



**دانشگاه تربيت مدرس**

**دانشكده مهندسي برق و کامپیوتر**

**گذارش سمینار کارشناسی ارشد**

**مهندسي کامپیوتر گرایش مهندسی­ نرم­افزار**

**سیستم­های تراکنش بین چند دفترحساب توزیع شده**

**دانشجو**

رضا حمیدپوربدوئی

**استاد راهنما**

دكتر صادق دری­نوگورانی

تیر 139

فهرست مطالب

[مقدمه و کلیات 1](#_Toc14093823)

[1-1 زنجیره­بلاکی 1](#_Toc14093824)

[1-2 دفترحساب توزیع شده 2](#_Toc14093825)

[1-3 قراردادهای هوشمند 3](#_Toc14093826)

[1-4 صرافی برخط 3](#_Toc14093827)

[سیستم های تبادل بین دفترهای توزیع شده موجود 5](#_Toc14093828)

[2-1 صرافی های متمرکز 5](#_Toc14093829)

[2-1-1 تولید سیستم تبادل رمزارز دیجیتال از پایه 6](#_Toc14093830)

[2-1-2 سیستم تبادل برچسب سفید 6](#_Toc14093831)

[2-2 صرافی های غیرمتمرکز 6](#_Toc14093832)

[2-2-1 غیرمتمرکز مبتنی بر مفهومی تحت عنوان تبادل های تجزیه ناپذیر 7](#_Toc14093833)

[2-2-1-1 استفاده از یک قراردادهوشمند برای تبادل 7](#_Toc14093834)

[2-2-12- پروتکل ارتباط بین دفتر حسابهای توزیع شده– ILP 8](#_Toc14093835)

[2-2-2 غیر متمرکز تحت کنترل یک مدیریت مشخص 9](#_Toc14093836)

[2-2-2-1 شبکه تبادل ارز Stellar 10](#_Toc14093837)

[2-2-2-2 شبکه Transledger 11](#_Toc14093838)

[2-2-3 تشریح کامل پروتکل ILP 13](#_Toc14093839)

[2-2-3-1 فرستنده،گیرنده ،اتصالدهنده 13](#_Toc14093840)

[2-2-3-2 لایههای پروتکل 13](#_Toc14093841)

[2-2-3-3 فرآیند انتقال 15](#_Toc14093842)

[2-2-3-4 انواع گرهها 17](#_Toc14093843)

[2-2-3-5 بستههای پروتکل ILP 18](#_Toc14093844)

[جمع بندی و نتیجه گیری پایانی 20](#_Toc14093845)

[منابع 22](#_Toc14093846)

فهرست شکل­ها

شکل 1-2 ساختار دفتر حساب کل2

شکل 1-2 الگوریتم اجراء روش تجزیه ناپذیر7

شکل 2-2 نحوه اتصال گره ها در ILP13

شکل 3-2 معماری کلی پروتکل ILP13

شکل 2-4 نحوه انتقال ارز در دفتر حساب توزیع شده15

شکل 2-5 نحوه انتقال ارز بین دو دفتر حساب توزیع شده16

شکل 2-6 نحوه انتقال ارز بین دو دفتر حساب توزیع شده به وسیله پروتکل ILP16

شکل 2-7 انتقال ارز از حالت سرمایه گذاری شده به حساب کاربران در پروتکل ILP17

شکل 2-8 نحوه بهم زنجیر شدن اتصال دهندگان در پروتکل ILP17

شکل 2-9 نحوه انتقال پیام های درخواست و انجام شدن در پروتکل ILP18

شکل 2-10 نحوه انتقال پیام های درخواست و رد پیام در پروتکل ILP19

چکیده

در سال 2009 با تولد بیت­کوین فصل جدیدی در فرآیندها و انتقالات مالی به وجود آمد که این امر باعث پررنگ شدن تکنولوژی بلاکچین و کاربردهای آن در این زمینه شد.از سمتی دیگر با به وجود آمدن شبکه­های رمزارز متفاوت دیگر و حتی استفاده آن­ها در فرآیندهای مالی روزمره انسان­ها ،نیاز به تبدیل این رمزارزها به یکدیگر بیش از پیش اهمیت پیدا می­کند به نحوی که می­توان گفت در سال 2019 مهم­ترین چالش­های پیش­روی دنیای رمزارز­ها سرعت انتقال،حجم­ تراکنش در لحظه و توان تبدیل آن­ها به یکدیگر می­باشد.از همین جهت در طی سال­های گذشته فعالیت­های بسیار زیادی برای ایجاد راه­حلی مناسب خصوص تبادل رمزارز­ها شده است اما می­توان گفت تنها تعداد کمی از آن­ها به صورت عملی پیاده­سازی شده­اند.در این خصوص ما سعی کرده­ایم آن روش­هایی که تا به این لحظه عملیاتی شده­اند را گردهم بیاوریم.

کلید واژه­ها : رمزارز ، صرافی­آنلاین،قرارداد هوشمند

فصل 1

مقدمه و کلیات

مقدمه

با توجه به اهمیت بیش از پیش تبادل رمزارز­ها به یکدیگر و اهمیت پیدا کردن ایجاد صرافی­های برخط[[1]](#footnote-1) که توان تبادل و تبدیل رمزارزها به یکدیگر را داشته باشند بیشتر از پیش احساس می­شود.تا به امروز نیز روش­های متفاوتی برای به وجودآمدن صرافی­های برخط پیش­نهاد شده است.به طور کلی می­توان روش­های ایجاد یک صرافی را به دو دسته صرافی­های متمرکز و صرافی­های غیرمتمرکز تقسیم کرد.در صرافی­های متمرکز ما هیچ سازوکار خاصی درجهت ایجاد یک شبکه برای تبادل رمزارز­ها نیاز نخواهیم داشت بلکه تنها این موضوع اهمیت پیدا می­کند که شخص مراجعه کننده به این صرافی­ها بتواند به آن صرافی اعتماد کند.

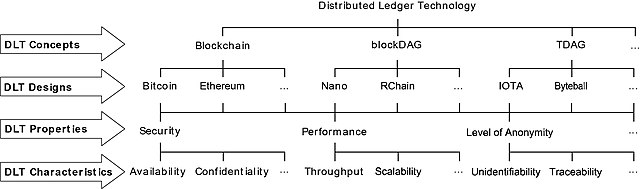
اما در روش دیگر یعنی صرافی­های غیرمتمرکز اساسا سازوکار بر پایه عدم اعتماد طرفین به یکدیگر ایجاد می­شود به همین دلیل برای به وجود آمدن این اعتماد از روش­های متفاوتی استفاده شده است.در این تحقیق ما در بخش اول ابتدا با مفاهیم کلی تکنولوژی بلاکچین و مفاهیمی دیگر همچون قراردادهای هوشمند آشنا خواهیم شد.همچنین یک توصیف کلی از مفهوم صرافی نیز خواهیم داشت.پس از آن در بخش دوم به راه­کارهای تبادل رمزارزها میپردازیم که هرکدام دارای چه چالش­هایی هستند و همچنین چه مزایی دارند.در نهایت در بخش سوم نیز یک توصیف کلی از تمامی روش­ها خواهیم داشت و نتیجه انجام کارکرد روش­ها را بایکدیگر مقایسه خواهیم کرد.

1-1 زنجیره­بلاکی

زنجیره­بلاکی[[2]](#footnote-2) ترکیبی از تکنولوژی­های رمزنگاری داده­ها ، شبکه و مدیریت­داده می­باشد که درآن داده­ها در قالب رکوردها ویا بلاک­های بهم زنجیر شده و غیر قابل تغییر، ذخیره­سازی و نگهداری می­شوند.در این تکنولوژی گره­های عضو یک شبکه زنجیره­بلاکی به صورت نظیربه­نظیربه یکدیگر متصل شده و برای ذخیره­سازی داده­ها و پایداری شبکه از الگوریتم­های اجماعاستفاده می­کنند.الگوریتم­های اجماع نیز براساس نحوه کارکردشان ارسال درخواست­های، ثبت یک بلاک جدید در شبکه و نحوه ثبت آن درخواست، در دفترحساب­کلشبکه را مشخص می­کنند. دفترچه­کل زنجیره­بلاکی محل ذخیره­سازی داده­های شبکه بلاکچین می­باشد،به عبارتی دیگر دفترچه­کل نقش پایگاه­داده توزیع شده را در شبکه­های زنجیره­بلاکی ایفا می­کند.محتوای دفترچه­های­کل شبکه زنجیره­بلاکی به وسیله گره­های داخل شبکه ایجاد می­شود که این گره­ها از نظر جغرافیایی در یک موقعیت یکسان قرار ندارند. ایجاد شبکه به این صورت در حالی است که در این ساختار ما هیچ نقطه مرکزی در شبکه نداریم به عبارتی دیگر ما هیچ گره کنترل کننده مرکزی ( سرور مرکزی) نخواهیم داشت.

تراکنش­ها به صورت سنتی به وسیله یک شخص ثالث مورد اعتماد مانند بانک­ها ویا نهادهای دولتی تایید و ثبت می­شدند.زنجیره­بلاکی یک روش نوین برای ثبت این دست از تراکنش­ها را فراهم آورده است،به صورتی که در این ساختار ما به جای اعتماد کردن به یک شخص ثالث تایید شده به گروهی از گره­های عضو شبکه اعتماد می­کنیم به این صورت که با تصمیم جمعی و اعتماد کردن به اکثریت اعضای شبکه مبنی بر صحت تراکنش، یک تراکنش در داخل شبکه ثبت شده و دیگر امکان تغییر آن وجود ندارد مگر به تصمیم اکثریت اعضای شبکه.در ابتدا مفهوم و تکنولوژی زنجیره­بلاکی در شبکه بیت­کوین استفاده شد که یک رمزارز است. اما امروزه این تکنولوژی در زمینه­های متفاوتی با اهداف وکاربردهای متفاوت مورد استفاده قرار می­گیرد‎[1].

1-2 دفترحساب توزیع شده

مفهوم بلاکچین به نحوه پیاده­سازی دفترچه­کل آن برمی­گردد.دفترچه­کل درواقع پایگاه­داده توزیع شده شبکه بلاکچین محصوب می­شودکه داده­ها[[3]](#footnote-3)در آن به صورت فقط­خواندنی ذخیره می­شوند.ویژگی فقط­خواندنی یکی از ویژگی­های اصلی این تکنولوژی می­باشد به نحوی که در آن تنها بلاک ویا رکورد جدید افزوده می­شود و هیچ تغییر ویا حذفی بر روی رکورد­های ماقبل آن امکان پذیر نمی­باشد.تکنولوژی دفترحساب­های توزیع شده مفاهیم متفاوت پیاده­سازی دفترحساب­های­کل را شامل می­شود که به طور کلی نحوه ذخیره­سازی تراکنش­ها و اعتبار­سنجی آنها با یکدیگر متفاوت می­باشد.برخی از این تکنولوژی­ها به نام­های بلاکچین، گراف­های جهت­دار مبتنی بربلوک[[4]](#footnote-4)و گراف­­های جهت­دار مبتنی تراکنش[[5]](#footnote-5) هستند.هرکدام از این مفاهیم دفترحساب­­های­کل ویژگی­های خاص خود را دارند و درواقع براساس میزان­کارایی و امنیتمتفاوت می­باشند.نمونه­هایی از شبکه­های پیاده­سازی شده با استفاده از دفترچه­کل­های بلاکچینی بیت­کوین[[6]](#footnote-6) ویا اتریوم[[7]](#footnote-7) می­باشند.ویا نمونه­ای از شبکه­ای که برپایه تکنولوژی گراف­های جهت­دار مبتنی­بر تراکنش پیاده­سازی شده است شبکه آیوتا[[8]](#footnote-8) می­باشد. تصویر 1-2-1 نمایی از شبکه­های مختلف با استفاده از تکنولوژی­های مختلف بلاکچین را بیان می­کند]1[.

شکل 1-2 ساختار دفترحساب­های کل

1-3 قراردادهای هوشمند

در شبکه­های زنجیره­بلاکی علاوه بر انجام تراکنش­ها و ثبت آن­ها می­توان برنامه­هایی را نیز اجراء کرد به نحوی که کد این دست از برنامه­ها در قالب یک تراکنش بر روی شبکه زنجیره­بلاکی ذخیره می­شوند و گره­های داخل شبکه آن­ها را اجراء می­شوند.به این دست از برنامه­ها که بر روی شبکه­های زنجیره­بلاکی به صورت توزیع شده اجراء می­شوند قراردادهای هوشمند[[9]](#footnote-9) می­گویند.در شبکه اتریومما با کمک یک زبان تورینگ کامل[[10]](#footnote-10) می­توانیم این دست از برنامه­ها را بنویسیم و بر روی شبکه زنجیره­بلاکی قرار دهیم.موضوع اصلی که در این دست از برنامه­ها وجود دارد این است که اولا قراردادهای­ هوشمند قطعی هستند.

به عبارتی دیگر نتیجه اجراء یک قرار داد هوشمند توسط چندین گره مختلف در شبکه یکسان می­باشد.دوما کد منبع قراردادهای هوشمند پس از قرار گرفتند بر روی شبکه زنجیره­بلاکی دیگر قابل تغییر نمی­باشند. یک قرارداد هوشمند توانایی دریافت یک تراکنش مالی و انتقال وجه را در شبکه­های زنجیره­بلاکی دارد همچنین قراردادهای هوشمند می­توانند با یکدیگر ارتباط برقرار کنند و یکدیگر را فراخوانی کنند.نکته قابل توجه درخصوص این برنامه ها این است که نمی­توان آن­ها را تحت یک قرارداد قانونی در نظر گرفت بلکه می­توان آن­ها را تحت بخشی از یک قرارداد واقعی در نظر گرفت.

1-4 صرافی برخط

امروزه با پر رنگ شدن ارزهای دیجیتال و رمزارزها تجارت­هایی مانند صرافی­های برخطنیز اهمیت بیشتری پیدا کرده اند]2،3[. به همین منظور می­توان صرافی­های ایجاد شده بر این بستر را به دو دسته متفاوت تقسیم کرد.صرافی­های متمرکز[[11]](#footnote-11) صرافی­های غیر متمرکز.صرافی­های متمرکز ،به صرافی­هایی گفته می­شود که برای تبادل ارز­ها به یکدیگر ابتدا شخص متقاضی کننده بایستی وجه مقصد خود (بیت­کوین) را به حساب صرافی انتقال دهد، پس از آن صرافی مورد نظر وجه معادل مشتری خود را در قالب یک ارز دیگر (اتریوم) به حساب مشتری بازپس می­دهد.

در اینگونه تبادل­های ارزی به صورت برخط موضوع اعتماد و حریم خصوصی برای مشتری بسیار پر رنگ می­باشد. به طوری که در ابتدا بایستی مشتری هویت و رسمیت صرافی را برای خود احراز کند تا بتواند با اطمینان عمل تبادل ارزی را انجام دهد. نوع دیگر صرافی­ ،صرافی­های غیرمتمرکز گویند.در این نوع صرافی­ها هیچ مرکزیتی وجود ندارد و کاربران در داخل یک شبکه با یکدیگر عمل تبادل ارزی را انجام می­دهند.به عنوان مثال کاربر A درخواست تبدیل بیت­کوین به ریپل[[12]](#footnote-12) را دارد.در این میان کاربر B نیز ارز ریپل دارد و می­خواهد آن را با بیت­کوین تبدیل کند.در صرافی­های غیر متمرکز ما عمل اتصال کاربر A به B را انجام می­دهیم و همچنین در این حالت ما ارز مقصد را به حساب صرافی انتقال نمی­دهیم و مستقیما به حساب تبدیل کننده انتقال می­دهیم.یکی دیگر از مزایای این نوع از صرافی­ها این می­باشد که ما اندوخته مالی­ای نیاز نداریم.

به عبارتی دیگر در این روش صرافی هیچ اعتبار از پیش مشخص شده ریپل­ای ندارد و تنها عمل اتصال دو طرف را انجام می­دهد.در این تحقیق ما نیز ما به سازوکار انواع مختلف این نوع صرافی می­پردازیم و سعی­ می­کنیم که نحوه کارکرد هر کدام را به صورت مختصر تشریح کنیم.

فصل 2

سیستم­های تبادل بین دفتر­های توزیع شده موجود

مقدمه

در این بخش ما در ابتدا یک تصویر کلی از انواع صرافی­ها ایجاد می­کنیم و مشخص می­کنیم که در هر روش چه مزایا و معایبی برای صرافی­ها و مشتریان آن­ها وجود دارد.پس از آن با برسی نمونه­های اجرایی در هر روش و معماری­های کلی آن­ها دیدی کلی از انواع صرافی­ها را ایجاد خواهیم کرد.

2-1 صرافی­های متمرکز

در این نوع از صرافی­ها همان­گونه که قبلا اشاره شد،تبدیل وجه به این صورت انجام می­شود که بایستی مشتری ابتدا وجه خود را به حساب صرافی انتقال دهد و پس از آن صرافی با اعمال نرخ تبدیل ارزها به یکدیگر و برداشت کارمزد تبدیل ، ارز تبدیل شده را مجدد به حساب مشتری برگرداند.همان­گونه که اشاره شد در این روش بایستی اعتماد در بین مشتری و صرافی وجود داشته باشد چرا که در این سازوکار ما هیچ گونه پیش شرط­ قانونی برای جلوگیری از تخلف صرافی نخواهیم داشت.نکته قابل توجه در این بخش این است که اغلب صرافی­های برخط برای کاهش محدودیت­های عملیاتی خود و دوری از برخی چالش­های سیاسی ، تابع قوانین حاکمیتی هیچ کشوری قرار نمیگیرند از همین رو بر روی عملکرد این دست صرافی­ها نظارت کاملی انجام نمی­شود.

برای ایجاد یک صرافی متمرکز به طور کلی ما دو روش پیاده­سازی سیستم را خواهیم داشت:

1. تولید سیستم تبادل رمزارز دیجیتال از پایه
2. سیستم­تبادل برچسب سفید

2-1-1 تولید سیستم تبادل رمزارز دیجیتال از پایه

در این حالت صرافی با جمع­آوری یک گروه نرم­افزاری به همراه اشخاص صاحب نظر در اینگونه سیستم­ها سعی بر پیاده­سازی یک سیستم تبادل رمزارز دیجیتال به صورت برخط را دارد.چالش اصلی در این سیستم­ها این است که به دلیل تازگی تکنولوژی­های به کار رفته در ساختار رمزارزها و عدم وجود مهارت­های کافی در بین برنامه­نویسان و توسعه دهندگان صنعت نرم­افزار با این دست از سیستم­ها سختی تولید و توسعه آن­ها را چندین برابر می­کند.از طرفی برای اینکه چالش­های اینگونه از سیستم­ها برای یک صرافی برخط به طور کامل شناسایی و پیاده­سازی شود نیاز به سرمایه گذاری بسیار زیادی می­باشد.

2-1-2 سیستم­تبادل برچسب سفید

پیش­از توصیف این روش در ابتدا فلسفه وجودی آن­ را به صورت مختصر شرح خواهیم داد.مفهومی تحت عنوان محصولات با برچسب سفید در دنیای تجارت وجود دارد به این صورت که یک محصول برچسب سفید، به محصولی گفته می­شود که به وسیله یک تولید کننده ایجاد شده است اما با تغییر برند تجاری آن توسط شخص دیگری به فروش می­رسد. با توجه به این توصیف یک صرافی می­تواند برای راه­اندازی سیستم صرافی خودش از سیستم­های تبادل رمزارزها که به صورت آماده هستند و به وسیله برخی شرکت­های دیگر تولید شده­اند استفاده کند. به طور کلی در این دو روش فوق یک صرافی برای تهیه یک سیستم تبادل رمزارز بایستی به چندین فاکتور توجه خاصی داشته باشد :

1. موتورهای تبدل رمزارزها به یکدیگر
2. دریافت نرخ تبدیل رمزارز به صورت برخط و در لحظه و اعمال آن برای تبدیل
3. تهیه اندوخته از پیش تعیین شده رمزارزها برای صرافی در جهت تبدیل رمزارزها به یکدیگر
4. برقراری و حفظ امنیت سرورهای تبادل رمزارزها
5. تهیه کیف­پول امن و مطمعن برای هریک از رمزارزها که صرافی مورد نظر قصد تبادل آن­ها را دارد

2-2 صرافی­های غیرمتمرکز

همانطور که در بخش 4-1 اشاره شد در صرافی­های غیرمتمرکز ما هیچ مدیریت مرکزی برای کنترل تراکنش­ها و مبادله رمزارزها با

یکدیگر نخواهیم داشت همچنین پول مبدا در ابتدا به حساب صرافی نخواهد رفت بلکه مستقیم به حساب تبدیل کننده پول خواهد رفت و سپس تبدیل کننده پول رمزارز درخواستی مشتری را به حساب آن ارسال می­کند.یکی از چالش­های اصلی در صرافی­های آنلاین ایجاد اعتماد در بین مشتری و صرافی می­باشد که در روش­های غیرمتمرکز با استفاده از سازوکارهای مختلفی سعی شده است

که این اعتماد را به وجود بیاورند.با توجه به چالش اصلی در این صرافی­ها –یعنی ایجاد حس اعتماد در مشتری-می­توان از این نقطه نظر صرافی­های متفاوت را با یکدیگر مقایسه کرد، به عبارتی نقطه تمایز ایجاد صرافی­های توزیع شده از دیدگاه ما نحوه ایجاد اعتماد و جلوگیری از دزدیده شدن رمزارز مشتری می­باشد.از همین رو ما دو دسته صرافی­های غیرمتمرکز را خواهیم داشت :

1. غیرمتمرکز مبتنی بر مفهومی تحت عنوان تبادل­های تجزیه­ناپذیر
2. غیرمتمرکز تحت کنترل یک مرکزیت مشخص

2-2-1 غیرمتمرکز مبتنی بر مفهومی تحت عنوان تبادل­های تجزیه­ناپذیر

موضوع تبادل تجزیه­ناپذیر به این مشکل برمی­گردد که دو شخص مختلف تحت نام­های علی و رضا می­خواهند دو سکه خود را به صورت برخط با یکدیگر مبادله کنند بطوری که هیچ شخص ثالث مورد اعتمادی بین آن­ها وجود نداشته باشد.یک روش تبادل تجزیه­پذیررا می­توان اینگونه بیان کرد که علی سکه خود را به رضا بدهد و رضا نیز سکه خود را به علی بدهد.اما در این میان رضا می­تواند پس از دریافت سکه علی دیگر سکه خود را به علی ندهد.پس می­توان گفت در یک تبادل تجزیه­پذیر رضا دو انتخاب دارد 1- طبق پروتکل بین علی و رضا عمل کند و سکه خود را به علی بدهد (پس از دریافت سکه علی) 2- طبق پروتکل عمل نکند و سکه خود را ندهد]5[.برای حل این مشکل راه­حل­های متفاوتی وجود دارد که برخی از آن­ها شامل

1. استفاده از یک قراردادهوشمند بین دو طرف
2. استفاده از پروتکل ارتباط بین دفترحساب­های توزیع شده (ILP)

2-2-1-1 استفاده از یک قراردادهوشمند برای تبادل

در اینجا ما با استفاده از یک قراردادهوشمند ویا با استفاده از یک مقدار تصادفی x تجزیه­ناپذیر بودن تراکنش را فراهم می­کنیم.به عنوان مثال به الگوریتم زیر دقت کنید :

A picks a random number x

A creates TX1: "Pay w BTC to <R's public key> if (x for H(x) known and signed by R) or (signed by A & R)"

A creates TX2: "Pay w BTC from TX1 to <A's public key>, locked 48 hours in the future, signed by A"

A sends TX2 to R

R signs TX2 and returns to A

1) A submits TX1 to the network

R creates TX3: "Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & R)"

R creates TX4: "Pay v alt-coins from TX3 to <R's public key>, locked 24 hours in the future, signed by R"

R sends TX4 to A

A signs TX4 and sends back to R

2) R submits TX3 to the network

3) A spends TX3, revealing x

4) R spends TX1 using x

شکل 2-1 الگوریتم اجراء روش تبادل تجزیه­ناپذیر]5[

طبق این الگوریتم در ابتدا علی ( A ) یک مقدار تصادفی x را انتخاب می­کند که با استفاده از دانستن مقدار x رضا می­تواند پول دریافتی از سمت علی در تراکنش1 ( TX1 ) را خرج کند ، درغیر اینصورت امکان خرج کردن آن سکه­ها وجود ندارد.در این الگوریتم هر طرف دو تراکنش را ایجاد می­کنند.تراکنش اول علی (TX1) که انتقال w بیت­کوین از علی به رضا است و تنها درصورتی رضا می­تواند این w بیت­کوین را خرج کند که مقدار H(x) ( هش مقدار تصادفی x ) را بداند ویا اینکه تراکنش توسط هم علی و هم رضا امضاء شود.

تراکنش دوم علی (TX2) که علی با دانستن مقدار H(x) می­تواند مقدار انتقال یافته در تراکنش TX1 را به حساب خود بازگرداند آن هم درصورت گذشت 48 ساعت پس از تراکنش TX1.تراکنش اول رضا (TX3) که مانند TX1 عمل می­کنند و تراکنش دوم نیز (TX4) نیز مانند تراکنش TX2 عمل می­کند. حالت­های مختلفی که میتواند روخ دهد در این الگوریتم به شرح زیر است :

* پیش از مرحله 1 در این الگوریتم : به دلیل آنکه هیچ تراکنشی در شبکه­های بلاکچین دو رمزارز انتشار پیدا نکرده پس بروز هرگونه مشکل در روند این الگوریتم فرآیند به پایان می­رسد.
* بین مراحل 1 و 2 : علی می­تواند با رد کردن تراکنش­ها پس از گذشت 48 ساعت پول خود را بازپس بگیرد.
* بین مراحل 2 و 3 : رضا می­تواند پس از 24 ساعت پول خود را دریافت کند درصورت بروز مشکل و همچنین علی نیز به بیش از 24 ساعت نیاز دارد تا پول خود را دریافت کند.
* پس از مرحله 3 : تراکنش به وسیله دو طرف به صورت کامل انجام شده است.علی بایستی سکه­های دریافتی از این تراکنش­ها را در 24 ساعت آینده خرج کند وگرنه رضا می­تواند پس از آن ادعای بازپس­گیری سکه­های خود را داشته باشد.همچنین رضا نیز باید تا 48 ساعت بعد سکه­های خود را خرج کرده باشد،چرا که علی نیز می­تواند پس از آن ادعای بازپس­گیری سکه­های خود را داشته باشد.

2-2-12- پروتکل ارتباط بین دفتر حساب­های توزیع شده– ILP

ILP [[13]](#footnote-13) که یکی از زیر پروژه­های هایپرلجر[[14]](#footnote-14) می­باشد با هدف انتقال ارز­ها ویا به عبارتی دیگر انتقال رمزارز­های مختلف در قالب بسته­های شبکه­ای می­باشد.در واقع در ابتدا هدف از ایجاد پروژه ILP فراهم کردن بستری برای ایجاد صرافی­های توزیع شده نبوده است.این پروتکل با این هدف ایجاد شده است که یک نرم­افزار توزیع شده[[15]](#footnote-15)  بتواند به راحتی منابع مورد نیاز خود را مانند حافظه، توان محاسباتی و ... را خریداری کند بدون هیچگونه وابستگی به دفترکل­های توزیع شده]6[ .در این پروتکل ما هیچ­گونه سرور مرکزی برای مدیریت و کنترل تراکنش­ها بین گره­ها وجود ندارد و رمزارزها ویا به عبارتی دیگر پول­ها در قالب بسته­های رمز شده از طریق شبکه به صورت امنی منتقل می­شوند]8[ .

یکی از چالش­های موجود در دنیای تکنولوژی امروز با روی کار آمدن اینترنت و ابزارها و تکنولوژی­های جدید انتقال وجه ویا پول می­باشد که در ساختار امروزه برای انتقال ارز­های مختلف به صورت بین­المللی درگیری­های بسیار زیادی وجود دارد.درواقع در سازوکار امروزی انتقال وجه در داخل یک سیستم بسیار ساده و کم هزینه می­باشد اما برای انتقال وجه بین دو سیستم مختلف به عنوان مثال تبادل دو رمزارز با یکدیگر کاری پر هزینه و سخت می­باشد.از طرفی برای تبادل دو رمزارز مختلف بایستی یک سیستم مطمعن واسط بین دو طرف وجود داشته باشد به شکلی که درخواست کننده با اعتماد کامل بتواند رمزارز خود را به حساب تبدیل کننده ارسال کند و ارز درخواست کننده توسط تبدیل کننده دزدیده نشود.

ILP با استفاده از دفترحساب­های­کل سپرده­هایی را فراهم می­کند به صورتی که درخواست کننده دارایی خود را در حالت قفل شده قرار می­دهد و تبدیل کننده با برسی صحت آن و انتقال رمزارز درخواستی ، درخواست کننده می­تواند دارایی قفل شده درخواست کننده را از حالت قفل خارج کند و پول خود را دریافت کند.ILP با افزوده شدن تعداد اتصال­دهنده­ها[[16]](#footnote-16) و دفترچه­های توزیع شده بیشتر به داخل شبکه سرعت تبادل رمزارزها افزایش می­یابد و همچنین باعث می­شود که فرآیند تبادل رمزارزها تسهیل می­یابد چرا که با زنجیره شدن اتصال­دهنده­ها به یکدیگر این فرآیند کم هزینه­تر و سریعتر انجام می­ شود.با توجه به اهمیت این پروتکل شرح کاملی از ساختار و معماری آن را در بخش بعد خواهیم داشت.

2-2-2 غیر متمرکز تحت کنترل یک مدیریت مشخص

همانگونه که پیش از این اشاره شد در بخش 2-2 یکی از چالش­های اصلی برای تبادل رمزارز­ها ویا به عبارتی کلی­تر برای تبادل ارز در دنیای دیجیتال ایجاد اعتماد در بین درخواست کننده تبدیل و تبدیل کننده می­باشد.به طور کلی در دنیای اقتصادی تبدیل­کنندگان را تحت عنوان صرافی­ها می­دانستیم پس به عبارتی ایجاد اعتماد بایستی بین درخواست کننده تبدیل و صرافی ایجاد شود تا در زمانی که درخواست­ کننده ارز خود را ( چه رمزارز و چه ارزهای رایج دولتی) به حساب صرافی انتقال می­دهد پس از آن ارز درخواست کننده توسط صرافی دزدیده نشود.

در بخش 2-1 برای رفع این مشکل از مفهومی تحت­عنوان انتقال تجزیه­ناپذیر استفاده کردیم که در آن هیچ­گونه اعتمادی دربین درخواست کننده تبدیل و تبدیل­ کننده وجود نداشت و با استفاده از ساز و کار­هایی هم­چون قراردادهای­هوشمند ویا رمزنگاری امکان بروز هرگونه تخلف را کم می­کردیم.در این بخش قصد داریم تا تبادلات برخط به صورت توزیع شده را به نحوی تشریح کنیم که تبدیل­کنندگان مورد تایید یک سازمان مشخص می­باشند پس می­توان گفت که با تایید شدن تبدیل کنندگان دیگر چالش ایجاد اعتماد بین درخواست کننده و تبدیل­ کننده وجود ندارد اما همچنان به صورت توزیع شده عملیات تبادل ارز انجام می­شود. در ادامه چند سیستم اجرائی دارای این ویژگی را معرفی خواهیم کرد.

2-2-2-1 شبکه تبادل ارز Stellar

Stellar یک شبکه توزیع شده برپایه زنجیره­بلوکی است که به وسیله مجموعه از سرور­های خود این شبکه ایجاد می­شود.در این شبکه هریک از سرورها ویا به عبارتی دیگر گره­های شبکه هرکدام یک کپی از دفترحساب توزیع شده شبکه را نگهداری می­کنند بطوری که در این دفترحساب­ توزیع شده علاوه بر توان ذخیره تراکنش­های انتقال ارز در داخل شبکه توان ذخیره­سازی درخواست تبادل ارز توسط کاربران را نیز دارا می­باشد. سرورهای شبکه بلاکچینی Stellar هم توان ثبت تراکنش­های انتقال درون شبکه را در دفترحساب توزیع شده دارند و هم توان ثبت درخواست­های تبدیل ارز را دارند]12[.در این شبکه بلاکچینی گره­ها با استفاده از الگوریتم اجماع FBA (Federated Byzantine Agreement) استفاده می­کنند]13[. این الگوریتم که در واقع نوع تغییر یافته الگوریتم BFT (Byzantine Fault Tolerance) می­باشد]14[ این مزیت را دارد که به تعداد گره­های شبکه محدود نمی­باشد و درواقع می­توان گفت که در این الگوریتم ما با این مشکل رو به رو نمی­شویم که اگر تعداد گره­های شبکه بسیار زیاد شوند شبکه در اجماع دچار مشکل شود.گره­های شبکه با استفاده از این الگوریتم اجماع بر روی تراکنش­های اعلام شده در داخل شبکه به توافق می­رسند.با توجه به توضیحات داده شده نحوه تبادل ارز ( چه رمزارز و چه ارزهای دیگر) در این شبکه به صورت زیر می­باشد که شخصی درخواست تبدیل دلار به یورورا به داخل شبکه اعلام می­کند(به سرورها اعلام می­کند) در بین سرورهای شبکه عمل اجماع هر 2-5 ثانیه یک بار انجام می­شود.پس از آن درخواست تبدیل ارز داده شده در داخل دفترحساب کل توزیع شده ثبت می­گردد و موضوع مورد توجه در این شبکه این است که اعضای داخل شبکه موجودی ویا دارایی خود را بایستی به وسیله یک رابط ویا لینک ارتباطیاثبات کند.

این رابط­ها را می­توان بانک­ها دانست که موجودی دلار درخواست کننده را دارند و به دفترحساب­ توزیع شده اعلام می­کنند.پس از آن شخص دیگری نیز اعلام تبادل یورو با دلار را در شبکه اعلام می­کند پس از آن به وسیله سرور­هایی که در شبکه Stellar قرار دارند این عمل تبادل انجام می­شود.چند نکته در این جا به وجود می­آید که اولا نقش رابط­ها در کلیت این سیستم چه می­باشد ، ثانیا چرا عمل تبادل ارزها بایستی در این شبکه انجام شود و ثالثا رابط­ها با شبکه چگونه ارتباط دارند.در پاسخ به این موارد بایستی ابتدا بیان کرد که رابط­ها در شبکه Stellar دو عمل مشخص را انجام می­دهند:

* آن­ها موجود کاربران شبکه را در خود نگهداری می­کنند و در دفتر حساب توزیع شده شبکه Stellar آن را در حساب کاربر اعلام و ذخیره می­کنند.
* همچنین کاربر می­تواند عمل تصویه­حساب را با رابط­ها انجام دهد یعنی پس از تبادل ارز و دریافت آن ارز به حساب کاربر که به وسیله رابط تایید شده است انتقال پیدا می­کند و کاربر برای دریافت آن می­تواند با رابط تصویه حساب کند.

درخصوص پاسخ به سوال دوم می­توان اینگونه توصیف کرد به­طور مثال در سیستم­های قبلی برای آنکه دو شخص که رابط­ آن­ها PayPal می­باشد عمل تبادل را انجام دهند بایستی هر دو در PayPal حساب داشته باشند تا بتوانند عمل تبادل ارزی را انجام­دهند، اما با استفاده از این سیستم می­توان گفت اشخاص با داشتن حساب در سیستم­ها ( رابط­ها)ی متفاوت می­توانند با یادیگر همکاری کنند.از طرفی رابط­ها در شبکه Stellar به وسیله خود شبکه ثبت می­شوند و مورد تایید شبکه Stellar می­باشند]15[.

2-2-2-2 شبکه Transledger

تا کنون ما روش­های متفاوتی را برای رمزارزها مشاهده کرده ایم که در هرکدام ما تنها یک موجودیت مشخص را از حسابی به حساب دیگر انتقال می­دادیم.در این میان هیچ رمزارز واسط دیگری به وجود نمی­آمد بلکه تنها رمزارزهای مبدأ و مقصد تراکنش به نحوی توسط واسط­ها انتقال پیدا می­کرد.در این بخش عمل انتقال به نحوی کاملا متفاوت انجام می­شود به طوری که وقتی رمزارزی مانند بیت­کوین بخواهد از حساب شخصی به نام علی انتقال پیدا کند و تحت رمزارز دیگری مانند اتریوم در حساب مقصد ( به عنوان مثال رضا ) قرار بگیرد به وسیله رمزارز معادل با ارزش بیت­کوین که درواقع نقش نمایندگی بیت­کوین را در حساب رضا دارد قرار می­گیرد.

در اینجا چون مبدأ بیت­کوین است پس نماینده بیت­کوین در حساب رضا را –iبیت­کوین می­نامیم.-iبیت­کوین می­تواند بعدا به اتریوم ویا حتی مجدد به بیت­کوین تبدیل شود و ارزش مالی آن با ارزش یک سکه بیت­کوین هیچ تفاوتی ندارد.در واقع می­توان گفت در شبکه Transledger فرآیند تبدیل یک رمزارز به رمزارز دیگر اتفاق می­افتد و این فرآیند در شبکه بلاکچینی Transledger ثبت می­گردد.

یکی از نکات قابل توجه و بسیار مهم در این شبکه این است که زمانی که یک تراکنش از شبکه بیت­کوین به شبکه اتریوم بخواهد اتفاق بیفتد پس از انتقال بیت­کوین از حساب فرستنده به شبکه Transledger یک سکه معادل با بیت­کوین در شبکه Transledger برای شخص انتقال دهنده رزرو میگردد و پس از آن ، آن سکه نماینده به حساب مقصد منتقل می­شود.در این حالت ما برای انتقال یک رمزارز از یک شبکه بلاکچینی به یک شبکه کاملا متفاوت مانند DAGویا شبکه بلاکچینی متفاوت ،هیچ محدودیتی نخواهیم داشت وعملیات به سادگی انجام می­شود.اما دلیل آنکه این شبکه را ما تحت عنوان صرافی غیرمتمرکز با کنترل متمرکز می­نامیم به این دلیل است که در این شبکه هرچند سازوکار انتقال و فرآیند ثبت تراکنش به وسیله یک شبکه بلاکچینی انجام می­شود و در یک دفترحساب توزیع شده تحت عنوان دفترحساب انتقال[[17]](#footnote-17)  ثبت می­شوند اما انتقال یک رمزارز به این شبکه به وسیله گره­های مشخص شده این شبکه اتفاق می­افتد که نقش ناظر برشبکه را ایفا می­کنند.

نحوه انتقال در این شبکه

پیش از توصیف یک سناریو از نحوه کارکرد این شبکه باید توجه کرد که تا به این لحظه شبکه Transledger تنها توان تبادل

شیش رمزارز را با یکدیگر دارد و رمزارز هفتم نیز درحال پیاده­سازی می­باشد.این رمزارز­ها شامل :

* بیت­کوین
* اتریوم
* لایت­کوین 1
* ریپل2
* استلار3
* بیت­کوین کش4
* EOS

می­باشد.این رمزارزها 80% نقل و انتقالات کل رمزارز­های موجود را در خود دارند ،یعنی این رمزارز­ها جزو ده رمزارز برتر دنیای ارزهای دیجیتال هستند]15[.

حال فرض­ می­کنیم که شخصی به نام علی قصد تبدیل دو بیت­کوین به چهار ریپل را دارد.(سناریو به طور فرضی است و ارزش دقیق آن­ها در نظر گرفته نشده است) ابتدا علی دو بیت­کوین خود را به شبکه Transledger انتقال می­دهد پس از ثبت شدن تراکنش انتقال دو بیت­کوین به شبکه Transledger در دفترحساب توزیع شده بیت­کوین کنترل­کننده رویداد5 در شبکهTransledger فراخوانی می­شود و یک تراکنش برای علی در شبکه ثبت می­شود و معادل با دو بیت­کوین علی دو –iبیت­کوین برای آن به حالت رزور در می­آید.حال علی قصد انتقال این دو –iبیت­کوین به شخص دیگری به نام رضا را دارد.عملیات انتقال توسط علی انجام می­شود و در شبکه Transledger دو –iبیت­کوین به حساب رضا منتقل می­شود حال رضا می­تواند این دو –iبیت­کوین را خرج کند ویا معادل با ارزش آن­ها (که درواقع هم ارزش دو بیت­کوین واقعی هستند)رمزارز دیگر مانند ریپل ویا حتی خود بیت­کوین را دریافت کند.

موضوعی که در اینجا بسیار اهمیت دارد این است که اول Transledger با شبکه­های تبادل رمزارز موجود متفاوت است به طوری که وقتی به ازای دو بیت­کوین دو –iبیت­کوین ایجاد می­شود می­توان بازهم این دو –iبیت­کوین را نیز تجزیه کرد و با آن­ها تراکنش انجام داد.ثانیا این نحوه انتقال با کانال­های انتقالی که در شبکه­های دیگری مانند Sidechain وجود دارد کاملا متفاوت است و به عبارتی دیگر ما دراینجا کانال ارتباطی بین دو طرف تبادل ایجاد نمی­کنیم بلکه یک انتقال در شبکه Transledger انجام می­دهد]17[.

2-2-3 تشریح کامل پروتکل ILP

همانگونه که در بخش 2-2-1 اشاره شد ILP یک پروتکل مناسب برای تبادل رمزارز­ها می­باشد به طوری که در یک شبکه توزیع شده بتوان بدون داشتن اعتماد به گره­های دیگر عمل تبادل رمزارز را انجام دهیم.در این بخش شرح کاملی از ساختار این پروتکل خواهیم داشت تا با معماری و جزئیات آن بهتر آشنا شویم.

2-2-3-1 فرستنده،گیرنده ،اتصال­دهنده

زمانی که دو شخص(فرستنده و گیرنده)بخواهند به یکدیگر پول ارسال کننده فرستنده پول را ارسال و گیرنده پول را دریافت می­کند.این حالت درصورتی است که فرستنده و گیرنده در یک سیستم قرار داشته باشند.حال اگر فرستنده در یک سیستم (در یک

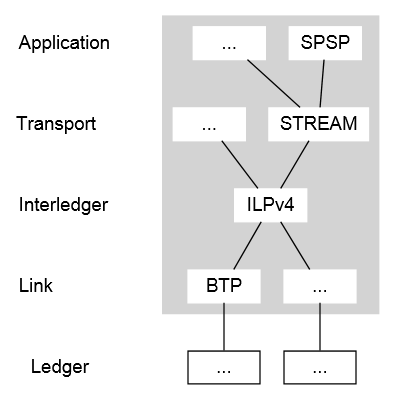
دفترحساب توزیع شده)و گیرنده نیز در یک سیستم دیگر (در یک دفترحساب توزیع شده متفاوت از فرستنده) قرار داشته باشد بایستی در این بین یک ویا چند اتصال­دهنده وجود داشته باشد تا پول را از فرستنده دریافت و به گیرنده ارسال کند.



شکل 2-2 نحوه اتصال گره­ها در ILP ]7[

براساس تصویر فوق می­توان گفت که اتصال­دهندگان پول­ها را از فرستنده به گیرنده ارسال می­کنند که این اتصال­دهندگان می­توانند نقش یک یک فرستنده ویا یک گیرنده و یا یک اتصال­دهنده را در شبکه ایفا کنند.اتصال­دهندگان برای انجام انتقال رمزارزها از فرستنده به گیرنده کارمزد دریافت می­کننده به همین منظور در شبکه ILP برای انتقال بسته­های پول بین اتصال­دهندگان رقابت به وجود می­آید.

2-2-3-2 لایه­های پروتکل



شکل 2-3 معماری کلی پروتکل ILP ]7[

Ledger

این لایه که بالاترین لایه در مدل ILP می­باشد مشخص کننده سیستم­های پرداختی است که اتصال­دهندگان آن­ها را به هم متصل می­کنند.در واقع این لایه می­تواند یک دفترحساب توزیع شده باشد ،یک بانک ویا هر سیستم پرداخت دیگری باشد.نکته قابل توجه نیز این است که پیش از انجام فرآیند پرداخت هر کدام از شرکت­کنندگان بایستی محدودیت­های خود را از قبیل این که چه میزان پول را می­تواند به صورت قرض قرار دهد و همچنین چه مدت می­تواند آن را در این حالت نگهداری کند ویا میزان پولی که می­خواهند انتقال دهند

می­باشد.

Link

همتایان[[18]](#footnote-18) در شبکه ILP نیاز به یک کانال ارتباطی امن با یک­دیگر دارند و از طرفی دفترحساب­های توضیع شده موجود هیچ راهکاری برای پیاده­سازی ارتباط دو طرفه تایید صلاحیت شده2 بین کاربران دارای حساب در آن دفترحساب­های توزیع شده نداشته­اند.همچنین در ILP ما نیاز به داشتن چنین کانال ارتباطی داریم. یک پروتکل لایه اتصال[[19]](#footnote-19) به طور معمول اطلاعات فوق را در شبکه ILP انتقال می­دهند :

* بسته­های داده­ای پروتکل ILP
* انتقال اطلاعات مانده­های واریز نشده

به عنوان مثال پروتکل انتقال Bilateral یک مثال برای این لایه می­باشد.

Interledger

پروتکل Interledger در واقع هسته اصلی شبکه ILP می­باشد که بسته­های گره­ها در شبکه به صورت زنجیره­ای به وسیله این لایه انتقال پیدا می­کنند.این پروتکل با هرنوع رمزارز ویا ارز دیگری سازگار می­باشد.در این لایه ما مقدار انتقالی­ را مشخص می­کنیم و همچنین عمل آدرس دهی نیز در این لایه انجام می­شود.در عمل آدرس دهی ،مشخص کردن گره­های میانی ویا به عبارتی دیگر اتصال­دهندگان نیز به وسیله این لایه می­باشد.در این لایه بسته­هایی که منطقل می­شوند با شرط­های مشخص شده توسط گیرنده

رمزنگاری شده­اند.زمانی که گیرنده بسته خود را دریافت کند پس از آن روند آزادسازی ارزها را برای دیگر گره­ها انجام می­دهد تا فرآیند انتقال به صورت کامل انجام شود.نکته قابل توجه این است که ،این لایه یک سطح انتضاعی لایه­های بالایی و پایینی ایجاد می­کند و این موضوع باعث می­شود که در این لایه تنها یک پروتکل بتواند قرار بگیرد.

Transport

لایه انتقال یک ارتباط نقطه­به­نقطه[[20]](#footnote-20)را بین فرستنده و گیرنده ایجاد می­کند به­طوری که در این لایه اتصال­دهندگان حظور ندارند و این ارتباط صرفا بین فرستنده و گیرنده ایجاد می­شود.در این ارتباط دو طرفه ما موراد زیر را مشخص می­کنیم که در لایه Interledger مورد استفاده قرار می­گیرند :

* مشخص کردن پیش­شرط­ها فرآیند انتقال
* گروه­بندی و بازیابی بسته­ها تا بتوانند نتایج درخواه را بدست آورند
* مشخص کردن نرخ تبدیل پول­های انتقالی
* رمزگذاری[[21]](#footnote-21) و رمزگشایی[[22]](#footnote-22) داده­ها

به عنوان مثال یکی از پروتکل­هایی که در این لایه می­تواند فعالیت کند پروتکل STEAM می­باشد.

Application

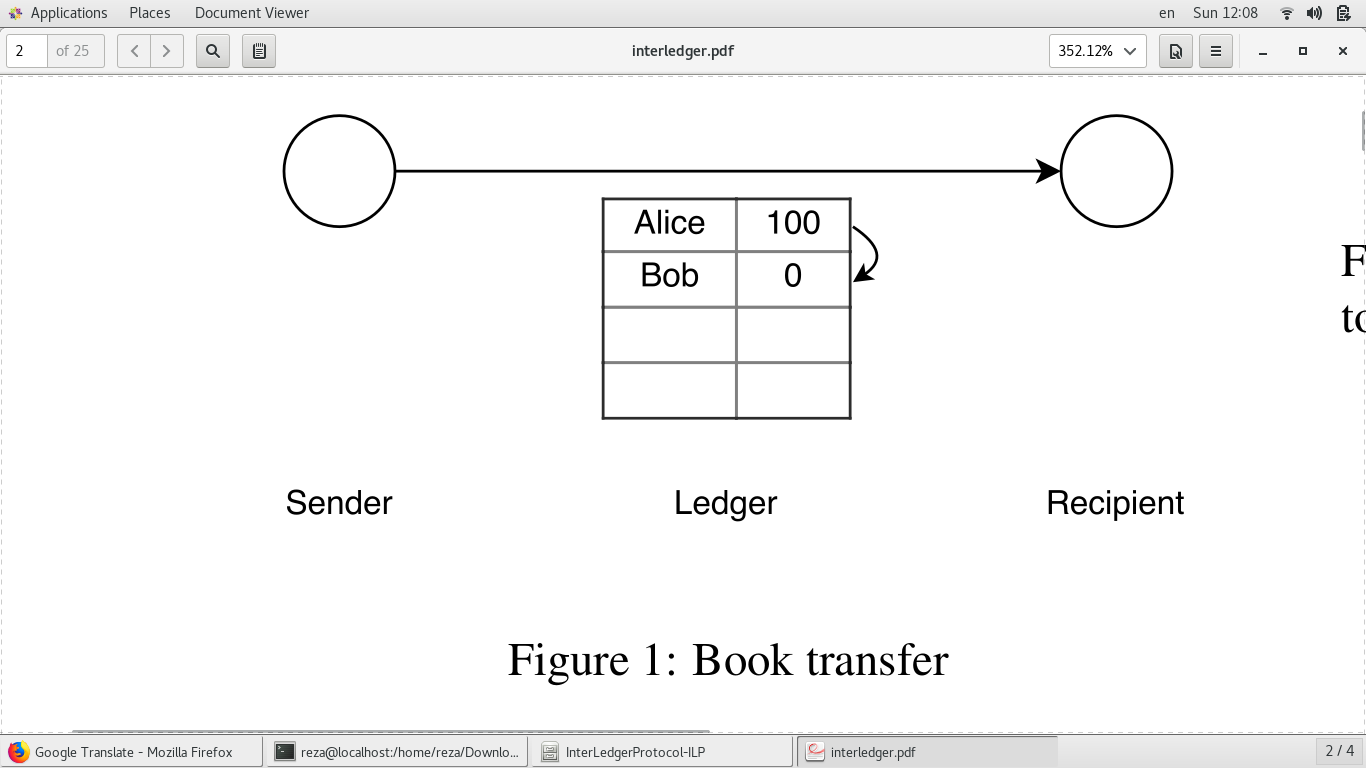
در این لایه تنها موارد غیر ضروری و پیش شرط­هایی که بایستی قبل از شروع کلی فرآیند مشخص شوند تعیین می­شوند به عنوان مثال مواردی همچون :

* مقصد انتقال کجا می­باشد
* چه میزان بایستی انتقال پیدا کند

و از این دست موارد]4[.

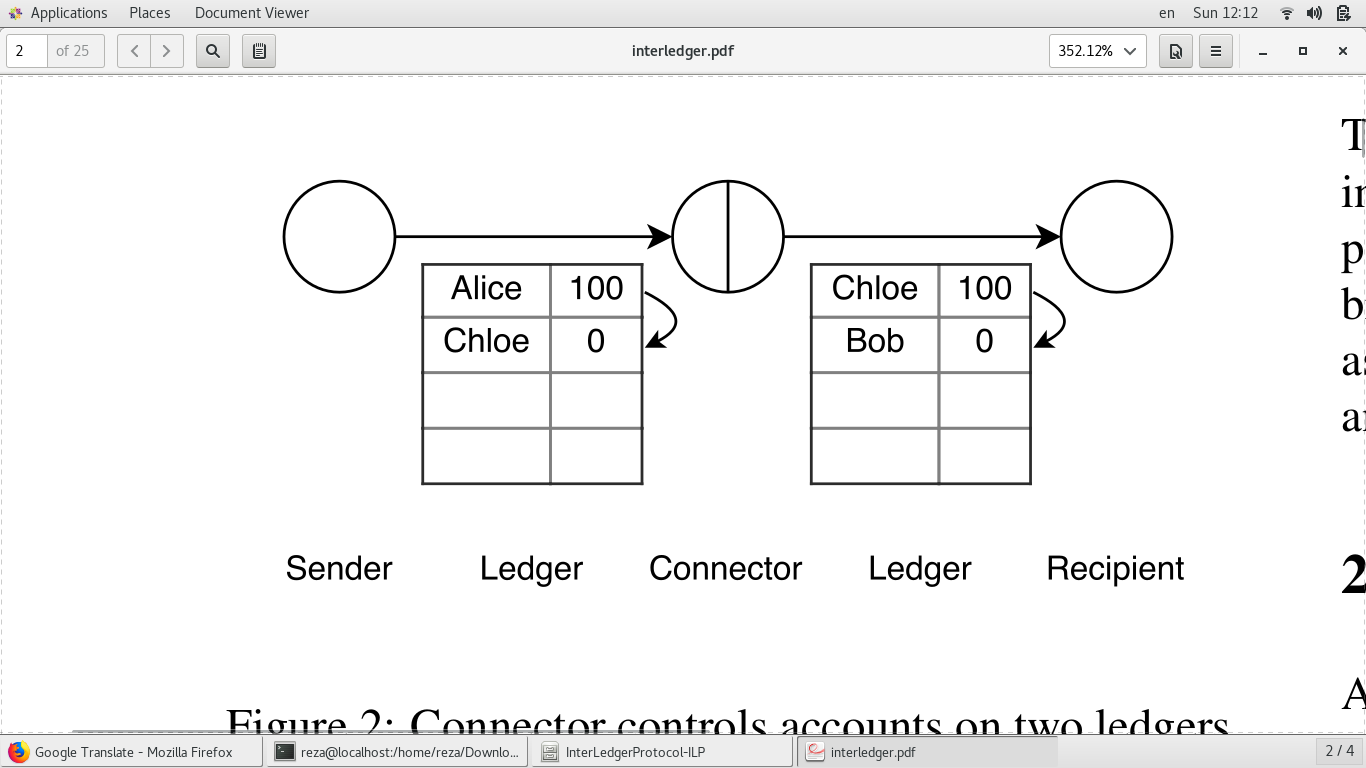
2-2-3-3 فرآیند انتقال

همان­گونه که در شکل 2-3 آمده است و قبلا نیز اشاره شد انتقال بین دو حساب در یک سیستم واحد به راحتی و بدون هیچ واسط میانی انجام می­شود.



شکل 2- 4نحوه انتقال ارز در دفترحساب توزیع شده ]8[

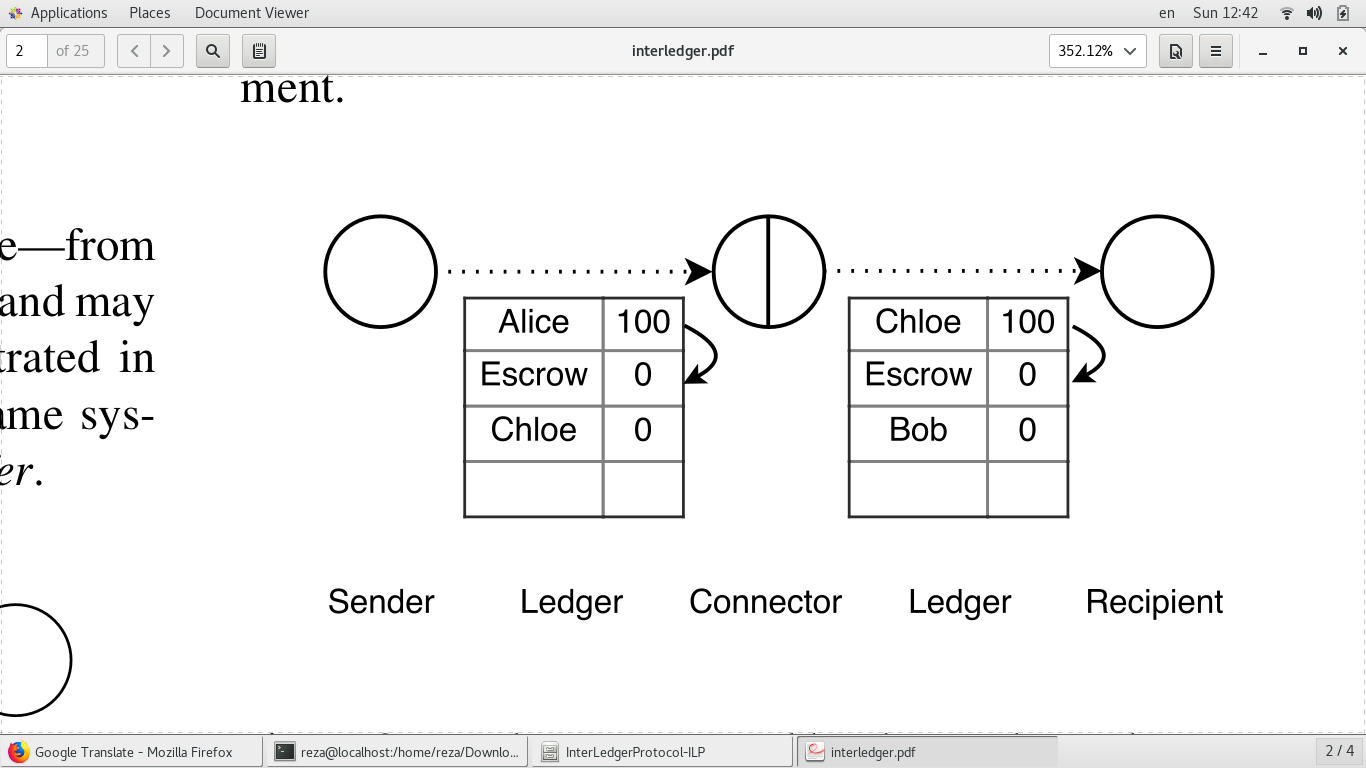
اما در صورتی که سیستم­ها متفاوت باشند یک اتصال­دهنده می­تواند باعث سرعت بخشیدن به فرآیند انتقال بشود.بطور کل یک اتصال­دهنده را می­توان یک کنترل­کننده انتقالات بین دو دفترحساب­توزیع شده دانست.همانگونه که در شکل 2-4 آمده است در ابتدا فرستنده در دفترحساب توزیع­شده اول ،پول خود را به حساب اتصال­دهنده ارسال می­کند و پس از آن اتصال­دهنده با دریافت آن پول ،پول خود را در دفترحساب توزیع شده دیگر به حساب گیرنده انتقال می­دهد.



شکل 2-5 نحوه انتقال ارز بین دو دفتر حساب توزیع شده ]8[

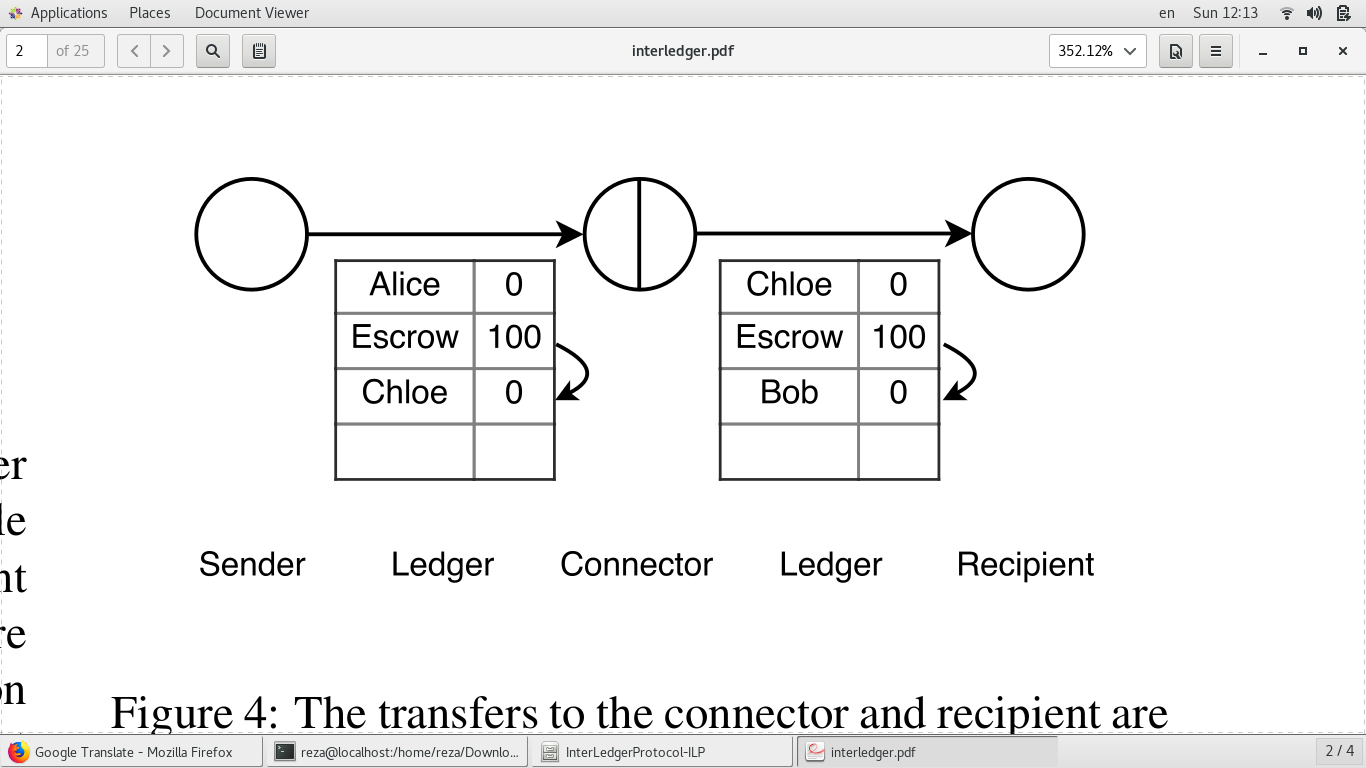
اما مشکل اصلی در این روش انتقال این مشکل وجود دارد که فرستنده بایستی به اتصال دهنده­ اعتماد کامل را داشته باشد تا معادل پول دریافتی از فرستنده را در دفترحساب توزیع شده دیگر به حساب گیرنده ارسال کند.همین چالش باعث به وجود آمدن سازمان­هایی برای انتقال­های مالی بوده و همچنین باعث به وجود آمدن شکاف­هایی در سیستم­های مالی شده است.سپرده­گذاری به وسیله

دفترحساب­های توزیع شدهراه­حلی برای این موضوع است که در انتقال­ بسته­ها در ILP تضمین می­کند که تنها زمانی که اتصال­دهنده رسید انتقال پول به گیرنده را بازپس دهد سپرده قرارگرفته در دفترحساب توزیع شده به اتصال­دهنده منتقل می­شود.



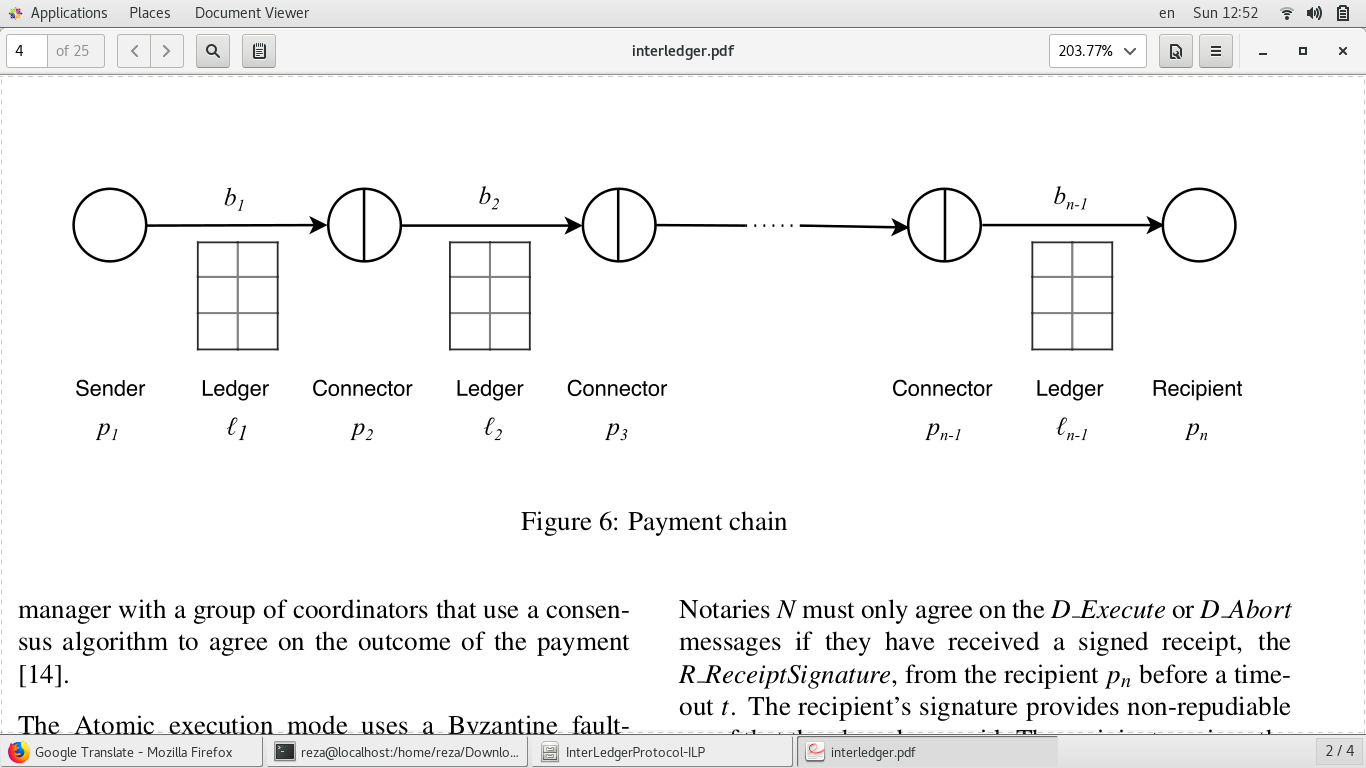
شکل 2-6 نحوه انتقال ارز بین دو دفتر حساب توزیع شده به وسیله پروتکل ILP ]8[

براساس شکل 2-5 ابتدا پول فرستنده ( Alice ) به حالت سپرده[[23]](#footnote-23) می­رود.پس از اثبات این موضوع توسط دفترحساب­توزیع شده، اتصال­دهنده (Chloe) پول را در دفترحساب­توزیع شده دیگر به حالت سپرده درمی­آورد و این موضوع به وسیله دفترحساب­توزیع شده برای گیرنده (Bob) اثبات می­شود.



شکل 2-7 انتقال ارز از حالت سرمایه­گذاری شده به حساب کاربران در پروتکل ILP ]8[

پس از انجام فرآیند توسط اتصال­دهنده و دفترحساب­ها پول­های سپرده­شده را به حساب گیرنده و اتصال­دهنده منتقل می­کنند.این گام از فرآیند به صورت تجزیه­ناپذیر می­باشد،به عبارتی دیگر نتیجه این مرحله یا انجام کامل فرآیند ویا شکست فرآیند می­باشد.نکته حائز اهمیت در این فرآیند این است که میتوان در یک فرآیند انتقال چندین اتصال دهنده وجود داشته باشد و این انتقال از طریق چند اتصال­دهنده صورت بگیرد، همانند شکل 2-7.



شکل 2-8 نحوه بهم زنجیر شدن اتصال­دهندگان در پروتکل ILP ]8[

2-2-3-4 انواع گره­­ها

یک پروتکل پرداخت کاملا امن نمی­تواند به هیچ یک از شرکت­کنندگان خود اعتماد کند تا امنیت را برقرار کنند، بلکه خود پروتکل بایستی به تنهایی توانایی مدیریت و کنترل فرآیند را در برابر حوادثی همچون بروز نقص به­طور بلغوه ،عملکرد­های مخرب ویا اهداف شخصی کاربران داشته باشد.به همین منظور در این پروتکل برای دسته­بندی گره­ها از مدل BAR ( Byzantine , Altruist , Rational )که در ]6[ توضیع داده­شده است استفاده می­کنیم.براساس این مدل شرکت­کنندگان در این پروتکل ممکن است براساس هر اتفاقی همچون بروز نقص در آن­ها ویا اهداف سودجویانه بخواهند از پروتکل سرپیچی کنند،با این وجود ما در این پروتکل تمامی شرکت­­کنندگان را به نحوی در نظر می­گیریم که تمامی آن­ها از نوع Byzantine ویا Rational هستند. در این پروتکل ما برای مشکل Byzantine fault tolerance مربوط به دفترحساب­های­­ کل­ توزیع شده هیچ سازوکاری را در نظر نخواهیم گرفت چرا که در هنگام پیاده­سازی دفترحساب­های کل توزیع شده می­توان برای این مشکل پیش­بینی­های لازم را در نظر گرفت.

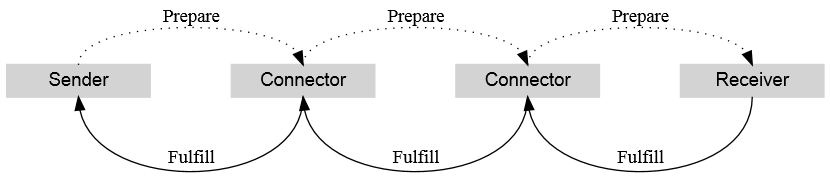
طبق عملکرد این پروتکل می­توان گفت فرستنده درخواست انتقال تبادل رمزارز تنها زمانی به انتقال­دهنده اعتماد می­کند که پول را انتقال داده است که رسید دریافت پول از سمت گیرنده را به وسیله انتقال­دهنده دریافت کند همچنین این شرط نیز وجود دارد که این رسید دریافتی اولا تکراری نباشد و ثانیا توسط انتقال­دهنده جعل نشده باشد تنها راه اطمینان برای این موضوع رمزنگاری[[24]](#footnote-24) این رسید به وسیله دفترحساب­های کل توزیع شده می­باشد.می­توان این­گونه بیان کرد که رمزنگاری یکی از راه ساده برای پاسخ­گویی به این مشکل می­باشد]5[.

2-2-3-5 بسته­های پروتکل ILP

در این بخش ما انواع بسته­های موجود در این پروتکل برای انجام فرآیند انتقال را تشریح میکنیم.به­طور کلی می­توان گفت در این پروتکل ما سه نوع بسته خواهیم داشت که شامل بسته­های :

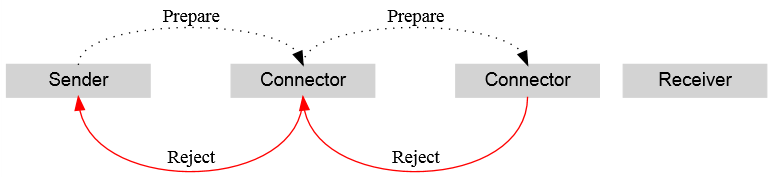
* بسته آماده­سازی
* بسته انجام شدن فرآیند
* بسته رد شدن فرآیند

که به ترتیب هرکدام از این بسته­ها مربوط به پیغام­های درخواست، پاسخو بروزخطامی­باشند.در این پروتکل شمای کلی انتقال بسته­ها به این صورت می­باشد که اتصال­دهندگان بسته­های درخواست را برای فرستنده به گیرنده ویا اتصال­دهنده دیگر انتقال می­دهند و در پاسخ بسته­های پاسخ ویا بروزخطا را تحت هرشرایطی به فرستنده برمی­گردانند که نحوه انتقال در تصاویر 2-8 و 2-9 توصیف شده است.



شکل 2-9 نحوه انتقال پیام های درخواست و انجام شدن در پروتکل ILP ]7[

با توجه به شکل 2-8 فرآیند انتقال با موفقیت انجام شده است به طوری که درخواست­ ارسالی از سمت فرستنده با موفقیت به گیرنده رسیده است و درپاسخ گیرنده پاسخ موفقیت­آمیز بودن (انجام­شدن فرآیند) را به فرستنده ارسال کرده است و در این میان تمامی اتصال­دهندگان وظایف خود را به درستی انجام داده­اند.



شکل 2-10 نحوه انتقال پیام­های درخواست و رد پیام در پروتکل ILP ]7[

با توجه به شکل 2-9 نیز فرآیند ارسال درخواست از سمت ارسال­کننده در دومین اتصال­دهنده به دلیلی همچون بروز مشکل در اتصال دهنده ویا رد کردن درخواست ارسال­کننده رد شده است و پاسخ رد شدن درخواست به فرستنده بازگشته است]9[.

فصل سوم

جمع­بندی و نتیجه­گیری پایانی

در فصل دوم ما روش­های کلی برای ایجاد یک صرافی­ برخط را توصیف کردیم.در حالت متمرکز مهم­ترین چالش این است که صاحبان صرافی باید برای آن­که بتوانند تبادلات بین حداقل شش رمزارز برتر دنیای ارزهای دیجیتال را انجام دهند بایستی در ابتدا یک اندوخته از پیش تأیین شده­ای از هر یک از رمزارزها داشته باشند ، همچنین برای تولید نرم­افزار تبادل رمزارزها نیز هزینه­های بسیار زیادی را بایستی پیرداخت کنند ویا اینکه از روش برچسب سفید برای انجام این امر استفاده کنند که در اینجا بایستی به سازمان ارائه­دهنده این نرم­افزارها اعتماد بسیار زیادی داشت.

در روش غیرمتمرکز مهم­ترین چالش برای تبادل در این موضوع مشخص می­شد که چگونه فرآیند تبادل بین دو شخص را مدیریت کنیم به نحوی که اولا هیچ نظارت مرکزی بر این فرآیند نباشد و ثانیا دو طرف هیچ شناختی از یکدیگر نداشته باشند.برای حل این موضوع نیز دو روش کلی وجود خواهد داشت یکی استفاده از مفهوم تبادل تجزیه­ناپذیر که پروتکل ILP یک مثال از این مفهوم به حساب می­آمد ویا استفاده از ناظران تاییده شده­ای که توسط راه­اندازان شبکه تبادل رمزارز تایید شده­اند، که در اینجا نیز روش­های پیاده­سازی شده توسط Stellar ویا Transledger نمونه­هایی از این دست بودند.اما موضوع مطرح در این بخش این است که در پروتکل ILP ما نیاز به محاسبات رمزنگاری زیادی خواهیم داشت که این امر باعث تاخیر بسیار زیاد در فرآیند کلی پروتکل می­شود و این موضوع یک چالش بسیار مهم می­باشد.

از طرفی دیگر در روش­های ارائه شده توسط Stellar ما از سطح مفهوم توزیع­شدگی فاصله می­گیریم چرا که در اینجا رابط­ها شبکه Stellar و کاربران درخواست­کننده تبادل مراکز تایید شده از سمت Stellar می­باشد. پس به عبارتی می­توان گفت که رابط­ها

بایستی با مدیریت مرکزی این شبکه همکاری داشته باشند و این امر حریم­خصوصی کاربران را برای انجام آزادانه تبادلات مالی به خطر می­اندازد.حتی در شبکه Transledger نیز از آنجایی که به ازای هر کاربر یک توکنمعادل با توکن ارسالی کاربر ایجاد شده و به وسیله آن تبادلات و نقل انتقالات صورت می­گیرد پس خود شبکه Transledger نظارت کاملی بر این فرآیند­ها دارد و می­تواند به راحتی تراکنش­های کاربران را ردیابی کند و تشخیص­دهد که هر کاربر چه فعالیت­هایی را انجام داده است.و این موضوع مجدد حریم­خصوصی کاربران را به خطر می­اندازد.چالش دیگری که در کل روش­ها وجود دارد این است که اندوخته مالی تبدیل کنندگان از کجا فراهم می­شود، به عبارتی دیگر اتصال­دهندگان بایستی این اندوخته را از قبل داشته باشند ویا اینکه با اضافه شدن به شبکه این اندوخته را بدست می­آورند (به وسیله توکن­هایی که شبکه به آن­ها نسبت می­دهد). موضوع دیگر بر سر زمان ثبت تراکنش­ها می­باشد که در تمامی روش­ها بسیار چشم­گیر می­باشد.به عنوان مثال در شبکه بیت­کوین برای ثبت یک تراکنش زمانی بین یک ساعت تا یک روز ممکن است نیاز باشد حال آن­که برای ثبت همان تراکنش در شبکه اتریوم شاید به زمانی کمتر از ده ثانیه نیاز باشد.برای آنکه اطمینان حاصل کنیم که تراکنش کاملا در شبکه ثبت شده است ویا خیر و چه اشکالاتی در روند اجراء این روش­ها مثل پروتکل ILP ایجاد می­شود همچنان جای ابهام وجود دارد و نیاز به تحقیقات بیشتر دارد.

منابع

1. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. and Rimba, P., 2017, April. A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE International Conference on Software Architecture (ICSA)* (pp. 243-252). IEEE.
2. Corbet S., Meegan A., Larkin C., Lucey B., Yarovaya L., Exploring thedynamic relationships between cryptocurrencies and other financial assets. Economics Letters(2018), <https://doi.org/10.1016/j.econlet.2018.01.004>
3. Li, X. and Wang, C.A., 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems*, *95*, pp.49-60.
4. Wikipedia, the free encyclopedia (21 May 2019). “White-label product”. [Online]. Available: <https://en.wikipedia.org/wiki/White-label_product> [Accessed: July, 16, 2019].
5. Bitcoin Wiki (21 February 2019). “Atomic swap”. [Online]. Available: <https://en.bitcoin.it/wiki/Atomic_swap> [Accessed: July, 16, 2019].
6. <https://medium.com/xpring/interledger-how-to-interconnect-all-blockchains-and-value-networks-74f432e64543>
7. Interledger W3C Community Group (2018). ”Interledger Architecture”. [Online]. Available: <https://interledger.org/rfcs/0001-interledger-architecture/> [Accessed: July, 16, 2019].
8. Thomas, Stefan, and Evan Schwartz. "A protocol for interledger payments." URL https://interledger. org/interledger. pdf (2015).
9. Aiyer, Amitanand S., et al. "BAR fault tolerance for cooperative services." *ACM SIGOPS operating systems review*. Vol. 39. No. 5. ACM, 2005.
10. Interledger W3C Community Group (2018). ”Interledger Protocol V4”. [Online]. Available: <https://interledger.org/rfcs/0027-interledger-protocol-4/> [Accessed: July, 16, 2019].
11. Stellar Development Foundation (2019). ”Stellar Basic - Major Stellar Concepts”. [Online]. Available: <https://www.stellar.org/how-it-works/stellar-basics/#how-it-works> [Accessed: July, 16, 2019].
12. Mazieres, D., 2015. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, p.32.
13. Castro, M. and Liskov, B., 1999, February. Practical Byzantine fault tolerance. In *OSDI* (Vol. 99, No. 1999, pp. 173-186).
14. Stellar Development Foundation (2019). ”Stellar Explainers”. [Online]. Available: <https://www.stellar.org/how-it-works/stellar-basics/explainers/#Ledger> [Accessed: July, 16, 2019].
15. <https://medium.com/interblockchain-io/we-are-now-transledger-d3ea4a84a16f>
16. Interblockchain Lab Inc.: UNLOCK COINS FROM THEIR SILOS. URL <https://transledger.io/whitepaper.pdf> (September 9,2018)
17. Interblockchain Lab Inc.: The InterBlockchain Architecture. URL <https://transledger.io/The_Interblockchain_Architecture.pdf> (2018)
18. Interledger W3C Community Group (2018). ” Relationship between Protocols”. [Online]. Available: <https://interledger.org/rfcs/0033-relationship-between-protocols/> [Accessed: July, 16, 2019].

1. 1- Online exchange [↑](#footnote-ref-1)
2. 2-Blockchain [↑](#footnote-ref-2)
3. -Data [↑](#footnote-ref-3)
4. 2-Block directed acyclic graphs [↑](#footnote-ref-4)
5. 3-Transaction-based directed acyclic graphs [↑](#footnote-ref-5)
6. 4-Bitcoin [↑](#footnote-ref-6)
7. -Etherume [↑](#footnote-ref-7)
8. -AIOTA [↑](#footnote-ref-8)
9. 1-Smart Contracts [↑](#footnote-ref-9)
10. -Complete Turing [↑](#footnote-ref-10)
11. -Central exchange [↑](#footnote-ref-11)
12. -Ripple [↑](#footnote-ref-12)
13. -InterLedger Protocol [↑](#footnote-ref-13)
14. -HyperLedger [↑](#footnote-ref-14)
15. -Distributed application [↑](#footnote-ref-15)
16. -Connector [↑](#footnote-ref-16)
17. -TransLedger [↑](#footnote-ref-17)
18. -Peer [↑](#footnote-ref-18)
19. -Link Layer [↑](#footnote-ref-19)
20. -Point to Point [↑](#footnote-ref-20)
21. -Encryption [↑](#footnote-ref-21)
22. -Decryption [↑](#footnote-ref-22)
23. -Escrow [↑](#footnote-ref-23)
24. -Cryptography [↑](#footnote-ref-24)