بلاک چین چیست و چگونه کار می کند؟

زهرا اسماعیلی[1] و زهرا انواری[2]

[1] دانشجوی مهندسی کامپیوتر دانشکده فنی مهندسی میانه، zesmaeili1998@gmail.com
[2] دانشجوی مهندسی کامپیوتر دانشکده فنی مهندسی میانه، gmail.com@zahraanvary1998

چکیده- بیت‌کوین، این واحد پول دیجیتالی که یک شیوه نوین در نظام پرداخت پول در سراسر جهان پدید آورده، شعارش این است: ما به رمزنگاری اعتماد داریم . بیت‌کوین آمده است تا افرادی که ما به آن‌ها اعتماد داشتیم، یعنی بانک‌داران، را از چرخه تبادلات مالی کنار بزند و رمزنگاری و کد را جایگزین سازد. در سیستم بانک‌داری سنتی، بانک بر هر تومان پولی که از حساب شما خارج می‌شود یا به آن افزوده می‌شود، اِشراف دارد. برای مثال، پولی که شما به یک فروشنده با کارتخوان پرداخت می‌کنید، پس از انجام یک سری تراکنش جابه‌جا می‌شود. بیت‌کوین (و نمونه‌های مشابه آن) با یک پایگاه داده توزیع شده و امن، بانک را از چرخه تبادلات مالی خارج می‌سازند. این پایگاه داده، زنجیره بلوکی (block chain) نام دارد. اولین و معروف ترین استفاده از فناوری بلاک چین در تراکنش های بیت کوبین اتفاق افتاد در واقع بیت کوبین اولین اپلیکیشن بلاک چین است.
نخستین ارمغان زنجیره بلوکی، حفظ حریم شخصی کاربران در حوزه تبادلات مالی است.در واقع، دیگر ترسی ناشی از سوء استفاده از اطلاعات شخصی از سوی بانک‌داران وجود ندارد. در این مقاله درباره مفهوم بلاک چین و طرز کارکرد و تاثیر آن در صنعت انرژی بررسی شده است.

کلمات کلیدي- ارز دیجیتال، انرژی، بیت‌کوین، پایگاه داده، رمزنگاری، زنجیره بلوکی

- **مقدمه**

بیت‌کوین موفق‌ترین نمونه از میان صدها ارز رمزنگاری شده است که اصطلاحا در زبان عامیانه به آن‌های ارزهای مجازی و یا حتی پول مجازی هم گفته می‌شود. اما چیزی که این روزها بیشتر از خود بیت‌کوین مورد توجه قرار گرفته و درهای جدیدی را به روی صنایع مختلف باز کرده است ، تکنولوژی بلاک چین (Block Chain) است که در زبان فارسی اصطلاحا به آن تکنولوژی زنجیره بلوک هم می‌گویند. تکنولوژی بلاک چین برای اولین بار به طور گسترده در بیت‌کوین مورد استفاده قرار گرفت .با استفاده از یک بلاک چین ، افراد زیادی می توانند گزارشات مختلفی را به یک نوع بایگانی اطلاعات وارد کنند و همچنین کاربران می توانند چگونگی ثبت و به روز رسانی اطلاعات را کنترل کنند .

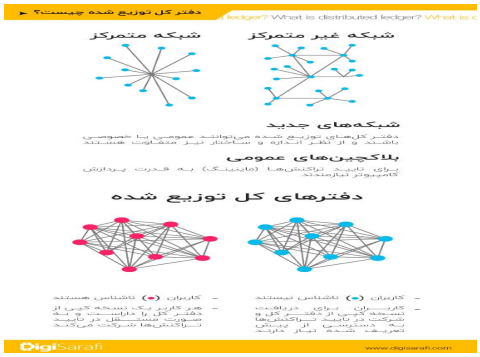
وقتی شما پول خود را به صورت سپرده در بانک سرمایه گذاری می کنید یک برگه ای به شما می دهند که شامل یک سری اطلاعات در مورد سپرده شما و حساب شما و موارد دیگر است که پس از تکمیل آنها در یک پایگاه داده بزرگ ذخیره می کنند .

بیت کوین هم کار مشابهی را برای حفظ اطلاعات حساب های کاربران انجام می دهد اما برخلاف یک بانک در بیت کوین با توجه به ماهیتی که دارد نمی توان به یک قدرت مرکزی که پایگاه داده را برای کاربران مدیریت و ذخیره کند ، اعتماد کرد .بیت کوین برای حل این مشکل ، پایگاه داده را به مجموعه های کوچکتری به نام بلاک ها تقسیم کرده است .

- **بلاک چین به زبان ساده**

بیشتر افراد برای انجام یک تراکنش مالی از یک واسطه نظیر بانک استفاده می‌کنیم. اما بلاک چین این امکان را به خریداران و فروشندگان (ارسال‌کنندگان و دریافت‌کنندگان پول مجازی) می‌دهد که به صورت مستقیم با هم در ارتباط باشند و نیاز به یک شخص ثالث به عنوان واسطه از بین برود. این شکل از تراکنش را «همتا به همتا» می‌نامند

بلاک چین از رمزنگاری به منظور ایجاد امنیت در تبادلات استفاده می‌کند. بر خلاف سیستم‌های بانکی که در یک موقعیت مشخص مستقر هستند و در اصطلاح متمرکز عمل می‌کنند، مرکزداده‌ای که بلاک چین‌ها در آن قرار دارند کاملا غیرمتمرکز بوده و در سراسر جهان پخش هستند. محل نگهداری بلاک چین‌ها را در اصطلاح «دفتر کل توزیع شده» می‌نامند. این دفتر کل به گونه‌ای است که هر کسی در شبکه می‌تواند جزییات آن را مشاهده کند. این شبکه در واقع زنجیره‌ای از رایانه‌هایی است که درستی تراکنش‌های صورت گرفته بین شما و طرف مقابل‌تان را تایید می‌کنند و پس از تایید، آن را نیز به بلاک چین اضافه می‌کنند.



شکل 1 : دفترهای کل توزیع شده

3- انواع بلاک چین

3-1- بلاک چین عمومی ضد انحصاری

در این بلاک جین هرکسی میتواند قرارداد های هوشمند ایجاد کند و یا پول یا داده ها را منتقل کند اطلاعات مهم در این بلاک چین هابه صورت رمزنگاری شده قابل ذخیره سازی هستند.

3-2- بلاک چین عمومی انحصاری

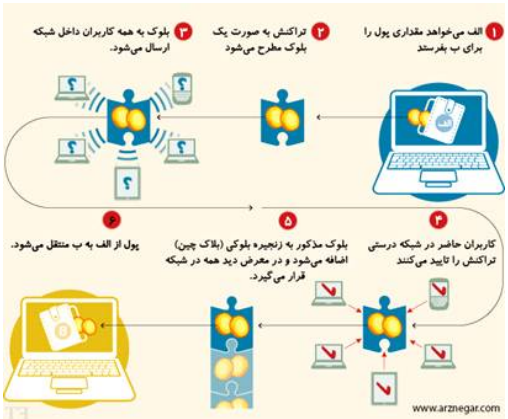
این نوع بلاک چین به صورتی است که افرادی خاص فعالیت ها را تایید می کنند. به عبارتی در بلاک چین عمومی انحصاری همه عموم می توانند داده ها را مشاهده کنند ولی تنها افراد خاصی قادر به تغییر آن ها هستند. به عنوان مثال فرض کنید شما دارای یک کشتارگاه هستنید که گوشت قرمز ارائه می دهید. شما با قرار دادن QR Code ها بر روی بسته بندی ها یم توانید اطلاعاتی از قبیل تاریخ ضبح، محل ضبح و .. را در اختیار عموم بگذارید و عموم تنها می توانند این اطلاعات را ببینند ولی شما قادرید این اطلاعات را تغییر دهید.

3-3- بلاک چین خصوصی انحصاری

از بلاک چین های خصوصی انحصاری می توان سیستم های پرداخت حقوق با بلاک چین را نام برد. در این نوع از بلاک چین ها فقط افراد خاصی می توانند فعالیت ها را تایید و نیز فقط افراد خاصی می توانند اطلاعات را مشاهده کنند.شرکتی را فرض کنید که اطلاعات خود را برای کارمندان به نمایش در می آورد ولی تنها رئیسان و سران آن شرکت قادر به تغییر آن اطلاعات می باشند.

4- عملکرد بلاک چین

برای درک بهتر کارکرد بلاک چین به زبان ساده به بیت کوین میپردازیم. بلاک چین در واقع اطلاعات و جزییات تک تک تراکنش‌های صورت گرفته با این ارز دیجیتال را در خود ذخیره می‌کند و اگر یک کاربر بخواهد از یک بیت کوین بیش از دو بار استفاده کند (یعنی کلاهبرداری کند) جلوی آن را می‌گیرد.



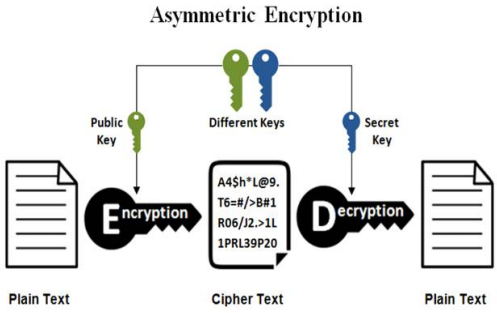
شکل 2: چگونگی کارکرد زنجیره قالب

5- بیت‌کوین چگونه کار می‌کند؟

برای شروع بحث، به‌اجزای نام زنجیره بلوکی می‌پردازیم: این‌که چرا زنجیر نام گرفته است؟ در واقع به این دلیل به آن زنجیر اطلاق می‌شود که اطلاعات تنها به انتهای فهرست اضافه می‌شود، درست مثل یک زنجیر که حلقه‌های جدید را می‌توان به یکی از دو انتهای آن اضافه کرد. هر بلوک، شامل اطلاعات تعدادی تراکنش، به تراکنش‌های قبلی در زنجیر ارجاع می‌دهد.

گروهی از کاربران موسوم به جویندگان (miners) وظیفه دارند درخواست تراکنش‌های جدید را شناسایی، آن‌ها را تجمیع، صحت‌سنجی و به‌صورت یک بلوک به انتهای فهرست اضافه کنند.

صحت‌سنجی به‌معنای آن است که بررسی شود پرداخت‌کننده واقعاً صاحب پول است و نیز این‌که پول در جای دیگر خرج نشده باشد. قبل از پرداختن به روش انجام کار، لازم است کمی به اصول رمزنگاری نامتقارن اشاره کنیم. در رمزنگاری نامتقارن، هر فرد یک کلید خصوصی (private key) و یک کلید عمومی (public key) دارد.



شکل 3 : رمزنگاری نا متقارن

این دو کلید با یک رابطه ریاضی به‌هم مربوط هستند و یکی را از روی دیگری به‌سادگی نمی‌توان به دست آورد. کلید خصوصی را تنها صاحب کلید دارد، اما کلید عمومی هر فرد در اختیار همه قرار می‌گیرد. من اگر یک متن را با کلید عمومی شما رمز کنم، تنها شما که کلید خصوصی را دارید قادر به رمزگشایی آن هستید. همچنین، اگر شما یک متن را با کلید خصوصی خودتان رمز کنید، هر فردی می‌تواند با کلید عمومی شما آن را رمزگشایی کند تا مطمئن شود این متن را شما فرستاده‌اید (زیرا فرد دیگری کلید خصوصی شما را ندارد).

این شیوه رمزنگاری برای احراز اصالت در بیت‌کوین مورد استفاده قرار می‌گیرد. در واقع، صاحب پول اطلاعات تراکنش را با کلید خصوصی خودش رمز کرده و یکسری محاسبات انجام می‌دهد تا درنهایت یک رشته عددی طولانی به دست آید. هر فرد دیگری که محاسبات مشابه را با کلید عمومی فرد مورد نظر روی عدد حاصل انجام دهد، می‌تواند بررسی کند که فرد مدعی پول واقعاً صاحب آن است یا خیر.

اما موضوع دیگری که در کنار احراز اصالت صاحب پول اهمیت دارد، این است که تراکنش‌ها برگشت‌ناپذیر و تکرارنشدنی باشند. به هر حال، بیت‌کوین مجموعه‌ای از جویندگان را در سراسر جهان دارد که قابل نظارت نیستند. پس باید یک مکانیسم طراحی شود که صحت تراکنش‌ها را بسنجد. که در بیت‌کوین، مکانیسمی بدین منظور ارائه شده است.

6- موارد استفاده‌ی تکنولوژی بلاک چین

بیشتر شهرت بلاک چین تا این لحظه، استفاده از آن به‌عنوان سامانه‌ای برای رمزنگاری معاملات پول اینترنتی یا همان بیت‌کوین (Bitcoin) است. از بیت‌کوین برای تبادلات بین‌المللی استفاده می‌شود که هزینه‌ی کمتری نسبت به فرایندهای تبدیل ارز به یکدیگر دارد. روزانه، میلیاردها دلار در قالب بیت‌کوین جابه‌جا می‌شود.

اما علاوه بر آن از فناوری بلاک چین می‌توان در زیرساخت‌های مالی موجود مانند سهام، اوراق قرضه و زمینه‌های بسیار دیگری استفاده کرد. استفاده از این فناوری و جایگزینی آن با فناوری‌های امروزی، می‌تواند روی سرعت دسترسی به اینترنت نیز تأثیر بگذارد.

همچنین از بلاک چین می‌توان در زمینه‌های صنعتی، پزشکی و زمینه‌های بسیار دیگری استفاده کرد. به‌عنوان‌مثال می‌توان آن را در بخش پزشکی -که سوابق بیماران دستکاری می‌شود- به کار گرفت. این فناوری به پزشکان اجازه می‌دهد تا پرونده‌ای از سوابق بیماران را با امنیت بالا ذخیره کرده و آن‌ها را در صورت لزوم در اختیار دیگر بیمارستان‌ها و مراکز درمانی قرار دهند. این کار علاوه برافزایش امنیت ذخیره‌سازی و انتقال داده‌ها، باعث کاهش خطرها و هزینه‌های مدیریت داده‌ها می‌شود.

از این فناوری می‌توان برای مقابله با دریافت محصولات چندرسانه‌ای به‌صورت غیرقانونی نیز استفاده کرد. از فناوری بلاک چین می‌توان برای اعتبارسنجی و جلوگیری از انجام تقلب در انتخابات الکترونیک نیز استفاده کرد

7- آینده‌ی تکنولوژی بلاک چین

فناوری بلاک چین نمی‌تواند به‌سرعت، اینترنت را تغییر دهد. وینکلسپکت می‌گوید: «موارد زیادی است که این فناوری را به چالش می‌کشد. مردم ممکن است متوجه شوند این فناوری، یک تحول ایجاد خواهد کرد؛ اما نمی‌دانند این فناوری چگونه به بهبود کسب‌وکار آن‌ها کمک می‌کند.»

8- بلاک چین و توزیع انرژی

شبکه های تولید انرژی امروزی توسط مراکز اداره می شوند، مراکزی که روی توزیع انرژی کنترل دارند و آن را مدیریت می کنند. با این حال، پیشرفت قابل توجه انرژی های تجدید پذیر مثل انرژی خورشیدی و یا حتی پیشرفت باتری ها، سبب می شود تا شبکه های توزیع محلی کوچک پدید آید.

بنابراین، اگر شما در خانه یا محل کار خودتان انرژی تولید می کنید، می توانید آن را درون باتری ها ذخیره کرده و هر زمان به آن نیاز داشتید، استفاده کنید. حتی می توانید آن را به همسایه تان بفروشید.

چنین اتفاقی می تواند منجر به حفظ انرژی و جلوگیری از هدر رفت آن شود. چون انرژی هر چه مسافت بیشتری طی کند، هدر رفت بیشتر و هزینه بیشتری خواهد داشت. با این شیوه، دیگر واسطه ای هم وجود ندارد و مردم می توانند خودشان خرید و فروش کنند.

به عبارت دیگر، نیروگاههای تولید انرژی از بین می روند و تمام کاربران از طریق انرژی خورشیدی اقدام به تولید برق می کنند و هر کس برق مازاد خود را به داخل شبکه می فرستد. با تایید تعدادی کاربران این برق مازاد به مشترکی که نیازمند آن است منتقل می شود. در ضمن هزینه بصورت بیت کوین به فرستنده پرداخت می شود.

9- نتیجه گیری

بلاک چین یک فناوری نوظهور است که نیاز دارد تا برنامه‌هایی سازگار با آن تولید شود. همچنین برای استفاده از این فناوری باید مجموعه‌ای مقررات تنظیم شود. این فناوری باید بتواند کارآمدی خود را اثبات کند تا بتواند به‌صورت گسترده به کار گرفته شود.

10- مراجع

]1[http://www.paydarsamane.com/blog/?p=509

[2] https://arznegar.com/blockchain-simplified

[3] http://news.citexcoin.com

[4] https://payment24.ir/blog/everything-about-bitcoin

[5] https://techrato.com/2017/11/12/blockchain-bitcoin-story

[6] https://www.civilica.com/Paper-ICEEC01-ICEEC01_269.html