هفتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲و۳ بهمن ۱۳۹۶
7th Annual Conference on Electronic Banking and Payment Systems

ارایه یک مکانیزم پرداخت امن مبتنی بر پول دیجیتال

A secure payment mechanism based on digital currency

حانیه فتح الهی، کارشناس آزمایشگاه رایانش ابری و خدمات ارزش افزوده دانشگاه الزهرا، fatholahi@ossl.ir
دکتر رضا عزمی، مدیر آزمایشگاه رایانش ابری و خدمات ارزش افزوده دانشگاه الزهرا، azmi@ossl.ir

چکیده

رشد روز افزون بلاک‌چین به عنوان یک تکنولوژی نرم افزاری فرد به فرد که از یکپارچگی اطلاعات دیجیتال فرد حفاظت می‌کند، از یک سو و همچین موفقیت چشمگیر این تکنولوژی در چند سال اخیر، باعث شده است که برای دیگر ارزهای رمزگذاری، خدمات امضای دیجیتال، سیستم های قرارداد هوشمند، کیف پول های امن، پیاده سازی زیرساخت های بانکداری و دیگر اپلیکیشن‌ها مورد استفاده قرار گیرد. و از سوی دیگر باعث شده است که مزایای این تکنولوژی به عنوان یکی از مسائل مهم بانکداری مطرح گردد. از جمله ی این مزایا می توان به رفع مشکل هزینه های هنگفت پیاده سازی و نگهداری سیستم های قدیمی بانک ها، هزینه های بالای جایگزینی، کندی در ارائه خدمات، عدم توانایی گسترش و رشد سیستم، وجود واسطه های فراوان در انجام تراکنش های مالی، اشاره کرد.

در ابتدا بلاک‌چین یک روش نگهداری رکوردهای متمرکز (به ویژه برای تراکنش های بانکی) بدون نیاز به احراز هویت بود، اما با توجه به کاربرد هایش می تواند یک جایگزین امن و راحت برای فرآیند های زمان گیر و گران بانکی نیز می باشد. از دیگر فواید این تکنولوژی می توان به کاهش تعداد واسطه های درگیر در تراکنش های مالی، افزایش سرعت و ارائه خدمات نوین اشاره نمود که از این سو تعدادی از بانک ها درصدد پیاده سازی بلاک‌چین به عنوان تکنولوژی اصلی بانکداری خود هستند. اما شایان ذکر است که به دلیل مدل غیر متمرکز این تکنولوژی و پیاده سازی آن در محیط غیر کنترلی، راه برای هکرها به منظور کشف سیستم ارز رمزنگاری و تولید تراکنش های تقلبی در جهت پولشویی و ایجاد تراکنش های جعلی، باز شده است. از دیگر نقاط ضعف می توان به حملات مرسوم در این تکنولوژی اشاره کرد. حمله کیف پول(امنیت سمت کاربر)، حمله به شبکه بلاک‌چین مانند DDoS و حملات استخراج بیت کوین که شامل دریغ کردن بلاک و رشوه خواری می شود، از این قبیل هستند.

حوزه ی اصلی بلاک‌چین در پرداخت های بین المللی مطرح شده است که پرداخت سریع و مطمئن، بدون نیاز به احراز هویت، را ممکن کرده است. در این مقاله می خواهیم یک مکانیزم eCurrency امن با استفاده از تکنولوژی دفترکل توزیع شده پیشنهاد نماییم، که علاوه بر مزیت های تکنولوژی بلاک‌چین و ارزهای رمزنگاری مانند بیت کوین که قبل تر اشاره شد، دارای یک کیف پول امن تر باشد. تمرکز این ارز روی پرداخت های داخلی سریع، امن و با تعداد واسطه های کمتر است. یکی دیگر از ویژگی های مهم این ارز استفاده از مکانیزم پول رنگی است. این مکانیزم اجازه می دهد که پرداخت بدون نیاز به احراز هویت انجام پذیرد، اما در زمان وقوع تقلب، جعل، دوبار خرج کردن پول و هرگونه اعمالی که پرداخت را بی اعتبار کند، امکان پیگیری پرداخت و ردیابی پول وجود داشته باشد. همچنین پشتیبانی از قرارداد هوشمند و ایجاد مدل های جدید تجاری باز

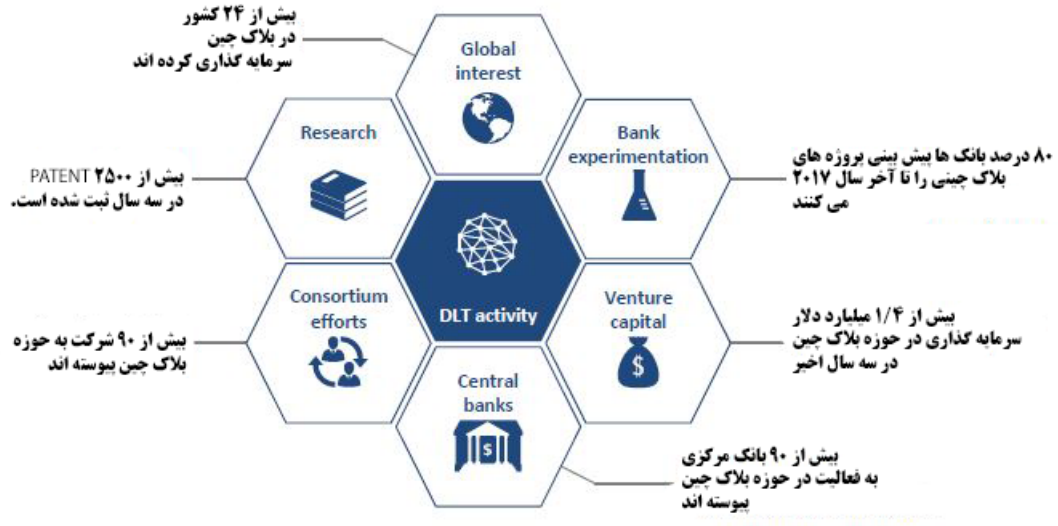
که باعث بهبود وضعیت رقابت در ارایه خدمات می شود نیز از ویژگی های این سیستم می باشد.

کلید واژه ها:

بلاک‌چین، پرداخت، تراکنش های مالی، ارز دیجیتال، کیف پول امن، ارز رنگی

مقدمه

چندی قبل بلاک‌چین همیشه در کنار بیت کوین مطرح می شد. اما پس از مطرح شدن بلاک‌چین یا در واقع دفترکل توزیع شده[۱] به عنوان یک تکنولوژی مستقل که این امکان را دارد تا وارد دیگر کاربرد های حوزه ی مالی و بانکی شود، تعداد کثیری از افراد در کشور های مختلف به سرعت به سمت استفاده از بلاک‌چین به عنوان تکنولوژی زیرساختی خود اقدام نمودند. بنابر آن چه گفته شد در این مقاله سعی شده است تا یک مکانیزم مبتنی بر تکنولوژی نوظهور بلاک‌چین با قابلیت های مختلف از جمله تراکنش های مالی سریع و مطمئن همچنین کاهش امکان جعل و کلاهبرداری، که با سیستم مالی کشور سازگار است ارائه شود. با در نظر گرفتن این موضوع که اولا بلاک‌چین می تواند راهکاری جامع و سریع برای این حوزه باشد و ثانیا این راهکار هم اکنون در سراسر جهان در حال طراحی و پیاده سازی است، اهمیت داشتن یک سیستم مبتنی بر بلاک‌چین به کاملا واضح است. شکل ۱. بیانگر فراگیر شدن بلاک چین در دنیاست.[۱]



شکل۱. آمار فعالیت در حوزه بلاک‌چین

در ابتدا خلاصه ای کوتاه در مورد تکنولوژی بلاک‌چین و بیت کوین به عنوان یک ارز دیجیتال و نحوه ی کارکرد آن ها ارائه می شود. سپس به شرح راهکار پیشنهادی در مقاله می پردازیم. پس از آن قابلیت های راهکار پیشنهادی را بررسی کرده و در نهایت یک نگاه اجمالی به نتایج حاصله از سیستم خواهیم داشت.

[۱] Distributed Leger Technology

بلاک‌چین یک دفترکل توزیع شده است که برای مبادله ارزهای دیجیتال، انجام معاملات و تراکنش ها استفاده می شود. هر عضو در شبکه بلاک‌چین یک کپی از به روز ترین دفترکل رمز نگاری شده را داراست و می تواند آن را تایید اعتبار کند و تراکنش جدیدی در آن ایجاد نماید. این سناریو توسط یک پایگاه داده ی توزیع شده اتفاق می افتد. این پایگاه داده تعداد زیادی از بلاک های داده ی تایید اعتبار شده در حال رشد را نگهداری می کند. بلاک های کامل شده به صورت خطی به ترتیب زمان تایید، به دفترکل اضافه می شوند. هر بلاک نیز دارای متادیتا می باشد که این متادیتا شامل برچسب زمان[۲] و یک آدرس که به بلاک کامل شده قبل اشاره می کند، می باشد. پایگاه داده بلاک‌چین اطلاعات همه تراکنش هایی که تا کنون انجام شده است را در خود نگهداری می کند. این پایگاه به کاربران شبکه اجازه می دهد اطلاعات دفترکل را به صورت امن تغییر دهند. برای ایجاد تغییر در اطلاعات بلاک جاری همه ی کاربران شبکه الگوریتم تایید اعتبار را اجرا می کنند تا آن را با تاریخچه ی موجود در دفتر کل اعتبار سنجی کنند. اگر اکثریت کاربران با اطلاعات موافقت کنند، بلاک تایید شده و به دیگر بلاک های تایید شده افزوده می شود. هر بلاک با یک عبارت hash شده توسط الگوریتم رمزنگاری SHA-256 که سرآیند آن را hash می کند، شناخته می شود. هر بلاک می تواند یک والد و چندین فرزند داشته باشد که به همان بلاک والد اشاره دارند. بنابراین شامل همان عبارت hash قبلی هستند. در واقع هر بلاک عبارت hash والدش رادر عبارت hash خودش دارد و این دنباله از عبارات hash که بلاک های تکی را به والد خود متصل می کند، یک زنجیره بزرگ از بلاک هایی که به بلاک اول اشاره دارند را تشکیل می دهد. این زنجیره به بلاک‌چین با زنجیره بلوکی معروف است.[۲]

بلاک‌چین زیرساخت مشترک ارزهای دیجیتال و ارزهای رمزگذاری است. در ادامه بیت کوین به عنوان مشهور ترین ارز دیجیتال را بررسی می کنیم.

بیت کوین یک ارز دیجیتال است که به عنوان یک نرم افزار متن باز[۳] در سال ۲۰۰۹ مطرح شد. این ارز رمزگذاری غیر متمرکز که توسط گره های شرکت کننده با یک نرخ تعیین شده در سیستم تولید می شود، یک شبکه ی peer-to-peer بدون نیاز به مجوز است که به هر کاربر اجازه اتصال به شبکه و ایجاد تراکنش جدید را می دهد. این بدان معناست که هر کاربر در این شبکه امکان ارسال تراکنش جدید برای تایید اعتبار و ایجاد بلاک جدید را دارد. الگوریتم به کار گرفته شده برای رمزنگاری بیت کوین SHA-2 است.

عملیات احراز هویت با bitID که یک پروتکل احرازهویت غیرمتمرکز است انجام می شود. این پروتکل اجازه دسترسی کاربران به شبکه را با بیت کوین فراهم می کند. تراکنش ها نیز با الگوریتم رمزنگاری ECDSA[۴] انجام می شوند تا اطمینان حاصل شود که افراد صاحب صلاحیت به سرمایه دسترسی دارند. بیت کوین از امضای دیجیتال برای یکپارچگی تراکنش ها استفاده می کند تا این اطمینان حاصل شود تراکنش ها پس از انجام امکان تغییر دادن نداشته باشند.[۲]

بیت کوین نیز مانند هر ارز دیگری با توجه به نوع استفاده از تکنولوژی بلاک‌چین دارای مزیت ها و معایب است از مزایای بیت کوین می توان به ۳ مورد زیر اشاره کرد.

---

[۲] Timestamp

[۳] Open-source

[۴] Elliptic Curve Digital Signature Algorithm

۱- هیچ سازمان یا شخصی امکان دستکاری کردن ارز را ندارد و نمی تواند قدرتی بر آن اعمال کند. از آن جایی که تراکنش ها در یک شبکه peer-to-peer انجام می شود این ارز دیجیتال دقیقا مانند پول فیزیکی عمل می کند. [۳]

۲- حفظ حریم شخصی با توجه به عدم نیاز به احراز هویت در شبکه بیت کوین بسیار بالاست و تراکنش ها با امضای دیجیتال صورت می گیرد.[۳]

۳- بیت کوین با توجه به نوع کارکردش می تواند اقتصاد جهانی را ارتقا دهد چون در هرکجا و هر زمان، با کمترین هزینه کار می کند.[۳]

برخی معایب بیت کوین نیز موارد زیر می باشد.

۱- عملیات استخراج بیت کوین در هر تراکنش پیچیده تر می شود و نیازمند منابع سخت افزاری بیشتری است. علاوه بر این زمان بیشتری (در حال حاضر حدود ۱۰ دقیقه) برای تایید تراکنش ها نیاز است.[۳]

۲- از آن جایی یک معتمد ثالث مانند بانک در میان نیست اگر گذرواژه اطلاعات فردی گم شود یا لو برود تمام دسترسی فرد از حسابش از دست می رود و احتمال وقوع جرم به وجود می آید.[۳]

۳- تراکنش های بیت کوینی در هیچ مرحله ای قابل بازگشت نیستند. در صورتی که فرد بخواهد تراکنش را برگرداند باید یک تراکنش جدید ایجاد کند که با مشکلاتی که در معایب شماره ۱ گفته شد روبه رو می شود.

۴- ساختار بیت کوین انجام فعالیت های غیرقانونی از جمله پولشویی و فرارمالیاتی را امکان پذیر می کند.

۵- نقاط ضعف اساسی امنیتی و آسیب پذیری در برابر برخی حملات

حملات امنیتی بیت کوین

در ادامه یکی از نقاط ضعف امنیت و حملات بیت کوین را شرح می دهیم و برخی را به نام می بریم. بیت کوین دارای کیف پول است که هر گره در شبکه با آدرس بیت کوینی خودش فعال است. این کیف پول می تواند سخت افزاری یا نرم افزاری باشد. کاربران می توانند تراکنش های خود را از طریق این کیف پول انجام دهند. نکته ی حائز اهمیت این است که هر کاربر موظف به حفظ امنیت کیف پول خود است و شبکه هیچ مسئولیتی در قبال امنیت کیف پول گره ها ندارد. از دست دادن کیف پول به منزله از دست دادن همه ی دارایی فرد است. اگر فردی کیف پول خود را گم کند بیت کوین ها در شبکه برای همیشه به خواب می روند و غیر قابل استفاده می شوند. در برخی موارد هم کیف پول تحت حمله قرار می گیرد و دزدیده می شود. در جدول۱. تعدادی حملات بیت کوین به همراه توضیحات مختصری بیان شده است.[۳]

جدول۱. برخی حملات بیت کوین

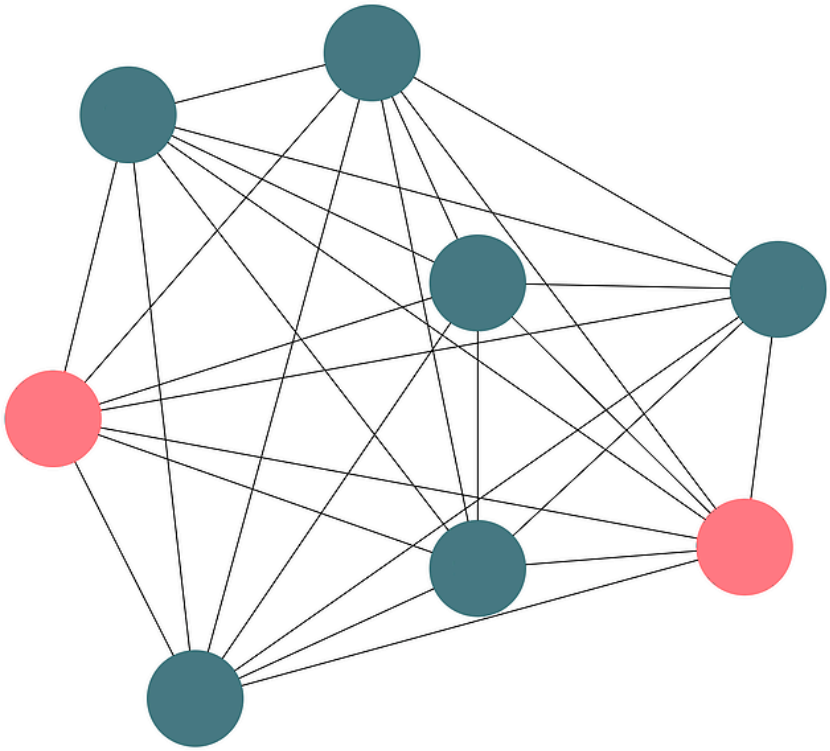
حمله	توضیحات	اهداف
حمله دوبار خرج کردن	خرج کردن پول های یکسان در دو تراکنش مجزا در یک زمان	مشتری و فروشنده
حمله ۵۱ درصدی	وقتی بیش از ۵۰ درصد توان پردازشی در اختیار یک گروه قرار می گیرد، آن ها می توانند تراکنش های فاقد اعتبار را تایید کنند، اطلاعات نادرست وارد دفترکل می شود.	شبکه بیت کوین، مراکز تبادل بیت کوین، کاربران
حملات رشوه	رقبا به استخراج کنندگان رشوه می دهند تا بیت کوین او را استخراج کنند.	استخراج کنندگان دیگر
سرقت کیف پول	رقبا کلید خصوصی را می دزدند یا آن را نابود می کنند.	کاربران
حمله DDoS	رقبا منابع سخت افزاری را با استفاده از چند حمله هدر می دهند.	شبکه بیت کوین، کاربران، کسب و کارها و استخراج کنندگان

راهکار پیشنهادی

راهکار پیشنهادی، ارائه یک ارز دیجیتال است. تکنولوژی زیرساختی این ارز همان طور که اشاره شد بلاک‌چین است. در ارائه این راهکار تلاش شده است از مزایای بلاک‌چین استفاده شود تا امکانات جدیدی در حوزه ی فناوری های مالی ایجاد شود. علاوه بر این، راهکار پیشنهادی با افزودن برخی نقش ها و فاکتور های نظارتی و کنترل کننده امنیت ارز را تامین کند تا بسیاری از نقاط ضعف دیگر ارز های دیجیتال در آن وجود نداشته باشد. همچنین در این ارز امکان پیگیری تراکنش های مالی و قابلیت پشتیبانی از قرارداد هوشمند وجود دارد.

شبکه و گره های شبکه

شبکه ی این ارز همان شبکه ای است که بلاک‌چین از آن استفاده می کند که معروف ترین آن ها شبکه اینترنت است و نیازمند زیرساخت خاصی نیست. تفاوت شبکه این ارز با بیت کوین و دیگر ارزهای دیجیتال دیگر در احراز هویت گره های شرکت کننده در شبکه است. نظارت در این شبکه توسط اعضای معتمد انجام می شود و اعضا نمی توانند فقط با دریافت یک آدرس وارد شبکه شوند و تراکنش ایجاد کرده و تراکنش ها را تایید اعتبار کنند. بدین ترتیب ورود اعضا به شبکه آزاد نخواهد بود، اما همچنان ناشناس بودن گره ها در شبکه رعایت می شود. این اعضا در شبکه اعضای قابل اعتمادی هستند که قدرت اعمال تغییرات در شبکه را دارند. این اعضا بانک ها هستند. اعمال تغییرات در شبکه بدان معنا نیست که می توانند در فرآیند تایید اعتبار تراکنش ها یا دیگر فرآیند ها که نیاز به تایید اکثریت اعضای شبکه دارد به صورت فردی اعمال نظر کنند. این اعضا صرفا می توانند در صورت بروز شرایط خاص در شبکه که روال را به خطر می اندازد برخی اعمال مدیریتی را انجام دهند. در بخش های بعدی این شرایط به تفصیل بیان می شود.



شکل۲. شبکه بلاک‌چین با اعضای معتمد

در شکل ۲. گراف بلاک‌چین نشان داده شده است. اعضای عادی شبکه با رنگ سبز مشخص شده اند و رنگ دیگر نشان گر اعضای معتمد شبکه است.

کیف پول امن

کیف پول در این ارز نیز مانند هر کیف پول دیگری کار می کند. اعضا باید در حفظ کیف پول خود بکوشند. این کیف پول یک ویژگی مهم دارد که آن را از دیگر کیف پول ها مجزا می کند. همان طور که پیش تر ذکر شد در کیف پول های معمولی فرد در صورت از دست دادن دسترسی به کیف پول خود تمام دارایی خود را ازدست می دهند.[۳] در این کیف امنیت به این صورت تامین می شود که افراد می توانند به اعضای معتمد شبکه این اجازه را بدهند تا یک footprint مختص به آن گره که فقط عضو معتمد از آن اطلاع دارد را به آدرس بلاک‌چینی آن ها اضافه کند. در این صورت عضو ناظر در شبکه می داند کیف پول مربوط به کدام آدرس گره است. اگر گره کیف پول خود را گم کند یا کیف پول به سرقت برود، عضو معتمد به راحتی می تواند دارایی گره در شبکه شناسایی کرده و آن را به صاحبش بازگرداند. این ویژگی می تواند مانع بسیاری از مشکلات امنیتی موجود در کیف پول های کنونی شود. نکته حایز اهمیت در حفظ امنیت کیف پول توسط عضو معتمد این است که ویژگی با حفظ حریم شخصی گره پیاده سازی می شود و همچنین در صورت استفاده از این گزینه، گره در تمامی تراکنش های خود برای دیگر گره ها همچنان ناشناس باقی خواهد ماند. اضافه شدن متادیتای footprint به صورت زیر خواهد بود.[۷]

$$\frac{AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D + footprint}{Blockchain\ address} = \frac{899164F50A9C68871417DF311BEDB3966F7B7A47}{Blockchain\ new\ address\ with\ footprint}$$

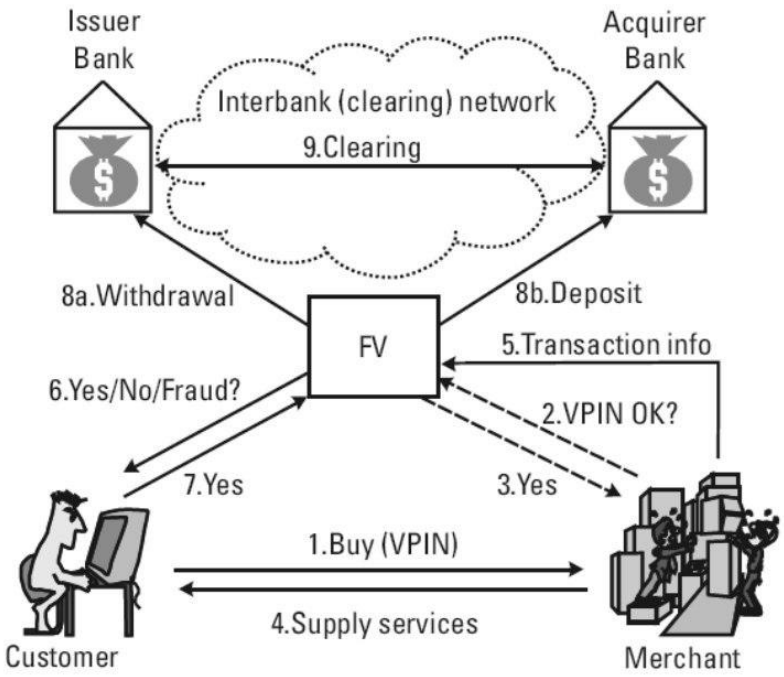
ارز رنگی

با توجه به خصیصه ای که در بخش کیف پول بیان شد، پول تراکنش هایی که شرکت کنندگان آن، گره های دارای footprint هستند دارای یک نشان می شوند. این نوع پول ها اصطلاحا ارز رنگی[۵] تلقی می شوند. ارز های رنگی خود به خود از دیگر ارز ها قابل تمییز هستند و امکانات جدیدی را به سیستم اضافه می کنند. اولا تراکنش ها قابل پیگیری هستند و صحت تراکنش تایید شده حتما مورد تصدیق است. ثانیا مکانیزم قوی تری برای جلوگیری از ارتکاب جرم به وجود می آید و یا اگر جرمی در سیستم اتفاق بیفتد، مجرم به راحتی شناسایی خواهد شد. این جرم ها شامل پولشویی، فرار مالیاتی و دوبار خرج کردن پول و غیره هستند.

پرداخت

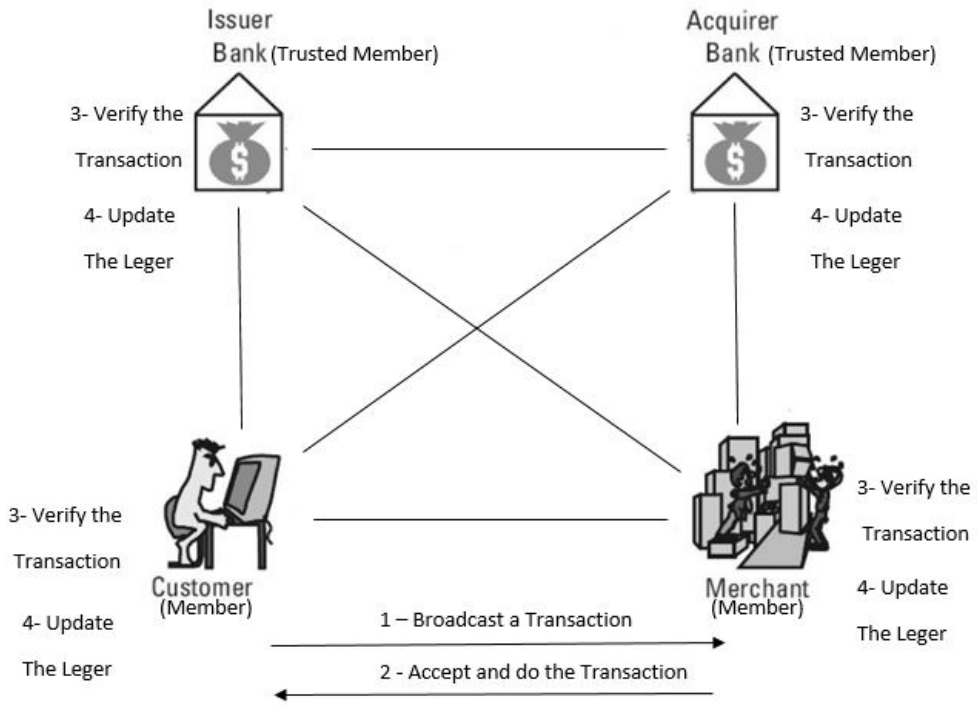
پرداخت در این شبکه با توجه به آن چه گفته شده است در قالب یک تراکنش صورت می گیرد. در پرداخت های عادی سیستم سه بازیگر اصلی مشتری[۶]، فروشنده [۷]و بانک دارد. بانک ها به عنوان واسطه ی مورد اطمینان بین فروشنده و مشتری قرار می گیرند و پرداخت را انجام می دهند. در این سیستم پیشنهادی نیز بازیگر های اصلی تغییری نمی کنند و فقط بانک ها از نقش واسطه خارج شده و به عنوان عضو معتمد ناظر بر موضوع ایفای نقش می کند و پرداخت توسط مشتری و فروشنده صورت می گیرد. در شکل ۳. پرداخت عادی و در شکل۴. پرداخت در سیستم زنجیره بلوک نمایش داده شده است. از آن جایی که پرداخت یک تراکنش است و تراکنش ها در این سیستم به صورت امن انجام می شوند این پرداخت یک پرداخت امن خواهد بود.

[۵] Colored coin
[۶] Customer
[۷] Merchant



شکل ۳. سیستم پرداخت کنونی

در سیستم کنونی مشتری درخواست خرید از فروشنده را به بانک خود می دهد. سپس بانک مشتری با بانک فروشنده تعامل می کند و پرداخت توسط بانک های فروشنده و خریدار بعد از بررسی فاکتور های دخیل در پرداخت انجام می شود. پس از پایان پرداخت بانک های مربوط به هر طرف آن ها را از نتیجه ی پرداخت آگاه می کنند و در نهایت خدمت یا کالا توسط فروشنده به خریدار ارائه می شود.



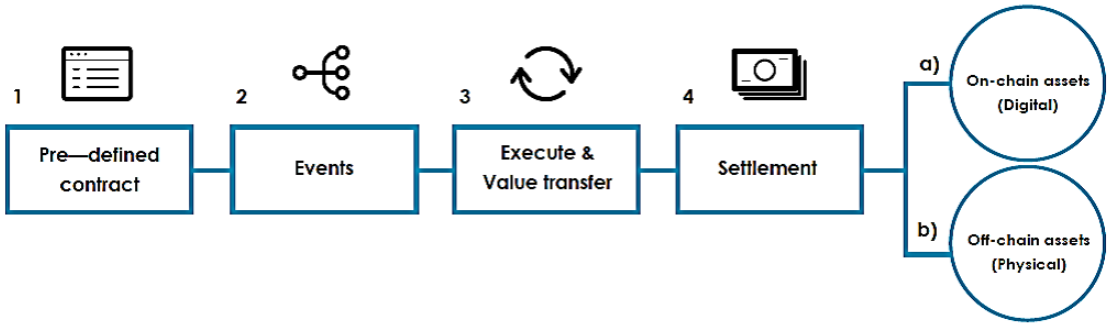
شکل ۴. سیستم پرداخت پشنهادی

در شکل ۴. پرداخت به این صورت انجام می شود که مشتری یک تراکنش در شبکه را ایجاد می کند. سپس خریدار و مشتری تراکنش را انجام می دهند. بانک ها به عنوان عضو معتمد تمام این سناریو را تحت نظر دارند. در صورت تایید اعتبار تراکنش توسط گره های شبکه بلاک چین همه ی گره ها دفترکل خود را به روز رسانی می کنند یعنی تراکنش را در آن ثبت می کنند. نهایتا خدمت یا کالا توسط فروشنده به مشتری ارائه می شود.

سیستم پرداخت امن مبتنی بر قرارداد هوشمند

سیستم پرداخت پیشنهادی از مکانیزم قرارداد هوشمند برای مبادله و تسویه حساب مالی بین مشتری، فروشنده و بانک (عضو معتمد شبکه) استفاده می کند.

قرارداد هوشمند، یک متد استفاده از ارز های رمزگذاری برای تشکیل یک قرار داد با انسان یا ماشین با استفاده از بلاک‌چین است. قرارداد به صورت خودکار اجرا می شود.[۸] زمانی که این قرارداد مشخص شد دیگر نیازی نیست که شخصی فرآیند آن را به صورت مرتب بررسی نماید. علاوه بر اجرای خودکار، قرارداد هوشمند خود مستقل است و هیچ گونه نیازی به سرمایه گذاری از طرف سازنده اش ندارد. در نهایت نیز به علت غیرمتمرکز بود ذات بلاک‌چین این قرارداد نیز در یک پایگاه داده مرکزی ذخیره نمی شود.



شکل۵. سناریو قرارداد هوشمند

در شکل ۵. قرارداد هوشمند به تصویر کشیده شده است. در قسمت ۱ ابتدا بند های قرارداد مشخص می شود مانند نرخ بهره متغیر[۸]، ارز پرداختی و نرخ ارز. همچنین شروط اجرای قرارداد نیز مشخص می گردد. در قسمت ۲ رویداد های شروع کننده اجرای قرارداد قرار می گیرند. تراکنش ها شروع می شوند و اطلاعات دریافت می شود. در قسمت ۳ مقادیر بر اساس بند های قرارداد تولید می شوند. در بخش ۴ برای ارزهای رمزگذاری شده حساب ها به صورت اتوماتیک تسویه می شوند. برای دیگر دارایی های خارج از بلاک‌چین مانند اوراق بهادار تغییرات در پایگاه داده صورت می گیرد و تسویه حساب باید بر اساس هر آنچه در پایگاه داده است انجام گیرد.

ساختار قرارداد های هوشمند بیشتر شبیه trigger های پایگاه داده است. به عنوان مثال اگر در قرارداد هوشمند این طور ذکر شده باشد که طرف A به محض دریافت پول آن را برای طرف B واریز نماید شبه کد پایگاه داده ی آن به صورت زیر خواهد بود.

```
CREATE TRIGGER forward_balance AFTER UPDATE on accounts
  FOR EACH ROW

    WHERE NEW.account_address = A_address

      BEGIN transaction;

       UPDATE account_balance SET account_balance = account_balance+ NEW.account_balance  WHERE
account_address = B_address;
       UPDATE account_balance SET account_balance = 0 WHERE account_address =   A_address;
      END transaction;
```

این شبه کد SQL در واقع یک trigger در پایگاه داده است و این بند قرارداد به صورت خودکار تا زمانی که قرارداد معتبر باشد اجرا می شود و دیگر نیازی به نظارت اشخاص بر اجرای صحیح قرارداد و صرف هزینه های چنینی نیست. هزینه هایی

[۸] Variable interest rate

که با اجرای قرارداد هوشمند کاهش پیدا می کنند نباید دست کم گرفته شوند. هزینه های مدیریتی و پرسنل برای اجرا و نظارت در اجرای قرارداد حذف می شوند. در اکثر موارد همین ویژگی باعث دلیل سرمایه گذاری برای قرارداد هوشمند است. در واقع این همان حذف هزینه های بالقوه ی موجود با پیاده سازی یک تکنولوژی است.

در نهایت می توان گفت هر رویدادی در سیستم قرارداد هوشمند با یک تراکنش پرداخت همراه خواهد بود. پرداخت ها در قرارداد هوشمند نیز دقیقا با سناریوی پرداختی که در بخش پرداخت توضیح داده شد انجام می شود. در این صورت قراردادی هوشمند با پرداخت امن خواهیم داشت.

نتیجه گیری

سیستم پیشنهاد شده صرفا یک مدل جدید در مباحث تکنولوژی های مالی است و هیچ تعارضی با سیستم کنونی ندارد. این سیستم علاوه بر افزایش امینت و سرعت می تواند بار سنگین پردازشی بانک ها را به مدل نظارتی تغییر دهد. این خود باعث کاهش هزینه های بالقوه ی بانک ها می شود. سیستم های جدید همیشه می توانند مدل های جدید ارائه سرویس به مشتریان را به وجود آورند. چنین سیستمی با ارائه خدمات در سطح بالا نیز چنین دیدگاهی را دارد.

مراجع

[1] (2016). The future of financial infrastructure, WORLD ECONOMIC FORUM.

[2] Sachchidanand Singh, N. S. (2016). Blockchain: Future of Financial and Cyber Security. 2016 2nd International Conference on Contemporary Computing and Informatics (ic3i), IEEE.

[3] Mauro Conti, S. K. E., Chhagan Lal, Sushmita Ruj (2017). "A Survey on Security and Privacy Issues of Bitcoin." IEEE.

[4] Puneet Kumar Kaushal, D. A. B., Dr. Rajeev Sobti (2017). Evolution of Bitcoin and Security Risk in Bitcoin

Wallets. International Conference on Computer, Communications and Electronics (Comptelix).

[5] Ingo Weber, V. G., Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, Paul Rimba, (2017). On Availability for Blockchain-Based Systems. IEEE 36th Symposium on Reliable Distributed Systems.

[6] James-Lubin, K. (2016). "Blockchains by analogies and applications." from https://www.oreilly.com/ideas/blockchains-by-analogies-and-applications.

[7] (2015). From https://en.bitcoin.it/wiki/Colored_Coins.

[8] Stark, J. (2016). "Introduction to Smart (legal?) Contracts." From https://medium.com/@jjmstark/introduction-to-smart-contracts-part-1-8f191a324d0a.