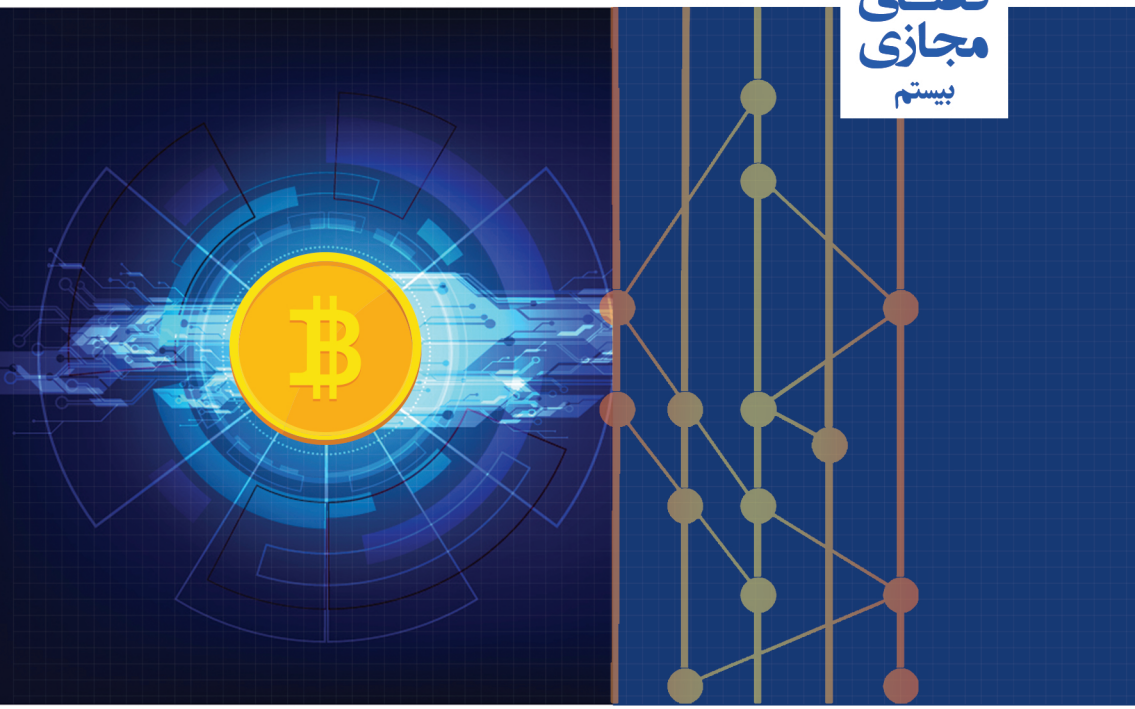
مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
بیستم



هش گراف
پایان بلاک چین؟

Hash graph
The end of the Chinese bloc?

جمهوری اسلامی ایران
مرکز ملی فضای مجازی

عنوان گزارش:

هش‌گراف: پایان بلاک‌چین؟

گزارش شماره ۲۰
آذر ماه ۱۳۹۸

تهیه شده در: پژوهشگاه فضای مجازی- گروه علوم و فناوری‌های نوین
تهیه‌کننده: حمیدرضا مازندرانی (دانشجوی دکتری دانشگاه صنعتی امیرکبیر)

ناظر علمی: محمد مهدی رضاپور

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰، کدپستی ۱۵۱۵۶۷۴۳۱۱
شماره تماس: ۸۶۱۲۱۰۶۱ http://www.majazi.ir

سخن نخست

فضای مجازی با شتاب شگرف و روبه تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را در نوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می دهد. لذا به نظر می رسد 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 می کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره کننده فضای مجازی و سایه گستری آن در حوزه ها و شئون بشر در یک دهه اخیر آن را چون سکویی می داند که بسیار فراتر از شأن ابزاری حیات انسان ها 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 داشته اند.

در همین راستا گزارش های عصر فضای مجازی تلاش می کند تا فهم سازمان ها و دستگاه های مرتبط با حوزه ی فضای مجازی را ارتقاء بخشیده و آن ها 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

هش‌گراف، پروتکلی است که همانند زنجیره بلوکی(بلاک‌چین)، امکان دستیابی به اجماع را در محیطی که اعتماد بین اعضاء وجود ندارد، فراهم می‌سازد. با این حال، تفاوت‌های اساسی در نحوه ذخیره اطلاعات و سازوکار دستیابی به اجماع میان هش‌گراف و پروتکل‌های زنجیره بلوکی وجود دارد، که منجر به برتری احتمالی هش‌گراف از نظر کارایی، امنیت و مصرف انرژی می‌گردد. این گزارش، به معرفی اجمالی هش‌گراف به عنوان نسل جدید پروتکل‌های دفترکل توزیع‌شده و تفاوت‌های آن با زنجیره بلوکی می‌پردازد.

واژگان کلیدی: هش‌گراف، زنجیره بلوکی، اجماع، ارز مجازی، لایه اعتماد

فهرست مطالب

مقدمه

فناوری زنجیره بلوکی[۱] توجهات فراوانی را در سالیان اخیر به خود جلب نموده است. این فناوری، که بیش از هر چیز در مرکزیت‌زدایی[۲] از تبادلات مالی خود را نشان داده است، به طور خلاصه یک مجموعه زنجیره‌وار از اطلاعات است که با مکانیزم‌های امضای دیجیتال و هش‌گیری،[۳] غیرقابل‌تغییر می‌گردد و مهم‌تر این‌که شماری از افراد که به یکدیگر اعتماد ندارند، در خصوص محتویات آن زنجیره به اجماع[۴] می‌رسند. برای مثال، در بیت‌کوین، به عنوان شاخص‌ترین پیاده‌سازی زنجیره بلوکی، تراکنش‌های مالی بین افراد در زنجیره بلوکی ثبت می‌شود. با توجه به مکانیزم اجماعی که برای بیت‌کوین طراحی شده است، امکان سرقت از سایرین یا دو بار خرج کردن پول غیرممکن است.

زنجیره بلوکی را می‌توان یک نظم و انسجام هدفمند از چندین فناوری شامل هش‌گیری، رمزنگاری غیرمتقارن، امضای دیجیتال و مکانیزم‌های اجماع دانست، که یک دفتر کل توزیع‌شده[۵]

---

[۱] Blockchain

[۲] Decentralization

[۳] Hashing: مکانیزمی که در آن ورودی با هر سایز دلخواه، به یک رشته کاراکتر با طول ثابت تبدیل می‌شود. با هر تغییر کوچکی در اطلاعات اولیه، هش کاملاً تغییر می‌کند. با این حساب، هش را می‌توان اثرانگشت یک سند اطلاعاتی دانست.

[۴] Consensus

[۵] Distributed Ledger

را پدید می‌آورد. کاربران نسبت به محتویات این دفتر کل توزیع‌شده اجماع نظر دارند؛ اجماعی که بدون نیاز به یک شخص ثالث مورد اعتماد[۱](TTP) حاصل می‌شود.

با این حال، ذهن کنجکاو پژوهشگران در یک نقطه متوقف نمی‌شود، بلکه همواره به دنبال ایجاد فناوری‌هایی است که برتر از فناوری‌های قبلی باشد و در عین حال معایب آن‌ها را نیز نداشته باشد. مفهومی به نام هش‌گراف[۲]نیز در ادامه فناوری زنجیره بلوکی مطرح شده است. هش‌گراف همچون زنجیره بلوکی یک دفترکل توزیع‌شده است، اما نحوه ثبت اطلاعات و مکانیزم اجماع آن با زنجیره بلوکی تفاوت اساسی دارد، که این تفاوت به ادعای طراحان هش‌گراف ویژگی‌های مثبتی همچون سریع و ارزان بودن را به ارمغان می‌آورد.

گفتنی است در سپتامبر سال جاری میلادی، یک نسخه پیاده‌سازی‌شده از پروتکل هش‌گراف با عنوان Hedera Hashgraph معرفی گردید.[۳]سه سرویس برای این پروتکل در نظر گرفته شده است: ارزمجازی، قرارداد هوشمند[۴]و سیستم ذخیره فایل.

یکی از ایرادات پروتکل هدرا، این است که کاملاً توزیع‌شده نیست. در واقع، شورای حکمرانی هدرا، کنترل و امن‌سازی شبکه را بر عهده دارد. این شورا شامل تعدادی از شرکت‌های بزرگ همچون بوییِنگ و دویچه‌تلکام است، که تغییرات نرم‌افزاری پروتکل را مدیریت می‌کنند.

با این حال، دور از انتظار نیست که هش‌گراف آینده روشنی چه در صنعت و چه در مراکز پژوهشی داشته باشد. در همین راستا، این گزارش سعی می‌کند مفهوم هش‌گراف را تبیین نموده، آن را با زنجیره بلوکی مقایسه نماید و در انتها نگاهی راهبردی به آینده این فناوری در کشور داشته باشد. منتها پیش از آن، فلسفه پیدایش فناوری دفترچه کل توزیع‌شده بیان می‌گردد تا زمینه ورود به بحث فراهم شود.

---

[۱] Trusted Third Party

[۲] Hashgraph

[۳] نشانی وبسایت رسمی هدرا: www.hedera.com

[۴] Smart Contract

فصل ۱- فلسفه پیدایش زنجیره بلوکی

۱-۱- از بیت‌کوین تا زنجیره بلوکی

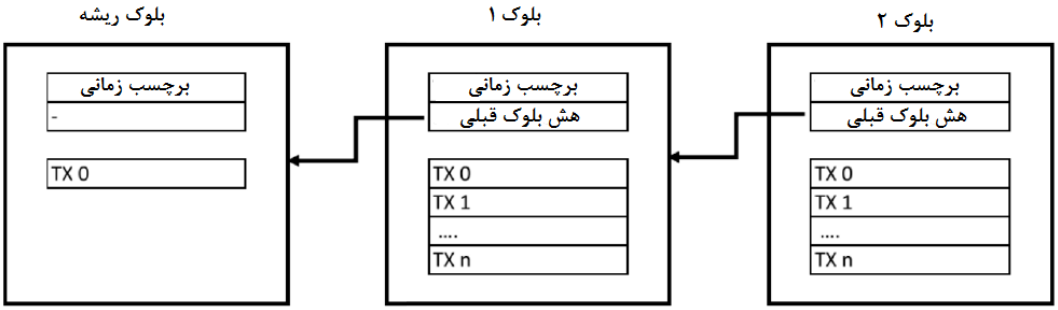
زمانی که ساتوشی ناکاموتو[۱] که هویت وی همچنان ناشناس مانده است، در سال ۲۰۰۸ با انتشار گزارشی پروتکل بیت‌کوین را به عنوان یک سیستم تبادل مالی همتابه‌همتا[۲]معرفی کرد، فناوری زنجیره بلوکی رسماً وارد دنیای تجارت گردید. این فناوری، در طول یک دهه گذشته پیشرفت‌های فراوانی داشته است، تا جایی که می‌توان آن را از فناوری‌های تحول‌ساز دهه اخیر نام برد. نکته‌ای که در این‌جا باید توجه داشته باشیم، این است که بیت‌کوین تنها یک پروتکل طراحی‌شده بر پایه فناوری زنجیره بلوکی است، در حالی که فناوری زنجیره بلوکی فراتر از بیت‌کوین است و کاربرد آن محدود به تبادلات مالی نیست.

به طور کلی، زنجیره بلوکی چنان‌چه از نام آن پیداست، زنجیره‌ای از بلوک‌ها است (شکل ۱). به بیان دیگر، زنجیره بلوکی یک ساختارداده[۳]است که اطلاعات در بلوک‌های آن ذخیره می‌شود.

---

[۱] Satoshi Nakamoto
[۲] Peer-to-Peer
[۳] Data Structure

هر بلوک حاوی هش بلوک قبلی است، که ارتباط آن را با بلوک قبلی برقرار می‌سازد. برای مثال در شکل ۱، هش بلوک شماره یک در بدنه بلوک شماره دو گنجانده شده است.



شکل ۱- ساختار زنجیره بلوکی

در هش‌گراف نیز مفاهیم هش و برچسب زمانی استفاده می‌شود، منتها با یک ساختارداده متفاوت که مزیت‌هایی نسبت به این شیوه دارد.

هر بلوک حاوی تعدادی تراکنش است، که در بیت‌کوین این تراکنش‌ها به معنای "انتقال یک مقدار پول از حسابی به حساب دیگر" است. اما انواع دیگری از تراکنش‌ها نیز قابل استفاده است، که در ادامه این فصل بدان اشاره می‌گردد.

هر عضو زنجیره بلوکی می‌تواند اطلاعات تمامی بلوک‌ها را ذخیره نماید و بدین صورت است که مرکزیت‌زدایی انجام می‌شود. مرکزیت‌زدایی معادل این است که هیچ عضوی نمی‌تواند به دلخواه اطلاعات را حذف نماید یا تغییر دهد. البته مشروط به این که تعداد اعضاء شبکه زیاد باشد و افراد خرابکار بخش کوچکی از شبکه را تشکیل دهند. چنین قابلیتی، با استفاده از یک پروتکل اجماع ایجاد می‌شود، که طبق آن اعضاء باید به نحوی بر روی یک زنجیره یکسان توافق نمایند.

انواع مختلفی از پروتکل‌های اجماع وجود دارد، که در [۱] شرح داده شده است. در بخش بعدی، مکانیزم اثبات سختی کار[۱](PoW) و مکانیزم اثبات سهام[۲](PoS) به عنوان دو نمونه از پروتکل‌های اجماع بیشتر شناخته‌شده، توضیح داده می‌شود.

[۱] Proof of work
[۲] Proof of Stake

۲-۱- اجماع در زنجیره بلوکی

به طور کلی، فرآیندهای اجماع در زنجیره بلوکی بدین صورت است که باید به نوعی محرز شود بلوک جدیدی که قرار است توسط یکی از اعضاء به زنجیره اضافه شود، درست است (شامل تراکنش‌های معتبر است).

در بیت‌کوین، مکانیزم اثبات سختی کار (PoW) به عنوان پروتکل اجماع استفاده می‌شود. در PoW، هر عضوی که می‌خواهد در ساختن زنجیره مشارکت نماید، باید یک پازل ریاضی را حل کند، که این کار به محاسبات فراوانی نیاز دارد. در واقع، صرف هزینه (و متعاقباً انرژی) برای انجام این محاسبات نشان می‌دهد که آن فرد صلاحیت ایجاد بلوک جدید را دارد و همگان می‌توانند به آن بلوک اعتماد نمایند.

پازلی که در بالا از آن نام برده شد، در واقع یک فرآیند هش‌گیری معکوس است که در آن از بلوکی که قرار است به زنجیره اضافه شود، به همراه یک عدد تصادفی، هش گرفته می‌شود. هش حاصله باید یک ویژگی خاص را داشته باشد (مثلاً ابتدای آن تعدادی صفر وجود داشته باشد). بدین منظور، عدد تصادفی مذکور باید آن‌قدر تغییر داده شود تا خروجی تابع هش حائز ویژگی مورد نظر گردد. زمانی که یک استخراج‌کننده[۱] به موفقیت دست یافت، نتیجه خود را به سایرین گزارش می‌کند، تا بلوک مورد نظر به زنجیره اضافه شود. ممکن است همزمان دو عضو شبکه پازل را حل نمایند، که در این صورت دو شاخه در انتهای زنجیره ایجاد می‌شود که در نهایت فقط یکی از آن‌ها پذیرفته شده و دیگری فسخ می‌شود. همین مسئله فرآیند اجماع در زنجیره بلوکی را زمان‌بر می‌سازد.

در پروتکل اثبات سهام (PoS) که برای حل مشکل مصرف بالای محاسبات و انرژی در PoW پیشنهاد شده است، اعضایی که سهام بیش‌تری داشته باشند، بلوک‌های جدید را تایید می‌کنند. به بیان دیگر، هر فرد به تناسب سهامی که دارد امکان انتخاب شدن به عنوان تاییدکننده بلوک‌های جدید را دارد. علی‌رغم کارایی بالاتر PoS نسبت به PoW، نگرانی‌هایی در خصوص امنیت این شیوه حصول اجماع وجود دارد.

---

[۱] Miner: به اعضایی که با حل کردن پازل، بلوک‌های جدید به زنجیره اضافه می‌کنند گفته می‌شود.

اتریوم که پس از بیت‌کوین، دومین پیاده‌سازی شاخص زنجیره بلوکی تا به امروز محسوب می‌شود، یک نسخه اصلاح‌شده از مکانیزم PoS را به نام CASPER طراحی کرده است که امنیت بالایی دارد و قرار است جایگزین مکانیزم مبتنی بر PoW فعلی در اتریوم شود.

۳-۱- چرا زنجیره بلوکی؟

زنجیره بلوکی، جایگزین مناسبی برای سیستم‌های سنتی ذخیره‌سازی تراکنش‌ها و ثبت دارایی‌ها به صورت توزیع‌شده است، زمانی که:

- طرف ثالث مورد اعتماد (TTP) وجود ندارد، یا نیت بر این است که طرف ثالث مورد اعتماد (برای مثال بانک) از میان برداشته شود. به همین دلیل، بیت‌کوین پناهگاه بسیاری از هکرهای غیرقانونی، کلاهبرداران و خلافکاران برای تبادل پول شده است، چرا که از نظارت بانک‌ها و نهادهای قانونی تا حدی مصون مانده است.[۱] البته این موضوع نباید مانع از به‌کارگیری این پروتکل شود، همچنان که اینترنت نیز اگر چه تبادل اطلاعات میان خلافکاران را ساده می‌نماید، مزایای آن بر کسی پوشیده نیست.

- اطلاعات تنها از نوع افزودنی[۲] باشد، چرا که در زنجیره بلوکی امکان حذف یا تغییر داده وجود ندارد. در واقع، زنجیره بلوکی امکان ثبت اطلاعات را برای همیشه فراهم می‌سازد، و مانع از سانسور یا دستکاری اطلاعات می‌شود.

پیش‌تر ذکر شد که تراکنش‌های ثبت‌شده در زنجیره بلوکی محدود به تراکنش‌های مالی نیست و انواع مختلفی از کاربردها را می‌توان پوشش داد، از جمله ساختن برنامه‌های توزیع‌شده (DApp) که در آن تعدادی گره به صورت توزیع‌شده یک برنامه را اجرا می‌نمایند. برای پیاده‌سازی DApp از قراردادهای هوشمند استفاده می‌شود. در قرارداد هوشمند، بر اساس یک منطق کلی، مجموعه‌ای از قواعد به صورت "اگر-آن‌گاه" نوشته می‌شود، که در صورت تحقق شرایط، تراکنش اجرا می‌شود. البته انواع پیشرفته‌تری از برنامه‌های توزیع‌شده وجود دارد که می‌توانند حلقه[۳] نیز

---

[۱] البته اخباری در خصوص ردیابی مجرمان در این فضا مشاهده می‌شود. برای مثال اخیراً یک شبکه بزرگ در دارک وب شناسایی شد و اعضای آن دستگیر شدند (www.independent.co.uk/news/world/americas/child-porn-bitcoin-arrests-us-jong-woo-son-a9159146.html)

[۲] Append-only

[۳] Loop

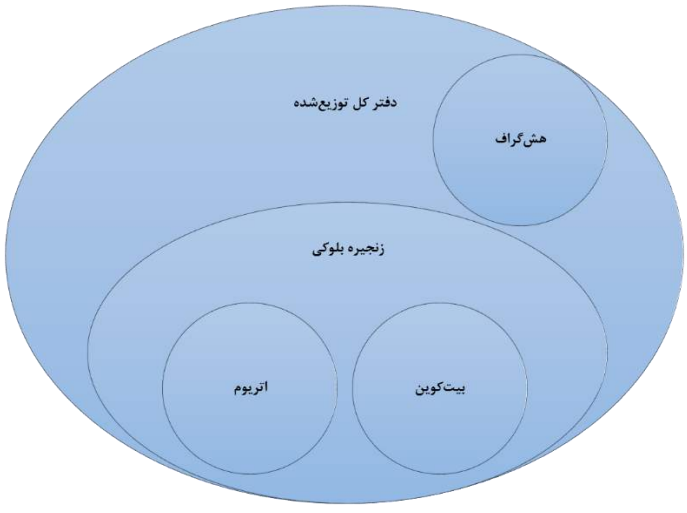
در ساختار خود داشته باشند. خوانندگان علاقه‌مند می‌توانند به مراجعی نظیر [۲] برای مطالعه بیش‌تر مراجعه نمایند.

ذخیره‌سازی اطلاعات به صورت توزیع‌شده نیز کاربرد دیگری است که سیستم‌های مبتنی بر زنجیره بلوکی می‌توانند ارائه دهند. از جمله می‌توان به FileCoin اشاره کرد که در آن، عده‌ای از کاربران، اطلاعات سایرین را ذخیره می‌نمایند. هش اطلاعات ذخیره‌شده، در زنجیره بلوکی ثبت می‌شود تا از صحت اطلاعات در هنگام بازیابی اطمینان حاصل شود.

۴-۱- فراتر از زنجیره بلوکی

زنجیره بلوکی، خود یک زیرمجموعه از فناوری‌های دفترکل توزیع‌شده (DLT) است (شکل ۲). در واقع هر فناوری که بتواند اجماعی را به صورت توزیع‌شده در خصوص یک مجموعه از اطلاعات، میان افرادی که به یکدیگر اعتماد ندارند، فراهم آورد یک دفترکل توزیع‌شده محسوب می‌شود. هش‌گراف، یک نمونه دیگر از فناوری‌های دفترکل توزیع‌شده است که موضوع این گزارش قرار گرفته است.

زنجیره بلوکی، علی‌رغم مزایایی که دارد، از چالش‌هایی همچون مقیاس‌پذیر نبودن، اثبات‌پذیر نبودن درستی اجماع و سربار خیلی زیاد رنج می‌برد. این مشکلات در فصل سوم تشریح شده است. چنین مشکلاتی توجه محققان و صاحبان صنایع را به انواع دیگر دفترکل توزیع‌شده (همچون هش‌گراف و IoTA) معطوف نموده است.



شکل ۲- ارتباط بین دفترکل توزیع‌شده، زنجیره بلوکی و بیت‌کوین

فصل ۲- آشنایی با هش‌گراف

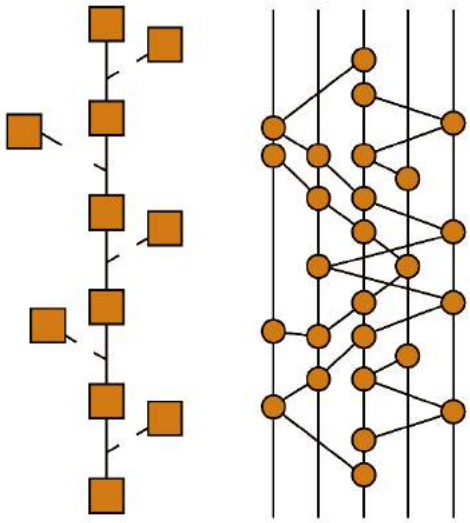
۲-۱- هش‌گراف چیست؟

هش‌گراف، یک پروتکل دفترکل توزیع‌شده (DLT) است که توسط دکتر لیمون بیرد[۱] هم‌بنیان‌گذار و مدیر فنی شرکت Swirlds، ابداع شده است [۳]. اطلاعات در هش‌گراف، نه به صورت یک زنجیره، بلکه به صورت یک گراف جهت‌دار بدون دور[۲](DAG) ذخیره می‌شود. DAG گرافی است که یال‌های آن جهت‌دار بوده و هیچ دوری در آن وجود ندارد؛ یعنی با حرکت از یک رأس در جهت یال‌ها نمی‌توان دوباره به آن رأس رسید. ثابت شده است که هش‌گراف تحمل خطای بیزانس نامتقارن[۳](aBFT) دارد، که معادل این است که اگر اعضای خرابکار کم‌تر از یک‌سوم کل اعضا را تشکیل دهند، اجماع حاصل می‌شود.

در زنجیره بلوکی، شاخه‌های فرعی همواره هرس[۴] می‌شود، تا یک زنجیره قابل‌کنترل و یکپارچه از اطلاعات باقی بماند. در نقطه مقابل، در هش‌گراف شاخه‌های فرعی نیز در فرآیند اجماع نقش ایفا می‌نمایند. این تفاوت در شکل ۳ قابل مشاهده است.

---

[۱] Leemon Baird
[۲] Directed Acyclic Graph
[۳] asynchronous Byzantine-Fault Tolerance
[۴] Prune



شکل ۳- مدل مفهومی زنجیره بلوکی (سمت چپ) و هش‌گراف (سمت راست)

۲-۲- مفاهیم اصلی

مفاهیم اصلی هش‌گراف شامل موارد زیر است. لازم به ذکر است برخی از این مفاهیم در نگاه اول ممکن است کمی پیچیده به نظر برسند، با این حال، با مطالعه بخش‌های بعدی، ابهامات رفع خواهد شد.

- *تراکنش*:[۱] همان مفهوم تراکنش در زنجیره بلوکی (از جمله بیت‌کوین) را دارد. هر عضو شبکه می‌تواند یک تراکنش امضاشده را صادر نماید، و سایرین نیز آن را دریافت نمایند و به یک توافق در خصوص تراکنش‌ها دست یابند.
- *رویداد*:[۲] یک ساختار داده در حافظه هر کدام از کاربران است که تعدادی تراکنش در آن ذخیره می‌شود. این مفهوم، مشابه مفهوم بلوک در زنجیره بلوکی است. هدف پروتکل هش‌گراف این است که توافقی در خصوص ترتیب رویدادها (و متعاقباً ترتیب تراکنش‌ها) حاصل شود.
- *انصاف*:[۳] بدین صورت تعریف می‌شود که برای گروه کوچکی از مهاجمان، تغییر ترتیب تراکنش‌های مورد توافق دشوار باشد.

---

[۱] Transaction
[۲] Event
[۳] Fairness

- *سخن‌چینی*:[۱] اطلاعاتی است که هر عضو به صورت تکرارشونده پخش می‌کند، بدین صورت که هر رویدادی را که از آن خبر دارد، به یکی دیگر از اعضا (که به صورت تصادفی انتخاب شده) ارسال می‌کند.
- *هش‌گراف*: یک ساختار داده که در آن اطلاعاتی شامل این که چه کسانی، به چه کسانی پیغام سخن‌چینی فرستاده‌اند، به همراه ترتیب ارسال آن‌ها ثبت می‌شود.
- *سخن‌چینی درباره سخن‌چینی*:[۲] اطلاعاتی که سخن‌چینی می‌شود، شامل تاریخچه همان سخن‌چینی است، و لذا این عنوان بدان اطلاق می‌شود. در بخش بعدی این موضوع تشریح خواهد شد.
- *رای‌گیری مجازی*:[۳] هر عضو یک کپی از هش‌گراف را دارد، و لذا می‌داند که دیگری اگر از یک پروتکل بیزانس کلاسیک استفاده می‌کردند، چه رای‌ای می‌داشته است. یادآوری می‌گردد در پروتکل بیزانس کلاسیک، اگر دو عضو همزمان تراکنشی را ارسال نمایند، برای رفع تداخل از مکانیزم رای‌گیری استفاده می‌شود. در پروتکل هش‌گراف، نیازی به ارسال رای‌ها نیست و همان اطلاعات موجود کافی است.
- *شاهدان معروف*:[۴] رویدادی است که بتوان نشان داد، اکثریت اعضای شبکه آن را خیلی زود دریافت نموده‌اند. شاهدان معروف برای شرکت در فرآیند اجماع انتخاب می‌شوند.
- *مشاهده قوی*:[۵] گفته می‌شود رویداد x رویداد y را به صورت قوی مشاهده می‌کند، اگر تعداد مناسبی[۶] مسیر مجزا و رو به پایین از x به y وجود داشته باشد.

۳-۲- کلیات عملکرد هش‌گراف

اجماع در هش‌گراف به وسیله پروتکل سخن‌چینی انجام می‌شود. در این پروتکل، هر کاربر یکی دیگر از کاربران را به صورت تصادفی انتخاب می‌کند، آن‌گاه تمامی رویدادهایی را که ذخیره کرده است به آن کاربر می‌فرستد. از آن جایی که این کار را همه کاربران به صورت تکرارشونده

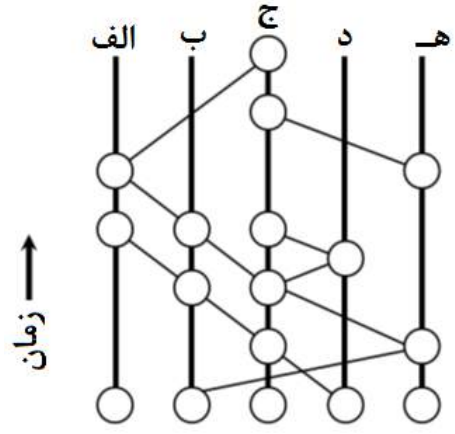
---

[۱] Gossip
[۲] Gossip About Gossip
[۳] Virtual Voting
[۴] Famous Witnesses
[۵] Strongly Seeing
[۶] منظور از تعداد مناسب این است که مسیرهایی شامل بیش از دوسوم اعضای دور قبل وجود داشته باشد.

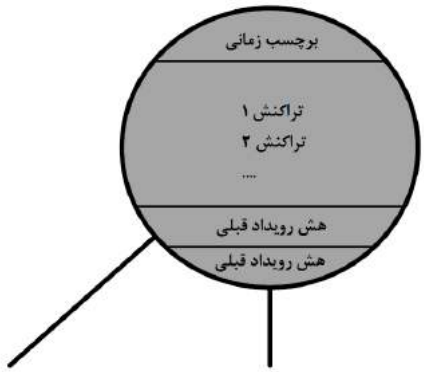
انجام می‌دهند، اطلاعات جدید به سرعت در تمام شبکه پخش می‌گردد و همگی از آن آگاه می‌شوند.

برای هر پروتکل سخن‌چینی می‌توان یک گراف مشابه شکل ۴ رسم نمود، که در آن هر ستون نشانگر یکی از کاربران است (کاربر *الف*، کاربر ب و الی آخر). هر رأس روی هر ستون نشان‌دهنده یک رویداد سخن‌چینی است. برای مثال، چنان‌چه کاربر *الف* پیغامی را از کاربر ب دریافت کند، آن را به صورت یک رأس در ستون *الف* نمایش می‌دهند. هر رأس، دو یال رو به پایین دارد، که به رئوس متناظر با دو رویداد سخن‌چینی قبلی متصل شده است.

البته این نکته را باید توجه داشت که چنین گرافی برای بحث در خصوص نحوه کار الگوریتم طراحی می‌شود و هیچ کدام از اعضای شبکه آن را به همین صورت ذخیره نمی‌کنند. در عوض، اعضای شبکه رویدادها را ذخیره می‌کنند. هر رویداد (رأس) رشته‌ای از اطلاعات است که توسط ایجاد کننده آن امضای دیجیتال می‌شود. محتویات یک رویداد در شکل ۵ قابل مشاهده است، که شامل برچسب زمانی، اطلاعات یک یا چند تراکنش، و هش دو رویداد قبلی آن است. لازم به ذکر است هر رویداد توسط سازنده آن امضای دیجیتال می‌شود.

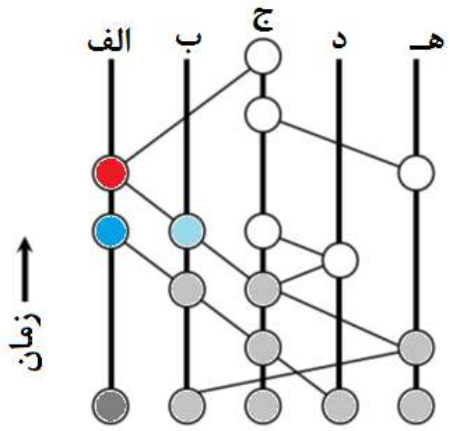


شکل ۴ - تاریخچه سخن‌چینی به صورت یک گراف جهتدار



شکل ۵ - محتویات یک رویداد

روند کار الگوریتم را در قالب یک مثال می‌توان این‌گونه شرح داد: هنگامی که کاربر *الف* پیغامی را از ب دریافت می‌کند، یک رویداد ایجاد می‌شود (راس قرمز رنگ در شکل ۶). این رویداد حاوی هش دو رویداد قبلی است: رویداد قبلی خودش (راس آبی پررنگ) و آخرین رویداد ب (آبی کم‌رنگ). همچنین این رویداد می‌تواند شامل محتوای تراکنش‌هایی باشد که کاربر *الف* در آن لحظه قصد ایجاد آن را دارد.



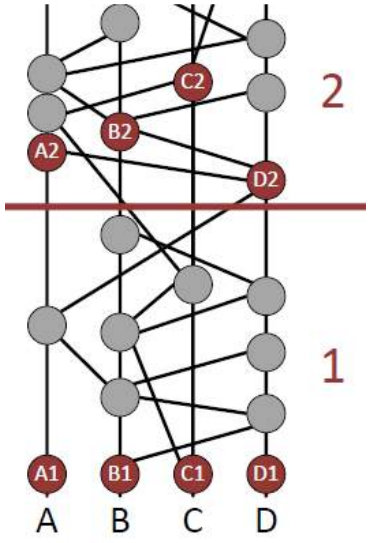
شکل ۶ – مثالی از فرآیند ایجاد رویداد در هش‌گراف

در این‌جا لازم است مفهوم دور[1](راند) توضیح داده شود. هر چند تا رویداد، متعلق به یک دور است، که با گذر زمان تعداد دورها افزایش می‌یابد. در شکل ۷، یک هش‌گراف شامل ۲ دور

[1] Round

مشاهده می‌شود. اولین رویداد هر کاربر در یک دور (در صورت وجود)، شاهد نامیده می‌شود. در این شکل، رویدادهای قرمزرنگ شاهد هستند.

در ابتدای کار یک هش‌گراف، همه کاربران در دور اول قرار دارند (رویدادهای A1 تا D1 در شکل ۷). هر رویداد، ماکزیمم شماره دور رویدادهای قبلی خودش را دارد، مگر این که بتواند بیش‌تر از دوسوم شاهدان دور قبل را به صورت قوی ببیند، که در آن صورت یک واحد به شماره دور افزوده می‌شود. برای نمونه، رویدادهای خاکستری رنگ در دور ۱ نمی‌توانند دوسوم رویدادهای A1 تا D1 را به صورت قوی ببینند، لذا جزو همان دور ۱ محسوب می‌شوند. اما رویداد D2 می‌تواند اکثریت رویدادهای دور اول را به صورت قوی ببیند و لذا اولین رویداد دور ۲ خواهد بود. پروسه محاسبه دور در شکل ۸ مشخص شده است.



شکل ۷ - یک هش‌گراف شامل ۲ دور

```
procedure divideRounds

for each event x
    r ← max round of parents of x (or 1 if none exist)
    if x can strongly see more than 2n/3 round r witnesses
        x.round ← r+1
    else
        x.round ← r
    x.witness ← (x has no self parent)
                or (x.round > x.selfParent.round)
```

شکل ۸ - پروسه محاسبه دور [۳]

برای هر شاهد، باید تعیین شود که آن شاهد از نوع معروف است یا خیر. شاهد معروف، شاهدی است که توسط بسیاری از شاهدان دور بعدی دیده شود. سازوکار دقیق تعیین معروف بودن یک شاهد، در پروسه decideFame در [۳] آورده شده است، که ذکر جزییات آن از حوصله این متن خارج است. همچنین برای مطالعه بیش‌تر در خصوص جزییات کارکرد هش‌گراف، مرجع [۴] پیشنهاد می‌گردد.

شاهدان معروف همانند بلوک‌های مورد اجماع در زنجیره بلوکی هستند، و صحت اطلاعات آن‌ها مورد قبول همگان قرار دارد. اما سوال اینجاست که با چه فرآیندی هر عضو در شبکه می‌تواند دارای یک رویداد از نوع شاهد معروف باشد، که پاسخ آن با فرآیند سخن‌چینی درباره سخن‌چینی داده می‌شود.

۴-۲- سخن‌چینی درباره سخن‌چینی

تاکنون پروتکل‌های سخن‌چینی برای بسیاری از مقاصد به کار گرفته شده‌اند، از جمله برای تبادل هویت اعضا یا اطلاعات تراکنش‌ها. اما در هش‌گراف یک رویکرد جدید در نظر گرفته شده است: از پروتکل سخن‌چینی برای تبادل اطلاعات سخن‌چینی استفاده شود. به بیان دیگر، کاربران اطلاعات رویدادهای قبلی خود را نیز در قالب پیغام‌های سخن‌چینی ارسال می‌نمایند. در نتیجه، اگر ب به الف پیغامی بفرستد، الف از تراکنش‌های ب و این که ب تراکنش‌ها را چگونه دریافت کرده است آگاه می‌شود. در نهایت می‌توان نتیجه گرفت همه کاربران یک نسخه از هش‌گراف را دارند.

رویه فوق، که با سربار پهنای باند[۱] کمی انجام می‌شود، این امکان را فراهم می‌آورد که اعضای شبکه از رویدادهای سایرین اطلاع داشته باشند. با این حال، داشتن چنین اطلاعی کافی نیست، بلکه لازم است ترتیب خطی رویدادها (و متعاقباً تراکنش‌ها) معین گردد. در پروتکل‌های معمول (آن‌هایی که راهبر ندارند)، این موضوع با ارسال رای‌های مثبت/منفی انجام می‌شود، و گاهی به چند دور رای‌گیری نیاز است. در هش‌گراف نیازی به رای‌گیری نیست، چرا که هر عضو تمامی اطلاعات هش‌گراف را دارد، و از این رو اصطلاحاً گفته می‌شود در هش‌گراف رای‌گیری مجازی انجام می‌شود. رای‌گیری مجازی علاوه بر این که در مصرف پهنای باند صرفه‌جویی می‌کند، این مزیت را دارد که حتی اگر یک عضو خرابکار باشد، نمی‌تواند با ارسال رای‌های اشتباه، دیگران را به اشتباه اندازد.

---

[۱] Bandwidth Overhead

باید توجه داشت ممکن است در یک لحظه از زمان، هش‌گراف دو کاربر اندکی متفاوت باشد، اما سازگار[۱] است. سازگاری بدین معنا است که اگر هر دو از یک رویداد x خبر داشته باشند، هر دو دقیقاً یک مجموعه از نیاکان[۲] x و یال‌های بین آن‌ها را ذخیره کرده‌اند. اما اگر فقط یکی از دو کاربر از رویداد x خبر داشته باشد، و اگر هر دو درستکار (غیرخرابکار) و فعال باشند، انتظار می‌رود که با پروتکل سخن‌چینی مشکل سریعاً برطرف شود. در صورت وجود کاربران خرابکار نیز تا زمانی که نسبت آن‌ها بیش‌تر از یک‌سوم اعضای شبکه نباشد، امکان تقلب وجود ندارد. جزییات این موضوع در مقاله اصلی آقای لیمون بیرد تشریح شده است [۳].

[۱] Consistent
[۲] Ancestor

فصل ۳- مقایسه هش‌گراف و زنجیره بلوکی

۳-۱- هش‌گراف و زنجیره بلوکی: دو ابزار برای یک هدف

ویژگی‌های زنجیره بلوکی، به بیان هیوز در [۵] به صورت زیر بیان شده است:

- یک دفتر کل توزیع‌شده است: تمامی اعضاء به همه اطلاعات سیستم دسترسی دارند، و در واقع همگی یک نسخه از زنجیره بلوکی را ذخیره می‌کنند. البته برخی از اعضای شبکه که اصطلاحاً گره سبک[۱] نامیده می‌شوند، به جای ذخیره کل زنجیره، تنها سرآیند بلوک‌ها را ذخیره می‌کنند. به هر حال، اکثر اعضای شبکه تمامی اطلاعات را در اختیار دارند و لذا اطلاعات در کنترل هیچ نهاد واحدی نیست.
- ارتباط مستقیم بین گره‌ها: هر گره به طور مستقیم به تبادل اطلاعات با سایرین می‌پردازد، و هیچ گره مرکزی برای برقراری ارتباط وجود ندارد.[۲]
- غیر قابل تغییر: هر تراکنشی، پس از این که در زنجیره ثبت بشود، به طور دائمی ذخیره خواهد شد و قابل تغییر نیست. ضمناً ترتیب تراکنش‌ها نیز غیر قابل تغییر است. به طور معادل می‌توان گفت زنجیره بلوکی یک مجموعه اطلاعات "فقط افزودنی" است.

---

[۱] Light Node

[۲] در پیاده‌سازی‌های فعلی، برای برقراری ارتباط گره‌های مرکزی از پیش‌تعیین‌شده وجود دارد، اما در حالت ایده‌آل چنین نیست.

- منطق محاسباتی: تراکنش‌ها می‌توانند برنامه‌ریزی شوند، به گونه‌ای که بر اساس خروجی یک الگوریتم امن و بدون دخالت یک نهاد مرکزی، به صورت خودکار اجرا شوند.

هش‌گراف نیز حائز تمامی ویژگی‌های فوق است، و لذا هر کاربردی که بتوان با زنجیره بلوکی پیاده‌سازی کرد، با هش‌گراف نیز قابل پیاده‌سازی است.

همچنین، روال کار برای ثبت تراکنش در زنجیره بلوکی در قالب یک مثال در [۵] ذکر شده، که شامل مراحل زیر است. در این مراحل، فرد *الف* می‌خواهد وجهی را به حساب فرد *ب* واریز نماید.

۱- *الف* باید تراکنش را با کلید خصوصی خودش و کلید عمومی *ب* امضاء نماید. در اینجا فرض می‌شود که اعضای شبکه کلید عمومی یکدیگر را دارند و هر پیامی که با کلید خصوصی یک عضو امضاء شده باشد، قابل صحت‌سنجی به وسیله کلید عمومی‌اش است.
۲- تراکنش توسط استخراج‌کنندگان (ماینرها) تایید می‌شود، تا مشخص شود که موجودی حساب *الف* کافی بوده است.
۳- تراکنش‌ها در قالب بلوک‌های اطلاعاتی ذخیره می‌شوند. (در بیت‌کوین، هر ده دقیقه یک بار، یک بلوک جدید ایجاد می‌شود)
۴- استخراج‌کنندگان، افزودن بلوک‌های جدید را به زنجیره تایید می‌نمایند. در مکانیزم اثبات سختی کار، این فرآیند با رقابت بین اعضاء در حل یک پازل ریاضی انجام می‌شود که در فصل اول شرح داده شد.
۵- پس از تایید صحت بلوک و اطمینان یافتن از این که زنجیره اصلی است، انجام تراکنش مذکور نیز تایید می‌شود.

در هش‌گراف، روال ثبت تراکنش در مرحله اول (صدور تراکنش) مشابه زنجیره بلوکی است، اما در مراحل بعدی که تایید تراکنش، ذخیره‌سازی اطلاعات و مکانیزم اجماع را شامل می‌شود، تفاوت دارد و طبق روالی است که در فصل قبلی شرح داده شد.

با این حال، هدف کلی هر دو پروتکل، دستیابی به اجماع در خصوص تراکنش‌های ثبت‌شده است، و لذا از جنبه‌های مختلف همچون امنیت، سرعت، کارایی و ... قابل مقایسه با یکدیگر هستند.

۲-۳- مزایا و معایب هش‌گراف نسبت به زنجیره بلوکی

متاسفانه در حال حاضر تعداد مراجع معتبری که اقدام به مقایسه بین زنجیره بلوکی و هش‌گراف کرده باشند، محدود است. در این بخش نیز بر اساس ادعای طراحان هش‌گراف در [۶] و نیز [۷] که مروری بر فناوری‌های دفترکل توزیع‌شده انجام داده است، مقایسه‌ای بین این دو انجام خواهیم داد.

مزایای احتمالی هش‌گراف نسبت به زنجیره بلوکی شامل موارد زیر است:

- *منصفانه* است، چرا که هیچ کس نمی‌تواند به تنهایی ترتیب تراکنش‌ها را تغییر دهد، یا این که مانع از ورود یک تراکنش به شبکه گردد. در حالی که در زنجیره بلوکی، ترتیب تراکنش‌ها برای درج در بلوک جدید ممکن است تغییر داده شود، و تراکنشی که زودتر صادر شده، از ورود به زنجیره باز ماند.
- *سریع* است، و تنها توسط پهنای باند محدود می‌شود. بنابراین اگر فردی پهنای باند کافی برای دریافت ۴۰۰۰ تراکنش در ثانیه را داشته باشد (در حد چندمگابیت‌برثانیه)، قابلیت پردازش کل تراکنش‌های سیستم مالی ویزاکارت را خواهد داشت. در زنجیره بلوکی نرخ ثبت اطلاعات محدود است.
- *خاصیت بیزانس*[۱] دارد، بدین معنا که هیچ گروه کوچکی از کاربران خرابکار[۲] نمی‌تواند فرآیند دستیابی به اجماع را متوقف سازد، یا اجماعی نادرست را به شبکه غالب نماید. در بسیاری از انواع زنجیره بلوکی، چنین تضمینی از لحاظ نظری وجود ندارد.
- *ارزان* است، چرا که نیازی به فرآیندهای پرمصرف از نظر انرژی و توان محاسباتی در راستای دستیابی به اجماع ندارد. البته باید توجه داشت در زنجیره بلوکی مکانیزم‌های با مصرف انرژی پایین همچون اثبات سهام (PoS) معرفی شده است.

مهم‌ترین نقطه ضعف هش‌گراف نسبت به زنجیره بلوکی، این است که هش‌گراف هنوز در عمل آزمون خود را پس نداده است، چرا که بهره‌برداری وسیعی از آن انجام نشده است.

یک مسئله مهم دیگر، به ثبت رسیدن مالکیت فکری هش‌گراف توسط موسسان آن است، که استفاده از آن را محدود به کسب رضایت از موسسه Swirlds می‌نماید.

جدول ۱ تفاوت‌های هش‌گراف و زنجیره بلوکی را به طور خلاصه نشان می‌دهد.

---

[۱] Byzantine

[۲] Malicious

جدول ۱ – تفاوت‌های هش‌گراف و زنجیره بلوکی

معیار	زنجیره بلوکی	هش‌گراف
ساختار داده	لیست پیوندی[1](زنجیره‌ای از بلوک‌ها)	گراف بدون دور جهتدار (DAG)
اجماع	مکانیزم‌های اثبات درستی بلوک جدید، از جمله اثبات سختی کار (PoW) و اثبات سهام (PoS)	رای‌گیری مجازی
کارمزد	دارد	ندارد
سرعت	محدود (در حدود ۱۰۰ تا ۱۰۰۰۰ تراکنش در ثانیه)	بیش از ۲۰۰هزار تراکنش در ثانیه
زمان تایید تراکنش	در مرتبه دقیقه	در مرتبه ثانیه
بلوغ	پیاده‌سازی‌های گسترده	به تازگی عرضه شده است.

[1] Linked List

فصل ۴- جمع‌بندی

اینترنت فعلی، با توجه به ویژگی توزیع‌شده بودن، جایگاه بی‌بدیلی را به عنوان بستر تبادل اطلاعات در سطوح ملی و بین‌المللی کسب نموده است. با این حال، فضای اینترنت به طور ذاتی عاری از اعتماد است، و لذا بایستی رویکردهایی مبتنی بر الگوریتم – و نه مبتنی بر روابط انسانی- جهت افزودن یک لایه اعتماد[۱] به اینترنت مبنای کار قرار گیرد. در همین راستا، پروتکل‌های زنجیره بلوکی با ایجاد اجماع بین کاربران، نیاز به وجود اشخاص یا نهادهای مورد اعتماد را حذف کرده یا کاهش داده‌اند [۵]. به طور خاص، رمزارزهایی نظیر بیت‌کوین و اتریوم، اعتماد را در حوزه تبادلات مالی برقرار نموده‌اند. به بیان دیگر، رمزارزها این امکان را فراهم می‌سازند که کاربرانی که به یکدیگر اعتماد ندارند، بدون نیاز به بانک و با اعتماد به یک الگوریتم، به تبادل پول بپردازند.

با این حال، چشم‌انداز زنجیره بلوکی محدود به تبادلات مالی نیست، بلکه هدف اصلی همان ایجاد لایه اعتماد در اینترنت است، این که بتوان هر قراردادی را بر بستر ناامن اینترنت منعقد نمود. تلاش‌های زیادی در این راستا انجام شده است، و هر روز اخباری مبنی بر استفاده از انواع مختلف زنجیره بلوکی در صنایع گوناگون همچون بیمه، خطوط تولید و توزیع کالا، حمل و نقل و ... به گوش می‌رسد. کاربردهای گسترده زنجیره بلوکی در [۸] ذکر شده است.

---

[۱] Trust Layer

گفتنی است در ادبیات پژوهشی، از زنجیره بلوکی به عنوان سیستم‌های اعتماد-آزاد[۱]نیز نام برده شده است [۹]، بدین معنا که در این سیستم‌ها نیازی به برقراری اعتماد بین کاربران نمی‌باشد و خود سیستم این اعتماد را ایجاد می‌کند.

علی‌رغم تمامی مزایا، زنجیره بلوکی یک ایراد بنیادین نیز دارد: این که یک زنجیره از اطلاعات باید مورد توافق همگان قرار گیرد، و ساختن چنین زنجیره‌ای آسان و بی‌دردسر نیست. برای مثال، مصرف انرژی بالای بیت‌کوین برای اثبات درستی بلوک‌های جدید، یک چالش جدی را ایجاد نموده است. محاسباتی که در [۱۰] انجام شده، نشان می‌دهد شبکه بیت‌کوین در زمان نگارش مقاله (سال ۲۰۱۸) حداقل ۲,۵۵ گیگاوات انرژی مصرف می‌کند.

در این میان، ویژگی‌های منحصر به فرد هش‌گراف، که در فصول قبلی گزارش مطرح شد، آن را یک گزینه احتمالاً مناسب برای ایجاد لایه اعتماد در اینترنت می‌سازد. در واقع، در هش‌گراف، اجماع بدون نیاز به ساخت یک زنجیره یکسان از اطلاعات و اثبات درستی آن حاصل می‌شود. در عوض، اعضای هش‌گراف با ارسال پیغام‌هایی با یک مکانیزم مشخص – و نسبتاً پیچیده – به دیگران، به طور ضمنی به یک دیدگاه مشترک جمعی دست می‌یابند.

۱-۴- نگاهی راهبردی به آینده

با توجه به عرضه رسمی هش‌گراف و نیز نقاط قوتی که در مقایسه با زنجیره بلوکی برای آن متصور شده است، می‌توان آینده روشنی برای هش‌گراف پیش‌بینی کرد. بنابراین، سرمایه‌گذاری در امور پژوهشی و مطالعات مرتبط با این فناوری و پیاده‌سازی خدمات قرارداد هوشمند بر پایه هش‌گراف، هوشمندانه خواهد بود. در واقع می‌توان با تعریف پروژه‌های آزمایشی در ابعاد محدود، پروتکل هش‌گراف را در عمل مورد ارزیابی قرار داد و پیاده‌سازی گسترده آن را امکان‌سنجی نمود.

در صورت موفقیت در فرآیند ارزیابی اولیه، و در راستای توسعه شبکه ملی اطلاعات، پیاده‌سازی و اجرای نسخه بومی‌سازی‌شده این فناوری به عنوان لایه اعتماد شبکه پیشنهاد می‌شود. این لایه اعتماد می‌تواند شتاب‌دهنده و هدایتگر رشد صنعت فناوری اطلاعات و ارتباطات در کشور باشد.

---

[۱] Trust-free

منابع

[1] Cachin, Christian, and Marko Vukolić. "Blockchain consensus protocols in the wild." arXiv preprint arXiv:1707.01873 (2017).

[2] Dannen, Chris. Introducing Ethereum and Solidity. Berkeley: Apress, 2017.

[3] Baird, Leemon. "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance." Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep. (2016).

[4] Baird, LEEMON. "Hashgraph consensus: Detailed examples." Swirlds Tech Report. Swirlds (2016).

[5] Hughes, Laurie, et al. "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda." International Journal of Information Management 49 (2019): 114-۱۲۹.

[6] Baird, Leemon, Mance Harmon, and Paul Madsen. "Hedera: A governing council & public hashgraph network." *The trust layer of the internet, whitepaper* 1 (2018).

[7] El Ioini, Nabil, and Claus Pahl. "A review of distributed ledger technologies." OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, Cham, 2018.

[8] Aras, Supriya Thakur, and Vrushali Kulkarni. "Blockchain and Its Applications–A Detailed Survey." International Journal of Computer Applications 180.3 (2017): 29-35.

[9] Beck, Roman, et al. "Blockchain–the gateway to trust-free cryptographic transactions." (2016).

[10] De Vries, Alex. "Bitcoin's growing energy problem." Joule 2.5 (2018): 801-۸۰۵.

همچنین در نگارش این گزارش، از صفحات اینترنتی ذیل استفاده شده است:

https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read

زنجیره بلوکی چیست، چگونه کار می‌کند و چرا جهان ما را متحول خواهد ساخت؟

https://towardsdatascience.com/what-is-a-dapp-a455ac5f7def

https://filecoin.io/faqs/

https://ipfs.io/

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir