک اطلاعات و سازوکار تأیید جمعی سهیم باشند. در بلاک‌چین خصوصی، شبکه برای همه باز نیست و مجوزهای نوشتن به‌صورت متمرکز برای یک گروه خاص محفوظ است.

بااین‌حال در بلاک‌چین عمومی، شبکه برای همه‌ی همتاها باز است و همه می‌توانند در ثبت اطلاعات و تأیید جمعی سهیم باشند و همه‌ی افراد حاضر در شبکه امکان خواندن تراکنش‌ها را دارند[۶].

بلاک‌چین خصوصی با مدل‌های کسب‌وکار و نظارت سنتی سازگار است. بلاک‌چین کنسرسیوم به استفاده از گره‌های خاصِ از پیش تعیین شده و همچنین افراد قابل اعتماد اشاره دارد. بنابراین، به نسبت بلاک‌چین عمومی که تأیید جمعی آن توسط گره‌های از پیش انتخاب شده کنترل می‌شود، ویژگی‌های امنیتی بیشتری دارد[۹].

ویژگی	عمومی	خصوصی	کنسرسیوم
مدیریت	بدون مدیریت متمرکز	سازمان منفرد	سازمان چندگانه
شرکت‌کنندگان	بدون مجوز	دارای مجوز	دارای مجوز
متمرکز بودن	خیر	بله	تا حدودی
کارایی	پایین	بالا	بالا
تأیید جمعی تصمیم‌گیری	همه استخراج‌کنندگان	مشارکت سازمان	استخراج‌کنندگان منتخب
مدت‌زمان تراکنش	طولانی	کوتاه	کوتاه

جدول ۱- انواع شبکه بلاک‌چین

بخش دوم

کاربردهای کنونی بلاک چین

بخش دوم

کاربردهـای کنونـی بلاک‌چین

صنایـع مختلفـی اسـتفاده از برنامه‌هـای بلاک‌چیـن در کسـب‌وکار خـود را آغـاز کرده‌انـد. به‌این‌ترتیـب، شـرکت‌ها قصـد دارنـد رویه‌هـا و شـیوه‌ی مدیریـت خـود را شـفاف‌تر کننـد. تصـور می‌شـود بلاک‌چیـن به‌عنـوان یـک عامـل توانمندسـازی عمـل کـرده و بـه رسـیدگی بـه مشـکلات امنیتی مختلـف ازجملـه مسـائل مربـوط بـه هویـت و مدیریـت کلاه‌بـرداری کمـک کنـد. سیسـتم‌های مبتنـی بـر بلاک‌چیـن بـه مؤسسـات مالـی ایـن امـکان را می‌دهنـد کـه مشـتری‌های خـود را بررسـی کـرده و بـا فعالیت‌هـای کلاهبردارانـه مقابلـه کننـد. بااینکـه بیشـتر سیسـتم‌های پرداختـی و بانکـداری گزینه‌هـای مناسـبی بـرای اسـتفاده از بلاک‌چیـن محسـوب می‌شـوند، کاربردهـای کیـف پـولِ توزیع‌شـده بـه خدمـات مالـی محـدود نمی‌شـود.

عملیـاتِ پایـدارِ مدیریـتِ تـدارکات و تجـارت B2B دومیـن حـوزه‌ی پرکاربـرد بـرای اسـتفاده از بلاک‌چیـن اسـت. بلاک‌چیـن بـا بهبـود همکاری بیـن مصرف‌کننـدگان و تولیدکننـدگان، بـه افـراد کمـک می‌کنـد وضعیـت پایدارتـری داشـته باشـند و بـه شـرکت‌ها کمـک می‌کنـد فراینـد اسـتفاده‌ی مجـدد و تأمیـن منابـع خـود را بهبـود ببخشـند. بلاک‌چیـن می‌توانـد بـا

کاهش پیچیدگی‌ها از طریق تأمین امنیت، شفافیت و قابلیت ردیابی، تأثیرات عمیقی روی مدیریت زنجیره‌ی تأمین داشته باشد. در مدیریت زنجیره‌ی تأمین، هر تراکنش در یک بلاک‌چین استاندارد و بدون نیاز به دریافت تأیید از مرکز معتبر انجام می‌شود. پرداخت‌ها پس از اتمام مرحله‌ی تحویل به‌صورت خودکار انجام می‌شوند. ازآنجاکه نظارت بر تراکنش توسط طرفین انجام می‌شود، بلاک‌چین می‌تواند تا حد زیادی به بهبود ردیابی سراسری و ایمنی محصولات کمک کند. بنابراین، می‌توان قبل از خرید محصول، اطلاعات دقیقی را در مورد تغییر فرایندها در اختیار مصرف‌کننده قرار داد[۱۰]. از مهم‌ترین مزایای این کار می‌توان به بهبود شفافیت، یکپارچگی، سرعت تراکنش و حذف واسطه‌ها اشاره کرد.

علاوه بر مزایای بالقوه‌ی استفاده از بلاک‌چین در صنایع مالی و مدیریت زنجیره‌ی تأمین، می‌توان از آن در خدمات هوشمند دیگر و برنامه‌های مبتنی بر اینترنت استفاده کرد. فناوری بلاک‌چین در حوزه‌ی انرژی نیز مورد استفاده قرار می‌گیرد. پروژه‌های برنامه‌ریزی و زمان‌بندی برای شارژ بهینه‌ی خودروهای الکتریکی و تجارت انرژی در سطح محلی از کاربردهای پیشنهادی دیگر برای بلاک‌چین است[۱۱]. این امکان برای دستگاه‌ها وجود دارد که همگام با دستگاه‌های اینترنت اشیای از پیش تعریف شده، انرژی را خرید و فروش کنند[۱۲].

هنگام استفاده از دستگاه‌های اینترنت اشیا برای جمع‌آوری داده به‌طور هم‌زمان، می‌توان داده را در زنجیره‌ی بلاک‌چین ذخیره کرد[۱۳و۱۴]. این کار به‌تدریج در تجزیه‌وتحلیل هم‌زمان کلان‌داده‌ها

مورد استفاده قرار خواهد گرفت. صنعت بیمه مثال دیگری است که از بلاک‌چین استفاده می‌کند. امروزه صنعت بیمه بر رابطه مبتنی بر اعتماد استوار است و شواهد نشان می‌دهد که در آینده می‌توان خطا یا تأخیر گاه و بیگاه را با استفاده از بلاک‌چین برطرف کرد. حوزه‌ی سلامت نیز یکی دیگر از بخش‌هایی است که امکان استفاده از فناوری بلاک‌چین در آن وجود دارد؛ در این حوزه، بلاک‌چین نقش ابزار مفیدی را بازی می‌کند و برای دست‌اندرکاران اصلی ازجمله ارائه‌کنندگان خدمات سلامت، تحقیقات بالینی، داروسازان و بیماران امکان دسترسی امن، سریع و پایدار به سوابق پزشکی الکترونیکی را فراهم می‌کند. می‌توان پیش‌بینی کرد که در آینده حوزه‌هایی که به امنیت، پایداری و شفافیت سفت‌وسخت نیاز دارند مانند ذخیره‌سازی ابری، سیستم‌های حمل‌ونقل، امنیت سایبری و مدیریت هویت، قابلیت ردیابی املاک و محصولات کشاورزی می‌توانند از مزایای بلاک‌چین بهره‌مند شوند[۱۵و ۱۶]. سیستم‌های رأی‌گیری الکترونیکی نیز حوزه نویدبخش اما چالش‌برانگیزی به نظر می‌آید که می‌تواند از مزایای بلاک‌چین بهره ببرد.

بخش سوم

سیستم‌های رای‌گیری الکترونیکی

بخش سوم

سیستم‌های رای‌گیری الکترونیکی

در این بخش، اطلاعات اولیه‌ای در رابطه با سیستم‌های رأی‌گیری الکترونیکی ارائه‌شده است. رأی‌گیری الکترونیکی روشی برای رأی‌گیری است که از دستگاه‌های الکترونیکی برای ثبت یا شمارش آرا استفاده می‌کند.

رأی‌گیری الکترونیکی معمولاً به‌نوعی از رأی‌گیری گفته می‌شود که از سخت‌افزار یا نرم‌افزار الکترونیکی برای کمک به فرایند رأی‌گیری بهره می‌گیرد. این نوع سیستم‌ها می‌توانند از توانایی پشتیبانی یا پیاده‌سازی وظایف مختلف، از مرحله‌ی آغاز انتخابات گرفته تا ذخیره‌سازی آرا، برخوردار باشند. انواع مختلفی از این سیستم‌ها وجود دارد، از کیوسک‌های موجود در مراکز انتخابات گرفته تا کامپیوتر یا حتی دستگاه‌های تلفن همراه. سیستم رأی‌گیری الکترونیکی حداقل باید مراحل ثبت‌نام، احراز هویت، رأی‌گیری و شمارش آرا را شامل شود (شکل ۱).

فرایندهای زیر در سیستم رأی‌گیری الکترونیکی گنجانده‌شده‌اند: فرایند اول ثبت‌نام رأی‌دهندگان است (مرحله ثبت‌نام). سپس مَراجع، اعتبار رأی‌دهندگان را در روز انتخابات بررسی می‌کنند (تأیید و احراز

هویت). پس‌ازآن افراد واجد شرایط برای مرحله‌ی بعد می‌توانند رأی بدهند(سازمان‌دهی رأی‌گیری). رأی باید رمزنگاری شود و درستی آن قابل بررسی باشد. محرمانه بودن، ناشناس بودن و دقت آرا باید تضمین شود و به‌هیچ‌وجه قابل تغییر یا حذف نباشد. در نهایت، شمارش آرای سیستم‌های رأی‌گیری الکترونیکی با جمع‌کردن تمام آرا مطابق با طراحی قبلی انجام می‌شود (ارائه‌ی نتایج شمارش). در برنامه‌های رأی‌گیری الکترونیکی، مرجع کنترل مرکزی همه‌چیز را تحت کنترل دارد. چنین سیستم‌هایی با ایرادات و خطرات احتمالی مواجه هستند. ازجمله نبود استانداردهای مشخص برای سیستم رأی‌گیری الکترونیکی، خطرات مربوط به امنیت و پایایی، آسیب‌پذیری در برابر هک شدن، امکان کلاه‌برداری، برنامه‌های نرم‌افزاری مخرب، هزینه‌ی بالای دستگاه‌ها و ذخیره‌سازی امن تراکنش‌ها.

اولین استفاده از سیستم رأی‌گیری الکترونیکی در سال ۲۰۰۰ توسط ایالات‌متحده انجام شد. پس‌ازآن کشورهایی همچون فرانسه (۲۰۰۱)، انگلستان (۲۰۰۲)، اسپانیا (۲۰۰۳)، ایرلند (۲۰۰۴)، استونی (۲۰۰۵)، پرتغال (۲۰۰۵)، هلند (۲۰۰۴، ۲۰۰۶، ۲۰۰۷)، پاراگوئه (۲۰۰۸)، فنلاند (۲۰۰۸)، اتریش (۲۰۰۹)، آلمان (۲۰۰۹)، نروژ (۲۰۱۱، ۲۰۱۳)، آرژانتین(۲۰۰۹، ۲۰۱۳)، اکوادور(۲۰۱۴) ، استرالیا (۲۰۰۷، ۲۰۱۵) و ایالات متحده (۲۰۱۸) از این سیستم استفاده کردند. استونی اولین کشوری بود که بعد از استفاده از این سیستم در انتخابات ۲۰۰۵ و در مقیاس کوچک، امکان رأی‌گیری الکترونیکی از راه دور را در انتخابات مجلس سال ۲۰۰۷ فراهم کرد. همچنین در انتخابات پارلمانی استونی ۲۰۱۹، ۴۳,۷۵٪ از کل رای دهندگان شرکت کننده رای خود را از طریق اینترنت داده اند.

بسیاری از کشورها پس از برگزاری آزمایشی انتخابات مبتنی بر رأی‌گیری الکترونیکی، به دلایل امنیت سایبری این نوع رأی‌گیری را مجاز ندانستند.

سیستم‌های رأی‌گیری مختلفی وجود دارد که برای اهداف متفاوتی از آن‌ها استفاده می‌شود. در این میان، پرکاربردترین سیستم‌های رأی‌گیری عبارت‌اند از پانچ کارت[1]، رأی‌گیری الکترونیکی مستقیم[2] (DRE)، رأی‌گیری الکترونیکی مستقیم در شبکه عمومی، شمارش مرکزی، رأی‌گیری کیوسکی یا شمارش حوزه‌ای[۱۷].

ویژگی‌های زیر باید در سیستم‌های رأی‌گیری الکترونیکی گنجانده شوند:

۱. **عدم ارائه‌ی رسید.** سیستم رأی‌گیری الکترونیکی نباید رسیدی تولید کند که نشان دهد رأی‌دهنده کدام نامزد را انتخاب کرده است[۱].

۲. **رعایت عدالت.** نباید نتایج اولیه در اختیار رأی‌دهندگان قرار بگیرد و روی تصمیم‌گیری آن‌ها تأثیر بگذارد[۱۸].

۳. **یکپارچگی داده‌ها.** اطمینان حاصل می‌کند که هر رأی طبق نظر رأی‌دهنده ثبت شده باشد و پس از ثبت آن هیچ‌گونه امکان دست‌کاری وجود نداشته باشد.

۴. **محرمانگی و ناشناس ماندن رأی‌دهنده.** هویت رأی‌دهندگان و نامزد انتخابی آن‌ها باید مخفی بماند[۱۹].

۵. **صلاحیت رأی دادن.** فقط افرادی که حق رأی دارند باید اجازه‌ی رأی دادن را داشته باشند.

۶. **پایایی و قدرت.** سیستم‌های انتخاباتی باید به شکلی ایمن و دقیق کار کنند. روش‌ها و نرم‌افزارها باید به‌گونه‌ای توسعه داده شوند

1. Punch Card
2. Direct-Recording Electronic

که هیچ‌گونه خطا یا کد مخربی در آن‌ها وجود نداشته باشد.

۷. منحصربه‌فرد بودن آرا. رأی‌دهندگان نباید این امکان را داشته باشند که بیشتر از یک بار رأی بدهند[۲۰و۲۱].

۸. قابلیت اعتبارسنجی. رأی‌دهندگان باید بتوانند این موضوع را تأیید کنند که رأیشان به‌درستی شمارش شده است[۲۲]. اخیراً پیشنهاد استفاده از سیستم‌های رأی‌گیری مبتنی بر بلاک‌چین مطرح شده است.

در شکل ۱ نمونه‌ای از سیستم رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین نشان داده شده است. فرایند انتخابات، اقدامات بسیار مهمی را قبل از انتخابات و در طول آن شامل می‌شود. همان‌طور که در شکل نشان داده شده در هنگام آماده‌سازی برای انتخابات (درست مانند سیستم‌های رأی‌گیری دیگر) باید فهرست رأی‌دهندگان فعلی، نامزدها و طرح آرا قبل از انتخابات آماده شود. برخلاف سایر سیستم‌ها، پس از ثبت‌نام رأی‌دهندگان، می‌توان از توکن مخصوص برای رأی دادن به نامزدها استفاده کرد. در طراحی سیستم رأی‌گیری واقعی، می‌توان از ساختار بلاک‌چین مجاز و گره کنترلی مستقل برای ایجاد محیطی امن‌تر استفاده کرد. این گره‌ها با یکدیگر ارتباط متقابل دارند.

گره‌ها مطابق با مجوز و شبکه‌ی توزیع‌شده‌ی سازمان‌هایِ شخص ثالثِ بی‌طرف و منتخب طراحی شده‌اند که سازوکارهای تأیید جمعی و پردازش تراکنش‌ها را در چارچوب بلاک‌چین ارائه می‌کنند. هدف این گره‌ها این است که تراکنش‌ها را طبق الگوریتم تأیید جمعی استخراج کرده و بلاک‌هایی را به کیف پول عمومی مخصوص رأی‌گیری اضافه کنند تا داده‌ها به‌صورت رمزنگاری‌شده در آن ذخیره

شوند. گره‌های مستقل نتایج رأی‌گیری را بررسی می‌کنند.

فعالیت‌های پیش از انتخابات شامل آماده‌سازی فهرست رأی‌دهندگان، نامزدها و مدت‌زمان انتخابات است. در مرحله ثبت رأی‌دهندگان، افراد دارای صلاحیت رأی دادن اعتبارسنجی می‌شوند. وظیفه‌ی ثبت‌نام قبل از انتخابات به عهده‌ی رأی‌دهندگان است. رأی‌دهنده از طریق گره بلاک‌چین رأی خود را اعلام می‌کند. پس از پایان انتخابات، مراجع آرا را شمرده و نتایج را اعلام می‌کنند. برگزارکننده‌ی انتخابات وظیفه‌ی تعیین تاریخ، مدت‌زمان و نوع انتخابات و همچنین نامزدها را به عهده دارد. یکی از وظایف اصلی برگزارکننده این است که فهرست رأی‌دهندگان و کسانی که برای رأی دادن ثبت‌نام کرده‌اند را آماده کند. این فهرست نشان می‌دهد چه کسانی مجاز به رأی دادن هستند. مراحل ثبت‌نام را می‌توان در دفاتر یا از طریق اینترنت انجام داد. پس از اتمام ثبت‌نام، حساب کاربری رأی‌دهنده از طریق پیامک، ایمیل یا نامه برای او ارسال می‌شود.

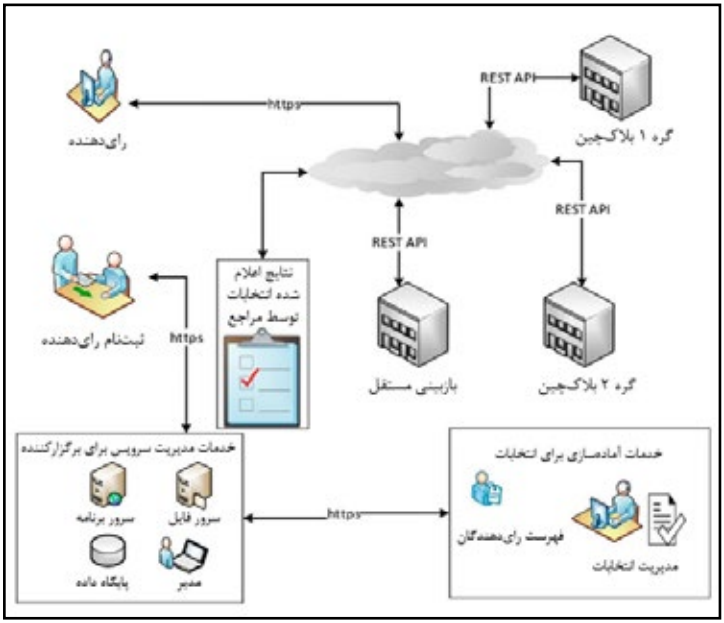
به‌منظور بهره‌وری بیشتر فرایند، رأی‌دهنده باید شماره شناسایی، اطلاعات شخصی یا کلید مخفی داشته باشد تا بتواند به سیستم دسترسی پیدا کرده و احراز هویت کند. در هنگام ثبت‌نام، سیستم باید از رأی‌دهندگان بخواهد کدهای مخفی ایجاد کنند تا بتوانند با استفاده از آن‌ها رأی بدهند. شهروندان واجد شرایط رأی دادن باید بتوانند با استفاده از این کدها به‌راحتی در انتخابات شرکت کنند. برگزارکننده باید علاوه بر ثبت سوابق عملیات‌های انجام‌شده، نتایج انتخابات را نیز به شکلی ایمن ذخیره‌سازی کند.

در این مرحله، سیستم‌های بلاک‌چین بیشتر از قبل مفید واقع می‌شوند

زیرا این امکان را فراهم می‌کنند که آرا در قالب تراکنش‌های جدید روی سیستم‌های بلاک‌چین ذخیره شود. علاوه بر این، گره‌های موجود در سیستم با استفاده از کنترل‌های لازم که در قراردادهای هوشمند موجود هستند و با توجه به طراحی سیستم، با یکدیگر هماهنگ می‌شوند. بخش نتایج، وظیفه‌ی شمارش و آماده کردن نتیجه‌ی انتخابات را بر عهده دارد.

از منظر توسعه، یکی از مزایای اساسی سیستم‌های رأی‌گیری الکترونیکی این است که کنترل‌های مختلفی را ارائه می‌کند که می‌توان هم در توسعه و هم در عملیات از آن‌ها استفاده کرد.

به‌عنوان‌مثال، هنگام استفاده از بلاک‌چین می‌توان با استفاده از تکنیک‌های رمزنگاری و بهره‌گیری از ساختارهای ضددستکاری، ناشناس ماندن رأی‌دهندگان را ممکن ساخت. این نقاط کنترل می‌توانند در افزایش اعتماد شهروندان نسبت به سیستم تأثیر مثبتی داشته باشند. در رابطه با موارد زیر باید اطلاعاتی در اختیار شهروندان قرار بگیرد: تصحیح هویت رأی‌دهندگان چگونه انجام می‌شود، چگونه از رأی‌گیری چندباره جلوگیری می‌شود و آرای شهروندان چگونه مخفی می‌ماند و به‌درستی شمارش می‌شود. علاوه بر این، می‌توان پیش‌بینی کرد که طی فرایند توسعه، استفاده از سیستم‌های بررسی و اعتبارسنجی مستقل می‌تواند اطمینان بیشتری را به همراه بیاورد.



شکل ۱-نمای کلی از ساختار یک سیستم رأی‌گیری مبتنی بر بلاک‌چین

بخش چهارم

شکاف‌های موجود
در سیستم‌های رای‌گیری الکترونیکی

بخش چهارم

شکاف‌های موجود در سیستم‌های رای‌گیری الکترونیکی

رأی‌گیری الکترونیکی نسبت به سیستم‌های رأی‌گیری سنتی مزایای زیادی دارد، به‌ویژه به دلیل هزینه‌ی عملیاتی، خطای انسانی کمتر و نتایج سریع‌تر. علاوه بر این، پیشرفت‌هایی که درزمینه‌ی رأی‌گیری آنلاین حاصل‌شده به دلیل ایجاد دسترسی برای معلولین، سالمندان و جوانان بی‌میل به شرکت در رأی‌گیری، مشارکت رأی‌دهندگان را افزایش می‌دهد. به‌علاوه، رأی‌دهندگانی که خارج از کشور زندگی می‌کنند راحت‌تر می‌توانند در انتخابات شرکت کنند. همچنین هزینه‌های چاپ و شمارش برگه‌های رأی را نیز کاهش می‌دهد[۲۱].

بااین‌حال از معایب احتمالی سیستم‌های رأی‌گیری الکترونیکی می‌توان به آسیب‌پذیری زیرساخت ارتباطی، نرم‌افزاری و سخت‌افزاری اشاره کرد[۲۹و۳۰]. مطرح‌ترین مشکلات امنیتی خاص در این سیستم‌ها عبارت‌اند از سرقت هویت، آلودگی کامپیوتر رأی‌دهنده به بدافزار (تروجان، جاسوس‌افزارها، ویروس‌ها و کرم‌ها)، حمله‌های نفوذ به سرور، جعل اطلاعات، صفحات وب جعلی، حمله DNS [۱] و DDoS [۲]. علاوه بر این، حملات داخلی نیز یکی از مشکلات بالقوه در همه نوع سیستم انتخاباتی محسوب می‌شود.

1. Domain Name Server
2. Distributed Denial of Service

به‌طور خاص آن دسته از سیستم‌های رأی‌گیری الکترونیکی که بر اساس ساختار متمرکز طراحی‌شده‌اند، در معرض انواع مختلفی از حمله‌های سایبری مانند حمله DDoS قرار دارند که می‌تواند سرور را از کار بیاندازد. به‌این‌ترتیب ممکن است در استفاده از سیستم، محرمانگی یا احراز هویت مشکلاتی رخ دهد[۲۱]. بااینکه ذخیره‌سازی داده‌ها در سرورهای ریموت ایمن فرض می‌شود، این موضوع امنیت در برابر حملات هکرها را تضمین نمی‌کند، اما اگر امنیت سیستم به‌خوبی مدیریت نشود ممکن است باعث از بین رفتن داده‌ها یا آسیب دیدن آن‌ها شود. علاوه بر این، پایگاه‌های داده‌ی سنتی توسط یک گروه واحد مدیریت می‌شود و این گروه بر پایگاه داده کنترل کامل دارد، مثلاً می‌تواند موارد ذخیره‌شده را دست‌کاری کند. به همین دلیل، در رأی‌گیری آنلاین ازنظر شمارش آرا و تقلب در انتخابات امکان دست‌کاری وجود دارد.

علاوه بر این، ممکن است به دلیل وجود نقطه‌ضعف‌های نرم‌افزاری و سخت‌افزار ناشناخته، حمله‌های غیر قابل پیش‌بینی (حمله TLS یا حمله مرد میانی[1][۳۱]) نیز رخ دهد. دستگاه‌های مشتری (تلفن‌ها، کامپیوترهای شخصی و لپ‌تاپ‌ها) ممکن است آلوده باشند. رأی‌گیری‌های آنلاین در معرض خطر حمله‌های بدافزاری قرار دارند که می‌توان از آن‌ها برای دست‌کاری آرا استفاده کرد. در رأی‌گیری آنلاین این احتمال وجود دارد که مهاجمان به‌نوعی بتوانند به مدارک اعتبارسنجی رأی‌دهندگان دست پیدا کنند. همچنین می‌توان از طریق نفوذ به سرور یا شبکه‌ی انتخابات، به سیستم رأی‌گیری آنلاین حمله کرد. بررسی دقت آرای ثبت‌شده

1. Man-in-the-middle attack

در نتایج انتخابات الکترونیکی کار دشواری است. ازآنجاکه آرا به‌صورت الکترونیکی منتقل می‌شوند، راهی وجود ندارد که بتوان اطمینان حاصل کرد پیام دریافتی با پیامی که رأی‌دهنده ارسال کرده مطابقت دارد. بنابراین، امنیت و خطر تغییر آرا دو مورد از مهم‌ترین موانع موجود در سیستم رأی‌گیری الکترونیکی به شمار می‌آیند. این امکان وجود ندارد که از قبل خطرات احتمالی برای همه‌ی دستگاه‌ها شناسایی شود، به‌ویژه وقتی روش‌های مختلفی برای رأی‌گیری وجود داشته باشد. ویروس‌های کامپیوتری و خرابی سخت‌افزار نیز می‌توانند باعث ایجاد اختلال در فرایندها شود[۳۲].

در حال حاضر نیز برنامه‌ها یا گروه‌های مختلفی وجود دارند که مورد حمله قرارگرفته‌اند. این حمله‌ها می‌توانند به‌راحتی در شبکه‌ی رأی‌گیری آنلاین اختلال ایجاد کنند، مخصوصاً زمانی که شبکه در حال کار کردن باشد. علاوه بر این، روند رأی‌گیری عموماً شفاف نیست[۲۰]. دسترسی به نرم‌افزار رأی‌گیری مورد استفاده، برای عموم ممکن نیست. این موضوع باعث می‌شود رأی‌دهندگان به مطمئن بودن نرم‌افزار تردید پیدا کنند و احتمال دست‌کاری آن توسط افراد دارای کنترل را در نظر بگیرند. مشکل دیگر این است که اگر کسی سعی کند رأی‌دهنده را مجبور کند به نامزد خاصی رأی بدهد، نمی‌توان سازوکاری برای اجتناب از این موضوع دایر کرد.

به‌غیراز موارد بالا، ایجاد سازوکاری برای بررسی متقابل شمارش آرا و نتایج توسط واحدهای مستقل کار آسانی نیست. به این منظور پیشنهاد می‌شود از بازبینی‌های محدودکننده‌ی خطر برای بررسی دقت نتایج استفاده شود. با توجه به خطاهای یافت شده در نتایجی

کـه توسـط روش‌هـای آمـاری حاصـل شـده، شـواهد محکمـی بـه دسـت آمـده کـه نادرسـت بـودن نتیجـه را نشـان می‌دهـد. روش‌هـای ناموفـق موجـود باعـث از بیـن رفتـن انگیـزه می‌شـود[۳۳]. بـا توجـه بـه ایـن مـوارد، می‌تـوان گفـت اعتمـاد بـه سیسـتم‌های رأی‌گیـری الکترونیکـی عمومـاً ضعیـف اسـت[۳۴].

دو برنامـه مهـم رأی‌گیـری الکترونیکـی کـه در سـال‌های اخیـر ایجـاد شـده‌اند نیـز خطـرات امنیتـی عمـده‌ای را نشـان داده‌انـد. پـس از انتخابـات سـال ۲۰۱۵ ویرجینیـا، آژانـس فنـاوری اطلاعـات ویرجینیـا (VITA) در بخش‌هـای مختلـف سیسـتم رأی‌گیـری الکترونیکـی خـود، آزمایش‌هـای امنیتـی مختلفـی انجـام داد. فرایندهـای فیزیکـی، شـبکه، سیسـتم‌عامل، داده‌هـا و شـمارش آرا مـورد آزمایـش قـرار گرفتنـد. VITA بـه ایـن نتیجـه رسـید کـه از پروتکل‌هـای امنیتـی غیرمطمئـن و رمزهـای ضعیفـی در سیسـتم اسـتفاده شـده بـود. عـلاوه بـر ایـن، مشـخص شـد کـه هکرهـا می‌تواننـد محرمانگـی و یکپارچگـی داده‌هـای مربـوط بـه رأی‌گیـری را بـه خطـر بیاندازنـد. بنـا بـه دلایـل گفتـه شـده، پیشـنهاد شـد اسـتفاده از سیسـتم رأی‌گیـری پیشـرفته ادامـه پیـدا نکنـد.

دولـت سـوئیس چندیـن سـال بـرای پیاده‌سـازی سیسـتم رأی‌گیـری الکترونیکـی در کشـور خـود تـلاش کـرده اسـت. شـرکت سوئیس‌پسـت[1] نیـز روی ایـن مسـئله کار کـرده و نهایتـاً در سـال ۲۰۱۹ برنامـه خـود را بـرای آزمایـش امنیـت آن در اختیـار عمـوم قـرار داده اسـت زیـرا بـه شـفافیت معتقـد اسـت[۳۵و۳۶]. متخصصـان بین‌المللـی IT متوجـه وجـود یـک خطـای اساسـی و امـکان دسـت‌کاری آرا شـدند، کـه در روش مختلـط مـورد اسـتفاده در کـد برنامـه سوئیس‌پسـت قابـل تشـخیص نبـود. ایـن

1. Swiss Post

ایـراد بـه هکرهـا اجـازه مـی‌داد آرای معتبـر را بـا آرای تقلبـی جایگزیـن کننـد. متخصصـان IT اعـلام کردنـد کـه ایـن کدهـا اسـتاندارد نیسـتند در نتیجـه دولـت سـوئیس اسـتفاده از ایـن سیسـتم را تـا جایگزینـی آن بـا یک سیسـتم جدیـد لغـو کـرد.

بخش پنجم

آیا بلاک چین می‌تواند سیستم‌های رای‌گیری الکترونیکی را بهبود ببخشد؟

بخش پنجم

آیا بلاک‌چین می‌تواند سیستم‌های رای‌گیری الکترونیکی را بهبود ببخشد؟

بسیاری از پژوهشگران اتفاق نظر دارند که بلاک‌چین می‌تواند سازوکار مناسبی برای سیستم رأی‌گیری الکترونیکی غیرمتمرکز باشد. به‌طور خاص حصول اطمینان از محرمانه بودن و یکپارچگی داده‌ها را می‌توان از مزایای سیستم‌های بلاک‌چین دانست. در ادامه برخی دیگر از ویژگی‌های مثبت سیستم‌های رای‌گیری مبتنی بر بلاک‌چین شرح داده شده است.

- حمله‌های DDOS یکی از مهم‌ترین چالش‌هایی است که امروزه متخصصان برتر حوزه حمله‌های سایبری با آن مواجه هستند. اگر تعدادی از گره‌های بلاک‌چین به دلیل حمله DDOS آفلاین شوند، سیستم به دلیل توزیع‌شدگی همچنان بدون اختلال به کار خود ادامه می‌دهد. بعد از برگشتن گره‌ها عمل همگام‌سازی برای حصول اطمینان از تناسب گره‌ها انجام می‌شود، به‌این‌ترتیب امکان پدید آمدن اختلال در پروتکل از بین می‌رود و خطری برای از دست رفتن داده‌ها وجود نخواهد داشت. ساختار کلی بلاک‌چین به‌گونه‌ای طراحی شده است که از نقاط شکست جلوگیری می‌کند. گره‌های بلاک‌چین مستقل

از یکدیگر و به‌طور هم‌زمان عمل می‌کنند. بنابراین بلاک‌چین امکان دسترسی را افزایش می‌دهد[۲۳و۲۴و۳۷].

• بلاک‌چین مانند دفتری تغییرناپذیر برای ثبت تراکنش‌ها است که همه کاربران می‌توانند به این دفتر توزیع‌شده و سوابق ثبت‌شده در آن دسترسی داشته باشند. هر تراکنش تغییرناپذیر فقط یک بار ثبت می‌شود و از قابلیت بررسی برخوردار است[۷]. بنابراین هیچ‌کدام از کاربران سیستم نمی‌توانند آن‌ها را حذف کنند یا تغییر دهند. به‌این‌ترتیب یکپارچگی و اعتماد به سیستم افزایش پیدا می‌کند.

• رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین شفافیت و محرمانگی را فراهم می‌کند. کاربران یا ناظران خارجی مستقل می‌توانند نتایج رأی‌گیری را که در بلاک‌چین ذخیره شده، تأیید کنند. بنابراین، می‌توان از یکپارچگی انتخابات اطمینان حاصل کرد[۲۴].

• سیستم‌های بلاک‌چین در طولانی مدت هزینه کمتری دارند. نصب و راه‌اندازی سیستم ذخیره داده امن در ساختار توزیع‌شده، هزینه بالا و خطرات امنیتی را به همراه دارد. گفته می‌شود بلاک‌چین نسبت به برنامه‌های استاندارد پایگاه داده، ایمن‌تر و کم‌هزینه‌تر است.

• بلاک‌چین نتایج را فوراً نشان می‌دهد. در بعضی از روش‌های رأی‌گیری الکترونیکی، آرا باید در حوزه‌های رأی‌گیری مختلف بازبینی‌شده و سپس در واحدهای مرکزی جمع‌آوری شوند. این رویه‌ها بسیار زمان‌بر است و ممکن است اعلام نتایج انتخابات زیاد طول بکشد. با استفاده از رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین، نتایج انتخابات به‌جای چندین ساعت در عرض چند دقیقه به‌صورت ایمن اعلام می‌شود.

• بعد از انجام اولین رأی‌گیری، رأی‌دهندگان بیشتری با اعتماد بیشتر در انتخابات شرکت می‌کنند[۲۵].

بااین‌حال طی سال‌های اخیر انتقادات مختلفی در رابطه با رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین مطرح شده است. بعضی از پژوهشگران عنوان می‌کنند که سیستم بلاک‌چین نمی‌تواند مشکلات رأی‌گیری الکترونیکی (مانند محافظت از تلفن همراه و کامپیوتر رأی‌دهنده در برابر بدافزارها) را حل کند. به‌عنوان مثال، متخصصان موسسه فناوری ماساچوست (MIT) متوجه وجود آسیب‌پذیری در یک برنامه رأی‌گیری تلفن همراه شدند که در انتخابات ۲۰۱۸ ویرجینیای غربی مورد استفاده قرار گرفته بود. این آسیب‌پذیری باعث می‌شد هکرها بتوانند رای‌ها را تغییر بدهند. علاوه بر این بلاک‌چین می‌تواند ایرادهای دیگری را هم به همراه بیاورد که در سیستم‌های غیربلاک‌چین دیده نمی‌شوند. برای مثال می‌توان به آسیب‌پذیری امنیتی قراردادهای هوشمند یا حمله ۵۱ درصدی[1] اشاره کرد که از نظر تئوری تهدید شناخته‌شده‌ای برای این سیستم‌ها به شمار می‌رود. علاوه بر این، ممکن است استخراج‌کنندگان تراکنش‌ها را کنترل کنند و مواردی را به آن‌ها اضافه کنند. سیستم‌های بلاک‌چین هم مانند سایر سیستم‌های رأی‌گیری الکترونیکی به زیرساخت نرم‌افزاری نیاز دارد که از آن برای افزودن رأی فرد به بلاک‌چین یا مشاهده آن استفاده می‌شود. خطاهای نرم‌افزاری، مشکلات مشابهی را برای این سیستم‌ها به‌همراه می‌آورند. این مشکلات می‌توانند خطاهای پیکربندی و رمزنگاری، مشکلات زیرساختی یا آسیب‌پذیری برنامه‌های تلفن همراه یا وب‌سایت را شامل شود.

1. 51% attack

بخش ششم

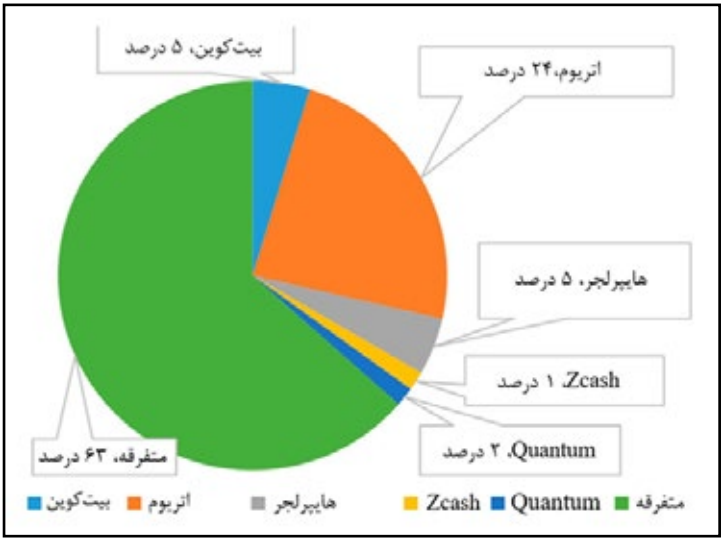
پلتفرم‌های بلاک‌چین یا مدل‌های تأیید جمعی مورد استفاده کدام‌اند؟

بخش ششم

پلتفرم‌های بلاک‌چین یا مدل‌های تأیید جمعی مورد استفاده کدام‌اند؟

سیستم‌های بلاک‌چین امکان توسعه برنامه‌های مبتنی بر بلاک‌چین را فراهم می‌کنند. بیت‌کوین، اتریوم، هایپرلجر[1] و R3 Corda مشهورترین چارچوب‌های بلاک‌چین هستند. بیشتر مقالات تعاریفی کلی ارائه می‌کنند و در مورد جزئیات پیاده‌سازی فنی اطلاعات کافی وجود ندارد. بیشتر مطالعات به مفهوم کلی رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین و موضوعات عمومی مرتبط با آن، می‌پردازند. به نظر می‌رسد در مورد ایده استفاده از بلاک‌چین در سیستم‌های رأی‌گیری الکترونیکی، اتفاق نظری کلی وجود دارد اما جزئیات فنی و طرح‌های اجرایی مشخصی ارائه نشده است. بااین‌وجود، براساس مطالعات انجام شده، توزیع میزان استفاده از بستر بلاک‌چین در شکل ۲ نمایش داده شده است.

1. Hyperledger



شکل ۲-نمودار میزان استفاده از بستر بلاک‌چین

اتریوم (۲۴٪) به دلیل داشتن قراردادهای هوشمند، بهترین بستر بلاک‌چین محسوب می‌شود. اتریوم بستر بلاک‌چین متن‌بازی است که به طیف گسترده‌ای از توسعه‌دهندگان امکان می‌دهد تا برنامه‌های غیرمتمرکزی را ایجاد و پیاده‌سازی کنند. علاوه بر این، اتریوم از برنامه‌های قرارداد هوشمند و ویژگی یکپارچه‌سازی و انعطاف‌پذیری برخوردار است که بسیاری از توسعه‌دهندگان آن را ترجیح می‌دهند. بیت‌کوین فقط برای تأیید تراکنش‌های پولی طراحی شده است اما شبکه اتریوم با استفاده از قراردادهای هوشمند، کاربردهای گسترده‌ای را ارائه می‌کند. اتریوم می‌تواند تراکنش‌ها را با ضوابط مندرج در قرارداد هوشمند انجام دهد. این تراکنش‌ها در مقایسه با بیت‌کوین با سرعت بالایی انجام می‌شوند. در بیشتر

طرح‌ها، الگوریتم تأیید جمعی به‌وضوح بیان‌نشده است. تنها سه پژوهشگر اعلام کردند که در سیستم‌های رأی‌گیری الکترونیکی استفاده از مدل تأیید جمعی DPoS مناسب‌تر از PoW است زیرا انرژی و منابع کمتری مصرف می‌کند[۷و۲۸].

بخش هفتم

پژوهش های آینده در ارتباط
با رای گیری الکترونیکی مبتنی بر بلاک چین

بخش هفتم

پژوهش‌های آینده در ارتباط با رای‌گیری الکترونیکی مبتنی بر بلاک‌چین

در کل، مزایای رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین به نحوه پیاده‌سازی سیستم بستگی دارد. یکی از اصلی‌ترین مسائلی که باید حل شود تردیدی است که نسبت به نقض احتمالی قوانین انتخابات موجود در قراردادهای هوشمند یا نتایج انتخابات وجود دارد. طبق تعریف، هرکس که یک گره کامل بیت‌کوین یا اتریوم در بلاک‌چین عمومی را در اختیار داشته باشد، می‌تواند به تمام داده‌های منتشر شده در آن دسترسی پیدا کند. یکی از راهکارهای موجود، استفاده از بلاک‌چین خصوصی است. اما در این صورت، نحوه دستیابی به شفافیت و حصول اطمینان از آن مشکلی است که به راه‌حل نیاز دارد.

دخالت حداقلی مراجع اصلی، ویژگی مطلوبی است. اما افشای نتایج به‌صورت تناوبی در طول فرایند رأی‌گیری ممکن است نامطلوب تلقی شود. برای اطمینان از اینکه اعلام نتایج تأثیری روی نتیجه‌ی نهایی نمی‌گذارد، نتیجه‌ی انتخابات باید تا پایان فرایند محرمانه باقی بماند. درنتیجه برای تضمین نتایج، باید سازوکاری برای افشای زمان‌بندی‌شده در نظر گرفته شود. علاوه بر این، مسائل ناشی از خود بلاک‌چین نیز همچنان نگران‌کننده است. مهم‌ترین مسئله،

مقیاس‌پذیری است. برای نمونه، عملکرد سیستم هنگامی که فشار کاری بالایی دارد، کاهش پیدا می‌کند. این امر به لزوم بهبود بیشتر سیستم اشاره می‌کند. در انتخابات سال ۲۰۱۸ ترکیه، مراجع انتخابات تعداد رأی‌ها را برابر با ۵۹,۳۶۹,۹۶۰ اعلام کرد[۳۸]. درنتیجه با حسابی سرانگشتی[1] معلوم می‌شود پلتفرم رأی‌گیری مبتنی بر بلاک‌چین باید این توانایی را داشته باشد که در هر ثانیه ۲۰۶۱/۴۶ رأی (تراکنش) را پردازش کند. بعضی از پژوهشگران استفاده از الگوریتم تأیید جمعی DPoS و کاهش دشواری حل مسأله برای استخراج‌کنندگان را پیشنهاد داده‌اند. طبق بررسی های انجام شده هیچ‌کدام از پژوهش‌ها، کارایی الگوریتم‌های تأیید جمعی را تحلیل نکرده است. الگوریتم‌های تأیید جمعی قابل استفاده در برنامه‌های واقعی باید به‌طور دقیق مورد بررسی قرار بگیرند؛ به‌ویژه نقطه‌ضعف‌های امنیتی برنامه‌ها و فرایندها باید به شکل دقیقی بررسی شود. در سال‌های اخیر، مطالعات نشان داده که بعضی از قراردادهای هوشمند دارای آسیب‌پذیری‌هایی هستند و با حملاتی مانند حمله ساختاری (fork)، حمله DDoS و حمله دو بار خرج کردن[2] مواجه هستند. این حملات، زیان‌های مالی را نیز به همراه دارند. با به خطر افتادن کلیدهای رمزنگاری، مهاجمان می‌توانند از کل سیستم سوءاستفاده کنند. بنابراین، الگوریتم‌های رمزنگاری مورد استفاده در چنین سیستم‌هایی باید بسیار قوی باشد. از این مشاهدات می‌توان نتیجه گرفت که عملکرد بلاک‌چین باید از نظر مقیاس‌پذیری، سرعت، توان عملیاتی، کارایی مالی، احراز هویت، محرمانگی و امنیت بهبود پیدا کند[۱۵و۱۶].

1. ((59,5369,960/8 h)/60 m)/60 s = 2061.46
2. Double spending

بخش هشتم

شرکت هایی که آماده‌ی فعالیت در زمینه‌ی رای گیری مبتنی بر بلاک چین هستند

بخش هشتم

شرکت هایی که آماده‌ی فعالیت درزمینه‌ی رای‌گیری مبتنی بر بلاک‌چین هستند

بعضی از شرکت‌ها در حال آزمایش کردن بلاک‌چین هستند که سوابق را از طریق رمزنگاری به هم پیوند داده و امنیت آن‌ها را تضمین می‌کند. شناساگرهای بیومتریک یکی از راهکارهای بالقوه برای به حداقل رساندن تقلبِ رأی‌دهندگان است. علاوه بر این، اینترنت به سازمان‌ها امکان می‌دهد تا انتخابات را خلاقانه‌تر از گذشته طراحی کنند.

اگر دولتی به استفاده از رأی‌گیری آنلاین یا الکترونیکی علاقه‌مند نباشد، شرکت‌ها و سازمان‌ها روش‌های دیگری (مانند ثبت‌نام رأی‌دهندگان و خدمات مدیریت اسناد) را برای انجام انتخابات ایجاد کرده‌اند. این شرکت‌ها و سازمان‌ها به مؤسسات دیگری مثل بنگاه‌های بزرگ، احزاب سیاسی و سازمان‌های ملی که از فرایند رأی‌گیری استفاده می‌کنند، خدمات می‌دهند. درعین‌حال، مصرف‌کنندگان روزمره می‌توانند خدماتی مثل Electronic Runner را تهیه کرده و در انجمن‌های محلی و دانش‌آموزی استفاده کنند.

این ۱۰ شرکت(که بدون ترتیب خاصی در زیر ارائه‌شده‌اند) باور دارند فناوری‌شان می‌تواند فرایند دموکراتیک رأی‌گیری را بهبود ببخشد.

Scytl: ایـن شـرکت کـه در سـال ۲۰۰۱ در اسـپانیا تأسیس‌شـده اسـت، وظیفـه برگـزاری ۱۲ انتخابـات سراسـری را بـر عهـده داشـته و در انتخابـات سـال ۲۰۱۶ از فناوری‌هـای آن در ۹۸۰ حـوزه انتخاباتـی در ۲۸ ایالـت آمریـکا مـورد اسـتفاده قـرار گرفـت. محصـولات ایـن شـرکت کـه در زمینـه‌ی رأی‌گیـری آنلایـن و ارائـه‌ی راهکارهـای انتخاباتـی فعالیـت دارد، عبارت‌انـد از: خدمـات ثبت‌نـام آنلایـن رأی‌دهنـدگان، مدیریـت کارکنـان حوزه‌هـای انتخاباتـی و تحویـل آرای الکترونیکـی. در خدمـات رأی‌گیـری آنلایـن ایـن شـرکت از رمزنـگاری سراسـری، امکان برگشـت رأی و سـرویس بررسـی اعلانـات اسـتفاده می‌شـود. مشـتری‌های Scytl عبارت‌انـد از: وزارت امـور خارجـه فرانسـه، حـزب سـبز اروپـا، مجلـس اتحادیـه اروپـا و کانتـون فریبـورگ[1] در سـوئیس. ایـن شـرکت در ژانویـه سـال ۲۰۱۲ نرم‌افـزار SOE را خریـداری کـرد. Scytl بیـش از ۴۰ حـق امتیـاز ثبت‌شـده و در حـال ثبـت دارد. ایـن شـرکت در سـال ۲۰۰۸ بـه اولیـن شـرکت رأی‌گیـری آنلایـن تبدیـل شـد کـه از وزارت امـور خارجـه فلوریـدا گواهی‌نامـه دریافـت کـرد.

Clear Ballot: ایـن شـرکت در سـال ۲۰۰۹ بـه صنعـت فنـاوری انتخابـات وارد شـد. از سـال ۲۰۱۷، ایـن شـرکت کـه در بوسـتون مسـتقر اسـت، بـا هدف رشـد کسـب‌وکار گسـترده‌ی خـود، ۱۸ میلیون دلار سـرمایه تأمیـن کـرده اسـت. خدمـات آن عبارت‌انـد از: سیسـتم‌های مدیریـت انتخابـات، راه‌کارهـای دسترسـی بـه آراء، روش‌هـای رأی‌گیـری در حوزه‌هـا، زمان‌بنـدی و گـزارش برنامه‌هـا و خدمـات بازبینـی. ایـن شـرکت هـم در ایالـت واشـنگتن و هـم در اوریـگان اجـازه‌ی فعالیـت دارد. Clear Ballot بـا بهبـود روش شـمارش آرا، تأییـد ناظـران انتخابـات را دریافـت کـرده اسـت.

1. Canton of Fribourg

Polyas: ایـن شـرکت در سـال ۱۹۹۶ کار خـود را آغـاز کـرد؛ زمانـی کـه بنیان‌گـذار آن ولفگانـگ یونـگ[1] اولیـن انتخابـات آنلایـن را در فنلانـد ترتیـب داد، کـه ۳۰،۰۰۰ رأی و سـه زبـان را شـامل می‌شـد. شـرکت نرم‌افـزاری Micromata ایـن سـرویس را گسـترش داد تـا اینکـه در سـال ۲۰۱۲ آن را بـه شـرکت فرعـی خـودش تبدیـل کـرد. امـروزه ایـن شـرکت خدمـات رأی‌گیـری آنلایـن، رأی‌گیـری حضـوری زنـده و رأی‌گیـری بـرای تصویـب و اصلاحـات را ارائـه می‌دهـد. مشـتری‌های Polyas (کـه پارلمـان جوانـان، کلیسـاها و شـرکت‌ها را شـامل می‌شـود) در ایجـاد برگه‌هـای رأی‌گیـری، آپلـود کـردن فهرسـت‌های انتخاباتـی، بررسـی فهرسـت‌های رأی‌گیـری و تعریـف اطلاعـات رأی‌دهنـدگان آزاد هسـتند. ایـن شـرکت دفاتـری در برلیـن، کسـل[2]، زوریـخ و اخیـراً در ونکـوور افتتـاح کـرده اسـت. مسـن‌ترین رأی‌دهنـده‌ی آنلاینـی کـه از سیسـتم Polyas اسـتفاده کـرده اسـت صـد سـال سـن دارد.

Sovereign: شـرکت غیرانتفاعـی Democracy Earth Foundation، برنامـه‌ی رأی‌گیـری آنلایـن و متن‌بـاز Sovereign را ایجـاد کـرده اسـت. ایـن پلتفـرم بـر تمرکززدایـی از داده‌هـای رأی‌دهنـدگان، حفاظـت از آراء در بلاک‌چیـن و تحقیـق در زمینـه‌ی «دموکراسـی سـیال» تمرکـز دارد، کـه نسـبت بـه رأی‌گیـری بله/خیـر انعطاف‌پذیـری بیشـتری دارد. به‌عنوان‌مثـال، می‌تـوان تعـداد مشـخصی «حـق رأی» بـه رأی‌دهنـدگان اختصـاص داد کـه بـا اسـتفاده از آن مصوبـه‌ای را تأییـد کننـد یـا نماینـده‌ای تعییـن کننـد. اولیـن اسـتفاده از پلتفـرم Sovereign در یـک همه‌پرسـی در ارتبـاط بـا توافـق غیررسـمی بیـن کلمبیـا و گـروه شورشـی FARC صـورت گرفـت.

1. Wolfgang Jung
2. Kassel

Intelivote: این شرکت که در سال ۲۰۰۳ تأسیس‌شده در زمینه رأی‌گیری الکترونیکی و انتخابات داخلی کانادا فعالیت دارد. از خدمات Intelivote می‌توان به نرم‌افزار رأی‌گیری، مدیریت فهرست رأی‌دهندگان، مشاوره درزمینه‌ی سیستم‌های انتخاباتی و پشتیبانی تدارکی برای کمک به برگزاری انتخابات اشاره کرد. در چین و افغانستان نیز از خدمات این شرکت استفاده شده است. ایالت نوا اسکوشیا[1] کانادا از سرمایه‌گذاران Intelivote است. این شرکت به برگزاری انتخابات در انگلستان و ایالات متحده کمک کرده است.

Votem: این شرکت که از سال ۲۰۱۴ کار خود را آغاز کرده و از فناوری بلاک‌چین نیز استفاده می‌کند، خدماتی ازجمله ثبت‌نام آنلاین رأی‌دهندگان، علامت‌گذاری رأی‌های الکترونیکی، پلتفرم رأی‌گیری سیار و غیره ارائه می‌کند. در ماه اوت، هیئت همکاری در انتخابات آمریکا اعلام کرد که در برنامه آزمایش و تأیید سیستم رأی‌گیری آنلاین با Votem همکاری خواهد کرد. این شرکت با موسسه‌ی تحقیقات بلاک‌چین و انجمن ملی دبیران امور خارجه همکاری می‌کند و امیدوار است تعداد کاربران این فناوری تا سال ۲۰۲۵ به یک میلیارد نفر برسد.

Smartmatic: این شرکت با الهام از دادگاه عالی بوش در مقابل الگور، در سال ۲۰۰۰ در Palm Beach فلوریدا کار خود را آغاز کرد. پس از آن شعبه‌ی دیگری در کشور استونی به راه انداخت و مرکز تعالی رأی‌گیری اینترنتی[2] را در سال ۲۰۱۴ راه‌اندازی کرد. این شرکت در زمینه‌ی امنیت و ایمنی عمومی، مدیریت هویت، راهکارهای حمل‌ونقل هوشمند و مدیریت سوابق تخصص دارد. Smartmatic

1. Nova Scotia
2. Centre of Excellence for Internet Voting

به‌غیر از استونی در فیلیپین، اوگاندا، ونزوئلا و انتخابات رئیس نمایندگان حزب جمهوری‌خواه در یوتا مورد استفاده قرار گرفته است و در آوریل ۲۰۰۷، به ۷۴۰۰۰ شهروند کمک کرد تا در انتخابات کوراسائو[1] شرکت کنند. علاوه بر این، این شرکت سریع‌ترین خدمات ثبت‌نام بیومتریک رأی‌دهندگان در جهان را در اختیار دارد.

Election Runner: این شرکت که در تگزاس مستقر است به کاربران این امکان را می‌دهد که در هر مکانی و با استفاده از هر دستگاهی رأی‌گیری را انجام بدهند. مدیرعامل این شرکت، شان استوارت[2] در سال ۲۰۱۶ آن را تأسیس کرد. مشتری‌های این شرکت عموماً مدارس و سازمان‌ها هستند که می‌توانند چندین انتخابات را در موسسه خود برگزار کنند و امکان تهیه اشتراک با تخفیف را دارند. رأی‌گیری‌هایی که حداکثر ۲۰ شرکت‌کننده داشته باشند رایگان هستند.

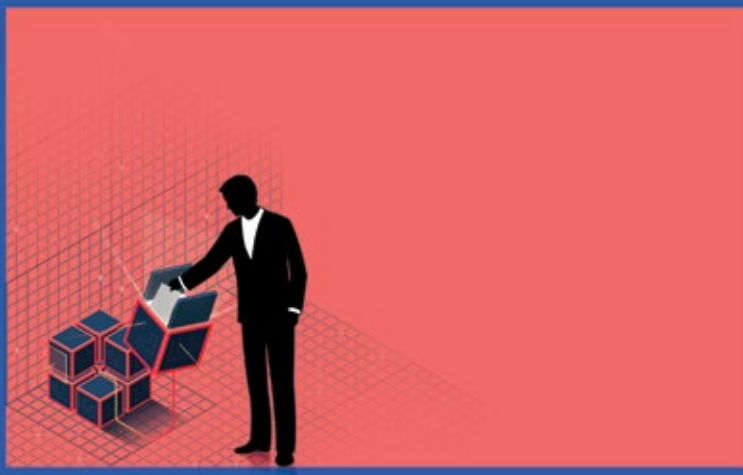
Votebox: مشتری‌های این شرکت از احزاب و دولت‌ها فراتر رفته و شرکت‌ها، انجمن‌ها، سازمان‌های آموزشی و اتحادیه‌ها را شامل می‌شود. Votebox که در ژانویه ۲۰۱۷ تأسیس‌شده، به کاربران اجازه می‌دهد رأی‌گیری خود را بر اساس برند خود، نحوه پیام‌رسانی، زبان‌های مورد نیاز و غیره «شخصی‌سازی» کنند. برگزاری رأی‌گیری برای تعداد کمتر از ۳۰ نفر رایگان است. برای رأی‌گیری‌های پیچیده‌تر، کاربران می‌توانند به‌صورت ماهانه ۱۷۵ یورو پرداخت کنند یا اشتراک سالانه را انتخاب کنند. مشتری‌ها می‌توانند رأی‌گیری را به‌صورت تک‌رای یا با رأی‌های نامحدود برگزار کنند.

1. Curacao
2. Sean Stewart

Boulé: این شرکت که در سال ۲۰۱۷ تأسیس‌شده، یکی دیگر از ارائه‌دهندگان خدماتی است که از بلاک‌چین استفاده می‌کند. این شرکت علیرغم تازه‌کار بودن عنوان کرده که قصد دارد در سه‌ماهه سوم ۲۰۱۸ شرکایی پیدا کند تا بتواند از سیستم‌های خود درآمد کسب کند. Boulé امیدوار است تا سال ۲۰۲۰ به یک پلتفرم رأی‌گیری با استانداردهای دولتی تبدیل شود. حنانه بوجمی[1]، مانوئل انریکه مورالس[2] و اسماعیل مالک[3] مشاوران این شرکت هستند[۲۷].

1. Hanane Boujemi
2. Enrique Morales
3. Ismail Malik

جمع بندی



جمع‌بندی

رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین صرفاً فرایند رأی‌گیری سنتی را به‌صورت دیجیتالی درنمی‌آورد بلکه گزینه‌ی جایگزینی را با مجموعه‌ای متفاوت از ارزش‌ها و مبانی سیاسی پیشنهاد می‌کند. در رأی‌گیری سنتی، روند اجرای انتخابات غیر شفاف، متمرکز و از بالا به پایین است. رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین برعکس است. می‌توان ادعا نمود که این فرایند توسط مردم اداره می‌شود و شفاف، غیرمتمرکز و از پایین به بالا است. میزان موفقیت فناوری بلاک‌چین در حوزه‌ی رأی‌گیری الکترونیکی به این موضوع بستگی دارد که تا چه حد می‌تواند ارزش‌ها و ساختار جامعه، سیاست و دموکراسی را بازتاب دهد.

بسیاری از دغدغه‌های مرتبط با رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین مانند اجبار، دسترسی و ناشناس بودن در سیستم‌های کاغذی سنتی نیز وجود دارند. اجبار به رأی، تهدیدی برای هر سیستم رأی‌گیری به‌حساب می‌آید که مشارکت از راه دور (مثلاً رأی‌گیری پستی)، آن را ممکن می‌سازد. اینجاست که متخصصان علوم اجتماعی وارد عمل می‌شوند تا سیستم‌های تشویقی‌ای را

طراحی کنند که مانع از خرید رای یا تهدید و اجبار شود. برای مثال، در استونی هر کس می‌تواند تا قبل از پایان انتخابات رای خود را چندین بار عوض کند. این موضوع باعث می‌شود کسی که رای را خریده نتواند به راحتی مطمئن شود که شخص به نامزد تعیین‌شده رای داده است.

قابلیت دسترسی برای همه‌ی رأی‌دهندگان یکی از دغدغه‌های اساسی در هر انتخابات به شمار می‌رود. رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین می‌تواند با ارائه‌ی گزینه‌های بیش از حد به شهروندان، مسائل را پیچیده‌تر کند. برای مثال، ممکن است رأی‌دهندگان این امکان را داشته باشند که از دستگاه اخذ رأی الکترونیک، کیوسک‌های سنتی یا دستگاه شخصی استفاده کنند. ممکن است برای شهروندانی که مایل‌اند از رأی دادن فراتر بروند و از حق خود برای دسترسی به داده‌ها استفاده کرده و صحت رویه‌ها را بررسی کنند، رابط‌های متفاوتی وجود داشته باشد. ناشناس ماندن، اغلب یکی از مؤلفه‌های اساسی در مشارکت دموکراتیک محسوب می‌شود، اگرچه انتخابات ملی بیشتر از «نام مستعار» استفاده می‌کند. یعنی به‌راحتی نمی‌توان فهمید هر فرد به چه کسی رأی داده اما امکان آن وجود دارد زیرا هر برگه رأی کدی دارد که با کد دفترچه‌ی رأی مطابقت دارد و اطلاعات شخص در آنجا ثبت‌شده است. ما چاره‌ای جز این نداریم که برای مخفی نگه‌داشتن هویتمان به مراجع اعتماد کنیم. رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین هم از «نام مستعار» استفاده می‌کند، پس گاهی امکان کشف این موضوع که شخص به چه کسی رأی داده، وجود دارد. آیا می‌توانیم به جامعه و فناوری برای مخفی ماندن هویتمان

اعتماد کنیم؟ هنوز برای ارائه‌ی راهکاری فنی برای این مسئله که بتواند شخص را کاملاً ناشناس نگه دارد، به زمان نیاز است. راهکار احتمالی دیگر اعتماد به یک مرجع مرکزی برای توزیع نام‌های مستعار و مخفی نگه‌داشتن آن‌ها است (درست همان‌طور که در حال حاضر در سیستم‌های رأی‌گیری کاغذی انجام می‌شود). بااین‌حال، برقراری یک قدرت متمرکز و اعتماد به این روش می‌تواند ایدئولوژی غیرمتمرکز بودن سیستم‌های مبتنی بر بلاک‌چین را به چالش بکشد.

سوال مهم دیگر این است که چطور می‌توان اعتماد گسترده به امنیت و قانونی بودن سیستم را تضمین کرد. برخلاف انتخابات کاغذی، منصفانه و معتبر بودن نتیجه کافی نیست. کل رأی‌دهندگان، حتی اگر از نتیجه ناامید شوند، باید قانونی و قابل اعتماد بودن فرایند را قبول داشته باشند. به‌این‌ترتیب، رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین باید علاوه بر تأمین امنیت و دقت حقیقی، اعتماد و اطمینان عمومی و گسترده‌ای را نیز ایجاد کند. به دلیل پیچیده بودن پروتکل بلاک‌چین، این موضوع می‌تواند مانع از پذیرش عمومی این نوع رأی‌گیری شود.

ازآنجاکه سیستم‌های رأی‌گیری الکترونیکی مبتنی بر بلاک‌چین هنوز به آزمایش بیشتری نیاز دارند، همچنان از تمام خطرات مرتبط با امنیت و مقیاس‌پذیری این سیستم‌ها اطلاعات کاملی در دست نیست. پیاده‌سازی روش‌های رأی‌گیری مبتنی بر بلاک‌چین می‌تواند خطرات و نقطه‌ضعف‌های امنیتی ناشناخته‌ای را به همراه داشته باشد. سیستم‌های بلاک‌چین باید طراحی پیچیده‌تری در

زمینه‌ی مهارت‌های نرم‌افزاری و مدیریتی پیدا کنند. این مسائل مهم باید با استفاده از تجربه قبلی و با جزئیات بیشتر در رویکردهای رأی‌گیری واقعی مورد بررسی قرار بگیرند. به همین دلیل، سیستم‌های رأی‌گیری الکترونیکی باید ابتدا در مناطق کوچک آزمایش شوند و سپس دامنه‌ی استفاده از آن‌ها گسترش داده شود.

نظر به مباحث طرح شده در این گزارش و به منظور بهره‌برداری ذیربطان امر انتخابات در کشور، موارد ذیل پیشنهاد می‌گردد:

۱. برگزاری رای گیری مبتنی بر بلاکچین در مقیاس کوچک مانند انتخابات محلی و یا رای دهندگان خارج از کشور

۲. در اختیار عموم قرار دادن سیستم طراحی شده رای گیری مبتنی بر بلاک‌چین جهت شفافیت و بررسی آن توسط متخصصان و امکان خطا یا بی

۳. جلب اعتماد عمومی با به کار گیری راهکارهایی همچون تامین امنیت و دقت حقیقی، استفاده از تکنیک‌های رمزنگاری و بهره‌گیری از ساختارهای ضددستکاری.

۴. تسهیل ثبت شرکت های ارائه دهنده ی بلاکچین جهت ایجاد فضای رقابتی برای ارائه ی خدمات و سیستم با امنیت بالاتر برای استفاده در رای گیری

۵. طراحی سیستم های تشویقی که مانع از خرید رای یا تهدید و یا اجبار شود. (برای مثال هر کسی بتواند تا پیش از پایان انتخابات رای خود را چندین با عوض کند. این موضوع باعث می‌شود کسی که رای را خریده نتواند به راحتی مطمئن شود که شخص به نامزد تعیین‌شده رای داده است.)

۶. استفاده از تجربیات گذشته جهت بررسی مهارت های نرم افزاری و مدیریتی مورد نیاز برای سیستم بلاکچین

۷. قرار دادن امکان رای دهی الکترونیکی در کنار روش سنتی رای گیری، جهت آماده سازی فضای ذهنی جامعه برای حرکت به سمت رای گیری الکترونیکی مبتنی بر بلاکچین

منابع

1. Ali, S.T.; Murray, J. An Overview of End-to-End Verifiable Voting Systems. arXiv 2016, arXiv:160508554.

2. Daramola, O.; Thebus, D. Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. Informatics 2020, 7, 16.

3. Esteve, J.B.; Goldsmith, B.; Turner, J. International Experience with E-Voting. Available online: https: //www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf (accessed on 15 July 2020).

4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 27 August 2019).

5. Bitcoin Homepage. Available online: https://bitcoin.org/ (accessed on 17 August 2019).

6. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. Int. J. Netw. Secur. 2017, 19.

7. Solat, S. RDV: An Alternative to Proof-of-Work and a Real Decentralized Consensus for Blockchain. arXiv 2019, arXiv:170705091.

8. Hölbl, M.; Kompara, M.; Kamišali´c, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. Symmetry 2018, 10, 470.

9. Hanifatunnisa, R.; Rahardjo, B. Blockchain based e-voting recording system design. In Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, Indonesia, 26–27 October 2017; pp. 1–6.

10. Tan, B.Q.; Wang, F.; Liu, J.; Kang, K.; Costa, F. A Blockchain-Based Framework for Green Logistics in Supply Chains. Sustainability 2020, 12, 4656.

11. Yahaya, A.S.; Javaid, N.; Alzahrani, F.A.; Rehman, A.; Ullah, I.; Shahid, A.; Shafiq, M. Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism. Sustainability 2020, 12, 3385.

12. Gupta, Y.; Shorey, R.; Kulkarni, D.; Tew, J. The applicability of blockchain in the Internet of Things. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 561–564.

13. Javed, M.U.; Javaid, N.; Aldegheishem, A.; Alrajeh, N.; Tahir, M.; Ramzan, M. Scheduling Charging of Electric Vehicles in a Secured Manner by Emphasizing Cost Minimization Using Blockchain Technology and IPFS. Sustainability 2020, 12, 5151.

14. Villegas-Ch, W.; Palacios-Pacheco, X.; Román-Cañizares, M. Integration of IoT and Blockchain to in the Processes of a University Campus. Sustainability 2020, 12, 4970.

15. DeCusatis, C.; Zimmermann, M.; Sager, A. Identity-based network security for commercial blockchain services. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 474–477.

16. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. Appl. Sci. 2020, 10, 4113.

17. Oo, H.N.; Aung, A.M. A Survey of Different Electronic Voting Systems. Int. J. Sci. Eng. Technol. Res. IJSETR 2014, 3, 3460–3464.

18. Fujioka, A.; Okamoto, T.; Ohta, K. A practical secret voting scheme for

large scale elections. In Advances in Cryptology—AUSCRYPT'92; Seberry, J., Zheng, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 718, pp. 244–251, ISBN 978-3-540-57220-6.

19. Zhang, W.; Yuan, Y.; Hu, Y.; Huang, S.; Cao, S.; Chopra, A.; Huang, S. A Privacy-Preserving Voting Protocol on Blockchain. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 401–408.

20. Bokslag, W.; de Vries, M. Evaluating e-voting: Theory and practice. arXiv 2016, arXiv:160202509.

21. Sun, X.; Wang, Q.; Kulicki, P. A Simple Voting Protocol on Quantum Blockchain. Int. J. Theor. Phys. 2019, 58, 275–281.

22. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. International Association for Cryptologic Research. 2017. Available online: https://eprint.iacr.org/2017/1043.pdf (accessed on 28 August 2019).

23. Bernhard, M.; Benaloh, J.; Alex Halderman, J.; Rivest, R.L.; Ryan, P.Y.A.; Stark, P.B.; Teague, V.; Vora, P.L.; Wallach, D.S. Public Evidence from Secret Ballots. In Electronic Voting; Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10615, pp. 84–109, ISBN 978-3-319-68686-8.

24. Stone, J. Backdoor Discovered in Swiss Voting System Would Have Allowed Hackers to Alter Votes. Available online: https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/ (accessed on 3 April 2020).

25. Specter, M.A.; Koppel, J.; Weitzner, D. The Ballot is Busted Before the

Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Available online: https: //www.usenix.org/system/files/sec20-specter.pdf (accessed on 3 June 2020).

26.https://www.computerworld.com/article/3430697/why-blockchain-could-be-a-threat-to-democracy.html(accessed on December 2020)

27.https://www.forbes.com/sites/rebeccaheilweil1/2017/12/02/eight-companies-that-want-to-revolutionize-voting-technology/?sh=7dd697fe12c1(accessed on December 2020)

28. Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted Voting on the Blockchain: Improving Consensus

in Proof of Stake Protocols. In Proceedings of the 2019 IEEE International Conference on Blockchain and

Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 376–384.

29. Abazorius, A. MIT Researchers Identify Security Vulnerabilities in Voting App. Available online: http:

//news.mit.edu/2020/voting-voatz-app-hack-issues-0213 (accessed on 3 April 2020).

30. Lauer, T.W. The risk of e-voting. Electron. J. E-Gov. 2004, 2, 177–186.

31. Cardillo, A.; Essex, A. The Threat of SSL/TLS Stripping to Online Voting. In E-Vote-ID 2018: Electronic Voting;

Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C., Eds.; Lecture Notes in

Computer Science; Springer: Cham, Switzerland, 2018; Volume 11143, pp. 35–50, ISBN 978-3-030-00419-4.

32. Susskind, J. Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election
System. San Diego Law Rev. 2017, 54, 785–821.
33. Palas Nogueira, J.; de Sá-Soares, F. Trust in E-Voting Systems: A Case Study. In Knowledge and
Technologies in Innovative Information Systems; Lecture Notes in Business Information Processing; Rahman, H.,
Mesquita, A., Ramos, I., Pernici, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 129, pp. 51–66,
ISBN 978-3-642-33243-2.
34. Achieng, M.; Ruhode, E. The adoption and challenges of electronic voting technologies within the South
African context. arXiv 2013, arXiv:13122406.
35. Lewis, S.J.; Pereira, O.; Teague, V. The Use of Trapdoor Commitments in Bayer-Groth Proofs and the
Implications for the Verifiabilty of the Scytl-SwissPost Internet Voting System. Available online: https:
//people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf (accessed on 3 April 2020).
36. Stone, J. Backdoor Discovered in Swiss Voting SystemWould Have Allowed Hackers to Alter Votes. Available
online: https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/ (accessed on 3 April 2020).
37. Pathak, A.;Wasay, A.; Singh, C.; Bhavan, R.; Umale, J. Design and imple

mentation of a secure and robust

voting system based on blockchain. Int. J. Adv. Res. Ideas Innov. Technol. 2018, 4, 869–875.

38. Domestic and Overseas Voters Gender Statistics. Available online: http://www.ysk.gov.tr/doc/dosyalar/docs/24Haziran2018/2018CBMV-SecmenCinsiyet.pdf (accessed on 18 August 2019).

39.https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf(accessed on December 2020)

40.https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/(accessed on December 2020)

csri.majazi.ir