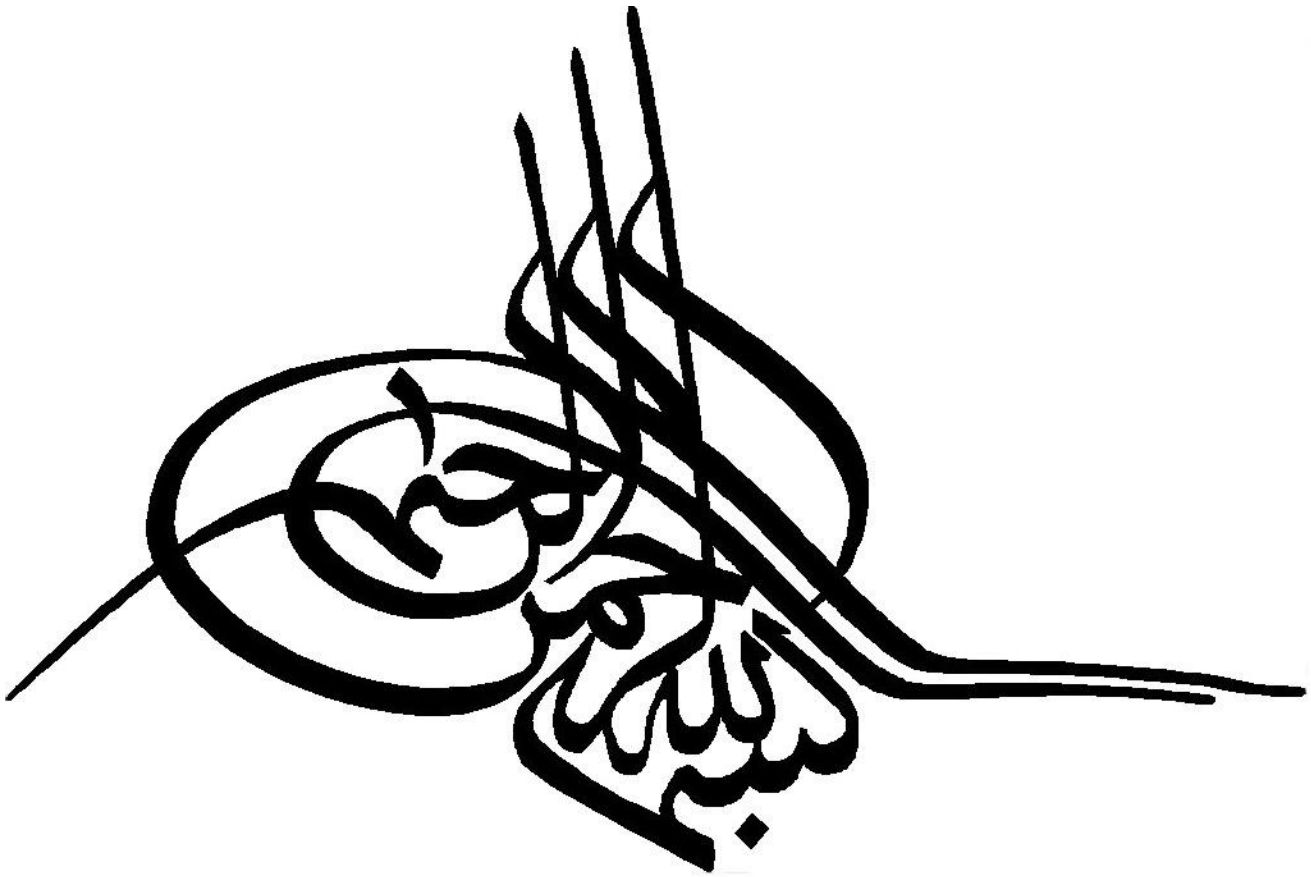

بسم الله الرحمن الرحيم

**دانشگاه تربیت مدرس**

**دانشکده مهندسی برق و کامپیوتر**

**گذارش سمینار کارشناسی ارشد**

**مهندسی کامپیوتر گرایش مهندسی نرم‌افزار**

# سیستم‌های تراکنش بین چند دفترحساب توزیع شده

**دانشجو**

رضا حمیدپوربدوئی

**استاد راهنما**

دکتر صادق دری‌نوگورانی

تیر ۱۳۹

# فهرست مطالب

# فهرست شکل‌ها

# چکیده

در سال ۲۰۰۹ 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 ۲۰۱۹ 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 ۱
# مقدمه و کلیات

## مقدمه

با توجه به اهمیت بیش از پیش تبادل رمزارزها به یکدیگر و اهمیت پیدا کردن ایجاد صرافی‌های برخط[۱] 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.

## ۱-۱ زنجیره‌بلاکی

زنجیره‌بلاکی[۲] 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 نظیربه‌نظیر به یکدیگر متصل شده و برای ذخیره‌سازی داده‌ها و پایداری شبکه از الگوریتم‌های اجماع استفاده می‌کنند.الگوریتم‌های اجماع نیز براساس نحوه کارکردشان ارسال درخواست‌های، ثبت یک بلاک جدید در شبکه و نحوه ثبت آن درخواست، در دفترحساب‌کل شبکه 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.

---

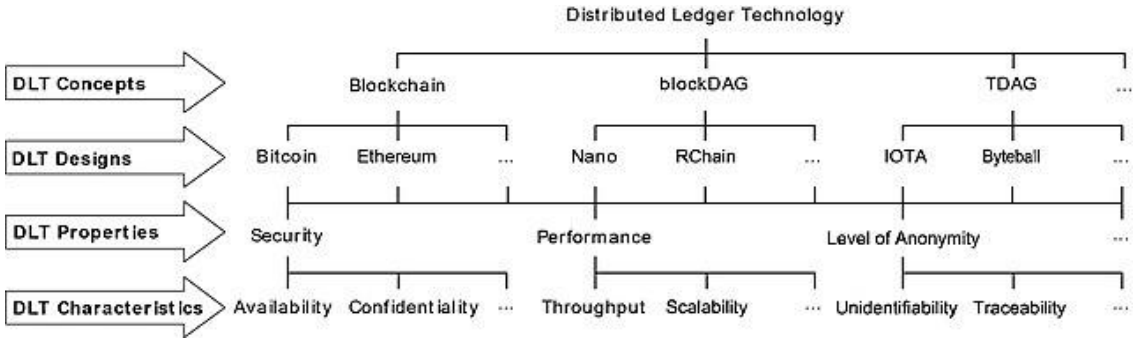
۱- Online exchange

۲-Blockchain

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[۱].

## ۱-۲ دفترحساب توزیع شده

مفهوم بلاکچین به نحوه پیاده‌سازی دفترچه‌کل آن برمی‌گردد.دفترچه‌کل درواقع پایگاه‌داده توزیع شده شبکه بلاکچین محصوب می‌شودکه داده‌ها[۱]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[۲] و گراف‌های جهت‌دار مبتنی تراکنش[۳] هستند.هرکدام از این مفاهیم دفترحساب‌های‌کل ویژگی‌های خاص خود را دارند و درواقع براساس میزان‌کارایی و امنیت متفاوت می‌باشند.نمونه‌هایی از شبکه‌های پیاده‌سازی شده با استفاده از دفترچه-کل‌های بلاکچینی بیت‌کوین[۴] ویا اتریوم[۵] می‌باشند.ویا نمونه‌ای از شبکه‌ای که برپایه تکنولوژی گراف‌های جهت‌دار مبتنی‌بر تراکنش پیاده‌سازی شده است شبکه آیوتا[۶] می‌باشد. تصویر ۱-۲-۱ نمایی از شبکه‌های مختلف با استفاده از تکنولوژی‌های مختلف بلاکچین را بیان می‌کند[۱].




شکل ۱-۲ ساختار دفترحساب‌های کل

۱-Data

۲-Block directed acyclic graphs

۳-Transaction-based directed acyclic graphs

۴-Bitcoin

۵-Etherume

۶-AIOTA

## ۱-۳ 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[۱] می‌گویند.در شبکه اتریوم ما با کمک یک زبان تورینگ کامل[۲] 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.

## ۱-۴ صرافی برخط

امروزه با پر رنگ شدن ارزهای دیجیتال و رمزارزها تجارت‌هایی مانند صرافی‌های برخط نیز اهمیت بیشتری پیدا کرده اند[۲،۳]. به همین منظور می‌توان صرافی‌های ایجاد شده بر این بستر را به دو دسته متفاوت تقسیم کرد.صرافی‌های متمرکز[۳] 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[۴] 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.

---

۱-Smart Contracts

۲-Complete Turing

۳-Central exchange

۴-Ripple

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 ۲

# 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 بررسی نمونه‌های اجرایی در هر روش و معماری‌های کلی آن‌ها دیدی کلی از انواع صرافی‌ها را ایجاد خواهیم کرد.

## ۲-۱ 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:

۱. تولید سیستم تبادل رمزارز دیجیتال از پایه
۲. سیستم‌تبادل برچسب سفید

### ۲-۱-۱ 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.

### ۲-۱-۲ 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 :

۱) موتورهای تبدل رمزارزها به یکدیگر
۲) دریافت نرخ تبدیل رمزارز به صورت برخط و در لحظه و اعمال آن برای تبدیل
۳) تهیه اندوخته از پیش تعیین شده رمزارزها برای صرافی در جهت تبدیل رمزارزها به یکدیگر
۴) برقراری و حفظ امنیت سرورهای تبادل رمزارزها
۵) تهیه کیف‌پول امن و مطمعن برای هریک از رمزارزها که صرافی مورد نظر قصد تبادل آن‌ها را دارد

## ۲-۲ صرافی‌های غیرمتمرکز

همانطور که در بخش ۴-۱ 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 :

۱- غیرمتمرکز مبتنی بر مفهومی تحت عنوان تبادل‌های تجزیه‌ناپذیر
۲- غیرمتمرکز تحت کنترل یک مرکزیت مشخص

### ۲-۲-۱ 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 تجزیه‌پذیر را 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 ۱- طبق پروتکل بین علی و رضا عمل کند و سکه خود را به علی بدهد (پس از دریافت سکه علی) ۲- طبق پروتکل عمل نکند و سکه خود را ندهد[۵].برای حل این مشکل راه‌حل‌های متفاوتی وجود دارد که برخی از آن‌ها شامل

۱- استفاده از یک قراردادهوشمند بین دو طرف

۲- استفاده از پروتکل ارتباط بین دفترحساب‌های توزیع شده (ILP)

#### ۲-۲-۱-۱ 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 ۲-۱ الگوریتم اجراء روش تبادل تجزیه‌ناپذیر[۵]

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 تراکنش۱ ( $TX1$ ) 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 ۴۸ 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 ۱ 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 ۱ و ۲ : علی می‌تواند با رد کردن تراکنش‌ها پس از گذشت ۴۸ ساعت پول خود را بازپس بگیرد.
- بین مراحل ۲ و ۳ : رضا می‌تواند پس از ۲۴ ساعت پول خود را دریافت کند درصورت بروز مشکل و همچنین علی نیز به بیش از ۲۴ ساعت نیاز دارد تا پول خود را دریافت کند.
- پس از مرحله ۳ : تراکنش به وسیله دو طرف به صورت کامل انجام شده است.علی بایستی سکه‌های دریافتی از این تراکنش‌ها را در ۲۴ ساعت آینده خرج کند وگرنه رضا می‌تواند پس از آن ادعای بازپس‌گیری سکه‌های خود را داشته باشد.همچنین رضا نیز باید تا ۴۸ ساعت بعد سکه‌های خود را خرج کرده باشد،چرا که علی نیز می‌تواند پس از آن ادعای بازپس‌گیری سکه‌های خود را داشته باشد.

## ۲-۲-۱-۲ پروتکل ارتباط بین دفتر حساب‌های توزیع شده – ILP

ILP[۱] که یکی از زیر پروژه‌های هایپرلجر[۲] 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[۳] بتواند به راحتی منابع مورد نیاز خود را مانند حافظه، توان محاسباتی و ... را خریداری کند بدون هیچگونه وابستگی به دفترکل‌های توزیع شده[۶] .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[۸] .

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.

---

۱-InterLedger Protocol

۲-HyperLedger

۳-Distributed application

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[1] 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.

### ۲-۲-۲ غیر متمرکز تحت کنترل یک مدیریت مشخص

همانگونه که پیش از این اشاره شد در بخش ۲-۲ 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 تبدیل-کنندگان 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 ۲-۱ 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.

---

۱-Connector

### ۲-۲-۲-۱ 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[۱۲].در این شبکه بلاکچینی گره‌ها با استفاده از الگوریتم اجماع FBA (Federated Byzantine Agreement) استفاده می‌کنند[۱۳]. این الگوریتم که در واقع نوع تغییر یافته الگوریتم BFT (Byzantine Fault Tolerance) می‌باشد[۱۴ ] 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 یورو را به داخل شبکه اعلام می‌کند(به سرورها اعلام می‌کند) در بین سرورهای شبکه عمل اجماع هر ۲-۵ 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 ارتباطی اثبات 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 انجام-دهند، 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[۱۵].

### ۲-۲-۲-۲ 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 i–بیت‌کوین می‌نامیم.i-بیت‌کوین 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 شبکهTransledger 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 DAG ویا 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[۱] 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 [۱]
- ریپل[۲]

- استلار[۳]
- بیت‌کوین کش[۴]
- EOS

می‌باشد.این رمزارزها ۸۰٪ نقل و انتقالات کل رمزارزهای موجود را در خود دارند ،یعنی این رمزارزها جزو ده رمزارز برتر دنیای ارزهای دیجیتال هستند[۱۵].

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 رویداد[۵] در شبکه Transledger 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 i–بیت‌کوین به شخص دیگری به نام رضا را دارد.عملیات انتقال توسط علی انجام می‌شود و در شبکه Transledger دو i–بیت‌کوین به حساب رضا منتقل می‌شود حال رضا می‌تواند این دو i–بیت‌کوین 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.

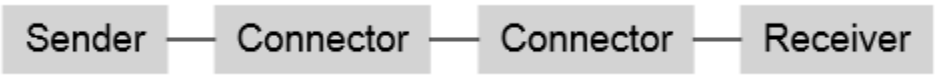
موضوعی که در اینجا بسیار اهمیت دارد این است که اول Transledger با شبکه‌های تبادل رمزارز موجود متفاوت است به طوری که وقتی به ازای دو بیت‌کوین دو i–بیت‌کوین ایجاد می‌شود می‌توان بازهم این دو i–بیت‌کوین را نیز تجزیه کرد و با آن‌ها تراکنش انجام داد.ثانیا این نحوه انتقال با کانال‌های انتقالی که در شبکه‌های 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[۱۷].

### ۲-۲-۳ تشریح کامل پروتکل ILP

همانگونه که در بخش ۲-۲-۱ 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.

## ۲-۲-۳-۱ فرستنده ،گیرنده ،اتصال‌دهنده

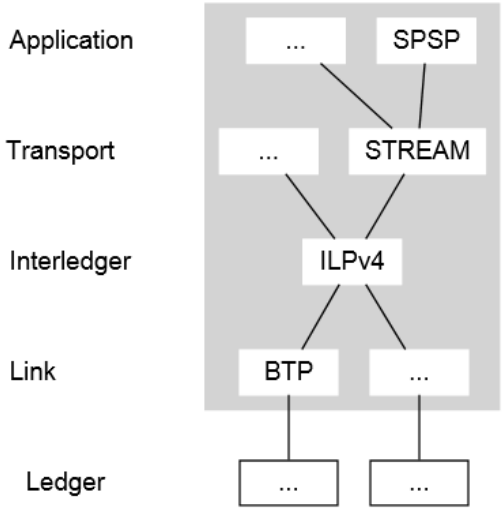
زمانی که دو شخص(فرستنده و گیرنده)بخواهند به یکدیگر پول ارسال کنند فرستنده پول را ارسال و گیرنده پول را دریافت می‌کند.این حالت درصورتی است که فرستنده و گیرنده در یک سیستم قرار داشته باشند.حال اگر فرستنده در یک سیستم (در یک دفترحساب توزیع شده)و گیرنده نیز در یک سیستم دیگر (در یک دفترحساب توزیع شده متفاوت 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 ۲-۲ نحوه اتصال گره‌ها در ILP [۷]

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.

## ۲-۲-۳-۲ لایه‌های پروتکل




شکل ۲-۳ معماری کلی پروتکل ILP [۷]

# 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[۲] 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 شده[۲] 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[۳] 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[۴]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[۵] و رمزگشایی[۶] داده‌ها

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

## Application

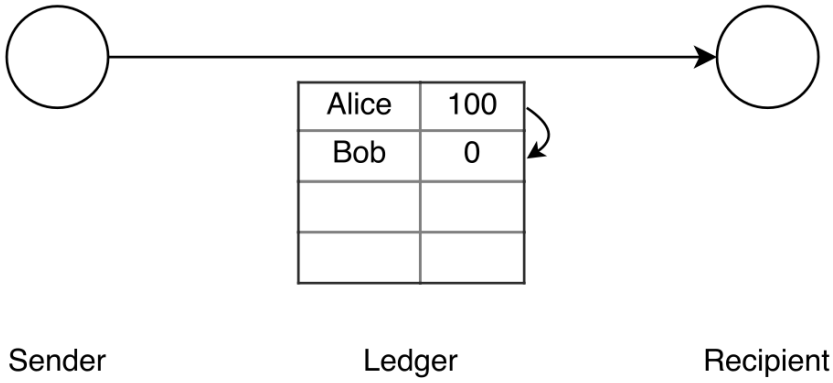
در این لایه تنها موارد غیر ضروری و پیش شرط‌هایی که بایستی قبل از شروع کلی فرآیند مشخص شوند تعیین می‌شوند به عنوان مثال مواردی همچون :

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

و از این دست موارد[۴].

## ۲-۲-۳-۳ فرآیند انتقال

همان‌گونه که در شکل ۲-۳ 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 ۲- ۴نحوه انتقال ارز در دفترحساب توزیع شده [۸]

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 ۲-۴ 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.

---

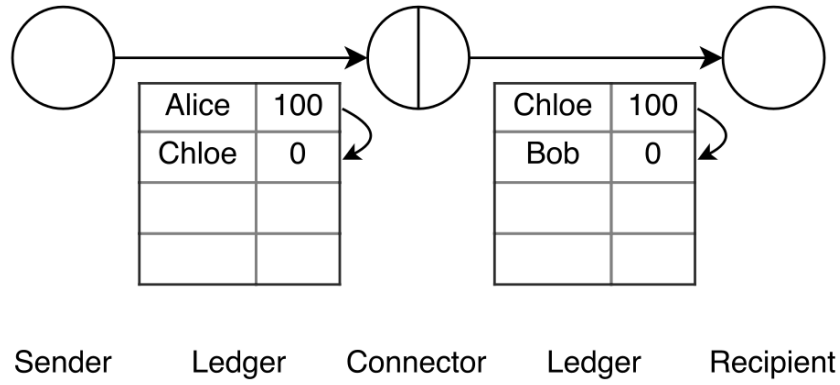
۲-Peer

۳-Link Layer

۴-Point to Point

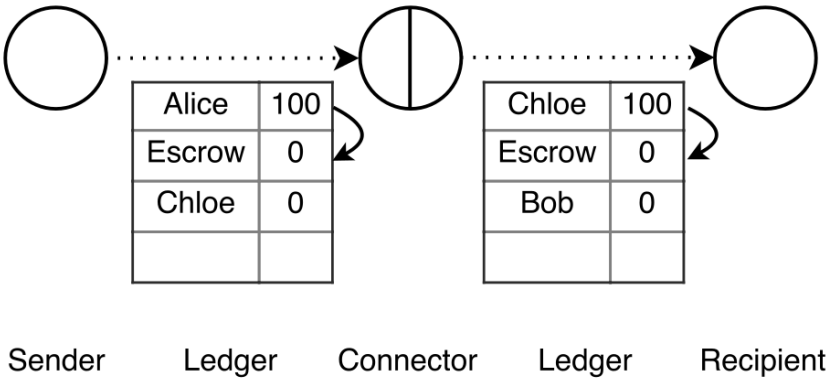
۵-Encryption

۶-Decryption




شکل ۲-۵ نحوه انتقال ارز بین دو دفتر حساب توزیع شده [۸]

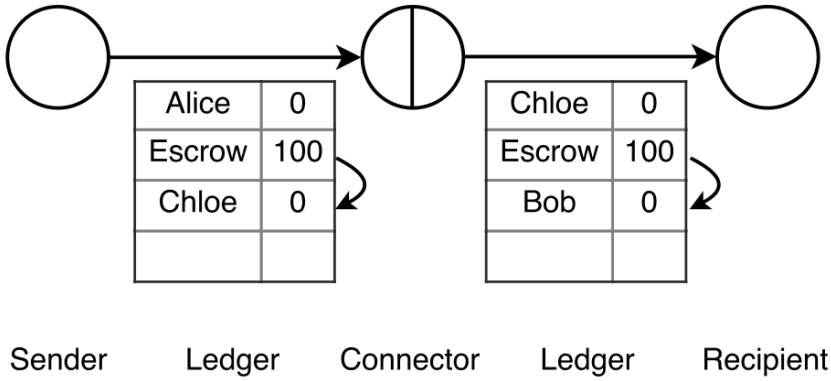
اما مشکل اصلی در این روش انتقال این مشکل وجود دارد که فرستنده بایستی به اتصال دهنده اعتماد کامل را داشته باشد تا معادل پول دریافتی از فرستنده را در دفترحساب توزیع شده دیگر به حساب گیرنده ارسال کند.همین چالش باعث به وجود آمدن سازمان-هایی برای انتقال‌های مالی بوده و همچنین باعث به وجود آمدن شکاف‌هایی در سیستم‌های مالی شده است.سپرده‌گذاری به وسیله دفترحساب‌های توزیع شده راه‌حلی 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 ۲-۶ نحوه انتقال ارز بین دو دفتر حساب توزیع شده به وسیله پروتکل ILP [۸]

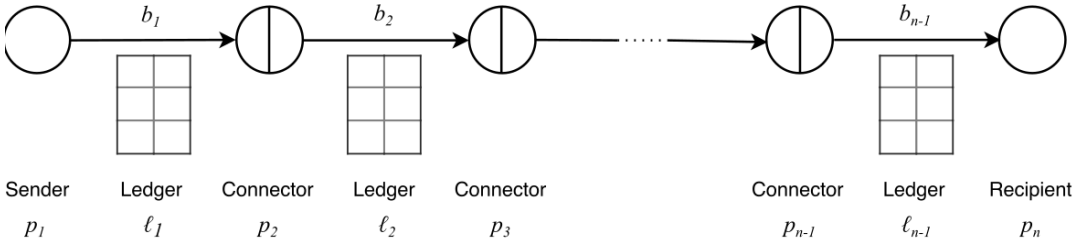
براساس شکل ۲-۵ ابتدا پول فرستنده ( Alice ) به حالت سپرده[۷] می‌رود.پس از اثبات این موضوع توسط دفترحساب‌توزیع شده، اتصال‌دهنده (Chloe) پول را در دفترحساب‌توزیع شده دیگر به حالت سپرده درمی‌آورد و این موضوع به وسیله دفترحساب‌توزیع شده برای گیرنده (Bob) اثبات می‌شود.

۷-Escrow




شکل ۲-۷ انتقال ارز از حالت سرمایه‌گذاری شده به حساب کاربران در پروتکل ILP [۸]

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 ۲-۷.




شکل ۲-۸ نحوه بهم زنجیر شدن اتصال‌دهندگان در پروتکل ILP [۸]

## ۲-۲-۳-۴ 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 [۶] 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.

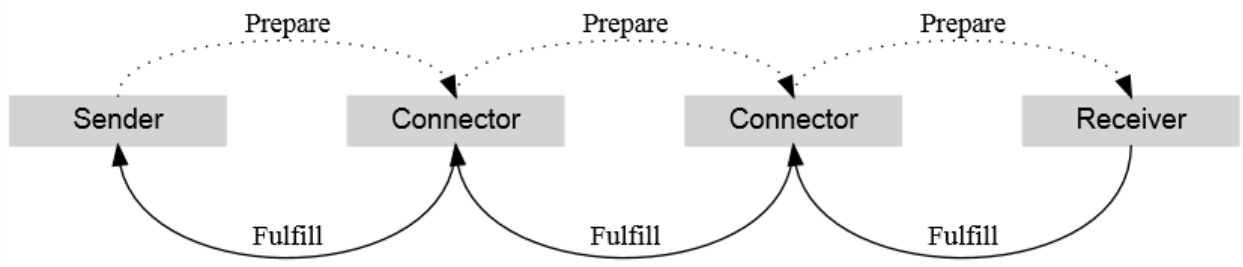
طبق عملکرد این پروتکل می‌توان گفت فرستنده درخواست انتقال تبادل رمزارز تنها زمانی به انتقال‌دهنده اعتماد می‌کند که پول را انتقال داده است که رسید دریافت پول از سمت گیرنده را به وسیله انتقال‌دهنده دریافت کند همچنین این شرط نیز وجود دارد که این رسید دریافتی اولا تکراری نباشد و ثانیا توسط انتقال‌دهنده جعل نشده باشد تنها راه اطمینان برای این موضوع رمزنگاری[8]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[۵].

## ۲-۲-۳-۵ 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

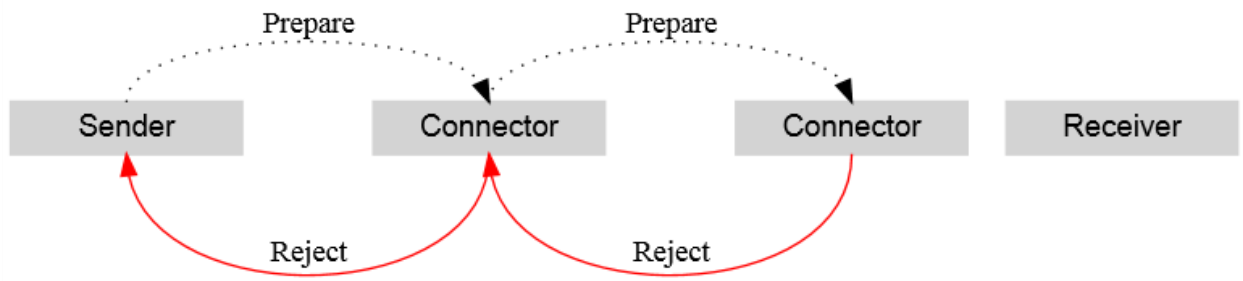
که به ترتیب هرکدام از این بسته‌ها مربوط به پیغام‌های درخواست، پاسخ و بروزخطا می‌باشند.در این پروتکل شمای کلی انتقال بسته‌ها به این صورت می‌باشد که اتصال‌دهندگان بسته‌های درخواست را برای فرستنده به گیرنده ویا اتصال‌دهنده دیگر انتقال می‌دهند و در پاسخ بسته‌های پاسخ ویا بروزخطا را تحت هرشرایطی به فرستنده برمی‌گردانند که نحوه انتقال در تصاویر ۲-۸ و ۲-۹ توصیف شده است.




شکل ۲-۹ نحوه انتقال پیام های درخواست و انجام شدن در پروتکل ILP [۷]

با توجه به شکل ۲-۸ 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.

8-Cryptography




شکل ۲-۱۰ نحوه انتقال پیام‌های درخواست و رد پیام در پروتکل ILP [۷]

با توجه به شکل ۲-۹ 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[۹].

# 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 توکن معادل 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].