فصلنامه دانش حقوق عمومی/ دوره چهاردهم، شماره ۳ (پاییز ۱۴۰۴)، شماره پیاپی ۴۹، صفحات ۱۲۵ تا ۱۴۵

آینده‌پژوهی برگزاری انتخابات مبتنی بر فناوری بلاک‌چین

هادی طحان‌نظیف[1*]، علی شکراللهی[2]

۱. دانشیار گروه حقوق عمومی و بین‌الملل، دانشکدهٔ معارف اسلامی و حقوق، دانشگاه امام صادق(ع)، تهران، ایران

۲. دانشجوی کارشناسی‌ارشد حقوق عمومی، دانشکدهٔ معارف اسلامی و حقوق، دانشگاه امام صادق(ع)، تهران، ایران

تاریخ دریافت: ۱۴۰۴/۰۲/۰۹ ـ تاریخ پذیرش: ۱۴۰۴/۰۴/۰۹

نوع مقاله: پژوهشی

DOI: 10.22034/qjplk.2025.2174.1937

چکیده

انتخابات از مهم‌ترین پایه‌های دموکراسی و مردم‌سالاری است که در کشورهای متعدد و در ابعاد مختلف صورت می‌پذیرد که البته با چالش‌ها و اشکالاتی روبه‌رو است و فناوری می‌تواند در کاهش این اشکالات نقش‌آفرینی کند. از جملهٔ این فناوری‌های نوظهور فناوری بلاک‌چین است. بلاک‌چین با قابلیت‌های مختلفی که در آن موجود است می‌تواند بستری قابل توجه برای برگزاری انتخابات در ابعاد کوچک و بزرگ در آینده باشد. وجود بستری امن و غیر قابل دستکاری، عدم نیاز به وجود ناظر ثالث، سرعت بالا و کم‌هزینه بودن، امکان استفاده در هر نقطه با کمک اینترنت، و ... از مزایایی است که سبب شده بسیاری از کارشناسان این فناوری را از جهت برگزاری انتخابات مورد بررسی جدّی قرار دهند و در برخی کشورها از آن به صورت محدود و آزمایشی برای انتخابات استفاده شود. در این پژوهش سعی بر آن است تا با روشی توصیفی‌ـ تحلیلی به بررسی ظرفیت و ویژگی‌های فناوری بلاک‌چین و بایسته‌ها و چالش‌های پیش روی آن پرداخته شود. از جملهٔ این چالش‌ها ایجاد ایمنی و حفاظت در برابر هک، حفظ حریم شخصی افراد، احراز هویت کامل و رأی‌دهی مطابق شرایط قانونی، حفظ شفافیت فرآیند رأی‌گیری، دسترسی برابر و رایگان به اینترنت، امکان نظارت بر فرآیند انتخابات در همهٔ مراحل توسط مراجع قانونی است که باید در طراحی نرم‌افزار مبتنی بر بلاک‌چین مد نظر فناوران قرار گیرد.

کلیدواژگان: بلاک‌چین، فناوری‌های نوین، انتخابات، رأی‌گیری، نظام انتخاباتی، شبکهٔ رمزگذاری‌شده، همتا به همتا.

دانشجوی کارشناسی‌ارشد حقوق عمومی، دانشکدهٔ معارف اسلامی و حقوق، دانشگاه امام صادق(ع)، تهران، ایران (نویسندهٔ مسئول)

* **Email:** a.shokrollahi@isu.ac.ir

مقدمه

امروزه دنیای فناوری با سرعتی خیره‌کننده در حال توسعه است و بسیاری از چیزهایی که تا دیروز غیر ممکن بوده یا حتی تصور آن نیز برای کسی قابل باور نبوده را محقق کرده است. این تحولات به گونه‌ای سریع در حال رخ نمایاندن است که شاید تا چند دهۀ دیگر دنیایی کاملاً متفاوت با آنچه در حال حاضر وجود دارد در برابر دیدگان انسان‌ها پدید آید. فناوری‌های نوظهور سبک زندگی جوامع را به‌شدت تحت تأثیر قرار داده و در حال رقم زدن مناسبات جدیدی در تعاملات بین افراد و همچنین بین افراد و دولت‌هاست و به نظر می‌رسد بسیاری از این تغییرات غیر قابل اجتناب است یا جلوگیری از آن با هزینۀ بسیار بالا در ابعاد مختلف خواهد بود. توسعۀ افسارگسیختۀ فناوری به‌خصوص در حوزۀ هوش مصنوعی سبب شد بیش از ۱۰۰۰ نفر از رهبران و فناوران برجسته و پژوهشگران در این زمینه طی نامه‌ای سرگشاده خواستار اتخاذ تدابیری جهت توقف و کنترل این فناوری شوند (Metz & Schmidt, 2023: 1).

از جمله اهدافی که در مواردی از این دست فناوری‌ها مشاهده می‌شود کاهش حوزۀ اعمال حاکمیت دولت‌ها و تمرکززدایی است. در این میان، فناوری بلاک‌چین جایگاه خاصی خواهد داشت. این فناوری به صورت بالقوه به افراد و جوامع اجازه می‌دهد تا تعاملات خود را در سیاست، تجارت، و اجتماع از طریق حذف نهادها و ساختارهای میانجی‌گرایانه و با کمک تراکنش‌های خودکار و ناشناس بازطراحی و بسیاری از اصول بنیادین نظامات سیاسی و حقوقی سنتی را دچار تزلزل کنند (Atzori, 2017: 49). در واقع بسیاری از حامیان بلاک‌چین ادعا می‌کنند که جامعۀ مدنی می‌تواند با جایگزین کردن عملکردهای دولت با خدمات مبتنی بر بلاک‌چین و پلتفرم‌های غیر متمرکز خود را به نحو مفیدتری از آنچه اکنون وجود دارد سازماندهی کند. در واقع دولت در این حوزه نوعی تنظیم‌گر خواهد بود. بر این اساس برخی از ایجاد قرارداد اجتماعی جدید سخن گفته‌اند که در آن نقش دولت‌ها کاملاً کم‌رنگ خواهد بود. برخی دیدگاه‌های افراطی‌تر این دست فناوری‌ها را نیرویی رهایی‌بخش معرفی کرده‌اند که ضد اقتدار دولت عمل می‌کند و بر این باورند که به کمک این نیرو می‌توان به‌تدریج از اقتدار و اختیارات دولت کاست و جامعه‌ای آرمانی با ساختاری هم‌سطح و بدون طبقه پدید آورد (Atzori, 2017: 49).

آثار و اهداف فناوری‌های جدید و به‌خصوص بلاک‌چین و فناوری‌هایی نظیر آن هر چه باشد چیزی از وابستگی جهان امروز به آن کم نمی‌کند. پژوهش حاضر نیز در پی بررسی مبانی آن و اثر بنیادین آن بر کیفیت حکمرانی نیست و سخن گفتن در این باب پژوهش مفصل و جداگانه‌ای می‌طلبد. آنچه در پژوهش پیش رو مد نظر نگارندگان است بررسی یکی از بخش‌هایی است که در عرصهٔ ارتباط بین مردم و دولت در عرصهٔ حکمرانی نقش مهمی ایفا می‌کند و در واقع ابزاری است تا به وسیلهٔ آن مردم به‌خصوص در نظام‌های دموکراتیک اعمال حاکمیت و نظرات خود را اعلام کنند. این ابزار، یعنی انتخابات و رأی‌گیری و نظرسنجی، از مواردی است که در جوامع مختلف و در اشکال متنوع موجود بوده و البته در عصر کنونی اهمیت ویژه‌ای یافته است. در جمهوری اسلامی ایران نیز انتخابات مورد توجه جدّی قانونگذار اساسی قرار گرفته است. در این میان بلاک‌چین با توجه به خصوصیات منحصربه‌فردی که دارد می‌تواند در آیندهٔ فرآیندهای انتخاباتی اثرگذار باشد. بنابراین مسئلهٔ اصلی این پژوهش آن است که ضمن بررسی این ویژگی‌ها و امکان‌سنجی برگزاری انتخابات در بستر بلاک‌چین به بایسته‌های برگزاری انتخابات متناسب با چارچوب نظام حقوقی ایران پرداخته شود و بر این اساس انتظاراتی که از حیث حقوقی در مسئلهٔ انتخابات وجود دارد به طور واضح بیان شود تا در طراحی‌های آتی مد نظر متخصصان این حوزه قرار گیرد. در مورد پیشینهٔ پژوهش باید اشاره کرد در آثار داخلی پژوهش مستقلی که به موضوع آیندهٔ انتخابات مبتنی بر فناوری بلاک‌چین پرداخته باشد یافت نشد. بنابراین عمدهٔ منابع پژوهش حاضر نیز از منابع لاتین است. گفتنی است برخی از منابع از حیث فنی به موضوع امکان و راهکارهای برگزاری انتخابات در بلاک‌چین پرداخته و برخی نیز به ابعاد حقوقی و سیاسی و اجتماعی این ابزار اشاره داشته‌اند. مثلاً مقالهٔ «آیندهٔ دموکراسی: رأی‌گیری بلاک‌چین»[۲] نوشتهٔ رایان آزگود[۳]، «تأثیر بلاک‌چین بر حقوق بشر، دموکراسی و حاکمیت قانون»[۴] نوشتهٔ فلورانس جیسل[۵] و فلوریان مارتین-باریتو[۶]، «بلاک‌چین برای دولت دیجیتال»[۷] نوشتهٔ دیوید آلسی[۸] و ماسیج سوبولوسکی[۹] و لورنزینو واکاری[۱۰] محل توجه است. در این تحقیق سعی خواهد شد ابتدا به توصیف فنی و ویژگی‌های این فناوری اشاره شود، سپس به سابقهٔ به‌کارگیری آن در کشورهای مختلف و چگونگی آن اشاره شود، و نهایتاً به بیان بایسته‌ها و الزامات رأی‌گیری در فضای بلاک‌چین مبتنی بر

اقتضائات موجود در نظام حقوقی ایران با روشی توصیفی-تحلیلی و با کمک منابع کتابخانه‌ای و بررسی پژوهش‌های روز دنیا پرداخته شود.

۱. معرفی فناوری بلاک‌چین و فلسفهٔ وجودی آن

می‌توان استفاده از فناوری بلاک‌چین و رمزارزها را از ویژگی‌های انقلاب صنعتی چهارم دانست (ابوذری، ۱۴۰۱: ۱۳۰). تلاش‌ها در حوزهٔ ایجاد الگوریتم‌های رمزنگاری جدید جهت ایمن‌سازی و اعتباربخشی به مبادلات در دههٔ هشتاد میلادی وارد مرحلهٔ تازه‌ای شد. در این میان ویتفیلد دیفی و مارتی هلمن مفهوم رمزنگاری کلید عمومی-خصوصی را ابداع کردند و با کمک آن یکی از مشکلات اصلی رمزنگاری یعنی احتیاج به توزیع امن کلید را مرتفع ساختند (Davies, 1997: 14-17). این نوع از رمزنگاری با امکان ارسال پیام‌های رمزنگاری‌شده بدون نیاز به کلید مشترک این مشکل را حل کرده است (دوفیلیپای و رایت، ۱۴۰۱: ۲۵). رمزنگاری کلید عمومی-خصوصی قادر است امضاهای دیجیتالی مورد اعتماد و معتبر را در برابر جعل پشتیبانی کند و زمینه را برای جایگزین شدن با ابزارهای کاغذی و قراردادنویسی سنتی فراهم سازد (Rudiger, 2001: 101-102). بر همین اساس، ساخت انواع پول نقد الکترونیکی، فعالیت با نام غیر واقعی، و پدیدار شدن اشکال جدید قرارداد هوشمند میسر شد (Richtel, 2001: 1). در ادامهٔ این مسیر، دیوید شوآم برای اولین بار در پایان‌نامهٔ خود در سال ۱۹۸۲ با عنوان «سیستم‌های کامپیوتری تأسیس، نگهداری، و مورد اعتماد توسط گروه‌های مشکوک متقابل»[11] پروتکلی شبیه به بلاک‌چین را پیشنهاد کرد (Sherman et al., 2018: 3). کار بیشتر بر زنجیره‌ای از بلوک‌های امن رمزنگاری‌شده در سال ۱۹۹۱ توسط استوارت هابر و دبلیو اسکات استورنتا شرح داده شد (Haber & Stornetta, 1991: 100-109). سرانجام اولین بلاک‌چین غیر متمرکز توسط شخصی نامعلوم با نام ساتوشی ناکاموتو در سال ۲۰۰۸ پدیدار و مفهوم‌سازی شد و بستر ایجاد ارز دیجیتال بیت‌کوین را فراهم آورد.

بلاک‌چین یا زنجیرهٔ بلوکی سیستم‌های دفتر کل توزیع‌شده و ایمنی هستند که می‌توانند از طریق رمزگذاری به طور مستقل و بدون نیاز به یک مرجع کنترل‌کننده یا هماهنگ‌کنندهٔ مرکزی عمل کنند و از این طریق نیاز به هر گونه ناظر و واسطه در عملیات‌های مختلف را از بین ببرند. در واقع فناوری بلاک‌چین یک دفتر کل دیجیتالی رمزگذاری‌شده است که داده‌های معامله را در یک دفتر کل غیر متمرکز[12] ذخیره می‌کند (صفری ورزرد، ۱۴۰۱: ۲). شبکهٔ بلاک‌چین دربردارندهٔ

رکوردهایی از داده‌هاست که در بلاک‌هایی در نقاط مختلف شبکه نگهداری می‌شود. همچنین هر بلاک متکی به یک مهر زمانی[۱۳] است که سلامت آن به وسیلهٔ الگوریتم نظارتی همهٔ مشارکت‌کنندگان تضمین می‌شود (Seebacher & Schüritz, 2017: 15). نوآوری برجستهٔ این فناوری آن است که شبکه کاملاً باز است و شرکت‌کنندگان می‌توانند بدون نیاز به شناخت یا اعتماد به سایرین با دیگران تعامل و معامله کنند. همچنین می‌توان تراکنش‌های الکترونیکی را به صورت خودکار توسط گره‌های شبکه از طریق الگوریتم رمزگذاری بدون دخالت انسان تأیید و ثبت کرد. حتی اگر برخی گره‌های ناصادق، غیر قابل اعتماد، و مخرب وجود داشته باشد شبکه می‌تواند تراکنش‌ها را از طریق فرآیند ریاضی به نام «proof of work»[۱۴] راستی‌آزمایی و از شبکه بدون دخالت و نظارت انسان محافظت کند. در واقع می‌توان گفت این سازکار نشان‌دهندهٔ تغییر موضع اعتماد از انسان به محاسبات ریاضی است.[۱۵]

با تأملی در ماهیت و اهداف پنهان و آشکار این فناوری می‌توان این‌گونه برداشت کرد که گسترش فناوری‌هایی از این دست با هدف کاهش و از بین بردن سلطهٔ دولت‌ها و شکل‌دهی جامعه‌ای آزاد در سراسر جهان دنبال می‌شود (Bedford Taylor, 2013: 16). بنابراین رمزنگاران به دنبال آن هستند که با طراحی پیام‌رسان‌های امن، تقویت قراردادهای هوشمند، و ... ضمن حفاظت از حریم خصوصی افراد نقش دولت‌ها را محدود و به نوعی سازکارها را با اصول دموکراتیک سازگار کنند. در واقع سعی می‌شود با تمرکززدایی از مضرات تجمیع قدرت کاسته شود و این دقیقاً آن چیزی است که برخی آن را شرط اساسی برای دستیابی شهروندان به کارایی سیاسی، برابری، شفافیت، و در نهایت آزادی دانسته‌اند (Atzori, 2017: 47).

۲. سابقهٔ به‌کارگیری بلاک‌چین به عنوان بستر رأی‌گیری

یکپارچگی انتخاباتی در کشورهایی که بر اساس آرای مردمی در انتخابات اداره می‌شوند امری ضروری است و در افزایش اعتماد و مسئولیت‌پذیری رأی‌دهندگان نقش بسزایی دارد. بر همین مبنا سیستم‌های رأی‌گیری سیاسی دارای اهمیت‌اند. در این میان سیستم‌های رأی‌گیری الکترونیکی ممکن است اعتماد و مشارکت را افزایش دهند و از سوی دیگر سبب کاهش هزینه‌های برگزاری انتخابات شوند (ابوذری، ۱۴۰۱: ۱۶۴). از سوی دیگر بخشی از مردم به جهت موانعی از مشارکت صرف‌نظر می‌کنند؛ بیماران و معلولان، سالخوردگان، ساکنان خارج از کشور، نظامیان در پایگاه‌های نظامی داخل و خارج، و افراد شاغلی که نمی‌توانند محل کار خود

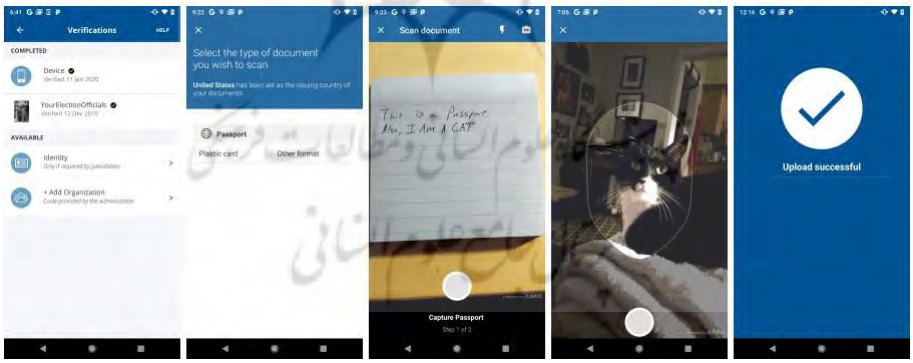
را ترک کنند از جمله گروه‌هایی هستند که ممکن است نتوانند در رأی‌گیری شرکت کنند. تغییر سبک زندگی و تمایل به‌خصوص نسل جوان به فضای الکترونیک نیز از عواملی است که اقبال به رأی‌گیری سنتی را ممکن است با کاهش مواجه کنند. وجود صف‌های طولانی و وقت‌گیر بودن فرآیند رأی‌گیری نیز عامل دیگری است که ممکن است بر میزان مشارکت اثرگذار باشد. همچنین هزینه‌های سنگین برگزاری انتخابات به روش سنتی نیز از عواملی است که دولت‌ها را تشویق به حرکت به سمت روش‌های نوین می‌کند. علاوه بر موارد فوق این امکان می‌تواند در شرایط اضطراری نظیر همه‌گیری بیماری (نظیر شرایطی که در دورهٔ همه‌گیری کرونا وجود داشت) نیز مورد استفاده قرار گیرد و ارتباط بین افراد را به حداقل برساند.

رأی‌گیری الکترونیکی با استفاده از ابزارها و تجهیزات محاسباتی برای رأی دادن و تولید نتایج با کیفیت بالا و دقیق مطابق با نظر رأی‌دهندگان همواره حوزه‌ای مورد توجه بوده است و تلاش‌های بسیاری جهت ارتقای آن صورت گرفته است. با وجود این، روش‌های رأی‌گیری الکترونیکی موجود با خطراتی از قبیل قدرت و تسلط مقامات برگزارکننده بر سیستم رأی‌گیری، محافظت از حریم خصوصی و محرمانگی، ناشناس ماندن رأی‌دهندگان، شفافیت فرآیند رأی‌گیری و شمارش آرا، و ... مواجه‌اند (Jafar et al., 2021: 2).

توسعهٔ فناوری بلاک‌چین در سال‌های اخیر و امکان‌های متعدد موجود در بستر آن سبب شده است بسیاری از رمزنگاران احتمالات مختلفی را در مورد رشد قابلیت‌های آن در آینده مطرح کنند (Mehboob Khan & Arshad, 2018: 54). این فناوری یک گره غیر متمرکز جهت رأی‌گیری آنلاین ارائه می‌دهد و به علت داشتن ویژگی‌های مختلف نظیر عدم تمرکز در کشورهای مختلف مورد استفاده قرار گرفته است. از جمله موارد استفادهٔ متعدد از آن در رأی‌گیری هیئت‌مدیره و شرکت‌های سهامی است (Gao et al., 2019: 115305). با این حال سؤال اساسی این است که آیا می‌توان از فناوری بلاک‌چین در انتخابات سیاسی و در ابعاد وسیع شهری و منطقه‌ای و ملی استفاده کرد یا خیر.

در سال ۲۰۱۵ دولت استونی از فناوری بلاک‌چین و سیستمی به نام i-voting در انتخابات پارلمانی خود استفاده و ۳۰٫۵ درصد آرا را از این طریق دریافت کرد (Srivastava et al., 2018: 509). در سال ۲۰۱۶ آزمایشگاه کسپرسکی[۱۶] و مجلهٔ *اکونومیست*[۱۷] مسابقه‌ای برگزار کردند که طی آن پژوهشگران ایالات متحده و انگلستان باید سیستم رأی‌گیری مبتنی بر

بلاک‌چین طراحی می‌کردند (Bondarchuk et al., 2016: 1). در پایان گروه Vote Book از دانشگاه نیویورک توانست بهترین مطالعهٔ موردی را انجام دهد و در جایگاه نخست قرار بگیرد (Srivastava et al., 2018: 509). در ۷ مارس ۲۰۱۸، سیرالئون به عنوان اولین دولتی در جهان شناخته شد که از تکنولوژی بلاک‌چین در انتخابات ریاست‌جمهوری خود استفاده کرد. این تکنولوژی به طور مستقیم برای رأی دادن استفاده نشد؛ بلکه در کنار فرآیند عادی به عنوان اثباتی بر امکان برگزاری انتخابات با استفاده از تکنولوژی بلاک‌چین مطرح شد. در ایالات متحده نیز ایالت ویرجینیای غربی نخستین ایالتی است که با کمک فناوری بلاک‌چین انتخاباتی را البته به صورت محدود برگزار کرده است. این انتخابات برای نظامیان خارج از کشور و خانواده‌هایشان تدارک دیده شد (Nguyen, 2018: 1). مسئول سیاست خارجی این ایالت، مک وارنر، ضمن ابراز رضایت از انتخابات برگزارشده بیان داشت: «من در این مرحله واقعاً نگران تعداد شرکت‌کنندگان نیستم بلکه به به‌کارگیری فناوری نگاه می‌کنم». این اقدام با کمک شرکت فناوری Tusk Ventures با استفاده از برنامهٔ تلفن همراه به نام Voatz صورت پذیرفت و رأی‌دهندگان توانستند به صورت آنلاین رأی خود را ثبت کنند و هویتشان نیز با ابزارهای بیومتریک نظیر اثر انگشت تشخیص داده شد و رأی در زنجیرهٔ بلوکی مورد تأیید قرار می‌گرفت.



تصویر ۱. فرآیند راستی‌آزمایی رأی‌دهندگان (به ترتیب از چپ به راست): ۱. قطعهٔ تأیید؛ ۲. انتخاب سند؛ ۳. بارگذاری شناسنامه؛ ۴. احراز هویت از طریق عکس‌برداری از شخص؛ ۵. پیام تأیید (Specter et al., 2020: 1540)

تصویر ۲. روند رأی‌گیری در یک انتخابات ساختگی (به ترتیب از چپ به راست): ۱. انتخاب رویداد؛ ۲. برگهٔ رأی؛ ۳. سؤال؛ ۴. مرور؛ ۵. ارسال؛ ۶. رمزگشایی؛ ۷. پیام تأیید (Specter et al., 2020: 1541)

با این حال جمعی از محققان دانشگاه MIT در مقاله‌ای از وضعیت برنامهٔ رأی‌گیری یادشده ابراز نگرانی کرده و به‌خصوص از جهت ملاحظات امنیتی و ضوابط حفظ حریم خصوصی به مسئولان امریکایی هشدار داده‌اند (Specter et al., 2020: 1535-1536). اما مجدداً در انتخابات ریاست‌جمهوری ۲۰۲۰ نیز این برنامه به صورت محدود یوتا مورد استفاده قرار گرفته است. همچنین کشورهای دیگر مانند روسیه[۱۸]، ژاپن[۱۹]، سوئیس[۲۰]، کرهٔ جنوبی[۲۱]، و هند[۲۲] نیز از چند سال گذشته تحقیقاتی را آغاز و به طور آزمایشی در سطوح مختلف در رأی‌گیری از آن استفاده کرده‌اند (Vinnakota, 2021: 1). علاوه بر این پژوهش‌های مختلفی در زمینهٔ بررسی ابعاد فنی بلاک‌چین صورت گرفته و مدل‌های مختلفی نیز ناظر به آن طراحی و پیشنهاد شده است[۲۳] و به نظر می‌رسد با توجه به تلاش‌های صورت‌گرفته نسخه‌های کم‌نقص‌تری ساخته و اجرایی شود.[۲۴]

۳. بایسته‌های رأی‌گیری مبتنی بر بلاک‌چین در نظام حقوقی ایران

از حیث کلی در نظام حقوقی ایران مانعی جدّی بر سر راه تغییر ابزاری در فرآیندهای رأی‌گیری وجود نداشته و بالعکس قانون‌گذار اساسی بستر ایجاد تغییرات متناسب با شرایط روز را فراهم آورده است. در بند «ب» از اصل دوم قانون اساسی بر استفاده از علوم و فنون و تجارب پیشرفتهٔ بشری و تلاش در پیشبرد آن‌ها تأکید شده و طبق بند ۸ از اصل سوم دولت جمهوری اسلامی ایران باید همهٔ امکانات خود را در جهت مشارکت عامهٔ مردم در تعیین سرنوشت سیاسی، اقتصادی، اجتماعی، و فرهنگی خویش به کار ببندد. در اصل ششم نیز به‌صراحت بر نقش آرای مردم در ادارهٔ امور کشور تأکیده شده است و روشن است که باید در این مسیر از به‌روزترین امکانات جهت تحقق این هدف بهره‌برداری کرد. گفتنی است در بند ۱۲ از سیاست‌های کلی انتخابات ابلاغی مقام معظم رهبری نیز به‌صراحت بیان شده است:

«بهره‌گیری از فناوری‌های نوین در جهت حداکثرسازی شفافیت، سرعت، و سلامت در اخذ و شمارش آرا و اعلام نتایج». در همین زمینه در سال‌های اخیر سخن از الکترونیکی شدن انتخابات مطرح شده و تبصره‌های ۶ و ۷ و ۸ از مادهٔ ۱۰ [۲۵] و مادهٔ ۱۱ [۲۶] قانون انتخابات مجلس شورای اسلامی به این موضوع اشاره دارد.[۲۷] این موضوع به شکل محدودتر در مادهٔ ۹ قانون انتخابات ریاست‌جمهوری نیز مورد اشاره قرار گرفته است.[۲۸] با وجود این، باید اشاره داشت که توجه قانون‌گذار در موارد یادشده عمدتاً به ابزارهای الکترونیک و بعد سخت‌افزاری بوده است؛ کما اینکه مثلاً در مادهٔ ۱۰۵ قانون انتخابات مجلس شورای اسلامی اصلاحی ۱۴۰۲/۰۵/۲۸ به‌صراحت از صندوق الکترونیکی برای اخذ آرا نام برده شده است. بنابراین با توجه به آنچه در بخش‌های قبل در توضیح فناوری بلاک‌چین و امکانات آن در فرآیند رأی‌گیری بیان شد به نظر می‌رسد به‌کارگیری این فناوری در فرآیندهای رسمی نیازمند قوانین خاص و دربرگیرندهٔ دقت‌های فنی خواهد بود. در واقع در بلاک‌چین با سطح متفاوتی از رأی‌گیری الکترونیک مواجه هستیم که از جهات مختلف با رأی‌گیری‌های الکترونیک مرسوم کنونی که در بسیاری از کشورها مورد استفاده قرار گرفته است تفاوت دارد. روش‌های کنونی عمدتاً بر مباحث احراز هویت و شمارش آرا مبتنی بر دستگاه‌های الکترونیک تمرکز دارد؛ درحالی‌که همان‌طور که بیان شد فناوری بلاک‌چین نه‌تنها یک ابزار جهت تسهیل امر بلکه جهانی با فلسفه‌ای متفاوت است. با وجود این، در ادامه سعی خواهد شد بایسته‌های رأی‌گیری و ملاحظات در زمینهٔ برگزاری رأی‌گیری در بستر بلاک‌چین مبتنی بر مقتضیات نظام حقوقی ایران بیان شود تا چارچوب مشخصی از حیث حقوقی برای فعالان و متخصصان حوزهٔ فناوری جهت طراحی الگوهای کارآمد و متناسب با نظام حقوقی کشور معرفی شود.

۳-۱. امن بودن در برابر هک و دستکاری

از جمله مواردی که در هر انتخابات و رأی‌گیری باید مورد توجه برگزارکنندگان باشد موضوع امنیت انتخابات و صیانت از آرای شرکت‌کنندگان است. بنابراین باید دید آیا فناوری بلاک‌چین این توانمندی را دارد که فضای امنی را در برابر هک شدن آرا و دستکاری و تقلب محافظت کند یا خیر. اگرچه فناوری بلاک‌چین به طور کلی غیر قابل نفوذ نیست، مکانیسم‌های امنیتی قابل توجهی برای یکپارچگی داده‌ها و ثبت سوابق در آن پیش‌بینی شده تا از دستکاری جلوگیری شود. بر این اساس هر بار که بلوکی از داده‌ها به دفتر کل بلاک‌چین اضافه می‌شود یک

هش[۲۹] از داده‌های قبلی موجود در بلوک قبلی را شامل می‌شود. به این ترتیب زنجیره‌ای از بلوک‌ها را تشکیل می‌دهد که با هر افزودن جدید تقویت می‌شود. این اولین لایهٔ تغییرناپذیری برای بلاک‌چین است. زیرا هر بلوک مشخصی را نمی‌توان بدون دستکاری در همهٔ بلوک‌های بعدی تغییر داد. چنانچه یک بلوک داده دستکاری شود هش این بلوک تغییر می‌کند و با هش ذخیره‌شده در بلوک بعدی مطابقت نخواهد داشت. در نتیجه همهٔ بلوک‌های بعدی کنار گذاشته می‌شوند. با این حال یک بلاک‌چین زمانی امن است که قدرت به طور مساوی بین اپراتورهای گره توزیع شده باشد. در واقع هر گونه تمرکز در قدرت یک تهدید امنیتی برای کل شبکه خواهد بود. هنگامی که یک بازیگر یا گروهی از بازیگران ۵۱ درصد از کنترل شبکه را در اختیار داشته باشند این توان را خواهند داشت که کل شبکه را در اختیار بگیرند و بتوانند تراکنش‌ها را حذف کنند یا تغییر دهند (G’sell et al., 2022: 7). این یکی از نمونه‌های تهدید امنیتی این فناوری است؛ اگرچه امکان وقوع آن در شبکه‌های با تعداد بالا از گره بسیار مشکل و پرهزینه خواهد بود. در هر حال، باید این اطمینان از فناوری بلاک‌چین حاصل شود که آرای اخذشده به‌درستی ثبت و حفظ شود و عامل خارجی نتواند آن را دچار مشکل کند و از طرفی اطمینان خاطر برای شرکت‌کنندگان به وجود آید که رأی ایشان ضبط می‌شود و قابل دستکاری و تغییر نیست. همچنین سیستم از خطا مصون باشد و رأی «الف» «ب» خوانده نشود.

بر اساس آنچه در بالا آمد قوانین انتخاباتی کنونی نیز نیازمند تحول خواهد بود. مثلاً قانون‌گذار موارد آرای باطله را متناسب با فرآیند رأی‌گیری کاغذی در نظر گرفته است که عملاً این موارد در رأی‌گیری با فناوری بلاک‌چین منتفی هستند. مثلاً در بند «ب» مادهٔ ۲۲ قانون انتخابات مجلس شورای اسلامی اصلاحی ۱۴۰۲/۰۵/۲۸ مواردی چون لاک و مهر نبودن صندوق انتخاباتی، آرای زائد بر تعداد تعرفه، آرای فاقد مهر انتخاباتی، و ... جزء موارد رأی باطله و غیر مأخوذه لحاظ شده است؛ حال آنکه در رأی‌گیری بلاک‌چین همهٔ این موارد بلاموضوع و اساساً مفهوم رأی باطله و غیر مأخوذه تهی از معنا خواهند شد. کما اینکه مواردی مانند رأی ناخوانا نیز وجود نخواهد داشت. در عوض باید قانون‌گذار ناظر به مواردی همچون هک شدن سیستم انتخاباتی، قطعی اتصال اینترنتی، دستکاری در فرآیند شناسایی هویت، و ... پیش‌بینی و قانون‌گذاری کند. همچنین گونه‌های حفاظتی فعلی نیز متحول خواهد شد. مثلاً مادهٔ ۱۹ قانون یادشده مأموران انتظامی را مسئول ایجاد نظم در محل اخذ رأی و حفاظت از

صندوق‌ها دانسته است؛ حال آنکه در رأی‌گیری در بستر بلاک‌چین محافظت‌های فیزیکی باید همراه با تدابیر محافظتی سایبری شود و قاعدتاً مرجع حفاظت یا روش حفاظت نیز متفاوت خواهد شد.

۳-۲. احراز هویت و ثبت دقیق رأی

مورد دیگری که در موضوع رأی‌گیری دارای اهمیت است هویت شخص رأی‌دهنده است. سیستم رأی‌گیری باید به گونه‌ای طراحی شود که اولاً تنها افراد دارای صلاحیت قانونی بتوانند در رأی‌گیری شرکت کنند. شرایطی نظیر سن قانونی، دارا بودن تابعیت کشور، و ... از جمله مواردی است که باید در احراز هویت شخص مورد ارزیابی قرار گیرد. ثانیاً باید این افراد شخصاً رأی خود را ثبت کنند و شخص دیگر نتواند با در اختیار داشتن اطلاعات ایشان حق رأی وی را ضایع یا مصادره کند. ثالثاً هر شخص فقط یک بار امکان رأی‌دهی داشته باشد (Tas & Tanrıöver, 2020: 6). در این مسیر باید قاعدتاً از ابزارهایی در احراز هویت اشخاص استفاده شود که کمترین خطا را داشته باشد و از طرفی برای شرکت‌کننده پیچیده و خسته‌کننده نباشد تا وی از دادن رأی به جهت سختی منصرف نشود و مشارکت با مانع مواجه نشود. در این زمینه می‌توان به جای احراز هویت از طریق اثر انگشت از سیستم‌های هوش مصنوعی که از داده‌های بصری و فنون مرتبط با پردازش تصویر[۳۰] و ... استفاده می‌کنند نیز بهره برد (ابوذری، ۱۴۰۱: ۱۶۳). همچنین همان‌طور که در بخش‌های قبلی نیز شرح داده شد بلاک‌چین موضوع احراز هویت را با استفاده از کلیدهای رمزنگاری[۳۱]، امضاهای دیجیتال[۳۲]، شناسایی غیر متمرکز[۳۳]، و مکانیسم‌های اثبات دانش صفر[۳۴] حل می‌کند. رأی‌دهندگان می‌توانند هویت خود را از طریق کلیدهای رمزنگاری منحصربه‌فرد تأیید کنند که امکان جعل را به حداقل می‌رساند. مثلاً مکانیسم اثبات دانش صفر یکی از نوآورانه‌ترین روش‌های رمزنگاری است که اجازه می‌دهد شخصی چیزی را ثابت کند بدون اینکه اطلاعات آن چیز را فاش کند. این دقیقاً همان چیزی است که در احراز هویت امن در رأی‌گیری می‌تواند مورد استفاده قرار گیرد. در فرآیند رأی‌گیری رأی‌دهنده با مکانیسم ZKP ثابت می‌کند که اولاً در فهرست افراد مجاز مشارکت‌کننده در رأی‌گیری قرار دارد، ثانیاً هنوز رأی نداده است، ثالثاً فقط مجاز به یک بار رأی دادن است بدون اینکه سیستم اطلاعاتی مانند نام یا شمارهٔ ملی یا رأی واقعی او را مشاهده کند. از این مکانیسم در انتخابات کشور استونی استفاده شده است.[۳۵]

در این حوزه نیز قوانین انتخاباتی دستخوش تغییرات خواهد بود. گزینش شیوهٔ احراز هویت و الگوی مختص آن از مواردی است که باید از سوی قانون‌گذار معین شود. همچنین با توجه به آنکه امکان تطبیق تصویر کارت شناسایی با چهره از جانب ناظر انسانی صورت نمی‌گیرد باید بانک اطلاعاتی هویت شهروندان به شکل دیجیتال تهیه و ضبط شود.

۳-۳. حفظ حریم خصوصی افراد

حریم خصوصی[۳۶] افراد مورد دیگری است که باید به طور کامل مورد حمایت و صیانت قرار گیرد. بنابراین دسترسی به اطلاعات یا افشای اطلاعات داخل در حریم خصوصی بدون رضایت شخص مجاز نیست[۳۷] (انصاری، ۱۴۰۰: ۱۵۶). مخفیانه بودن رأی و عدم امکان شناسایی صاحب رأی، ایجاد فضای امن برای کاربر، و اخذ تدابیر امنیتی جهت جلوگیری از دستیابی شخص ثالث به آرا از مواردی است که باید در طراحی مورد توجه جدّی قرار گیرد (Anane et al., 2007: 23-26). در سامانه‌های رأی‌گیری مبتنی بر بلاک‌چین اطلاعات هویتی رأی‌دهنده و رأی واقعی او در دو مسیر جداگانه مدیریت می‌شود. همان‌گونه که بیان شد ابتدا هویت فرد با مکانیسم‌هایی مثل امضای دیجیتال یا ZKP احراز می‌شود، اما محتوای رأی بدون هیچ‌گونه وابستگی به هویت روی بلاک‌چین ذخیره می‌شود. رأی‌ها پیش از ارسال به شبکه رمزگذاری می‌شوند. این یعنی فقط یک موجودیت تأییدشده (مثلاً یک تابع رمزگشای رسمی یا نرم‌افزار شفاف متن‌باز) می‌تواند در زمان شمارش رأی آن را رمزگشایی کند. در این حالت، حتی نودهای بلاک‌چین هم رأی واقعی را نمی‌بینند. فرآیند احراز هویت نیز بدون آنکه نیاز به شناسایی شخص باشد صورت می‌گیرد.[۳۸] به طور کلی فناوری بلاک‌چین از طریق جداسازی لایه‌های هویتی، رمزنگاری پیچیده، و الگوریتم‌های اثبات بی‌نیاز از افشا این امکان را فراهم می‌کند که هم رأی‌ها شفاف و معتبر باشند هم هیچ‌کس نتواند بفهمد چه کسی به چه کسی رأی داده است. پروژهٔ Helios Voting[۳۹] و پروژهٔ رأی‌گیری بلاک‌چینی در شهر زوگ سوئیس[۴۰] دو نمونه‌ای است که در این حوزه قابل مطالعه است.

در این زمینه مثلاً اصل ۶۲ قانون اساسی بر مخفی بودن آرای انتخابات مجلس شورای اسلامی تأکید کرده است و مادهٔ ۱۰ قانون انتخابات ریاست‌جمهوری نیز مقرر کرده انتخابات به صورت مستقیم و عمومی و با رأی مخفی خواهد بود. پر واضح است که در تحول قانونی انتخابات مبتنی بر بلاک‌چین نیز این مورد باید مورد توجه قرار گیرد و ضمانت‌های اجرایی

لازم جهت مخفی بودن آرا و حفظ حریم خصوصی افراد در استفاده از مکانیسم‌های مختلف در نظر گرفته شود.

۳-۴. حفظ شفافیت فرآیند رأی‌گیری

شفافیت از عواملی بوده است که فناوری بلاک‌چین را برای مخاطبان جذاب کرده است. این ویژگی باید در فضای رأی‌گیری نیز مورد توجه قرار گیرد. در واقع این اطمینان باید برای نامزدها (در رأی‌گیری‌هایی که نامزدمحور است) و رأی‌دهندگان به وجود بیاید که فرآیند رأی‌گیری کاملاً سالم است و عوامل برگزارکننده و ناظر انتخابات هیچ‌گونه دخالت غیرقانونی در فرآیند رأی‌گیری ندارند. از سوی دیگر فرآیند شمارش آرا و اعلام نتایج نیز باید به گونه‌ای باشد که شرکت‌کنندگان بتوانند به طور کامل نظارت داشته باشند و اعتماد کنند (Liu & Wang, 2017: 5). همچنین باید اطمینان‌خاطر به نامزدها نیز از جهتی داده شود تا منجر به اعتراض ایشان نسبت به نتیجه نشود یا در صورت اعتراض امکان بررسی و اثبات نتیجه وجود داشته باشد.

در این خصوص واضح است که سازکارهای فعلی قانونی نظارت، مانند حضور نمایندگان نامزدها در محل‌های اخذ رأی و نظارت ایشان بر فرآیند شمارش آرا و صورت‌جلسه کردن موارد قانونی، منتفی است و باید متناسب با اقتضائات این فناوری راهکارهای اطمینان‌بخش جهت حراست از سلامت انتخابات پیش‌بینی شود تا هم نهادهای نظارتی و در رأس آنان شورای نگهبان و نیز نامزدها و طرفداران ایشان از نتایج رأی‌گیری اطمینان حاصل کنند.

۳-۵. دسترسی برابر و رایگان به اینترنت

مورد دیگر که در رأی‌گیری‌های آنلاین باید مورد توجه قرار گیرد وجود دسترسی برابر به اینترنت است. در واقع باید به گونه‌ای جامعهٔ مخاطب از دسترسی به اینترنت برخوردار باشد که مانع رأی دادن ایشان نشود. این مورد به‌خصوص در مناطق محروم و نقاطی که دسترسی به اینترنت در آن با اختلال مواجه است باید مد نظر قرار گیرد. از طرفی این دسترسی نباید همراه با صرف هزینهٔ جدّی برای رأی‌دهنده باشد که موضوع مشارکت تحت‌الشعاع قرار نگیرد. نگاهی کلی به آمار مربوط به ضریب نفوذ اینترنت در کشور و روند آن در دههٔ گذشته نشان می‌دهد که ایران از نظر ضریب نفوذ اینترنت با چالش جدّی مواجه نیست، بر این اساس که در طول دههٔ گذشته ضریب نفوذ اینترنت در کشور یک روند افزایشی را تجربه کرده و بالاتر از

میانگین جهانی بوده و فاصلهٔ میان رتبهٔ کشور با رتبهٔ کشورهای منطقه که ضریب نفوذ بالاتری دارند زیاد نیست، اما فاصلهٔ زیادی میان ضریب نفوذ اینترنت پهن‌باند ثابت و سیار در کشور به چشم می‌خورد (اخوان و همکاران، ۱۴۰۳: ۱۴). همچنین در ارتباط با شاخص کیفیت اینترنت در ایران آمار و گزارش‌های دیگری نیز وجود دارد که نشان می‌دهد کیفیت اینترنت ایران در همهٔ ابعاد وضعیت بحرانی ندارد (اخوان و همکاران، ۱۴۰۳: ۱۴). بنابراین از حیث دسترسی به اینترنت و سرعت آن کشور وضعیت نامناسبی ندارد و می‌توان حداقل در بسیاری از مناطق از بستر فناوری بلاک‌چین در حوزهٔ رأی‌گیری بهره برد.

۳-۶. امکان نظارت بر فرآیند انتخابات در همهٔ مراحل

به‌رغم اینکه بلاک‌چین به صورتی طراحی شده است که از دستکاری محفوظ باشد و همهٔ اعضا بتوانند کنش‌ها را زیر نظر داشته باشند، وجود امکان نظارت برای نهادهای نظارتی بر همهٔ مراحل فرآیند برگزاری انتخابات ضروری می‌نماید. فلسفهٔ نظارت بررسی و حصول اطمینان از اتقان کار بر اساس طرق پیش‌بینی‌شده در قانون است تا کار بر مدار قانون انجام شود و انحرافی از چارچوب‌های پیش‌بینی‌شده در قانون صورت نگیرد. در نظام حقوقی ایران طبق اصل ۹۹ قانون اساسی شورای نگهبان نظارت بر انتخابات مجلس خبرگان رهبری، ریاست‌جمهوری، مجلس شورای اسلامی، و مراجعه به آرای عمومی و همه‌پرسی را بر عهده دارد و بر اساس نظریهٔ تفسیر شمارهٔ ۱۲۳۴ مورخ ۱۳۷۰/۰۲/۲۲ این نظارت شامل همهٔ مراحل اجرایی انتخابات خواهد بود. بنابراین باید فرآیند انتخابات در بلاک‌چین به صورتی طراحی شود که امکان نظارت برای شورای نگهبان فراهم باشد و این شورا بتواند اطمینان کامل را ناظر بر حفظ سلامت انتخابات احراز کند.

نتیجه‌گیری

فناوری امکان‌های مختلفی را پیش روی نظام‌های انتخاباتی قرار داده است که یکی از آن‌ها فناوری بلاک‌چین است. الگوهای ارائه‌شده در برگزاری انتخابات در بستر بلاک‌چین در صورتی مفید خواهند بود که بتوانند اطمینان کافی را برای حکومت و دستگاه‌های نظارتی از یک سو و رأی‌دهندگان از سوی دیگر فراهم سازند. کاهش احتمال دستکاری و هر گونه اختلال در سیستم و ایمن بودن در برابر هک از دیگر مواردی است که باید به طور خاص

مورد توجه قرار گیرد. حفاظت از حریم خصوصی افراد، مخفی ماندن آرا، احراز هویت صحیح، و ثبت دقیق رأی از دیگر الزاماتی است که باید رعایت شود.

در حال حاضر به‌کارگیری این فناوری به طور گسترده در نظام انتخاباتی ایران ممکن است با تردیدهایی مواجه باشد. اما این مسئله نافی سرمایه‌گذاری در حوزهٔ پژوهش و طراحی الگوهای مناسب توسط فناوران در این زمینه نیست و در صورت تضمین بایسته‌های طرح‌شده در این پژوهش قابلیت استفادهٔ آزمایشی و در سطح محدود را در مراحل ابتدایی خواهد داشت. این استفاده قاعدتاً نیازمند قانون‌گذاری و تحول در قوانین انتخاباتی کشور است. چون عملاً فضای برگزاری انتخابات را دستخوش تغییر جدّی و بسیاری از موارد یادشده در قوانین انتخاباتی را بلاموضوع می‌کند و برخی لوازم جدید را می‌طلبد که نیازمند پیش‌بینی در قانون است که در این پژوهش سعی شد متناسب با برخی سرفصل‌ها به برخی از مصادیق آن اشارهٔ گذرا شود.

در نهایت باید توجه داشت که این دست فناوری‌ها با هدف کاهش اقتدار دولت و ایجاد بستر تحقق حداکثر آزادی پدید آمده است و باید مناسبات این رویکرد با نظریهٔ حکومت اسلامی مد نظر قرار گیرد و استفاده از آن صرفاً به عنوان ابزاری کمک‌کننده و آن هم با رعایت الزامات و قواعد متناسب با نظام حقوقی ایران صورت پذیرد. از طرفی باید به این نکته نیز توجه داشت که گسترش این نوع فناوری و افزایش نفوذ آن ممکن است منجر به شکل‌گیری مرحله‌ای جدید در نظم سرمایه‌داری شود و فناوری تبدیل به ابزاری جهت پیشبرد خواسته‌های سرمایه‌داری و نقض حقوق عموم افراد شود. بنابراین هر گونه به‌کارگیری و استفاده از فناوری باید با چشمانی باز و با آگاهی کامل به مبانی و جزئیات آن صورت گیرد تا منجر به ایجاد آشفتگی در نظام اجتماعی نشود.

یادداشت‌ها

1. The Future of Democracy: Blockchain Voting
2. Ryan Osgood
3. The Impact Of Blockchains for Human Rights, Democracy, and the Rule of Law
4. Florence G'sell
5. Florian Martin-Bariteau
6. Blockchain for digital government
7. David Allessie
8. Maciej Sobolewski
9. Lorenzino Vaccari

10. Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups
11. distributed ledger
12. timestamp

۱۳. اثبات کار شامل یک معمای ریاضی دشوار و وقت‌گیر است که به گره‌های شبکه به نام «ماینرها» به عنوان شرطی برای قابل اعتماد بودن، تأیید تراکنش‌های شبکه، و دریافت پاداش نیاز است. به کل فرآیند «ماینینگ» می‌گویند. تولید اثبات کار دشوار است. اما تأیید آن برای سایر گره‌ها آسان خواهد بود.

http://www.coindesk.com/information/how-bitcoin-mining-works/

۱۴. جهت مطالعهٔ بیشتر ←

http://radar.oreilly.com/۰۲/۲۰۱۴/bitcoin-security-model-trust-by-computation.html

15. Kaspersky Labs
16. *Economist* newspaper

۱۷. یک سیستم رأی‌گیری مبتنی بر بلاک‌چین در سپتامبر ۲۰۱۹ در مسکو جهت انتخابات شورای شهر استفاده شده است.

18. https://thenextweb.com/news/japan-city-blockchain-voting
19.https://www.swissinfo.ch/eng/business/crypto-valley- -switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928
20. https://en.yna.co.kr/view/AEN20221124003100320
21.https://inc42.com/buzz/india-explores-blockchain-based-e-voting-by-2024-general-elections/

۲۲. جهت مطالعهٔ بیشتر ←

1. An E-voting Protocol Based on Blockchain, Yi Liu, Qi Wang, Published in IACR Cryptology ePrint… 2017
2. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology, Gautam Srivastava, Ashutosh Dhar Dwivedi and Rajani Singh, Conference: International Conference on Security and, 2018
3. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system, (Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed), Journal of King Saud University – Computer and Information Sciences 34 (2022)

۲۳. جهت مشاهدهٔ نظر مخالف ←

Going from Bad to Worse: From Internet Voting to Blockchain Voting, (Sunoo Park, Michael Specter, Neha Narula and Ronald L. Rivest), Journal of Cybersecurity Publisher, Oxford University Press (OUP)

۲۴. تبصرهٔ ۶. وزارت کشور موظف است ظرف شش ماه از زمان تصویب این قانون نسبت به نوین‌سازی شیوه‌های أخذ رأی و شمارش آرا به منظور دقت، سلامت، و نظارت بهتر در أخذ، شمارش، و اعلام نتایج و همین‌طور استانداردسازی صندوق‌های أخذ رأی در حدود اعتبارات مصوب و پس از تأیید شورای نگهبان اقدام نماید.

تبصرهٔ ۷. وزارت کشور موظف است با هماهنگی و موافقت شورای نگهبان تمام مراحل انتخابات را در حدود اعتبارات مصوب با استفاده از روش‌ها و فناوری‌های نوین برگزار کند.

تبصرهٔ ۸. در انتخابات الکترونیکی با تأیید شورای نگهبان از امضاهای الکترونیکی مجریان و ناظران استفاده می‌شود. همچنین در صورت برگزاری هم‌زمان چند انتخابات در هر شعبهٔ أخذ رأی از یک دستگاه به طور مشترک برای تمامی انتخابات در أخذ رأی و شمارش آرا با تأیید شورای نگهبان استفاده می‌شود.

۲۵. مادهٔ ۱۱. در هر مرحلهٔ انتخاباتی، هر شخص واجد شرایط می‌تواند فقط یک بار با ارائهٔ اصل یکی از مدارک کارت ملی، شناسنامه، گذرنامه، گواهینامهٔ رانندگی، یا کارت خدمت دورهٔ ضرورت نظام وظیفه رأی دهد. همچنین در مواردی که احراز مشخصات هویتی رأی‌دهنده و انطباق آن با اطلاعات دستگاه احراز هویت از طریق اثر انگشت یا سایر نشانه‌های زیست‌سنجی (بیومتریک) امکان‌پذیر باشد از رأی‌دهنده ثبت‌نام به عمل می‌آید. بر اساس داده‌های دستگاه احراز هویت، شرکت و رأی دادن فرد در سوابق سجلی رأی‌دهنده در سازمان ثبت احوال کشور ثبت خواهد شد.

۲۶. همچنین در مادهٔ ۱۱۰ قانون برگزاری انتخابات مجلس شورای اسلامی آمده است:

مادهٔ ۱۱۰. وزارت کشور موظف است در صورت موافقت شورای نگهبان در اولین انتخابات پس از تصویب این قانون با در نظر گرفتن سهولت رأی دادن، تسریع در شمارش آرا، و حضور و مشارکت رأی‌دهندگان فرآیند رأی دادن و شمارش آرا را در حداقل یک‌هشتم حوزه‌های دارای تعدد کرسی مجلس به صورت کاملاً الکترونیکی برگزار کند. توسعهٔ فرایند الکترونیکی در دوره‌های انتخاباتی بعدی مجلس منوط به در نظر گرفتن شرایط اجتماعی، اقتصادی، سیاسی، و امنیتی و موافقت شورای نگهبان است. وزارت کشور موظف است به گونه‌ای برنامه‌ریزی کند که حداکثر یک هفته قبل از روز اخذ رأی کلیهٔ فرایندها و امکانات الکترونیکی برای برگزاری انتخابات ثبت شود و به تأیید شورای نگهبان برسد.

تبصره- فرایند ثبت‌نام رأی‌دهندگان در شعب اخذ رأی و احراز هویت آن‌ها در کلیهٔ حوزه‌های انتخابیهٔ کشور به صورت الکترونیکی خواهد بود.

۲۷. مادهٔ ۹ (اصلاحی ۱۳۷۲/۰۲/۲۸). چنانچه در همه یا بعضی از شهرستان‌های یک استان شمارش آرا با دستگاه شمارشگر صورت پذیرد سیستم کامپیوتری انتخابات باید به نحوی طراحی و اجرا شود که دسترسی به نرم‌افزارها و سخت‌افزارهای آن در کلیهٔ مراحل انتخابات بدون حضور نمایندگان شورای نگهبان میسر نباشد. تصمیمات لازم جهت حفظ نرم‌افزارها و سخت‌افزارها مشترکاً توسط شورای نگهبان و وزارت کشور اتخاذ می‌شود و کلیهٔ نسخه‌های نرم‌افزاری قبل از انتخابات به تأیید شورای نگهبان رسیده و مهر و موم (قفل نرم‌افزاری) می‌شود تا در زمان مورد توافق با حضور نمایندگان شورای نگهبان و وزارت کشور روی سیستم‌های کامپیوتری هر حوزهٔ انتخاباتی نصب و راه‌اندازی گردد. هر گونه تغییر در نرم‌افزارها باید با اطلاع و تأیید شورای نگهبان انجام گیرد.

۲۸. هش (Hash) در علوم کامپیوتر و کریپتوگرافی رشته‌ای با طول ثابتی از کاراکترها است که توسط تابعی ریاضی به نام تابع هش (Hash Function) تولید می‌شود. ورودی تابع هش که به آن مسیج یا پیام (Message) گفته می‌شود می‌تواند طول نامحدود داشته باشد (مثلاً به کوچکی یک کاراکتر یا به بزرگی همهٔ اطلاعات روی اینترنت). اما خروجی یا هش همیشه طول ثابت دارد. هشینگ (Hashing) به فرآیند ورود داده یا پیام به منظور تولید رشته‌ای از کاراکترها یا هش گفته می‌شود. یک ورودی یکسان همیشه خروجی هش یکسان دارد. اما کوچک‌ترین تغییری در ورودی منجر به تولید هش متفاوت می‌شود.

29. computer vision
30. cryptographic keys
31. digital signature
32. decentralized identity
33. zero-knowledge proofs

۳۴. جهت مطالعهٔ بیشتر ← پایان‌نامهٔ کارشناسی‌ارشد منتشرشده در دانشگاه فناوری تالین (Tallinn University of Technology) با عنوان « Proving Vote Correctness in the Estonian Internet Voting System» نوشتهٔ Taaniel Kraavi، منتشرشده در سال ۲۰۲۴.

35. privacy

۳۶. این موضوع در اسناد مختلف به دلیل اهمیت آن مورد توجه قرار گرفته است؛ مثلاً ←
سند مقام ناظر اروپایی حمایت از داده‌ها مربوط به هوش مصنوعی: هوش مصنوعی، رباتیک، حریم خصوصی و حمایت از داده (اکتبر ۲۰۱۶)

https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en

۳۷. مثلاً میکسینگ (Mixing) و شبکه‌های ناشناس‌ساز برخی سامانه‌ها از تکنیک‌هایی مشابه coin mixing یا network anonymization استفاده می‌کنند تا مسیر رأی از هویت فرد کاملاً جدا شود. مثلاً رأی‌دهنده رأی خود را به یک مخزن مشترک می‌فرستد و سپس از آنجا به صورت تصادفی در بلاک‌چین ثبت می‌شود تا امکان ردیابی فردی حذف شود. علاوه بر این حفظ محرمانگی حتی در هنگام شمارش در برخی سیستم‌ها از الگوریتم‌هایی استفاده می‌شود که امتیاز یا انتخاب رأی‌ها را جمع می‌کنند بدون اینکه لازم باشد هر رأی را افشا کنند. به این تکنیک‌ها گاهی Homomorphic Encryption گفته می‌شود که در آن می‌توان محاسبات ریاضی را روی داده‌های رمزنگاری‌شده انجام داد.

۳۸. Helios یک سامانهٔ رأی‌گیری متن‌باز و رمزنگاری‌شده است که در دانشگاه‌ها، اتحادیه‌ها، و حتی انتخابات داخلی برخی احزاب سیاسی استفاده شده است. این سیستم از رمزنگاری انتها به انتها (end-to-end encryption) و رمزنگاری هم‌ریخت (homomorphic encryption) برای حفظ محرمانگی آرا استفاده می‌کند.

https://vote.heliosvoting.org/privacy

۳۹. در سال ۲۰۱۸، شهر زوگ (Zug) در سوئیس یک آزمایش رأی‌گیری مبتنی بر بلاک‌چین را با همکاری شرکت Luxoft و پلتفرم uPort انجام داد. این پروژه از Hyperledger Fabric برای ثبت آرا و از هویت دیجیتال مبتنی بر بلاک‌چین برای احراز هویت استفاده کرد.

40.https://www.swissinfo.ch/eng/politics/digital-democracy_switzerland-unveils-second-blockchain-voting-system/44226544

منابع

کتاب‌ها

ابوذری، م. (۱۴۰۱). *حقوق و هوش مصنوعی*. تهران: میزان.

انصاری، ب. (۱۴۰۰). *حقوق داده‌ها و هوش مصنوعی*. تهران: شرکت سهامی انتشار.

دو فیلیپای، پ. و رایت، آ. (۱۴۰۱). *بلاک‌چین و حقوق*. مترجم: حسین صادقی. تهران: حقوق‌یار.

مقالات

صفری ورزرد، ا. (۱۴۰۱). بلاک‌چین و قراردادهای هوشمند: سازکارها و کاربردها. *چهارمین کنفرانس بین‌المللی مدیریت، گردشگری، و تکنولوژی*، ۱ ـ ۱۷.

گزارش

اخوان، م. و همکاران (۱۴۰۳). پویاشناسی مسائل و نابه‌سامانی‌های فضای مجازی در ایران. تهران: مرکز پژوهش‌های مجلس شورای اسلامی.

References

Articles

Abouzari, M. (2022). Hoghoogh va Hoosh-e Masnoo'i [Law and Artificial Intelligence]. Tehran: Nashr-e Mizan.

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary?. Journal of Governance and Regulation, 7(1), 45-62.

Davies, D. (1997). A brief history of cryptography. [Publisher information missing].

De Filippi, P., & Wright, A. (2022). Blockchain va Hoghoogh [Blockchain and Law]. (H. Sadeghi, Trans.). Tehran: Hoghoogh Yar. [Note: Original publication details not provided].

G'sell, F., & Martin-Bariteau, F. (2022). The impact of blockchains for human rights, democracy, and the rule of law. Council of Europe.

Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An anti-quantum e-voting protocol in blockchain with audit function. IEEE Access, 7, 115304-115316. [Note: Journal name 'IEEE Access' inferred from Vol 7 format].

Gorman, J. M. (1996). Medication and emotional health. New York: St. Martin's Press.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, [Volume/Issue missing], 99-111.
J., Serra, A., & Zhu, C. (2016). Kaspersky Lab Cyber, economist. [Source Information Missing], pp. 1-11. [Note: Needs clarification if 'economist' is part of title or source].
Jafar, U., Ab Aziz, M. J., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors, [Volume/Issue missing], 1-23.
Khan, K. M., & Arshad, J. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53-65.
Liu, Y., & Wang, Q. (2017). An E-voting protocol based on blockchain. International Association for Cryptologic Research ePrint Archive, pp. 1-13. [Note: Source format might need adjustment based on specific archive style].
Murphy, M. A., Lai, D., & Sookraj, D. (1997). Evaluation of the neighborhood (congregate) meal program: Final report. Kelowna, BC: Kelowna Home Support Society.
Proceedings of the 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), Tokyo, Japan, July 23-26. [Page numbers missing].
Richtel, M. (2001). Technology: With napster down its audience fans out. [Source information missing].
Rudiger, S. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Proceedings of the First International Conference on Peer-to-Peer Computing. [Page numbers missing].
Rutherford, B. J. (2006). Reading disability and hemispheric interaction on a lexical decision task. Brain and Cognition, 60(20), 55-63.
Safari Varzard, (2022). Blockchain and Smart Contracts: Mechanisms and Applications, Fourth International Conference on Management, Tourism and Technology،https://civilica.com/doc/1461078, pp. 1-17. (in Persian)
Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review. Exploring Services Science, pp. 12-23. [Note: Assuming 'Exploring Services Science' is the proceedings/book title].
Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2018). On the origins and variations of blockchain technologies. IEEE Security & Privacy, [Volume, Issue, and Page numbers missing].
Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting

application used in U.S. federal elections. Proceedings of the 29th USENIX Security Symposium, pp. 1535-1552.
Srivastava, G., Dwivedi, A. D., & Singh, R. (2018). Crypto-democracy: A decentralized voting scheme using blockchain technology. Proceedings of the International Conference on Security and Cryptography (SECRYPT), pp. 508-513.
Tas, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. Symmetry, [Volume/Issue missing], 1-24.
Taylor, M. B. (2013). Bitcoin and the age of bespoke silicon. Proceedings of the International conference on compilers architectures and synthesis for embedded systems (CASES), Piscataway, NJ. [Page numbers missing].
Vinnakota, R. (2021). Which Countries Are Casting Votes Using Blockchain?. [Source Information Missing].Articles & Conference Papers Anane, R., Freeland, R., & Theodoropoulos, G. (2007). e-Voting requirements and implementation.

Websites

"Elon Musk and Others Call for Pause on A.I., Citing ‘Profound Risks to Society’". (2023, March 29). The New York Times. Available: https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html
West Virginia to offer mobile blockchain voting app for overseas voters in November election. The Washington Post. Available T. (2018, August 10): https://www.washingtonpost.com/technology/۱۰/۰۸/۲۰۱۸/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election/