Vol. 3, No. 6, Apr-Jun 2023, (1-23)

Journal of New Achievements in Electrical, Computer and Technology (JNAECT)

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری

دوره ۳، شماره ۶، بهار ۱۴۰۲(۲۳-۱)

journal homepage: https://jnaect.ir

مروری بر دفاتر کل متمرکز و غیرمتمرکز(توزیع شده)

بهروز مرامی استیار[۱] ، دکتر محمد علی جبرئیلی جمالی [۲]

[۱] موسسه آموزش عالی غیرانتفاعی ـغیردولتی سراج تبریز ، behroz.ma.1367@gmail.com

[۲] دانشگاه آزاد اسلامی واحد شبستر ، m_jamali@itrc.ac.ir

چکیده

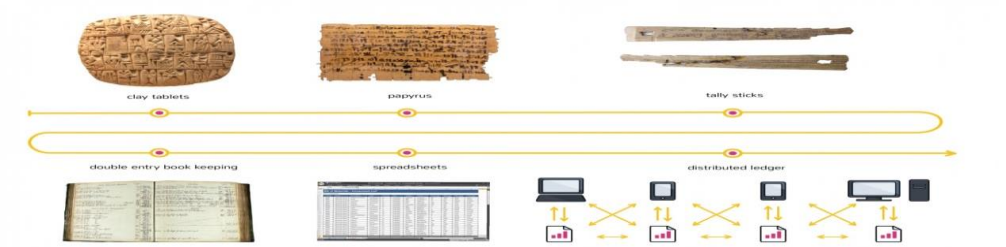
دفاتر کل به دفاتری اطلاق می گردد ، که در شرکت های و سازمان ها برای ذخیره تراکنش های مالی مشتریان ، مشخصات فردی در قالب رکورد مورد استفاده قرار می گیرند . دفاتر کل از نظر تکنولوژی کاربردی به دو دسته متمرکز و غیرمتمرکز تقسیم می گردند . البته در حالت کلی به دفاتر کل غیرمتمرکز ، دفاتر کل توزیع شده هم اطلاق می گردد ولی درواقعیت با هم تفاوت دارد که در ادامه به تشریح هر کدام به طور مفصل پرداخته شده است . دفاتر کل توزیع شده در خیلی از زمینه ها کاربرد منحصربفردی دارد ؛ در فناوری اینترنت اشیا جهت افزایش و بهبود امنیت مورد استفاده قرار می گیرد . در این مقاله مطالعه مروری به سیستم های متمرکز و غیر متمرکز و توزیع شده ، انواع دفاتر کل مبتنی بر سیستم های توزیع شده (بلاک چین ، تنگل ، هش گراف ، تمپو) پرداخته شده است .

واژه‌های کلیدی: دفاتر کل توزیع شده ، سیستم های متمرکز و غیرمتمرکز، بلاک چین ، تنگل ، هش گراف ، تمپو

۱. مقدمه

اغلب یک متن حسابداری به عنوان یک دفتر کل درنظرگرفته می شود ؛ که البته ممکن است به غیر از اطلاعات ریز درقبال حساب های مالی ، شامل مشخصات فردی ، تولیدی باشد . شرکت ها جهت ذخیره اطلاعات ریز در قبال انواع تراکنش ، از یک دستورالعمل خاص و کلی استفاده می کنند ؛ در واقع این دستورالعمل ها ، اشاره به نحوه ذخیره سازی ،الزامات سطوح دسترسی و میزان اهمیت هر رکورد دارد. [1]

دفاتر کل از گذشته تا به امروز شاهد تغییرات بسیاری در نحوه ساخت و استفاده بوده اند ؛ که میتوان به لوح سفالین ، کاغذ (پاپیروس) ، چوب خط ، حسابداری دو طرفه (کاغذ) ، سیستم های دیجیتال (صفحات گسترده ذخیره شده به صورت متمرکز) و امروزه هم سیستم های توزیع شده اشاره کرد[۲] .

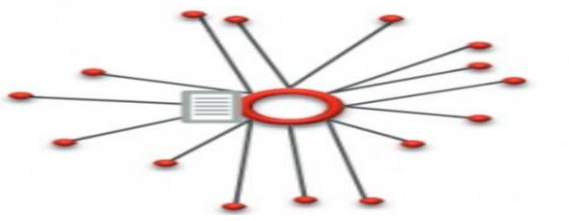


شکل ۱ تارخچه دفاتر کل

1-1 - انواع دفتر کل

متمرکز:

در این نوع از دفاترکل ، یک نهاد مرکزی وظیفه کنترل داده های کل یک سیستم را بر عهده دارد . به عبارتی وظیفه تایید صحت داده ها و برقراری سطوح و مکانیزم های دسترسی در رابطه با تامین امنیت داده ها بر عهده این نهاد مرکزی می باشد . زمانی که صحبت از نهاد مرکزی به میان می آید ، نا خداگاه مسائلی همچون همگام سازی و نگهداری در رابطه با چگونگی و زمان اتصال وفرایند های ناسازگاری به وضوح قابل مشاهده می گردد ، که توجه به آن ها امری ضروری و غیرقابل اجتناب است . اعتماد به نهاد مرکزی در قبال تایید صحت داده ها امری ضروری و غیرقابل اجتناب است ، چرا که اطلاعات مهم و حیاتی یک سازمان (مالی و غیر مالی) در آن نهاد مرکزی به طور متمرکز ذخیره می گردد و باید آن قابل اطمینان باشد . اعتماد به یک نهاد مرکزی جهت کنترل و مدیریت داده ها در دفاتر کل متمرکز نیاز به پرداخت هزینه و حق کمسیون خواهد بود . به عبارتی در رابطه با تامین امنیت ذخیره سازی و داده ای توسط نهاد مرکزی باید متحمل پرداخت هزینه شد [۳] .



شکل۲ دفاتر کل متمرکز

• مدیریت کل سیستم متمرکز برعهده نهاد مرکزی می باشد ، بنابراین مدیریت و نگهداری و کنترل آن آسان خواهد بود.

• با بهره بردن از نهاد مرکزی از هزینه کرد اضافی بابت سخت افزارها و نرم افزارهای متعدد جلوگیری بعمل می آید ، به عبارتی گره های عضو دیگر در سیستم یا دفترکل متمرکز به عنوان ترمینال در نظر گرفته می شوند و تنها فقط نهاد مرکزی باید الزاما سخت افزار و نرم افزارهای متعدد و قوی باید دراختیار داشته باشند.

• اگر در سیستم متمرکز یک ترمینال به هر دلیلی از کار بیافتد ، در اینصورت کاربر ضمن ارتباط از طریق یک ترمینال دیگر با نهاد / سرور مرکزی ، می تواند به داده های ذخیره شده خود در آن نهاد مرکزی دست پیدا کند .

• امنیت فیزیکی داده ها ، با بکارگیری نهاد مرکزی در سیستم های متمرکز تضمین می گردد .

• با بکارگیری نهاد مرکزی در سیستم های متمرکز ، از تکرار بی رویه داده ها جلوگیری بعمل آمده و درنتیجه به ظرفیت ذخیره سازی کمتری نیاز خواهد بود .

• یکپارچگی داده ها با بکارگیری و مدیریت و کنترل نهاد مرکزی تضمین می گردد ، به عبارتی یکپارچگی داده ها اشاره به تایید درستی و پایداری داده ها در طول حیاتشان دارد [۴] .

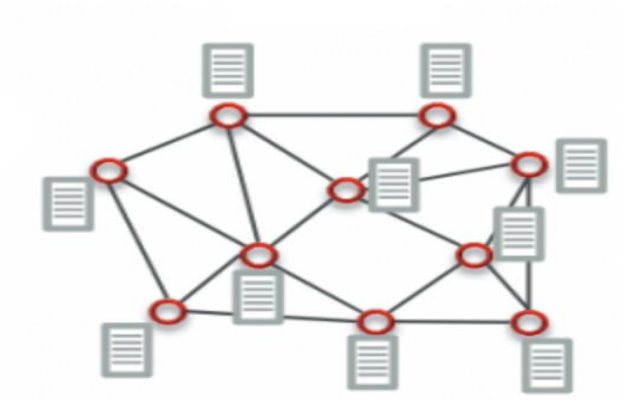
غیرمتمرکز:

در این نوع از سیستم ها ، به جای یک نهاد مرکزی وظیفه کنترل داده های کل یک سیستم را چندین نهاد یا سرور را بر عهده دارد. [4]

به عبارتی وظیفه تایید صحت داده ها و برقراری سطوح و مکانیزم های دسترسی در رابطه با تامین امنیت داده ها بر عهده این نهاد های مرکزی خواهند بود . البته در یک سیستم غیرمتمرکز ، گره های عضو با برقراری ارتباطات P2P اقدام به تبادل داده و اطلاعات با هم می کنند . هر گره عضو در سیستم های غیرمتمرکز ، مسئولیت تایید ، اعتبار سنجی و تصمیم گیری در قبال داده ها و اهداف از پیش تعریف شده را خودش بر عهده می گیرد . گره های عضو با بهره جسن از این روش (P2P) ارتباط با یکدیگر را امکان پذیر می کنند. [4]

در یک شبکه همتا به همتا ، همتایان که همان سیستم های کامپیوتری هستند ، می توانند از طریق اینترنت و بدون استفاده و کمک گرفتن از هرگونه نهاد ثانویه (سرور مرکزی) جهت مدیریت ، کنترل و هرگونه اعتبار سنجی لازم ، اقدام به برقرای ارتباط و اشتراک گذاری داده های خود با یکدیگر نمایند. [4]

سیستم های غیرمتمرکز به دو دسته ، غیرمتمرکز محض و غیرمتمرکز سازمانی تقسیم می گردند . در سیستم های غیرمتمرکز محض تمام گره های عضو ، مسئول تصمیم گیری ها در قبال وظایف خود هستند . این گره ها هیچ گونه قدرت مدیریت ارتباطی و عملیاتی درقبال دیگر گره های عضو شبکه مورد نظر را ندارند . در سیستم های غیرمتمرکز سازمانی ، ابتدا یک شبکه خودش به چندین زیر شبکه تقسیم می گرددو سپس هریک از زیر شبکه ها یک گره مافوق را به خود اتخاذ می کند . وظیفه گره مافوق (Supernode) ،کنترل و مدیریت گره های زیر شبکه خود است . در ضمن اطلاعات و داده های زیر شبکه با برقراری ارتباط گره های مافوق با همدیگر ، به اشتراک گذاشته می شوند .



شکل۳ دفاتر کل غیرمتمرکز

• کنترل و عملکرد عملیاتی سیستم توسط سرور مرکزی کاهش می یابد ، در عوض به هر گره عضو در سیستم غیرمتمرکز اجازه شرکت در هرگونه عملیات تصمیم گیری را داده می شود.

• سیستم های غیرمتمرکز ، عملیات تصمیم گیری را به نزدیکی مکان های رخداد تراکنش ها هدایت می کنند ، که نتیجه آن ضمن گرفتن تصمیمات سریع ، کسب منفعت را نیز شامل خواهد شد.

• سیستم های غیرمتمرکز قابل مقیاس پذیر است ، به طوریکه گسترش شرکت ها و سازمان ها را ضمن تسهیل کردن ، ایجاد یک کسب و کار در هر نقطه جغرافیایی را امکان پذیر می نماید.

• در مقایسه با ساختار سیستم متمرکز ، شکست یا اختلال یک گره در سیستم های غیرمتمرکز باعث از کار افتادگی کل سیستم نخواهد شد[۴] .

توزیع شده:

یک سیستم توزیع شده ، مجموعه ای از گره های مستقل است که هرکدام دارای ظرفیت ذخیره سازی و قدرت پردازشی مجزا ،می باشند.

در این سیستم همتایان ، که همان سیستم های کامپیوتری هستند با پاس دادن اطلاعات به هم دیگر با یکدیگر ارتباط برقرار می کنند [۴] . دفترکل توزیع شده ، یک تکنولوژی چند منظوره می باشد ، که جهت به اشتراک گذاشتن داده ها مابین گره های مختلف در هر نقطه از دنیا به وجود آمده است . به عبارت دیگر یک ساختار داده عمومی را با تجمیع کردن یک سری از گره های غیرقابل اعتماد در محیط و بر مبنای توزیع پذیری فراهم کرده است .

دردفاتر کل توزیع شده ، دیگر به یک سرور مرکزی جهت مدیریت و برقراری مکانیزم های اعتماد سازی نیاز نمی باشد ، چراکه روش های های برقراری اعتماد سازی از طریق پیگیری مالکیت گره های عضو در شبکه حاصل خواهد شد .

شکل۴ دفاتر کل توزیع شده

• سیستم های توزیع شده با دارا بودن قدرت ذخیره سازی و پردازشی بسیار بالا ، قادر به انجام وظایف بسیار پیچیده ، عظیم و صد البته سریعتر هستند ، نسبت به سیستم هایی که وظایف خود را بعد از تقسیم بندی به چندین زیر وظایف ، جهت اجرا و پردازش در گره های موجود درزیرشبکه پخش و سپس نتایج حاصله از هرکدام را در گره اصلی تجمیع می کنند.

• بار محاسباتی عملکرد کل سیستم بین گره های عضو دیگر در شبکه تقسیم می گردد ، که در نتیجه آن شاهد حداقل بار ممکن در هر گره و افزایش کارایی و عملکرد کل سیستم خواهیم بود.

• شبکه قابل اعتماد خواهیم داشت ، به طوریکه با کناررفتن یک گره عضو درشبکه ، عملکرد کلی شبکه تحت تاثیرقرار نخواهدگرفت.

• در سیستم های توزیع شده عملیات کل سیستم مابین گره های مختلف پخش می گردد ، بنابراین می توان گفت که سیستم مذکور یک سیستم مقیاس پذیر است ، به طوریکه منابع پردازشی را می توان متناسب با عملیات و کارهای منحصربفرد تنظیم کرد.

• دفتر کل توزیع شده یک پتانسیل قوی در نحوه تغییر عملکرد فعالیت ها و حفظ منافع دولتی به همراه دارد ، به طوریکه می توان از آن در فعالیت های جمع آوری مالیات ، امنیت اجتماعی ، صدورگذرنامه ، اعطای مجوزها ورای گیری استفاده سودمندانه کرد.

• همچنین از آن می توان در کاربردهای دیگری اعم از موسیقی ، مالی ، امنیت سایبری ، خدمات عمومی و مراقبت های بهداشتی استفاده کرد. [4]

•در سیستم های توزیع شده به خاطر اینکه انجام عملیات و استفاده از داده مبتنی بر رویکرد اشتراک محور مابین گره های عضو می باشد ، توجه شدید به مباحث امنیتی و محرمانگی نیاز مبرم خواهد داشت.

• اگر یکی از گره های عضو ، گره مخرب در سیستم توزیع شده باشد ، در اینصورت مسائل و مباحث جدی را بدنبال خواهد داشت.

• در سیستم های توزیع شده ، گره های عضو با استفاده از بسته های پیام یا داده ای ارتباط برقرار می کنند ، که می توانند در بستر سیستم مذکور حذف یا گم شوند ، که در اینصورت مشکل جدی در برقراری ارتباط و تصمیم گیری به وجود خواهد آمد.

• در سیستم های توزیع شده برای انتقال داده ها با اندازه بزرگ به پهنای باند بالا نیاز است ، برای ایجاد تغییر در ارتباطات شبکه ای ، نیاز به صرف هزینه بسیار لازم خواهد بود .

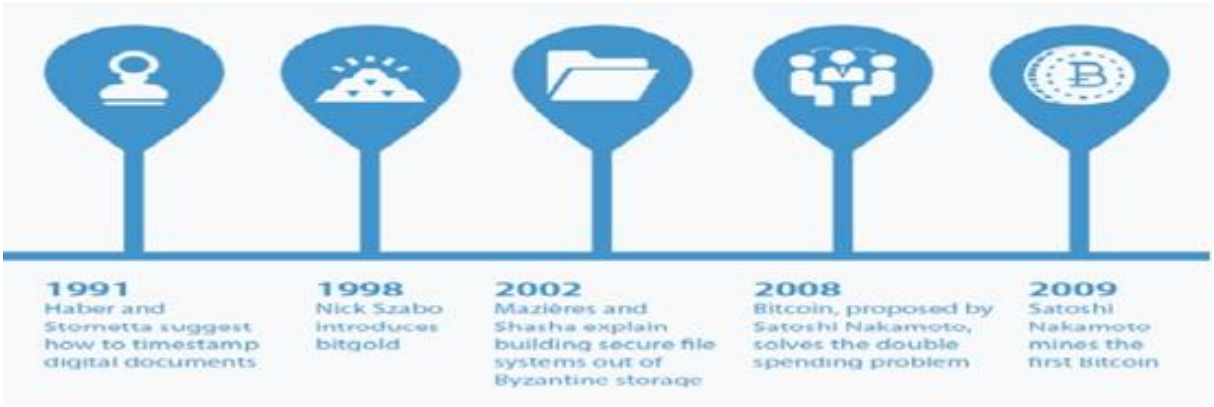
تاریخچه دفاتر کل توزیع شده

انجام تحقیق بر روی چگونگی انجام Time-Stamp بر روی اسناد دیجتالی و چاپ آن توسط Stuart Haber و W.Scott Stornettaدر قالب مقاله " How to Time-Stamp a Digital Document در سال ۱۹۹۱ برمبنای یک روش عملی در رابطه با تصدیق اسناد ایجاد / تغییر یافته.

انجام تحقیق بر روی چگونگی ذخیره داده ها در درون بلاک و چاپ آن توسط David Mazières و Dennis Shasha درقالب مقاله " Building secure file systems out of Byzantine storage " در سال ۲۰۰۲ که بر روی پروتکل ساختار داده و شبکه ای چند کاربره تمرکز داشتند که با نام SUNDR یا امن کردن مخازن داده ای غیر قبال اعتماد (Secure Untrusted Data Repositoryمطرح گردید.

اولین ارز رمز دیجتالی غیرمتمرکز توسط دانشمند علوم رایانه (Nick Szabo) در سال ۲۰۰۵ ایجاد شد . این ارز Bit Goldنام داشت ولی هرگز اجرایی نشد و از آن به عنوان سرآغاز ایجاد ارز رمز دیجیتالی BitCoin یاد می گردد .

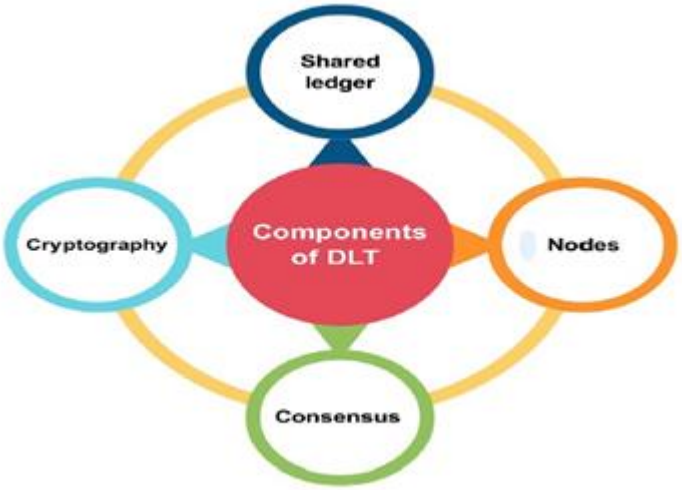
ارز رمز دیجتالی BitCoin توسط یک مبتکر ناشناس به نام Satoshi Nakamoto در سال ۲۰۰۸ ایجاد شد . این ارز رمز دیجیتال اجازه انجام تراکنش ها به صورت P2P و بدون دخالت هر گونه واسط یا نهاد مرکزی را می دهد . Satoshi Nakamoto اولین بیت کوین را در سال ۲۰۰۹ استخراج کرد [۵] .



شکل۵ تاریخچه دفاتر کل توزیع شده

2-1- مولفه های دفاترکل توزیع شده

دفاتر کل توزیع شده از ۴ مولفه اصلی دفتر به اشتراک گذاشته شده ، رمزنگاری ، گره ها و پروتکل و قوانین ای دررابطه با اجماع در شبکه بهره می برند . در ادامه به تشریح هرکدام پرداخته شده است .



شکل۶ مولفه های دفاترکل توزیع شده

دفتر مشترک : (Shared ledger) یک پایگاه داده مشترک است که جهت ذخیره کلیه تراکنش و سوابق مرتبط به آن ها که توسط گره های عضو در شبکه ایجاد شده اند . به خاطر اینکه چندین کپی از دفتر مشترک در نقاط مختلف در سطح شبکه پخش شده اند ، نیاز به زمان کوتاه جهت بروزرسانی و همگام سازی خواهد بود.

رمزنگاری : (Cryptography) تراکنش های مابین دو گره ارتباطی ، توسط پروتکل رمزنگاری ثبت ، نگهداری و ایمن می شوند . هر گره حاضر درشبکه می تواند به طور امن اقدام به ایجاد تراکنش و پخش آن در سطح شبکه نماید ، بدون آنکه نیاز به یک نهاد مرکزی جهت بررسی و تایید آن ها باشد . در واقع رمزنگاری نقش مهمی در رابطه با اعتبارسنجی تراکنش ها و تسهیل در توافق برمبنای پروتکل اجماع در زمان های بروزرسانی دفتر کل توزیع شده (DLT) از طریق گره های تایید شده دارد . به عبارتی دیگر ، برای هر گره حاضر در شبکه یک امضا دیجیتالی رمزنگاری شده اختصاص پیدا می کند ، تا قبل از هرگونه ایجاد تراکنش و یا تغییر در درون شبکه هویتش از منظر سایر گره های عضو در شبکه مورد وارسی قرار گیرد.

مکانیزم اجماع یا توافق : (Consensus Mechanism) فرآیندی است که همه گره های حاضر در شبکه جهت اعتبار سنجی محتوای دفترکل از آن بهره می برند . اجماع به طور کلی شامل دو مرحله اعتبار سنجی و توافق بر روی بروزرسانی دفتر کل می باشد . مکانیزم های اجماع مختلفی وجود دارد ولی از رایج ترین آن ها می توان به (proof of Work) Pow و Pos (Proof of Stake) اشاره کرد . تفاوت مابین مکانیزم های اجماع در نحوه انتخاب نمایندگان تصدیق و نحوه اختصاص پاداش در قبال تایید یک تراکنش می باشد.

گره ها : (Nodes) بیانگر کاربران مشارکت کننده در عملیات یک شبکه هستند . گره ها حاضر در شبکه می توانند نقش های مختلفی را به خود بگیرند. [4]

نقش مدیر سیستم :(System administrator) گره ای که نقش مدیر سیستم به خود می گیرد ، ضمن کنترل و دسترسی سیستم می تواند به ارائه سرویس های مدیریتی خاص در سطح شبکه بپردازد.

نقش صادر کننده دارایی : (Asset issuer) گره ای که این نقش را به خود می گیرد ، اجازه میدهد دارایی های جدید به سیستم اضافه گردد.

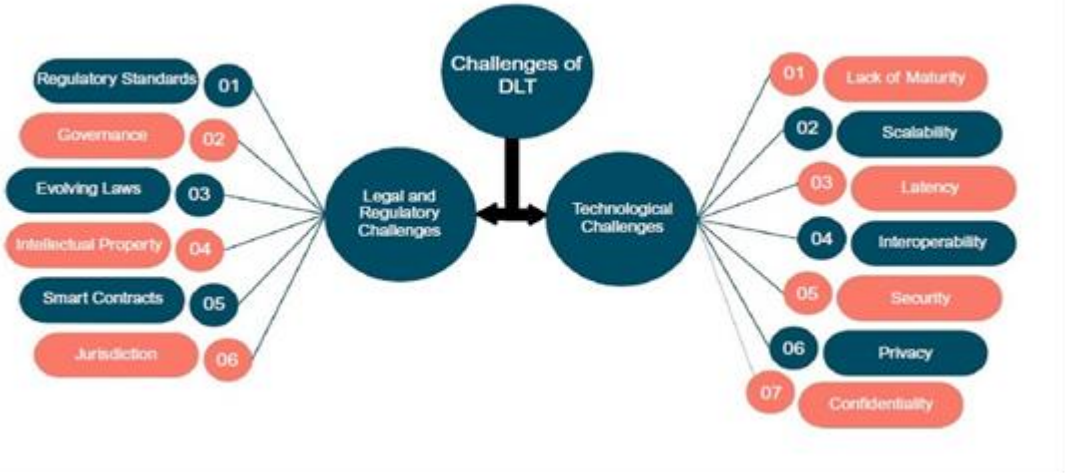
نقش پیشنهاد دهنده : (Proposer) گره ای که این نقش را به خود می گیرد ، می تواند در زمان های مختلف پیشنهاد هایی را در قبال بروز رسانی دفترکل ارائه نماید.

نقش اعتبارسنجی : (Validator) این نقش را به خود می گیرد ، می تواند تغییرات افتاده در یک دفتر کل را ر هرزمان تایید نماید.

نقش ممیزی (Auditor) : گره ای که این نقش را به خود می گیرد ، می تواند دفتر کل را فقط مشاهده نمایدو مجوز بروزرسانی و تغییر در آن را نخواهد داشت . به عبارتی کم اهمیت ترین نقش را در بین سایر نقش های مطرح شده در قبال سایر گره ها دارد[۴] .

3-1- چالش های پیشرو در قبال دفاترکل توزیع شده

دفاتر کل توزیع شده با تمام مزایایی که دارد ، چالش های نظارتی / قانونی و چالش های فنی را نیز به همراه آن ها خواهد داشت .



شکل۷ چالش های دفاترکل توزیع شده

1-3-1-چالش های قانونی و نظارتی(Legal and regulatory challenges)

استانداردهای نظارتی : (Regulatory standards) برای کاربردهای مختلف استانداردهای نظارتی منحصربفرد لازم و ضروری است . اما این استاندارد ها هنوز در مراحل اولیه پیشرفت خود قرار دارند . برای اطمینان از صحت اطلاعات ذخیره شده در دفترکل توزیع شده به یک استاندارد قانونی و واحد نیازمند است . تنظیم استاندارد هایی برای تایید هویت گره های حاضر در شبکه و محافظت از داده ها در درون شبکه لازم و ضروری می باشد . محققان بسیاری در سرتاسر جهان در حال تحقیق درباره نحوه طراحی و پیاده سازی استانداردها درقبال دفاترکل توزیع شده هستند ولی هنوزاستانداردهای بیشتری ارائهداده نشده اند.

قوانین حاکمیتی : (Governance) در محیط هایی که از دفاترکل توزیع شده (DLT) استفاده می نمایند ، هیچ نهاد مرکزی در مدیریت و کنترل آن نقشی ندارد ، به همین دلیل چند مسئله درباره تضمین فعالیت های دولتی در کل زیرساخت مورد استفاده مطرح می گردد . در زیر ساخت های متمرکز ، تنظیم کننده های استاندارد دفاتر کل ، از قوانین حاکمیتی استفاده می کنند و تاثیر پذیری قابل توجه ای هم خواهند داشت . اما در در دفاتر کل توزیع شده (DLT) مجاز و غیرمجاز ، فرد تنظیم کننده استاندارد ها و همچنین نحوه بکارگیری قوانین حاکمیتی در پیاده سازی زیرساخت مدنظر به طور واقع غیرشفاف است.

اما وجود مدیردر قبال پیاده سازی زیرساخت های مبتنی بر دفاتر کل توزیع شده بر مبنای استفاده از قوانین حاکمیتی با لحاظ کردن ماهیت دفاتر کل توزیع شده می تواند یک راه کار خوب باشد.

تکامل قوانین : (Evolving Laws) قوانین در توسعه و نوآوری فناوری وقفه ایجاد می کند ، این یک امر بدیهی است و دفاترکل توزیع شده (DLT) هم از این ویژگی به دور نیست . قوانین مربوط به اشتراک گذاری اطلاعات باید تغییر یابند ، تا شرکت ، سازمان ها ، سرمایه گذارها و حتی مشتریان در مقابل حملات و دسترسی های غیرمجاز در امان باشند . دفاترکل توزیع شده (DLT) یک بستر کاملا شفاف و قابل مشاهده را برای بسیاری از کاربردهای متنوع فراهم ساخته است ، و این نوع دیدگاه از بستر مذکور باعث ایجاد پیشرفت های چشم گیری در تنوع تولیدات و سرویس ها شده است ولی برای چنین سیستمی با دارا بودن مزایای بالا ، فقدان قوانین و مقررات یک مسئله حیاتی به نظر میرسد.

مالکیت معنوی : (Intellectual Property) با ظهور فناوری دفاترکل توزیع شده (DLT) به عنوان یک تکنولوژی جدید ، شرکت ها در حدود ۱۰۰۰ اختراع کاربردی با الهام گرفتن از مزایای نهفته در آن به ثبت رسانیده اند . اگر چه هسته فناوری دفاتر کل توزیع شده منبع باز می باشد ، ولی در واقعیت شاهد ثبت اختراعات کاربردی مشابه با بهره گرفتن از آن می شویم . به عبارتی دیگر ، وقتی یک شرکتی با بهره جستن از فناوری دفاترکل توزیع شده اقدام به ثبت اختراع کاربردی می نماید ، انتظار آن را دارد که مورد حمایت قرار بگیرید و از حقوق مالکیت معنوی در قبال اختراع خود محافظت بعمل آورند . بنابراین ممکن است چندین شرکت اقدام به ثبت اختراعات مشابه نمایند ، که در اینصورت به طور قابل تامل برانگیزی شاهد پرونده های بی شمار و ناقص درباره حق مالکیت ثبت اختراعات خواهیم بود . با توجه به این نکات ، شرکت ها و سازمان های که مایل به ثبت اختراع و اجرای آن در بستر دفاتر کل توزیع شده هستند ، باید مراقب باشند تا هیچ اختراعی را نقض نکنند.

قراردادهای هوشمند : (Smart Contracts) با ظهور فناوری های جدید و مخصوصا فناوری دفاترکل توزیع شده چندین مسئله حقوقی و قانونی هم با آن پدیدار می گردد . به عنوان مثال یک قرارداد هوشمند به صورت کد نرم افزاری پیاده سازی می گردد و این کد ها هستند که مدت و شرایط یک قرارداد هوشمند را تعیین می کنند . قراردادهای هوشمند ممکن است به طور مشهود ، ماهیت حقوقی و قانونی قرارداد ها را می تواند به چالش بکشاند و این دشواری بیشتری را در رابطه با کار با فناوری جدید درقبال دادگاه ها به همراه خواهد داشت . قراردادهای هوشمند بر اساس کدهای نرم افزاری پیاده سازی می شوند و اگر قرار بر این باشد که قراردادهای سنتی برمبنای قراردادهای هوشمند پیاده سازی گردند ، در اینصورت قابلیت اجرایی آن ها خود یک مسئله و سوال خواهد بود .

علاوه بر موارد مطروحه ، قراردادهای هوشمند در یک بستر غیرمتمرکز قابل پیاده سازی هستند و اگر اختلافاتی ناشی از اجرای قرارداد های هوشمند پدیدار گردند ، در اینصورت به علت عدم وجود یک نهاد مرکزی جهت حل و فصل آن اختلاف خودیک مسئله دیگرخواهد بود.

حوزه قضایی : (Jurisdiction) طبق فرهنگ لغت کمبریج ، Jurisdiction به معنای اختیار یک حوزه دادگاهی یا یک سازمان رسمی در قبال تصمیم گیری و داوری در یک مسئله ویژه است . از آن جایی که دفاترکل توزیع شده ، گره های حاضر در بستر مذکور را از طریق چندین حوزه قضایی مختلف مستقر در سرتاسر جهان به یکدیگر وصل می نماید ، از منظر قضایی خود چالش های را به همراه خواهد داشت . اصول حاکم بر قراردادها در حوزه های مختلف قضایی در رابطه با یک قرارداد خاص متفاوت خواهد بود ، بنابراین تعریف قانون ثابت و استوار برای حل و فصل اختلافات آتی بسیار دشوار خواهد بود.

1-2-3- چالش های فنی(Technological challenges)

عدم رسیدن به بلوغ : (Lack of maturity) نگرانی های جدی در مورد مقاوم و انعطاف پذیر بودن دفاتر کل توزیع شده (DLT)در قبال انجام تراکنش ها به تعداد زیاد ، تنظیم و تهیه استانداردهای سخت افزاری و نرم افزاری وکسب مهارت های حرفه ای لازم ، خواهیم داشت . عدم وجود درک درست در محیط های کسب و کار ، استفاده کنندگان وقانون گذاران از چگونگی پیاده سازی و استفاده از اصول فنی دفاتر کل توزیع شده خود یک مسئله دیگر هست .

هرچند سازمان هایی همچون IBM و Microsft اقدام به ارائه سرویس های متنوع و برنامه های خود با بهره گرفتن از ویژگی های اعتماد و اطمینان پذیری نهفته در دل دفاترکل توزیع شده در سطح بسیار وسیع نموده اند ، اما هنوز نیاز به یک

فرصت تحقیقاتی در قبال رشد و تکامل دفاتر کل توزیع شده نیاز خواهیم داشت تا در آینده نزدیک بتوانیم ازتمام مزایای نهفته دراین فناوری انقلابی به طورکامل بهره ببریم.

مقیاس پذیری : (Scalability) نمونه هایی از دفاتر کل توزیع شده موجود ، نگرانی هایی را در رابطه با ویژگی های مقیاس پذیری از منظر انجام تعداد و سرعت تایید تراکنش ها به وجود آورده است ، چراکه دفاتر کل مذکور در قبال سرعت انجام تراکنش و اندازه بلاک محدودیت قائل هستند . هرچند مسائل مطرح شده در قبال مقیاس پذیری در طول زمان قابل حل هستند ، اما تمرکز بر روی مسئله مقیاس پذیری باید بر مبنای دیدگاه جهانی مدنظر قرارگیرد و عدم توجه به این نکته ، دفاترکل توزیع شده را به سمت متمرکزیت بیشتر با شفاعیت کمتر سوق داده و مانع از بهره مند شدن از مزایای نهفته در آن خواهد شد.

تاخیر : (Latency) با افزایش تعداد تراکنش ها ، ضمن افزایش اندازه دفاتر کل توزیع شده به طور چشمگیر و با سرعت بیشتر ، زمان تاخیر انجام وتایید تراکنش ها هم افزایش پیدا خواهد کرد .با افزایش تعداد کاربران و به طبع آن تراکنش ها در دفاترکل توزیع شده ، زمان تاخیر تایید تراکنش ها به صورت لگاریتمی افزایش پیدا می کند . با توجه به مسئله تاخیر می توان این طور بیان کرد که دفاتر کل توزیع شده (DLT) برای تراکنش ها به تعداد بیشتر مناسب نخواهند بود.

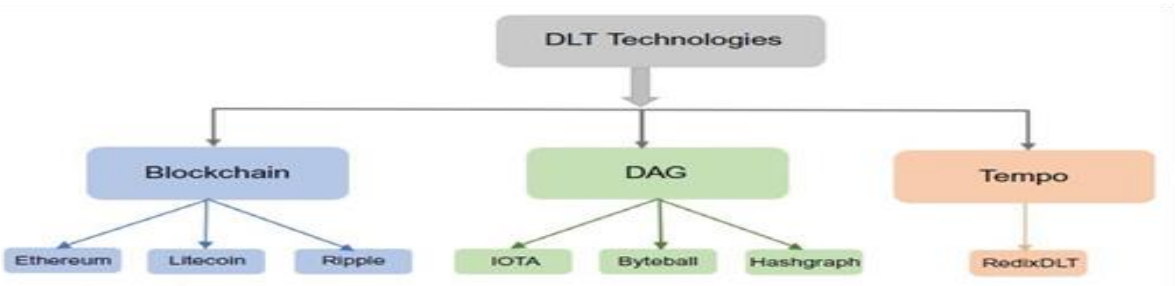
امنیت : (Security) دفاترکل توزیع شده نیاز به سرور مرکزی جهت ذخیره سازی داده ها گره های حاضر در شبکه را حذف نموده است ، ولی از یکسری حملات سایبری می تواند تهدید گردد . به عبارتی دیگر به خاطر مدیریت و دستیابی به دفاترکل بر مبنای توزیع شده توسط گره های مختلف عضو ، می تواند خود دلیلی بر وجود تهدید امنیتی باشد . همچنین با قائل شدن تفاوت در سطوح امنیتی و رمزنگاری ، یک عضو مخرب ضمن نفوذ و رخنه به شبکه ، میتواند آن را با خطر مواجه سازد.

حریم خصوصی : (Privacy) دفاترکل توزیع شده (DLT) ، برمبنای مشارکت گره های عضو در به اشتراک گذاری تراکنش ها و داده ها توسط گره های عضو در شبکه شکل می گیرد . اطلاعات و داده های تراکنش های ارسالی توسط گره عضو در شبکه شخصی و یا حتی حساس (داده های پزشکی ، شماره حساب بانکی) ، می تواند برای سایر گره های عضو در شبکه برای مشاهده باشد . بعلاوه این گره های مختلف می توانند از تمام نقاط دنیا در ایجاد دفاترکل نقش داشته باشند ، پس توجه به قوانین و الزامات حقوقی و اجرایی آن منطقه از اهمیت ویژه ای برخودار خواهد بود.

محرمانگی : (Confidentiality) ویژگی های محرمانگی را می توان شبیه ویژگی های حریم خصوصی تصور کرد ، چرا که اطلاعات و داده های به اشتراک گذاشته در دفاتر کل به صورت عمومی توسط همگان قابل مشاهده هستند . مکانیزم های محرمانگی می توانند توسط هر دو گروه از دافترکل توزیع شده عمومی / خصوصی به کار گرفته شود . اگر سازمان یا شرکتی بخواهد جهت پیش برد اهداف خود از دفاتر کل توزیع شده استفاده نماید ، باید روش ها و مکانیزم های محرمانگی ویژه و خاصی را در رابطه با محافظت از داده ها و اسرار تجاری خود در برابر انواع حملات سایبری اتخاذ نماید .

با توجه به مطالب مطروحه در بالا ، نیاز به کشف رویکرد های نوین برای حفظ محرمانگی اطلاعات و داده های در دفاتر کل توزیع شده جهت جلوگیری از هرگونه حملات و تهدیدات سایبری در آینده خواهد بود . به طور کلی امنیت در سیستم های توزیع شده در رابطه با یک فرد خاص می تواند شامل احرازیت ، حریم خصوصی و یکپارچگی و رمزنگاری داده باشد [۴] .

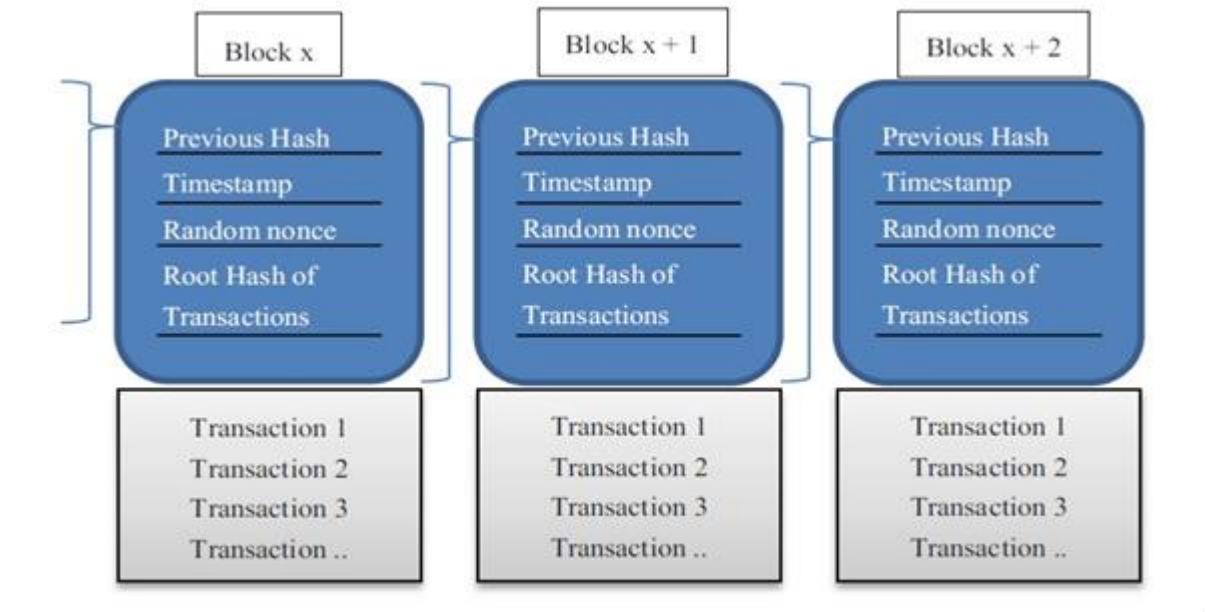
2-انواع دفاتر کل توزیع شده :



شکل۸ فناوری های مبتنی بر دفاترکل توزیع شده

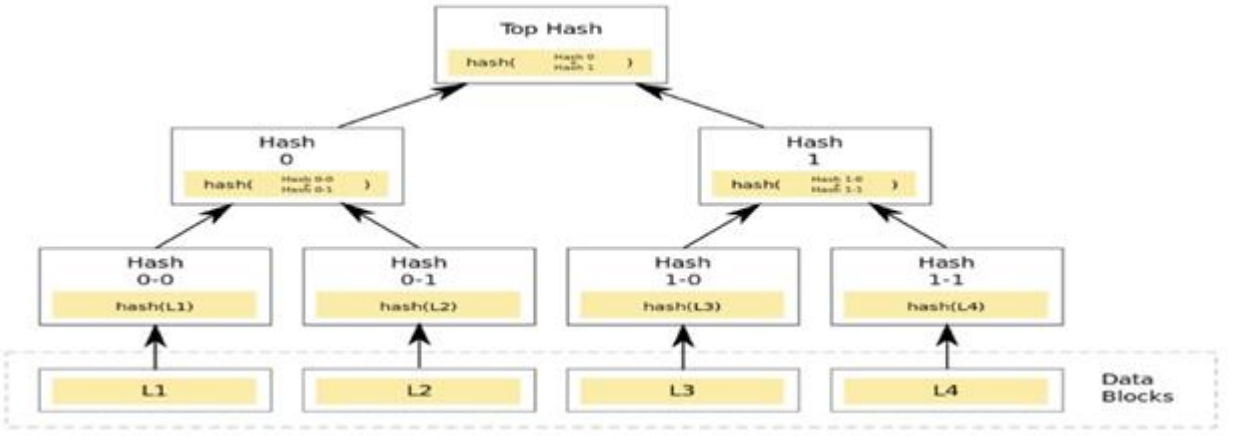
1-2- دفاتر کل توزیع شده بلاک چین(Blockchain)

تراکنش ها در قالب بلاک ها مابین تمام گره های حاضر در شبکه توزیع و از هرگونه کنترل نهاد مرکزی و تقلب مصون می مانند . هر بلاک حاوی اطلاعات (مالی ، شخصی) جهت پردازش در قبال انجام کاری خاص می باشد . هرگره حاضر در شبکه اقدام به ایجاد تراکنش و جای سازی آن در بلاک می نماید ، سپس آن را در سطح شبکه برای گره های عضو دیگر توزیع می کند ، در صورتی که گره ای عضو در شبکه موفق به تایید بلاک گردد ، در اینصورت بلاک مذکور توسط دیگر گره ها در شبکه بلاک پذیرش و به آن اضافه می شود و به این ترتیب رشد دفترکل توزیع شده بلاک چین ادامه پیدا می کند . نحوه شکل گیری زنجیره بلاک چین در شکل ها و جداول ذیل بیان می گردد[۶] [۴] .



شکل۹ زنجیره ای از بلاک چین

برای ایجاد هش یک بلاک از درخت مرکل استفاده می گردد ، که در شکل ۱۰ فرآیند هش کردن یک بلاک نمایش داده شده است [۶].



شکل۱۰ فرایند شکل گیری هش بلاک توسط درخت مرکل

در دفاترکل توزیع شده مبتنی بر بلاک چین ویژگی های کاربردی و کیفی بسیاری وجود دارد ، که باعث محبوبت و اثر بخشی در کاربردهای متنوع شده است . در جدول شماره ۱ به برخی از ویژگی ها اشاره شده است .

جدول ۱ پارامترهای دخیل در بلاک چین

نام پارامتر	شرح پارامتر
Trustless	گره های عضو مسئولیت کنترل اطلاعات تبادل شده را مابین دو گره دیگر را به عهده دارند و نیاز به نهاد یا سرورمرکزی دیگر را حذف می کنند .
Integrity	اجرای تراکنش ها دقیقا بر مبنای توافق و دستورات از قبل مشخص انجام می گیرد .
Transparency	تمامی اطلاعات تراکنش ها و داده ها بر تمامی گره های عضو در شبکه به طور عمومی قابل دسترس و مشاهده هستند .
Quality data	داده ها در بلاک چین کامل ، پایدار و تغییر ناپذیر نیز هستند .
Reliability	بلاک چین ها از شبکه های توزیع شده استفاده می کنند ، بنابراین در صورت خرابی یک گره،کل شبکه دچاراختلال نمی گردد. اشاره به عدم متکی بودن به سرور یا نهادی مرکزی در یک شبکه دارد .

چالش های بلاک چین

ظرفیت ذخیره سازی ومقیاس پذیری : زنجیره بلاک چین همواره با نرخ MB 1 به ازای هر بلاک در در فواصل زمانی ۱۰ دقیقه رشد و توسعه می گردد و می توان به بلاک های حاوی تراکنش های مربوط به ارز Bitcoin در رابطه با این نوع از رشد و توسعه اشاره کرد ، اگر بلاک های تولید شده توسط گره های عضو بخواهند بر اساس معماری بلاک چین ذخیره گردند ، در این صورت با زنجیره ای طولانی از بلاک ها مواجه می گردیم و با توجه به محدودیت فضای ذخیره سازی هر گره در رابطه با کپی کل زنجیره بلاک چین در خود ، به مسئله چالش برانگیزی در رابطه با فضای رسانه ذخیره سازی روبرو خواهیم گشت.

اعتبار سنجی تراکنش ها در شبکه بلاک چین جز کلیدی ترین مسائل در پیاده سازی پروتکل های توافق می باشد ، چرا که گره های حاضر در شبکه بلاک چین مایل به تصدیق و اعتبار سنجی تراکنش های موجود در درون یک بلاک هستند[۶] .

جدول ۲ پروتکل های مطرح در بهبود مقیاس پذیری بلاک چین

پروتکل	شرح پروتکل
Bitcoin_NG	با در نظر گرفتن مدل اعتماد و محدودیت های مقیاس پذیری Bitcoin ، پروتکل مبتنی بر تحمل پذیری اشکال با نام Bitcoin_NG پیشنهاد داده شد ، که میزان تاخیر حاصل از توافق جمعی را نسبت به Bitcoin بهبود می بخشید . این پروتکل جهت حل مسئله مقیاس پذیری بر روی دو گزینه افزایش اندازه بلاک ها و کاهش تاخیر مابین بلاک ها تمرکز دارد ، هر چند تمرکز بر روی دو گزینه مطروحه ، منجر به افزایش نرخ تولید Forke خواهد شد . یک فورک ، بلاک چین را به چندین شاخه تقسیم می نماید ، به طوریکه دیگر شاهد یک زنجیره از بلاک چین نخواهیم بود ، در این مواقع ، سیستم قابلیت تصمیم گیری نخواهد داشت ، به عبارت دیگر ممکن است بعضی از بلاک ها در اثر Forke به وجود آمده خذف شوند . زمانی که یک Forke ایجاد خواهد شدکه یک تراکنش توسط چندین Miner تایید برسد . فورک سبب به وجود آمدن دو مسئله امنیتی کاهش امنیت شبکه در مقابل هکر هاو ایجاد یک انشعاب جدید از زنجیره بلاک چین می گردد . توانمندی Bitcoin بر مبنای قدرت استخراج (Mining) بیان

Bitcoin_NG	می گردد ، البته با توجه به وجود انشعابات حاصل قدرت استخراج بر پایه انحصاری در این انشعابات هیچ تاثیری در تامین امنیت زنجیره اصلی بلاک چین نخواهد داشت . اگر ۱/۴ بلاک ها تشکیل یک انشعاب و زنجیره مجزا از بلاک چین را تشکیل دهند ، در اینصورت این انشعاب با دو حمله ۵۱٪ و Selfish (گره های خودخواه) مواجعه خواهد شد .
Litecoin	از لحاظ فنی با مدل Bitcoin یکسان می باشد ، ولی به علت بهره مند شدن از ویژگی هایی مانند ، زمان تصدیق سریع تراکنش ها ، استفاده از حافظه دستگاه برای ماینینگ و کاهش زمان تولید بلاک ها از ۱۰ به ۲.۵ دقیقه بر اساس مکانیزم Scrpyt عملکرد بهتری دارد ، نسبت به پروتکل Bitcoin که از الگوریتم SHA-256 استفاده می نماید . در Scrpyt تراکنش های موجود در بلاک به صورت پشت سر هم اجرا می شوند ولی در الگوریتم SHA-256 با کمک گرفتن از دستگاه های استخراج ASIC به صورت موازی اجرا می گردند .
Ghost	رمزنگاری بر مبنای مدل گراف جهت دارغیر مدرور (Directed Acyclic Graph) مطرح و باعث شکل گیری ساختار غیرمتمرکز دفاتر کل (Ledger) و بهبود مقیاس پذیری با تغییر در قوانین فرایند انتخاب و شکل گیری زنجیر گردیده است . راه حل ها در پی انجام تراکنش ها در خارج از شبکه زنجیره ای مطرح و در قالب راه حل های غیر زنجیره ای معرفی شدند ، ولی با توجه به افزایش پهنای باند در این مدل ، بسته های داده ای بیشتر به نظر میرسد ازبین خواهند رفت . یک راه دیگر در رابطه با مسئله مقیاس پذیری ، کاهش تاخیر انتشارو افزایش اندازه بلاک در پروتکل Bitcoin می باشد ، البته ممکن است امنیت شبکه بلاک چین با خطر جدی مواجع گردد [۷] . راه حل دیگر بکارگیری جداول جست وجوی برگشت ناپذیر IBLT (Invertible Bloom Lookup Table) است که می تواند در رابطه با یک مورد خاص برخی از ویژگی های ساختار داده ای مبتنی بر HASH را با هم ترکیب و بر کاهش تراکنش های متناقص و مغایرت پذیر کمک نماید[۸] . در پروتکل Ghost به جای زنجیر طولانی تر ، بزرگترین فورک که دارای بیشترین وزن تراکنش از سطح ریشه را دارد ، انتخاب می گردد . کم کردن زمان ایجاد و انتشار بلاک ها را مدنظر قرار می دهد . ماینرها با قدرت پردازش کمتر ، می توانند اقدام به استخراج و دریافت پاداش نمایند . Ghost مخفف Greedy Heaviest-Observed Sub-Tree است [۸] .
BigchainDB	به جای اینکه قابلیت مقیاس پذیری را در بلاک چین افزایش دهد ، برخی از ویژگی های بلاک چین را به یک پایگاه داده غیرمتمرکز اضافه می کند . BigchainDB برای اولین بار در سال ۲۰۱۶ مطرح شد و به علت برخورداری از ویژگی های بارز بلاک چین و پایگاه داده به عنوان پایگاه داده بلاک چینی شناخته می گردد . BigchainDB همانند بلاک چین از ویژگی های عدم تمرکز ، تغییرناپذیری و کنترل مبتنی بر خود مالکیت بهره می برد . BigchainDB همچنین دارای تاخیر کمتر ، نرخ تراکنش های بالا و فضای ذخیره سازی وسیع را به همراه دارد [۹]. منظور از کنترل مبتنی بر خود مالکیت (Owner-Controlled Assets) ، یعنی اینکه خود صاحب دارایی و داده و اطلاعات می تواند آن را انتقال بدهد و فرد دیگر این امکان را ندارد[۹] .
IPFS	پروتکل مذکور یک سیستم فایل توزیع شده همتا به همتا می باشد که به دنبال اتصال دستگاه های محاسباتی با سیستم فایل های یکسان است . از بعضی جهات شبیه وب است ، اما IPFS را می توان به عنوان BitTorrent Swarm درنظر گرفت که می توان به تبادل داده در مخازن GIT پرداخت . به عبارت دیگر IPFS یک مدل ذخیره سازی بلاک مبتنی بر محتوا را از طریق ابرلینک ها فراهم می نماید . IPFS در واقع یک ساختار داده ای مرکل مبتنی بر DAG است ، که می توان بر روی آن سیستم فایل

IPFS	مبتنی بر ردگیری نسخه ای ، بلاک چین و حتی وب دائمی ایجاد کرد .IPFS قصد دارد کارایی وب را همزمان با حذف فایل های تکراری و دنبال کردن تاریخچه هر فایل افزایش دهد . منظور از حذف فایل های تکراری ، این است که فقط یک فایل در شبکه امکان ذخیره شدن را دارد و منظور از دنبال کردن تاریخچه ، یعنی اینکه فایل بروز شده به فایل قدیمی اشاره دارد . لازم بذکر است که در این پروتکل ، دستیابی به فایل به روش داده گرا می باشد . منظور از داده گرا ، یعنی فایل از طریق هش منحصربفرد خودش مورد دستیابی قرار می گیرد ،که این کار باعث می گردد تا فایل تغییرناپذیر گردد [۱۰] . IPFS در واقع از ترکیب جدواول HASH توزیع شده ، انگیزش تبادل بلاکی و Self-Certifying Namespace را با هم ترکیب نموده است [۱۰] . سیستم فایل مبتنی بر ردگیری نسخه ای (Versioned File Systems) : این امکان را میدهد تا تغییرات اعمال شده (تاریخچه نسخه ها) در فایل های ذخیره شده را ردگیری نماییم[۱۰] . Self-Certifying Namespace : یک سیستم فایل توزیع شده و غیرمتمرکز عمومی ، که برای استفاده در سیستم عامل ها بر پایه یونیکس طراحی شده است . شفافیت رمزنگاری ارتباطات و همچنین احراز هویت را فراهم نموده است . در طراحی آن ، هدف ایجاد سیستم فایل توزیع شده عمومی برای دسترسی متحد الاشکل به یک سرور قابل در دسترس مدنظر بوده است[۱۰] . وب دائمی : در واقع اشاره به ایجاد و دستیابی وب با استفاده از IPFS و هش محتوایی به جای آدرس وب دارد[۱۰] .
Filecoin	از قدرت ذخیره سازی سایر گره های موجود درشبکه استفاده می کند . به عبارتی دیگر ، گره ها مقداری از فضای ذخیره سازی خود را در اختیار دیگر گره های حاضر در شبکه قرار میدهند و در قبال آن پاداش می گیرند[۱۰] .

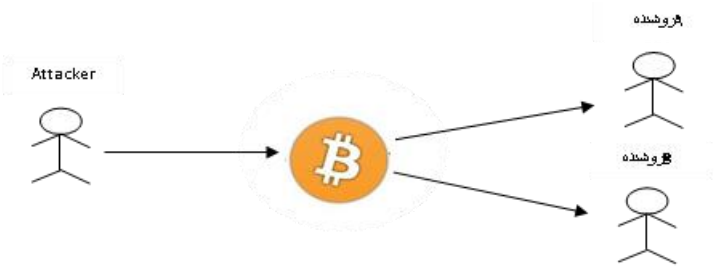
2-1-1- چالش های امنیتی: امنیت در هر فناوری یک مسئله بسیار چالش برانگیز است و توجه به آن بسیار مهم و حیاتی است . در بحث امنیت حملات موجود بر روی بستر بلاک چین و به طور ویژه و خاص بر روی BITCoin به طور مفصل بررسی شده است که در ادامه به شرح هرکدام پرداخته خواهد شد .

حمله ۵۱٪ (حمله اکثریت) : شایع ترین حمله شناخته شده درشبکه Bitcoin مبتنی بر Block chain ، حمله ۵۱٪ می باشد . بسیاری از مکانیزم های اجماع ، مطرح شده در بلاک چین ، در مقابل حملات اکثریت حساس هستند . حمله ۵۱٪ (حمله اکثریت) زمانی رخ می دهد ، که گروه های بلاک چینی بیش از ۵۱٪ قدرت محاسباتی شبکه بلاک چین را دراختیار بگیرند . توسعه سریع استخرهای استخراج ، احتمال رخداد این نوع حمله را افزایش میدهد . نمونه ای از استخرهای استخراج مشهور و شناخته شده ، استخر استخراج Ghash.IO4 می باشد . بنیاد Ghash.IO4 که وظیفه استخراج Bitcoin بر اساس سخت افزارهای شخصی و قدرت محاسباتی ابر متعلق به خود را داشت ، در سال ۲۰۱۳ تاسیس شد . در سال ۲۰۱۶ استخر Ghash.IO4 بسته شده است [۶] .

حملات مبتنی بر رشوه : محققان بحث هایی را درباره احتمال بکارگیری رشوه ، درجهت دستیابی به استخراج با توان بسیار بالا را مطرح کردند . راه حل استخراج به طور کاملا انحصاری و یا به طور همتا به همتا (P2P) ، در جهت کمک به کم کردن میزان اثربخشی و کاهش حمله مبتنی بر رشوه مطرح گردید . این نوع از توجه زمانی قابل تامل می گردد ، که به توافق درمیان تعدادی محدودی از کاربران نیاز باشد. [6]

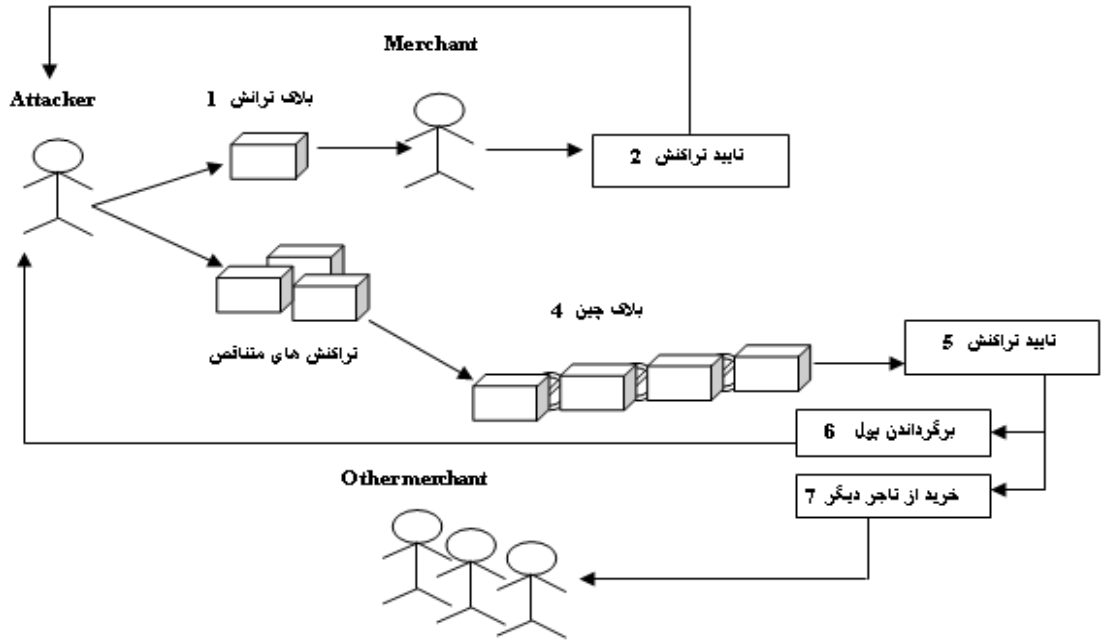
حمله دوبار خرج کردن (Double _Spend) : منظور از حمله مذکور ، هزینه کردن دوباره یک Coin در قبال دو تراکنش متفاوت می باشد . در بیت کوین یک تراکنش تایید شده ، تنها بعد از بلاک ذخیره شده ای مطرح می گردد ، که دارای عمق معین در زنجیره بلاک چین باشد . به عبارت دیگر باید به مقدار عمق معین ، یک بلاک منتظر بماند تا بلاک های

قبل از آن در زنجیره بلاک چین اضافه گردند ، و بعد از اضافه شدن آنها ، بلاک مذکور می تواند به زنجیره بلاک چین اضافه گردد. معمولا این مقدار مابین ۵ یا ۶ بیان می گردد . لازم بذکر است که میانگین زمان انتظار یک تراکنش در درون یک بلاک از انتشار ، تایید و الحاق به زنجیره بلاک چین مابین ۲۰ تا ۴۰ دقیقه می باشد . در سناریوها با قابلیت تراکنش سریع ، تاجران نمی توانند با این مقدار از تاخیر زمان کنار بیایند . پس در این نوع سناریو ها همیشه با حمله دوباره خرج کردن روبرو خواهیم بود [۶] .



شکل۱۱ حمله دوبار خرج کردن

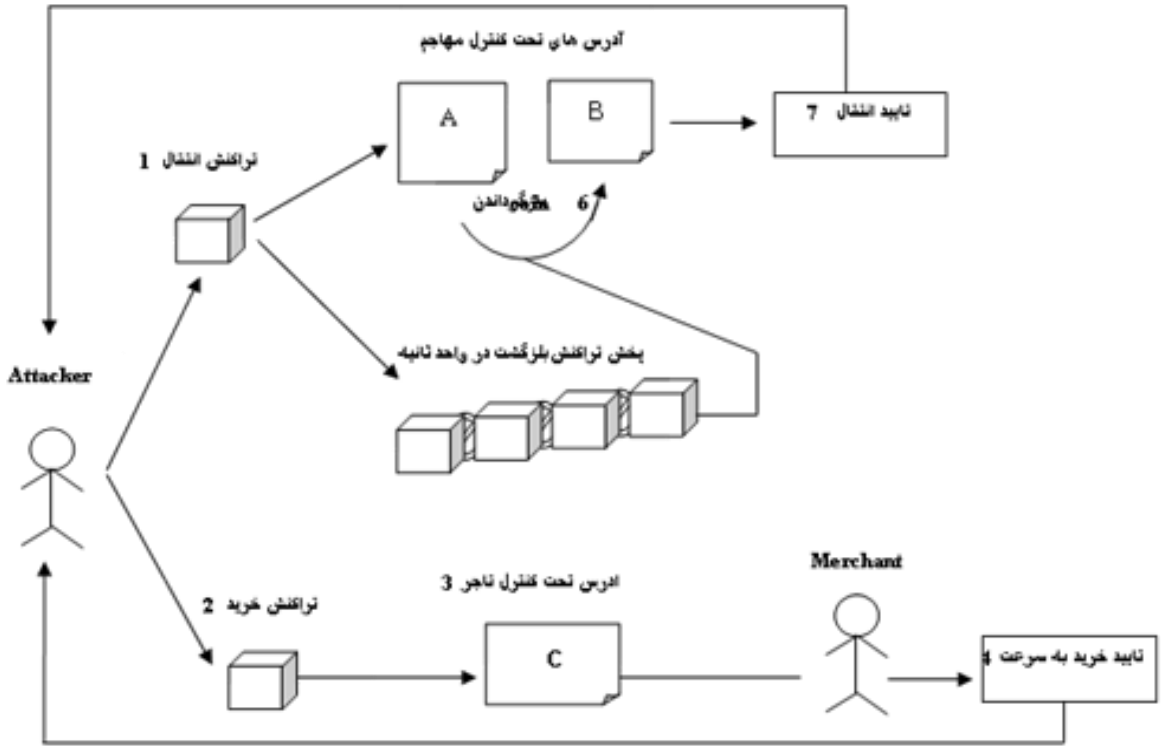
حملات نژادی (RACE) : حملات مسابقه ای می توانند در سناریوهای شبیه به سناریو (Double _ Spend) بکارگرفته شوند . برای انجام این حمله ، کاربر یک تراکنش را به طور مستقیم و بدون واسطه به تاجری که امکان پذیرش تراکنش از طرف آن به سرعت امکان پذیر است ، ارسال می کند . پس از پذیرش و تایید تراکنش از سوی تاجر ، کاربر اقدام به ارسال چندین تراکنش متناقص بر روی شبکه می کند و به متناوب آن مبادرت به بازگشت سریع سکه های پرداختی به حساب خود می نماید . تراکنش های متناقص به احتمال زیاد توسط دیگر Miner ها ممکن است مورد تایید قرار بگیرید و در اینصورت تاجر فریب می خورد [۶] .



شکل۱۲ حمله نژادی

حملات فینی : (Finney) حمله Finney یک نوع از حمله (Double_Spend) می باشد . این حمله نیازمند یک Miner اختصاصی است . زمانی این حمله قابل انجام خواهد بود که گره تاجر تراکنش های تایید نشده را مورد پذیرش قرار دهد ؛ در ضمن یک گره مهاجم نیازمند به استخراج و کنترل محتوای بلاک ها در آدرس مختص خود خواهد بود ، که این کار را با هر نرخ هش بلاک در شبکه انجام می دهد ، ولی به طور خاص کمتر از ۵۰٪ قدرت نرخ هش بلاک های شبکه لازم خواهد بود . کاربر مهاجم در ابتدا مایل به انجام ۲ تراکنش است ، که اولین تراکنش در رابطه با گره قربانی و دومین تراکنش در رابطه با اعتبار بخشیدن به خودش می باشد.

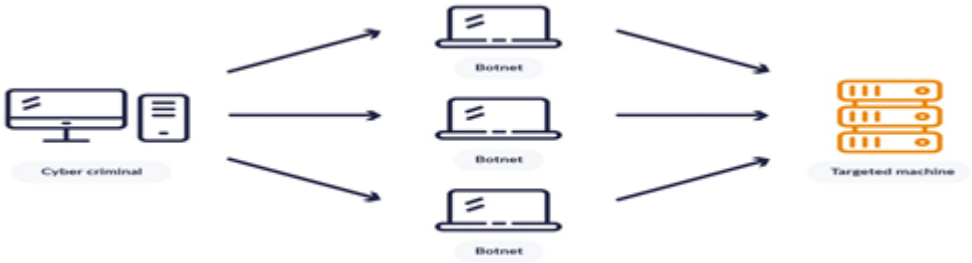
کاربر مهاجم درخواست تراکنش خرید را دارد ، که باید از آن تا موقع نیاز نگهداری کند (به طور مثال ، تراکنش خرید از ناحیه آدرس دهی C) . سپس کاربر مهاجم اقدام به تولید یک بلاک حاوی تراکنش انتقال Coin از آدرس A به آدرس B تحت کنترل خود می نماید . ضمن این که مهاجم کنترل این بلاک را در اختیار دارد ، مایل نیست آن را بر روی شبکه پخش کند . (مهاجم دارای دو ناحیه آدرس دهی A و B میباشد ، که کنترل هر دو را در اختیار خود دارد) ، هنگامی که کاربر مهاجم موفق به استخراج بلاک شد ، به سرعت اقدام به خرید کالا توسط اولین تراکنش خود از ناحیه آدرس C می نماید ، سپس در واحد ثانیه بلاک حاوی تراکنش بازگشت Coin به خود را بر روی شبکه پخش می کند . به این ترتیب اولین تراکنش انجام شده نامعتبر خواهد شد ، حتی اگر بلاک حاوی تراکنش مذکوردر قالب یک بلاک در سطح شبکه پخش شده باشد . علت نامعتبر شدن ، در منتظر نماندن برای گرفتن تاییدیه تراکنش از زنجیره بلاک چین می باشد [۶] .



شکل ۱۳ حمله فینی

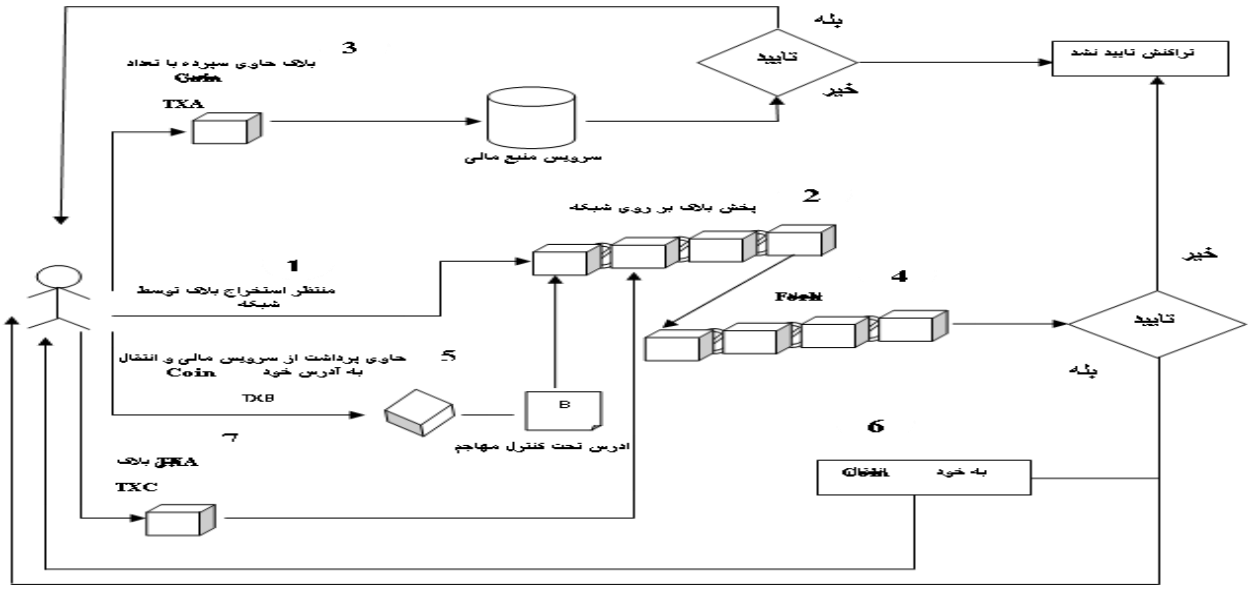
حملات ایجاد اختلال در شبکه (Dos & DDos) : این حملات در واقع باعث ایجاد اختلال در روند اجرای عادی عملیات شبکه می گردد . اگر مهاجم برای حمله از یک میزبان استفاده کند به این نوع حمله DOS و زمانی که چندین سیستم به‌طور هم‌زمان پهنای باند یا منابع سیستم مورد هدف را با بسته‌های سیل‌آسا مورد حمله قرار می دهند در اینصورت به این نوع از حمله DDOS گفته می شود [۶].

شکل ۱۳ حملات Dos



شکل ۱۴ حملات DDos

حملات وکتور (Vector76) : حمله Vector76 به عنوان یک حمله مبتنی بر تایید در نظر گرفته می شود و ترکیبی از دو حمله Finney و Race می باشد . زمانی این حمله به وقوع می پیوندد که یک تراکنش در صورت تایید شدن برای گرفتن دوباره Coin استفاده گردد . یک کلاینت متقلب می تواند توسط یک بلاک از قبل استخراج شده حمله Vector76 را انجام دهد . تفاوت اصلی مابین یک حمله Finney و Vector76 در این است که ، به جای تاجر یا فروشنده خاص ، هدف خود تراکنش در قبال یک تبادل خواهدبود . بلاک از پیش استخراج شده توسط کلاینت متقلب ، شامل یک تراکنش انتقال سپرده به یک منبع یا صندوق مالی است [۶] .



شکل ۱۵ حملات وکتور

یک شبکه به محض مشاهده بلاک جدید بر روی بستر بلاک چین ، فورا به دیگر کلاینت ها آن را اعلان می کند ، در اینصورت کلاینت متقلب پیشنهاد یک تراکنش مبنی بر انتقال سپرده به صندوق و یا منبع مالی را میدهد ، در عین حال به علت همزمانی در پاسخ ماینرها ، ممکن است یک Forke ایجاد گردد .

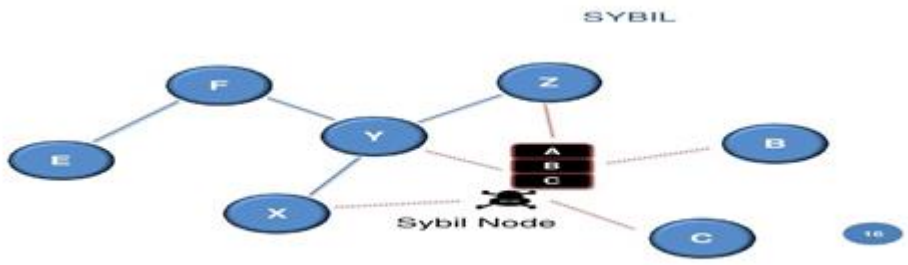
اگر Forke ساخته شده خنثی و یا متوقف شود ، در اینصورت هیچ مبادله سپرده انجام نمی گردد . هر چند یک کلاینت متقلب می تواند درخالی کردن منبع و یا صندوق مالی موفق باشد[۶] .

حملات مردمیانی (man in the middle) : در اوایل ظهور پروتکل یا ارز BitCoin ، آدرس ها بر پایه IP (همانند ۱۰۴.۲۵.۲۴۸.۳۲) بودند ولی بعد ها جهت جلوگیری از حمله مرد میانی آدرس ها بر پایه کلیدی عمومی و خصوصی پیشنهاد داده شدند . مهاجم ممکن است پس از دریافت یک بلاک خاص ، نسبت به تغییر اطلاعات آن جهت کسب سود به نفع خود اقدام نماید . حمله مرد میانی ، بر اساس تغییر آدرس کیف پول های نرم افزاری و سخت افزاری به نفع خود می باشد [۶] .

شکل ۱۶

حملات مرد میانی

حمله Sybil : مهاجم حمله را براساس ایجاد چندین هویت جعلی بر روی شبکه انجام میدهد . هویت های جعلی ایجاد شده توسط مهاجم از دیدگاه ناظران بیرونی به عنوان گره های دارای هویت حقیقی شناخته می شوند ، در حالی که این گره ها به عنوان هویت های جعلی در جهت ایجاد اختلال در شبکه مبتنی بر بلاک چین مطرح هستند [۶] .



شکل ۱۷ حملات سیبل

ناشناس بودن و حریم خصوصی داده : حریم خصوصی در طراحی پروتکل Bitcoin در حالت کلی مدنظر قرارنگرفته است ، اما کلیدی اصلی پروتکل Bitcoin ، ویژگی شفافیت آن است . درسیستم مبتنی بر Blockchain ، تراکنش ها (از اولین تراکنش تا آخرین تراکنش) می توانند از زمان ایجاد مورد بررسی و ردیابی قرار بگیرند . در واقع این یک سطح جدید از شفافیت است که بدون شک به ایجاد اعتماد مابین ارتباطات گره های موجود در سیستم کمک شایانی خواهد نمود [۶] .

رویکرد شفافیت (Transparency) : با این حال این شفافیت می تواند در ایجاد حریم خصوصی مطمئن تاثیری بسزایی بگذارد، حتی اگرهیچ گونه ارتباطی مستقیمی مابین کیف پول و افراد وجود نداشته باشد . اما به نظر میرسد که کاربر با هویت غیرقابل شناسایی ، از طریق کانال خصوصی می تواند کنترل و دسترسی محدود شده به اطلاعات به اشتراک گذاشته بر روی شبکه اقدام نماید . با بهره جستن از این مکانیزم قوی ، اعضای حاضر در شبکه می توانند از طریق هویت های عمومی خود ضمن قابل شناسایی بودن ، در راستای برقراری ارتباط با همدیگرگام برمی دارند ، اما نکته قابل توجه این است که اعضای شبکه از اطلاعات به اشتراک گذاشته شده بر روی شبکه و هویت مالک اطلاعات هیچ آگاهی نخواهند داشت[۶] .

2-2- دفترکل توزیع شده تنگل(DLT of Tangle)

ایده اصلی تنگل برمبنای تایید تراکنش یک گره منحصربفرد ، در قبال تایید تراکنش های سایر گره هایی است که به شبکه ارسال شده اند ، پایه ریزی شده است . به عبارتی می توان گفت که کاربرانی که اقدام به ارسال تراکنش نموده اند ، در تامین امنیت شبکه مشارکت می کنند . در تنگل فرض بر این است که هیچ کدام از تراکنش های ارسالی توسط گره های عضو باهم دیگر مغایرت نداشته باشند ؛ بررسی و تشخیص مغایرت تراکنش ها بر عهده گره های عضو در شبکه است . اگر یک گره در شبکه تنگل یک تراکنش متناقض را با پیگیری در تاریخچه تنگل پیدا نماید ، در اینصورت تراکنش مذکور را به طور مستقیم/ غیرمستقیم تایید نخواهد کرد[۲۲] . ساختار داده ای آن برپایه گراف جهت دار است که به هیچ وجه دوری را شامل نشده و از یک نظم توپولوژی خاص استفاده می نماید [۴] .

2-2-1- مزایای دفاتر کل توزیع شده مبتنی بر DAG نسبت به بلاک چین

- عدم نیاز به پرداخت پاداش ، به علت عدم وجودMiner که بخواهد با همتایان خود درجهت تایید تراکنش ها رقابت نماید.
- امنیت و مقیاس پذیری شبکه مبتنی برDAG ، بر خلاف بلاک چین ، با بیشتر شدن تعداد گره ها و تراکنش ها افزایش پیدا می کند.
- شبکه مبتنی بر DAG ضمن تقسیم شدن به چندین زیر شبکه ، می توانند به شبکه اصلی از طریق اینترنت متصل گردند.
- اگر زیر شبکه های مبتنی بر DAG به اینترنت متصل نباشند ، باز هم می توانند به فرآیند عادی عملیات خود ادامه دهند [۴] .

2-2-2- روش های انتخاب فراز(Tip)

الگوریتم : (uniform random tip selection) URTS فراز مورد نظر از داخل لیست فراز ها (Tip) ، به صورت تصادفی انتخاب می گردد. [11]

الگوریتم MCMC (Markov Chain Monte Carlo) : از یک گام زن تصادفی برای حرکت از ریشه به سمت تراکنش ها استفاده نموده و برحسب وزن تجمعی تراکنش ها ، تراکنش بعدی را برای گام بعدی در قبال تایید انتخاب می نماید . از این روش زمانی استفاده می گردد که فراز های کند (Lazy Tip) ، با جدیدترین وضعیت تنگل همراه نشده و تراکنش های از قبل تایید شده یا قدیمی را دوباره تایید می کند ، که این حالت هیچ کمکی به شبکه نمی کند ، چرا که هیچ تراکنش جدیدی را تایید نکرده است [۱۱] .

2-3- مروری بر دفاتر کل توزیع شده هش گراف

پلتفرم Hedera Hashgraph پیاده سازی مبتنی بر اجماع(Byzantine-Fault Tolerant) BFT است . این طرح توسط لیمون برید (Leemon Baird) در سال ۲۰۱۶ با عنوان تحمل پذیری خطای ناهمگام مورد بررسی قرار گرفته است[۱۲] . با ایجاد یک شبکه عمومی، هش گراف هدرا مزیت سرعت یک محیط خصوصی و انحصاری را از دست می دهد . البته این امر نیز با اتخاذ یک مکانیزم اجماع مشابه با اثبات سهام نمایندگی شده می تواند جبران شود . در این مدل شبکه توسط یک شورای ۳۹ نفر مورد اعتماد از صنایع و جغرافیای مختلف اداره خواهد شد . نتیجه هش گراف یک نوآوری جدید در استفاده از تمرکززدایی و هش کردن برای ایجاد یک دفترکل سریع و توزیع شده است تا بتواند هزاران تراکنش را در ثانیه پردازش کند[۱۲] . ساختار داده ای هش گراف (Hashgraph) و الگوریتم اجماع ، بستری برای رسیدن به اجماع برمبنای

توزیع شده فراهم کرده است . هدف از اجماع توزیع شده ، این است که به کاربران یک جامعه ، انجمن و یا سازمان اجازه ایجاد و اعتبار سنجی تراکنش ها را می دهد ، درحالی که هیچ کدام از اعضای حاضر در شبکه به همدیگر اعتماد ندارند[۱۲] . در واقع می توان گفت این سیستم بستری است که ، برای پیاده سازی مکانیزم های اعتماد و اطمینان طراحی شده است ، با توجه به اینکه افراد قبل از پیاده سازی آن به همدیگر اعتماد نداشتند . هش گراف پیاده سازی این نوع از اعتماد و اطمینان را به روش کاملا جدید انجام می دهد [۱۲] .

2-3-1-مزایای دفاتر کل توزیع شده مبتنی بر هش گراف:

• زنجیره بلاک چین ، همانند یک درخت است و به طور مداوم هرس می شود . هرس کردن در دفترکل توزیع شده بلاک چین برای جلوگیری از رشد شاخه ها لازم و ضروری است . در هش گراف به جای هرس کردن یک شاخه جدید ، به بدنه هش آن ساختار تنیده می گردد.

• در هر دو ساختار بلاک چین و هش گراف ، تراکنش ها در درون قالبی قرار می گیرند که از آن به عنوان بلاک یاد می گردد ؛ این بلاک ها بعداز ایجاد ، بر روی هر کدام از بستر های ذکر شده پخش می گردند . در بلاک چین زمانی که دو ماینر به طور همزمان دو بلاک را را استخراج می کنند ، یکی از بلاک ها نادیده گرفته می شود . همانند درخت ، که یک شاخه در حال رشد است و شاخه های دیگر قطع می گردند . در هش گراف تمامی تراکنش ها در بلاک دور انداخته نمی شوند و این به معنای کارآمدتر بودن آن در قبال بلاک چین است.

• اگر بلاک های جدید در بلاک چین به طور چشمگیری سریع به زنجیره بلاک چین اضافه گردد ، در اینصورت شبکه مذکور با ایجاد شاخه های متنوع همراه خواهد شد ؛ به عبارت دیگر شبکه بلاک چین با مشکل جدی روبرو خواهد شد ، بنابراین برای جلوگیری از اتفاق چنین رویدادی ، فرآیند اثبات کار در بلاک چین بکارگرفته می گردد . اما در ساختار داده ای هش گراف هیچ چیزی کنار گذاشته نمی گردد ، به عبارت دیگر هیچ گونه آسیب رسانی در قبال رشد فزآینده ساختار داده ای مذکور اتفاق نخواهد افتاد . در نهایت هش گراف نیاز به هرس کردن درساختار داده ای را حذف کرده است ، ولی به جای آن ، از تعهد محاسباتی قدرتمند مبتنی بر ریاضیات ، مانند توافق Byzantine و Fairness بهره می برد.

• الگوریتم هش گراف از ویژگی هایی همچون Fair ، fast، Byzantine، ACID compliant، Efficient، Inexpensive، Timestampedو مقاوم بودن در مقابل حملات DOS بهره می برد.

• ACID compliant اشاره به خواصی از قبیل (همه یا هیچ) Atomicity، (سازگاری) Consistency ، (اجرا به صورت همزمان ولی عدم تاثیر گذاری بر روی همدیگر) Isolation ، (مانایی) Durability دارد[۱۲] .

جدول ۳ پارامترهای عادلانه بودن هش گراف

منصفانه بودن (Fairness)	Timestamp	در بلاک برای اختصاص برچسب زمانی اطمینان در قبال تراکنش ها ، برعهده یک ماینر است ؛ در حالی که در هش گراف اختصاص برچسب زمانی اطمینان بر مبنای مکانیزم رای گیری توسط گره ها وبه طور دموکراتیک انجام می گیرد .
	ACCESS	هش گراف اساسا منصفانه است ، چرا که هیچ کس نمی تواند مانع از ورود یک تراکنش به تنگل گردد . هیچ کس نمی تواند تاخیر بسیاری در ورود یک تراکنش به سیستم انجام دهد .
		در بلاک چین تراکنش ها پس از پخش شدن در سطح شبکه ، یک ماینر در نظر گرفتن یک سری ویژگی ها (کارمزد تراکنش ها) نسبت به جمع آوری و قراردادن آن ها در یک بلاک گام برمی داشت و سپس برچسب زمانی را فقط

منصفانه بودن (Fairness)	TRANSACTION ORDER	در قبال آن بلاک تعیین می کرد ؛ این یعنی اینکه ، بلاک چین منصفانه نیست . در هش گراف تراکنش ها بر مبنای برچسب زمانی بدنبال هم و با نظم و ترتیب قابل قبول قرار می گیرند . از آن جایی که برچسب زمانی بر خلاف بلاک چین در قبال یک تراکنش اختصاص داده می گردد ،در اینصورت می توان گفت که هش گراف کاملا منصفانه است .

2-4- مروری بر دفاترکل توزیع شده تمپو

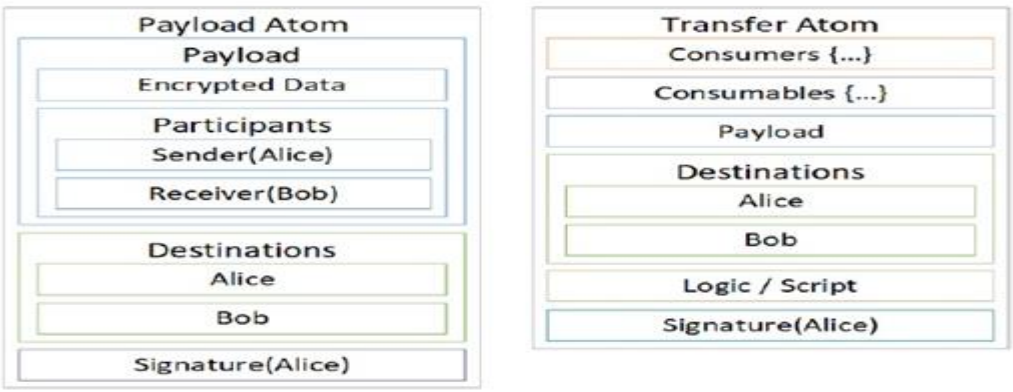
رادیکس یک بستر جدید همانند بیت کوین ، اتریوم و سایر بسترهای مبتنی بر توزیع شده است . اما این بستر نسبت به بسترهای توزیع شده مشابه دیگر ، از ویژگی هایی همچون مقیاس پذیری بالاتر ، ساخت آسان تر و استفاده راحت تر بهره می برد . در پیاده سازی بستر رادیکس به جای استفاده از بلاک چین و داگ ، از روش کاملا جدیدی استفاده شده است ، تا در سرتاسر جهان هرکس/ هر دستگاه بتواند بدون سازش کردن و حتی متکی بودن به یک نهاد متمرکز از آن استفاده نماید.

رادیکس یک جایگزین سریع برای بلاک چین است . رادیکس از تکنیک های بسیار قوی همچون ساعت های منطقی (Logical Clocks) ، پایگاه داده قابل تقسیم (Database Sharding) ، پروتکل شایعه پراکنی (Gossip) ، اثبات موقت (Temporal Proof) ، ساعت های برداری (Vector Clocks) بهره می برد ، که در ادامه به تشریح هریک پرداخته خواهد شد[۱۳] .

2-4-1- مفاهیم و اصطلاحات موجود در رادیکس- تمپو

پایگاه داده شاردینگ : (Database Sharding) در واقع اشاره به پایگاه داده بسیار بزرگی دارد که به چندین بخش شکسته شده است . این پایگاه داده بزرگ به چندین بخش کوچک تقسیم می گردد ، که به هریک از این بخش های کوچک و زیر مجموعه از پایگاه داده که در این جا از آن به عنوان دفتر کل یاد می گردد ، شارد (Shard) گفته می شود . در رادیکس هر یک از گره ها به جای پردازش تمام دفترکل ، بخشی از آن که شارد نامیده می گردد را پردازش می نمایند . از این تکنیک جهت افزایش سرعت پردازش و مقیاس پذیری استفاده می گردد . در حال حاضر در سرتاسر جهان حدود quintillion 18.4یا (10^{48}) شارد وجود دارد. [13]

آتم (Atom) : هر رویداد در Universe مانند یک تراکنش ، شی ، پیام و انتقال در اتم قرار می گیرد . البته اتم ها دارای دو نوع مختلف هستند ، که می توان به اتم های پیام و اتم های انتقال اشاره کرد . اتم های پیام ، شامل پیام های ارتباطی است ؛ مانند ارسال یک ایمیل فوری به یک چند نفر اشاره کرد . اتم های انتقال جهت انتقال مقدار واحد پولی به یک بخش دیگر می باشند[۱۳] .



شکل ۱۸ ATOM

اتم ها بسته به هدفشان می توانند شامل داده های متنوع دیگری نیز باشند ؛ داده های اضافی می تواند شامل موقعیت مقاصد ، مالک ها ، مشارکت کنندگان ، انجمن ها و متا داده های برنامه های کاربردی باشند. [13]

تغییرات حالت : (Partial) در دفتر کل توزیع شده ، تمام مشارکت کنندگان باید بر روی مجموعه ای از قوانین حاکم بر نحوه تغییر و بروزرسانی دفترکل توزیع شده با هم توافق نمایند . در رادیکس یک گره نمی تواند تمام حالت های مربوط به تغییرات در قبال دفتر کل توزیع شده را ذخیره نماید ، در این هنگام یک حالت تغییر به چندین حالت تغییر کوچک تقسیم و بدون نیاز به سایر حالت های تغییر دیگر اعتبار سنجی خواهند شد . برای انجام این کار ، یک حالت تغییر باید به صورت صریح و روشن تعریف گردد ، سپس توسط مکانیزمی در قالب یک واحد مورد پذیرش یا رد قرار بگیرد . در رادیکس این حالت ها تغییر ، Partial نام دارد . این پاراتیل ها در داخل Atom ها به دفتر کل توزیع شده ارسال می گردند . [13]

ساعت های منطقی : (Logical Clocks) اساس اجماع و توافق در دفترکل توزیع شده رادیکس تمپو ، برپایه ساعت های منطقی است . ساعت های منطقی ابزار ساده ای هستند ، که وظیفه فراهم کردن نظم و ترتیب نسبی و بر مبنای Partial ، رویداد های دفترکل توزیع شده را دارد . در تمپو ، همه گره ها دارای یک ساعت منطقی هستند ؛ یک عدد صحیح رو به افزایش ، که بیانگر تعداد رویداد های مشاهد شده توسط یک گره خاص است . زمانی که یک گره ، رویدادی را که قبلا مشاهده نکرده است را ببیند ، در اینصورت ضمن افزایش ساعت منطقی خود ، ساعت منطقی فعلی خود را هم با آن ذخیره می نماید . این رکورد می تواند ، برای معتبر سازی نظم و ترتیب موقت رویداد های پیشین در صورت نیاز کمک کند. [13]

اثبات موقت (Temporal Proof) : یک Univers به چندین بخش تقسیم می گردد ، که به هریک از بخش های مورد نظرشاردگفته می شود .گره ها به جای ذخیره کل دفتر کل ، فقط بخشی از آن ،که شارد گفته می گردد ذخیره می کنند ؛ با این حال ، بدون وجود یک مکانیزم و الگوریتم قوی در قبال وارسی حالت های تغییر ، ممکن است یک Item در چندین شارد مجزا ذخیره گردد ؛ برای جلوگیری کردن از این خرج کردن دوبار Item ، اثبات موقت به عنوان یک راهکار آسان و مقاوم معرفی شده است[۱۳] .

3- نتیجه گیری:

داده های خام و دانش بدست آمده از آن در بعضی از مواقع بسیار مهم و حتی ممکن است حیاتی باشند . در این مقاله سعی بر آن شد ، تا مروری بر دفاترکل متمرکز و غیرمتمرکز (توزیع شده) پرداخته شود ؛ مزایا و معایب هر کدام ، هرچند مختصر بیان گردید . در طول توسعه دفاتر کل ، تلاش بر حفظ حریم خصوصی ، تغییر ناپذیری داده ها ، دسترس پذیری به داده ها همیشه مطرح بوده و هست . در دفاترکل متمرکز امنیت برپایه یک نهاد مرکزی و در دفاتر غیرمتمرکز / توزیع شده بر پایه P2P راهکاری مبتنی بر اجماع مطرح شده است . امنیت برمبنای راهکارهای اجماع در دفاتر کل توزیع شده ، بهتر و کارآمد تر نسبت به دفاترکل متمرکز می باشد . اما چالش دیگر در قبال دفاتر کل توزیع شده ، مقیاس پذیری آن ها بود ؛ برای حل مسئله مقیاس پذیری پروتکل های متنوعی در بلاک چین مطرح شده است ولی چندان مورد پذیرش نبودند . راهکارهای مبتنی بر تنگل و هش گراف ، ضمن اینکه از مزایای بلاک چینی بهره می بردند ، از از پارامترها ، راهکارها ، پروتکل ها و الگوریتم های متنوع دیگری نیز در جهت افزایش مقیاس پذیری استفاده می کردند . در ادامه راهکار غیر بلاک چینی مطرح شد ، که از آن به عنوان بستر رادیکس یا دفاترکل توزیع شده تمپو یاد می گردد .

منابع و مراجع

1. https://www.myaccountingcourse.com/ACCOUNTING-DICTIONARY/LEDGER%0AHTTPS://BLOG.LIQUID.COM/DISTRIBUTED-LEDGER-TECHNOLOGY%0A.
2. https://blog.liquid.com/distributed-ledger-technology.
3. D. Burkhardt and M. Werling, “Distributed Ledger,” 2018 IEEE Int. Conf. Eng. Technol. Innov., pp. 1–9, 2018.
4. H. F. Atlam and G. B. Wills, Intersections between IoT and distributed ledger, 1st ed. Elsevier Inc., 2019.
5. https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011.
6. B. Tavares and F. F. Correia, “A Survey of Blockchain Frameworks and Applications,” vol. 1, pp. 308–317.
7. Y. Sompolinsky and A. Zohar, “Secure High-Rate Transaction Processing in.”
8. P. Lamb, “Invertible Bloom Lookup Table Cache,” 2016.
9. B. Gmbh, “The Blockchain Database,” no. May, pp. 1–14, 2018.
10. J. Benet, “IPFS - Content Addressed , Versioned , P2P File System,” no. Draft 3.
11. B. Ku, P. Staupe, and A. Gal, “Extracting Tangle Properties in Continuous Time via Large-Scale Simulations,” 2018.
12. M. Harmon and P. Madsen, “Hedera : A Public Hashgraph Network & Governing Council The trust layer of the internet.”
13. D. Hughes, “Radix - Tempo,” no. September, pp. 1–15, 2017.

Overview of centralized and decentralized head ledgers (distributed)

Behroz Marami Stiyar , Mohammad Ali Jabraeil Jamali
Seraj.university.tabriz, behroz.ma.1367@gmail.com
Islamic Azad Univ., Shabestar, Iran, m_jamali@itrc.ac.ir

Abstract— General ledgers are ledgers, which are used in companies and organizations to store customers' financial transactions, personal details in the form of records. In terms of applied technology, general ledgers are divided into centralized and decentralized categories. Of course, in general, decentralized general ledgers are also referred to as distributed general ledgers, but in reality, they are different, each of which is described in detail below. Distributed head ledgers have unique applications in many areas; It is used in IoT technology to increase and improve security. In this paper, a review study of centralized and decentralized and distributed systems, types of general ledgers based on distributed systems (Blockchain, Tangel, Hash graph, Tempo) is discussed.