پروژه ی نرم افزار دوره کارشناسی

گزارش شماره ۱ - مقدمه

آریا رادمهر - ۹۷۴۶۳۱۲۵

دکتر سجاد حق زاد کلیدبری

October 17, 2021

فهرست

پیشگفتار

مسیر تبدیل تکنولوژی های دیجیتال بر بستر بلاکچین ها به چیزی که امروزه نظاره گر بر آن هستیم، همواره مسیری مملو از تلاش های نافرجام زیادی بوده است. از ابتدای سال ۱۹۹۱ که بلاک چین تحت عنوان زنجیره ای از داده ها توسط محققین ابداع و معرفی شد، لیستی نامحدود از ایده ها، نیاز ها، و یا مشکلات و چالش ها به سمت این تکنولوژی سرازیر شد تا شاید بلاکچین نقش عنصری حیاتی و نجات بخش را برای آنها بازی کند. از ایده هایی بر محور مقالات آکادمیکی که به تعداد زیادی به عنوان مرجع مورد استفاده قرار گرفته بودند تا سیستم های عملیاتی واقعی که جدا از روی کاغذ، توسعه پیدا کرده و تست شده بودند.

برای درک بلاکچین ها لازم است تا نگاهی تاریخی حتی به قبل از پیدایش بلاکچین ها داشته باشیم که همواره این سوالات را در یک ذهن کاوشگر ایجاد میکند : بلاکچین چگونه کار میکند؟، تکنولوژی های موفق بر بستر بلاکچین کدام ها هستند و چگونه در این مسیر متلاطم راه خود را پیدا کردند؟، چگونه تکنولوژی های بلاکچینی با پیشرفت و تکامل تبدیل به ایده های تجاری شدند؟

درکی درباره ی بلاکچین

نگاه تاریخی:

از ابتدایی که آدمیزاد شروع به مکتوب کردن وقایع، رویداد ها، اعتبارات و یا حتی دارایی های خود کرد، همواره نیاز به وجود یک تشکل جامع بود تا بتواند صحت مکتوبات آدمی را تایید کند. به شرطی که آن تشکل جامع، مقبولیت عام را به همراه خود داشته باشد. با دو مثال این تشکل ها را در مسائل متفاوت بررسی میکنیم.

مثال ۱:

در زمان قدیم اگر تعدادی خانواده ساکن درکنار یک رود، زمین های کشاورزی داشتند که میبایست در انتهای فصول از آنها برداشت میکردند، خود میدانستند که سهم هر یک چه میزان از زمین های زیر کشت میباشد تا هنگام درو با یکدیگر به مشکل نخورند. مدتی بعد که تعداد افراد این جوامع رشد کرد، دیگر نیاز بود تا برای جلوگیری از وقوع اختلاف و هرج و مرج در روستا یا ده، فردی شناخته شده و تحت مقبولیت همه یا اکثریت افراد وجود داشته باشد تا با حکمیت وی در مسائل، دیگر جای شکی باقی نماند. برای مثال فردی بمانند ریش سفید یا کدخدا در ده وجود داشت که اگر دو کشاورز برسر اراضی زیر کشت خود به مشکل برخوردند، آن فرد راه حلی را مطرح کند که گره گشای مشکل باشد. در واقع در آن زمان ریش سفید یا کدخدا سندی بر اثبات درستی یک مسئله بود. برای مثال اگر کد خدا میگفت که نیمی از زمین برای کشاورز الف و نیمی دیگر برای کشاورز ب میباشد، دیگر کسی نمیتوانست زیر حرف او بزند و گفته هایش را نقض کند زیرا کدخدا همان تشکل جامعی بود که مقبولیت عام را به همراه داشت.

با بزرگتر شدن جوامع دیگر یک کد خدا نه تنها کافی نبود بلکه اراضی تحت مالکیت انسان ها به گونه ای زیاد و بزرگ شد که وجود چند کد خدا نیز چاره ی کار نبود. این شد که حکومت های اولیه در پی مدیریت اراضی، طومار هایی را شکل دادند که با مقید کردن یک محدوده زمین به یک شخص، سعی در بوجود آوردن همان تشکلی کنند که قبل از آن با عنوان کد خدا وجود داشت. دیگر اگر شخصی مدعی میشد که بخشی از اراضی الف را داراست و برای حرف خود طومار با مهر رسمی آن حکومت را ارائه میداد، کسی برای مخالفت با حرف او بر نمیخواست زیرا

آن طومار سندی بر حرف او بود و آن حکومت که حق قانونی استفاده از زمین را به شخص میداد مورد مقبولیت اکثریت افراد بود.

به مجردی که جوامع گسترش پیدا کردند و عصر تکنولوژی آمیخته با زندگی بشر شد، طومار های یاد شده جای خود را به اسناد و مدارکی دادند که به موجب اعتبار خود، از دارایی های افراد در برابر دیگران حفاظت و حراست میکرد.

مثال ۲:

زمان قدیم را تصور کنید؛ هنگامی که افراد برای بدست آوردن کالا های مورد نیاز خود از اجناسی را با یکدیگر تبادل میکردند. برای مثال فرض کنید فرد الف دارای چندین راس گوسفند بود اما نیاز به یک زمین برای نکهداری آنها داشت. فرد الف برای بدست آوردن یک زمین به سراغ فردی (برای مثال فرد ب) میرفت که دارای قطعه ی بزرگی زمین بود اما از قضا نیاز به چندین راس گوسفند برای مزرعه خود داشت. فرد الف و ب سپس با انجام توافقی با یکدیگر سعی بر برآورده کردن نیاز های خود میکردند. برای مثال فرد الف با دادن تعدادی راس گوسفند به فرد ب، قطعه ای زمین را صاحب میشد. حال فرض کنید که فرد ب بجای گوسفند نیاز به چندین راس اسب داشت. سپس فرد الف میبایست به سراغ فردی (برای مثال فرد ث) میرفت که در ازای گرفتن تعدادی راس گوسفند تعدادی راس اسب را به او میداد. حال فرد الف با داشتن تعداد اسب های کافی میتوانست به سراغ معامله ی زمین برود تا با دادن اسب ها به فرد ب، همان قطعه زمین را صاحب شود. این پیچیدگی تبادل در زندگی بشری باعث اختراع ۱- پول و ۲- اعتبار شد. از این پس فرد الف قادر بود تا در ازای مبلقی از پول یا در ازای داشتن اعتباری ثابت شده در برابر فرد ب، قطعه ای از زمین او را صاحب شود. سپس با بزرگتر شدن جوامع بشری موسسه هایی تشکیل شدند که اعتبارات یا پول های افراد را ثبت میکردند تا هم امنیت آنها را تضمین کنند و هم در ازای اعتبارو دارایی های غیر پولی افراد (که ممکن بود شامل زمین، ملک و مابقی دارایی ها باشد) به آنها مقدار پولی را اختصاص دهند. این موسسات که همان نقش تشکل جامع دارای مقبولیت عام را داشتد، بعد ها به بانک ها تبدیل شدند.

حال در مثال شماره ۱ ، تصور که فردی با داشتن روابطی بهتر با کد خدای روستا ، زمین و دارایی فرد دیگری را صاحب میشد و یا تصور کنید کسی سندی را نزد اهالی روستا میاورد که نشان میداد تمام زمین های آن روستا را او صاحب شده است. در این صورت مشکل از چه بود؟ آیا مشکل از کد خدا و یا آن حکومت بود؟ آیا آنها به اشتباه اعتباری را به آن فرد داده بودند؟ آیا در پس این جریانات فسادی در کار بود؟

یا مثال دوم را بررسی کنید؛ فردی به یکباره صاحب ثروتی گزاف میشد، یا یک فرد که برای بازپس گیری مقداری از دارایی های خود نزد بانک میرفت و بانک به او اعلام میکرد که او هیچ مقدار پول و یا اعتباری نزد بانک ندارد. مشکل از کجا پیش می آمد؟ آیا خطایی توسط بانک پیش آمده بود؟ آیا فردی بواسطه ی دوستی خود با رئیس بانک اموال فرد دیگری را تصاحب کرده بود؟

اگر با دقت به این دو مثال بنگریم، متوجه خواهیم شد که آن تشکل های جامعی که از آن یاد کردیم (برای مثال ۱ سیستم مدیریت اراضی و برای مثال ۲ سیستم بانکی) ، دارای یک نقطه ی ضعف بسیار مهم میباشد و آن نقطه ضعف در متمرکز بودن آن تشکل ها بود. تشکل های مثال ۱ و ۲ تشکل های جامعی بودند و همچنین مقبولیت عام را داشتند اما توسط یک نفر و یا تعداد معدودی از انسان ها مدیریت میشدند که شخص ثالث بودند.

این چالش نیز بعد ها باعث بوجود آمدن سیستم بلاکچین شد. این فناوری از ابتدای پیدایش خود سعی بر آن داشت تا سیستم های متمرکز را تبدیل به سیستم ها و تشکل های غیر متمرکز و توزیع شده کند. همین ویژگی خاص غیر متمرکز سازی و توزیع شدگی سیستم ها است که بلاک چین را بسیار محبوب کرد، زیرا غیر متمرکز و توزیع شدگی سیستم ها با دیدگاه بلاکچین خود ویژگی های مهم دیگری را بوجود می آورند که به تفضیل به آنها میپردازیم.

تعریف استاندارد و منطقی:

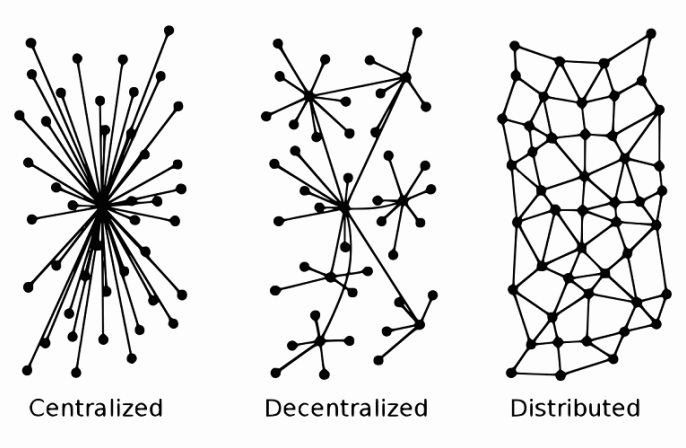
به طور خلاصه بلاکچین سازوکاری برای مرتب سازی و تأیید تراکنش ها در ساختمان دادهای به نام دفتر کل میباشد. بنا بر تعریف میتوان بلاکچین را نوعی ساختمان داده با ویژگی های منحصر به فرد مانند توزیع شده بودن، امنیت و ... در نظر گرفت. به طورکلی یافتن تعریف رسمی و واحد از بلاکچین کاری دشوار و شاید، به سبب تازگی و نو پا بودن، ناممکن باشد ولی با مراجعه به منابع مختلف ازجمله تعاریف ارائه شده توسط بزرگان و تأثیرگذاران این عرصه میتوان به تعریف کامل و قابل قبولی رسید. در همین راستا کمیته ای فنی در سال 2016 در سازمان ایزو تشکیل شد که تعاریفی در این زمینه ارائه دهد. این کمیته بلاکچین را اینگونه توصیف میکند: "یک دفتر کل توزیع شده و غیرقابل ویرایش که توانایی ثبت تراکنش های تولیدشده توسط طرفین معامله و تعامل کنندگان کسب و کار را دارد." در قسمتی دیگر از تعریف آمده که: "بلاکچین یک بستر دیجیتال است که توانایی ذخیره و تأیید صحت تراکنش ها را به شیوهای امن و شفاف دارد؛ به طوریکه نیازی به موجودیت های میانی حقیقی مانند ناظرین و واسطه ها نباشد." شرکت فناوری IBM به عنوان موجودیتی تأثیرگذار در این زمینه تعریفی مشابه را از بلاکچین ارائه میدهد: "بلاکچین یک دفتر کل مشترک و غیرقابل ویرایش برای ذخیره سازی تاریخچه تراکنش ها است."

بلاکچین یک معماری توزیع شده کامپیوتری و نرم افزاری است که یک کامپیوتر در صورت شرکت در شبکه آن، یک گره نامیده میشود. هر گره اطلاعات کامل و دقیقی از تمامی تراکنش های انجام شده دارد و تمامی اطلاعات در خصوص تراکنشها مابین گره ها مشترک است. تراکنش ها به طور پیوسته در قالب گروه هایی با نام بلوک دسته بندی شده و در پایگاه داده توزیع شده ذخیره میشوند. تنها یک بلوک در واحد زمان اجازه اضافه شدن به پایگاه داده را دارد و حاوی الگویی ریاضیاتی و محاسبه شده میباشد که صحت بلوک قبلی را تأیید میکند. به این ترتیب بلوک ها به طور سلسله وار به یکدیگر متصل میشوند و موجودیتی واحد را تشکیل میدهند. تعریف بالا را میتوان به عنوان توصیفی کلی و جامع از بلاکچین در نظر گرفت به طوریکه اکثریت پیاده سازی ها و توزیع های بلاکچین را دربر می گیرد.

ویژگی ها و نقاط مثبت

تعاملی بودن سیستم ها بر بستر بلاکچین

یک تفاوت عمده سیستم های مبتنی بر بلاکچین توانایی ساخت محیطی کاملا توزیع شده، در مقایسه با سیستم هایی که تکنیک های توزیع سازی را در اموری با ماهیت مرکزی اعمال میکنند میباشد.



در توضیح سیستم تعاملی هیچ سرور مرکزی که میزبان نسخه اصلی اطلاعات باشد وجود ندارد. بلکه اجزای این نوع سیستم میتوانند با بهره گرفتن از بستر تعاملی با یکدیگر همکاری کنند. با حذف موجودیت یا موجودیت های مرکزی ویژگی منحصربه فردی از بلاکچین متولد میشود و آن مهم این است که اجزای این سیستم میتوانند بدون هماهنگی و کسب اجازه از موجودیتی بالادستی اقدام به برقراری قرارداد هوشمند و کسب وکار جدیدی کنند و این توانایی یکی از تعاریف تعاملی بودن سیستمهای بلاکچین است. قراردادهای هوشمند یکی از بازوان اصلی تعامل اجزای سیستمهای مبتنی بر بلاکچین میباشند که در ادامه تعاریف و ویژگیهای آن آورده شده است: قابلیت تعاملی بودن بلاکچین ویژگیهای دیگری ازجمله قابلیت تحمل و مدیریت بحران بالا را ایجاب میکند به طوری که با قطع ارتباط یک گره سیستم دچار بحران نمیشود و تنها بخش کوچک و قابل اغماضی از سیستم از مدار خارج میشود. در ضمن اجزای یک سیستم تعاملی میتوانند در مقابله با سو رفتار و تهاجم خارجی با یکدیگر همکاری کرده و مشکل را برطرف سازند و این خود موجب افزایش امنیت این سیستم ها خواهد شد.

شفافیت

ماهیت توزیع شده بودن سیستمهای مبتنی بر بلاکچین امکان دیگری با عنوان شفافیت را به سیستم اضافه میکند که از حیث اهمیت در کسب کارها و صنایع جایگاه انکارناپذیری دارد. توزیع شده بودن و تعاملی بودن موجب ایجاد سابقه برای اعضا میشود و این خود به مرور موجب ایجاد اعتبار بین هر دو عضو دلخواه سیستم میشود. این ویژگی ازآنجا ناشی شد که هر تغییری در سیستم برای تمامی اعضا (چه اعضای دخیل در آن تغییر و چه باقی اعضا) قابل مشاهده است و نیز ویرایش اطلاعات در بلاکچین ناممکن است. در اهمیت موضوع شفافیت این نکته قابل ذکر است که در قشر خاصی از کسب وکارها هرچه میزان شفافیت بالاتر باشد تقاضا برای همکاری و یا سرمایه گزاری افزایش می یابد و این موجب افزایش بهره وری و کارایی کلی سیستم میشود.

امنیت

در بالا به لزوم وجود شفافیت در برخی زمینه ها اشاره شد ولی این نکته ناگفته ماند که مسئله امنیت و محرمانگی بخش جدانشدنی از کسب وکارها میباشد و لازم است تمهیدی جهت ایجاد توازن و مصالحه بین این دو مهم انجام شود. تکنولوژیهای مبتنی بر بلاکچین در این راستا و جهت کنترل شفافیت تعریف جدیدی به بلاکچین اضافه کرده اند : بلاکچین های خصوصی و بلاکچین های عمومی

در تعریف بلاکچین های عمومی ذکرشده که هر موجودیت که متمایل باشد میتواند اطلاعات درون شبکه بلاکچین را مشاهده کرده و آنها را به اختیار خود تغییر دهد. درحالیکه بنا بر تعریفی که برای بلاکچین های خصوصی ارائه شده در این نوع از سیستمها برای مشاهده، تغییر و مشارکت در فرایند سیستم باید اجازه ای از سمت مالکان و تصمیم گیرندگان سیستم به موجودیت ها داده شود. به این ترتیب اقدامی جهت کنترل مسئله شفافیت و مخفی نگه داشتن اطلاعات کسب و کار از دسترسی موجودیت های رقیب و خارجی انجام شده است.

چالش های پیش رو

در فرایند سازگاری کسب وکارها با تکنولوژی های جدید، اصول پایه آن تکنولوژی نقش مؤثری دارد. کسب وکارها در اکثر مسائل تمایل به استفاده از راه حل ها و سازوکارهای پیشین و پیاده سازی شده دارند. از آنجایی که تکنولوژی بلاکچین و نیز پیاده سازی دیگر سیستم ها بر بستر بلاکچین دارای مفاهیم جدید و نو بنیان هستند نحوه سازگاری کسب و کارها با آنها به طور عمده به چالش های پیش رو در این تکنولوژی ها بستگی دارد.

دشواری پیش رو در ساخت سیستم های بر بستر تکنولوژی بلاکچین در شرایطی ایجاد میشود که هم سؤال مطرح شده و هم پاسخ پیشنهادی نوظهور و نسبتا نابالغ هستند. تکنولوژی بلاکچین تنها یک دهه قدمت دارد. نو پا بودن این تکنولوژی منجر به تغییر و تحولات نسبتا سریع در این زمینه شده است و این خود لزوم انعطاف پذیری و قدرت تطبیق را برای کسب و کارهایی که بلاکچین را اساس تعاملات خود قرار میدهند ایجاد کرده است. با پیشرفت مفاهیم پایه و بهبود استاندارد های موجود در این زمینه کسب و کارها تمایل بیشتر به انتقال به بستر بلاکچین و بهره مندی از مزایای آن خواهند داشت و دسترسی به این ثبات و استانداردها نیازمند گذر زمان است.

در چنین شرایطی تنها مزیت های عمده و تضمین شده هستند که کسب و کارها را به استفاده از مدلسازی پیشنهادی متمایل خواهند کرد. ازاین رو کلید حل این معادله در ایده پردازی ها و پس از آن در پژوهش ها و نتایج امید بخش در حوزه های آکادمیک خواهد بود.

دیگر مسئله غیرقابل انکار در توسعه تکنولوژیهای جدید این است که احساس نیاز، منجر به راه حل میشود. در حال حاضر در جهان صدها کسب وکار کوچک مرتبط با بلاکچین وجود دارد که در تلاش برای جذب استعداد های موجود در این زمینه با یکدیگر به رقابت میپردازند و این در حالی است که نرخ رشد افراد علاقه مند به این حوزه از نرخ افزایش نیاز به نیروی کار و پژوهش به میزان قابل توجهی کمتر است.

چالش بعدی تکنولوژی های مبتنی بر بلاکچین وابستگی به اکوسیستم توزیع شده است. این اکوسیستم شامل مواردی چون فضای ذخیره سازی ابری غیرمتمرکز، بستر ارتباطات غیرمتمرکز، سامانه های نام دامنه غیرمتمرکز و... میباشند. بیشتر تکنولوژیهای ذکر شده هنوز به میزان کافی توسعه نیافته اند. این امر منجر به افزایش خطر سرمایه گذاری در این عرصه شده است.

اهداف پایان نامه

در این پایان نامه سعی بر ساخت یک سیستم بلاکچین میشود که بر بستر آن میتوان سیستم هایی مثل مدیریت ارز های دیجیتال، سیستم توکن سازی اشیا فیزیکی، سیستم ذخیره ی سوابق پزشکی، ایجاد دفاتر ثبت اسناد رسمی، جمع آوری مالیات و ... را ایجاد کرد و توسعه داد.