عنوان: بررسی مدل پرداخت مبتنی بر بلاکچین و افزایش امنیت در سیستم های پرداخت با استفاده از بلاکچین غیرمتمرکز

فاطمه کولیوند
دانشجوی کارشناسی ارشد، گروه مهندسی فناوری اطلاعات، دانشکده فنی مهندسی، دانشگاه آزاد واحد تهران جنوب
فائزه مجرد
دانشجوی کارشناسی ارشد، گروه مهندسی فناوری اطلاعات، دانشکده فنی مهندسی، دانشگاه آزاد واحد تهران جنوب
فاطمه خداپرست
استاد گروه مهندسی فناوری اطلاعات، دانشکده فنی مهندسی، دانشگاه آزاد واحد تهران جنوب

چکیده
با توسعه سریع تجارت الکترونیک جهانی، بهبود کارایی و راحتی پرداخت های تجاری الکترونیک اهمیت فزاینده ای پیدا می کند. سیستم‌های پرداخت فعلی تجارت الکترونیک برای کارت‌های اعتباری یا چک به یک دروازه پرداخت PG نیاز دارند. این امر مستلزم هزینه های PG است که به نوبه خود هزینه درگیر شدن در تجارت الکترونیک را افزایش می دهد. فناوری بلاک چین یک دفتر کل توزیع‌شده است که به شرکت‌کنندگان این فرصت را می‌دهد تا با استفاده از مکانیزم رمزنگاری و الگوریتم‌های اجماع، و غیره، توافق اعتباری را بر روی مجموعه‌ای از حقایق مشترک بدون اعتماد متقابل ایجاد کنند. ویژگی‌های تمرکززدایی، تداوم، ناشناس بودن و قابلیت حسابرسی فناوری بلاک چین، ویژگی‌های تغییرناپذیری، شفافیت و تسویه حساب طبیعی، در واقع کاملاً با تقاضای حوزه پرداخت الکترونیک مطابقت دارد. بخشی از این مقاله یک مدل پرداخت ساده را پیشنهاد می‌کند که از ویژگی‌های اساسی ارزهای دیجیتال، مانند کلید عمومی، کلید خصوصی، و امضای دیجیتال استفاده می‌کند تا نیاز به واسطه تراکنش‌ها مانند گواهی کلید عمومی و PG را از بین ببرد. از طرف دیگر همچنان نگرانی هایی در رابطه با حفظ حریم خصوصی و امنیت در بلاکچین غیر متمرکز وجود دارد که بخش دیگری از این تحقیق، Hyperledger Fabric و الگوریتم های BPS برای بالا بردن امنیت و سرعت در بلاکچین غیر متمرکز معرفی و مورد بررسی قرار گرفته است.

کلید واژه ها: سیستم های پرداخت، امنیت، بلاکچین غیرمتمرکز، Hyperledger Fabric ، BPS.

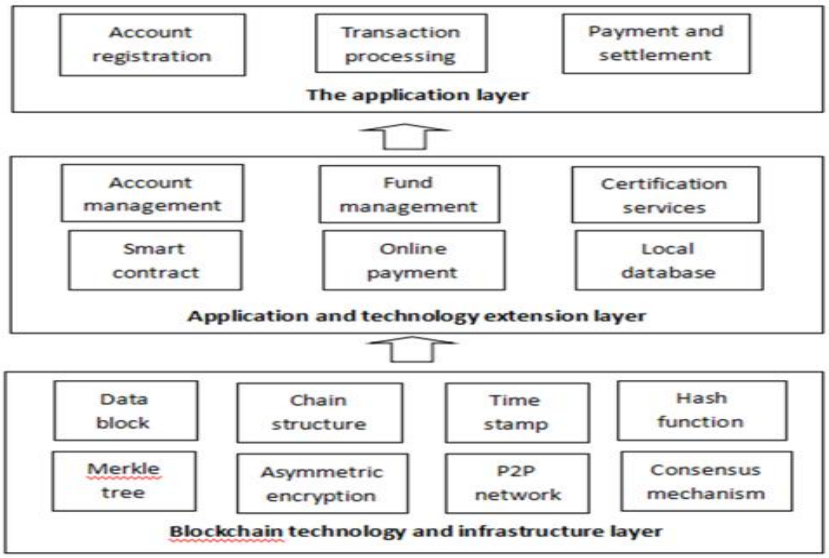
مقدمه

سیستم پرداخت یک عامل حیاتی و ضروری در تجارت الکترونیک است. یک سیستم پرداخت الکترونیکی قابل اعتماد مستلزم احراز هویت متقابل است که از طریق آن طرفین معامله می توانند هویت یکدیگر را تأیید کنند. محرمانه بودن، یکپارچگی و عدم انکار. اکثر مصرف کنندگان هنگام خرید اقلام از طریق تجارت الکترونیک از کارت های اعتباری یا چک استفاده می کنند. در چنین موارد، یک درگاه پرداخت PG برای اطمینان از یکپارچگی و عدم انکار، پرداخت های کارت استفاده می شود. این به طور اجتناب ناپذیری کارمزد تراکنش را ایجاد می کند زیرا نهادهای واسطه مانند PG یا شرکت های شبکه ارزش افزوده در فرآیند پرداخت دخالت می کنند. چنین کارمزدهایی در گذشته موضوع جدی نبود، زیرا پرداخت‌های کارت اعتباری از نظر مبلغ نسبتاً بیشتر و از نظر تعداد تراکنش‌ها کمتر بود. با این حال، توزیع فزاینده پایانه های کارت اعتباری، تغییر در نرخ های کسر مالیات، خدمات ارزش افزوده بیشتر ارائه شده توسط شرکت های کارت اعتباری، و افزایش تعداد فروشگاه های رفاهی که حجم بیشتری از پرداخت های کوچک را پردازش می کنند، به سرعت در حال تولید هستند. مشکلات بازار تجارت الکترونیک، مصرف کنندگان و کسب و کارهای کوچک را به طرح موضوعی در رابطه با کارمزدهای متصل به سیستم های پرداخت الکترونیکی سوق می دهد. این مشکل را می توان با استفاده از فناوری بلاک چین برطرف کرد، زیرا از فناوری های مؤلفه ای مانند هش، الگوریتم رمزنگاری نامتقارن و گواهی کلید عمومی استفاده می کند. احراز هویت نیاز به یک گواهی کلید عمومی ساختار یافته با زیرساخت کلید عمومی (PKI)، علاوه بر فناوری های امنیتی مانند رمز عبور یک بار مصرف (OTP)، کارت هوشمند، و سرویس پیام کوتاه دارد. در همین حال، سیستم‌های بلاک چین ذاتا دارای کلید عمومی، کلید خصوصی و ویژگی‌های امضای دیجیتال هستند که بدون نیاز به اجرای اقدامات امنیتی خارجی، یکپارچگی و عدم انکار تراکنش‌های پرداخت را برای کاربران خود فراهم می‌کنند. مطالعه حاضر قصد دارد یک پلتفرم پرداخت الکترونیکی را بر اساس عناصر اصلی فناوری بلاک چین، یعنی کلید عمومی، کلید خصوصی و امضای دیجیتال پیشنهاد کند. سیستم پیشنهادی با سیستم تجارت الکترونیک بلاک چین معمولی که توسط واسطه های تراکنش استفاده می شود متفاوت است. سیستم بلاک چین دارای یک احراز هویت غیرمتمرکز در یک دفتر کل است که شامل توافق‌نامه‌ها و تراکنش‌های بین گره‌های مشارکت‌کننده از طریق سیستم ارزهای دیجیتال بلاک چین است. شرکت‌کنندگان به‌عنوان گره‌های بلاک چین می‌توانند شهادت تراکنش را ارائه دهند و به سرعت آن را در کل شبکه پخش کنند، که صحت و اعتبار رکورد تراکنش را بدون شخص ثالث و یک واسطه متمرکز ثابت می‌کند. هیچ طرف ممتازی برای نگهداری دفتر مورد نیاز نیست. این ساختار سیستم را ساده می‌کند و نیاز به ماژول‌های ویژگی خارجی را از بین می‌برد، در نتیجه توسعه کلی سیستم و هزینه‌های عملیاتی را کاهش می‌دهد و در نتیجه هزینه‌های کمتری را برای بازرگانان دریافت می‌کند(Kim & Kim, 2022). پلتفرم پرداخت بین‌المللی تجارت الکترونیک مبتنی بر بلاک چین، از تراکنش‌های نقطه به نقطه بین تامین‌کنندگان و مشتریان، بدون نیاز به تسویه مبادلات بین بانک‌ها و تنظیم‌کننده‌ها پشتیبانی می‌کند. ساختار سه سطحی بلاک چین و مدیریت داده های طبقه بندی در بلاک چین، کارایی عملیات زنجیره اتحاد را تا حد زیادی بهبود می بخشد. یکی از چالشهای استفاده از این فناوری این است که: با استفاده از فناوری زنجیره بلوک برای انجام تسویه حساب، چون سیستم صورتحساب دیجیتال ساخته شده توسط زنجیره بلوک با اتصال سیستم به پلتفرم های دیگر مشکل دارد، سرویس رمز عبور فناوری زنجیره بلوک نیز نیاز به ایجاد تبادل داده با سیستم سایر پلتفرم های فنی دارد. بسیاری از پلتفرم‌ها از رابط‌ها و الگوریتم‌های فنی مختلفی در توسعه استفاده می‌کنند، با یکدیگر "گفتگو" نمی‌کنند و ارسال، دریافت و درک اطلاعات مبادله‌ای را نمی‌توان یکپارچه کرد. برای این منظور، ایجاد یک استاندارد بین‌المللی از پروتکل، ساختار، پلتفرم‌ها و غیره ضروری است (Li, 2021). برای اطمینان از ثبات دفتر کل بلاکچین، داده‌های تراکنش در سیستم‌های پرداخت

غیرمتمرکز اولیه عمومی هستند. این دارای چالش های مربوط به حریم خصوصی است، به عنوان مثال در حریم خصوصی هویت و ارزش تراکنش منتقل می‌شود، اگرچه این سیستم‌ها اقداماتی برای اطمینان از حریم خصوصی هویت دارند، اما از آنجایی که تمام سیستم‌های پرداخت عمومی هستند، حالت تراکنش نیز عمومی است. بنابراین مهاجم می‌تواند سوابق تراکنش‌ها را در زنجیره بلوکی تجزیه و تحلیل کند تا ارتباطی بین آدرس‌های کاربران ایجاد کند و حتی هویت واقعی کاربر را به دست آورد. در بخشی از این تحقیق برای غلبه بر این چالش از فناوری Hyperledger Fabric و دو الگوریتم استفاده می‌شود. با استفاده از هر کدام از روش ها هیچ کس نمی‌تواند از خارج از شبکه به سیستم دسترسی داشته باشد، هزینه تراکنش ها کمتر شده و سرعت انجام معاملات افزایش می‌یابد (Al-Amin et al, 2022).

ساختار سلسله مراتبی پلتفرم پرداخت

پلتفرم پرداخت به سه لایه تقسیم می شود. لایه زیرین، فناوری بلاک چین و لایه زیرساخت است که از آخرین فناوری زنجیره بلوک تشکیل شده است و یک دفتر کل غیرمتمرکز را براساس شبکه P2P تشکیل می دهد. لایه میانی لایه توسعه برنامه و فناوری است که منطق تجاری و واحد پشتیبانی برنامه بلاک چین را پوشش می دهد، از جمله پایگاه داده محلی که برای ایجاد مدیریت حساب، مدیریت سرمایه، پرداخت شبکه و سایر عملکردها استفاده می شود. لایه بالای پلتفرم خدمات کاربردی را برای تکمیل خدمات اولیه مانند ثبت نام، تراکنش و پرداخت ارائه می دهد که در شکل ۱ نشان داده شده است (Li, 2021).



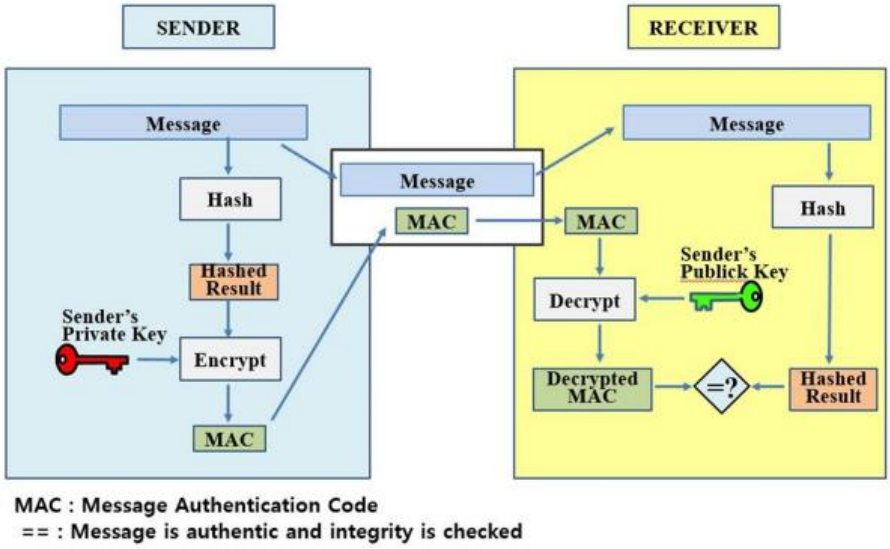
شکل ۱. ساختار سلسله مراتبی پلتفرم پرداخت

احراز هویت

رواج تلفن های هوشمند، تعداد تراکنش های پرداختی را که از طریق دستگاه های تلفن همراه پردازش می شوند، افزایش می دهد. کدهای QR تعریف شده در استانداردهای بین المللی برای وارد کردن یک شناسه یا مقدار کلید در طول تراکنش های تجارت الکترونیک گوشی های هوشمند استفاده می شوند، زیرا می توانند داده های بیشتری نسبت به بارکدها داشته باشند. در اینجا، یک نهاد شخص ثالث برای مدیریت گواهی‌های PKI تعیین می‌شود و تاجر اطلاعات پرداخت را با استفاده از کلید عمومی ارائه‌شده

توسط این شخص ثالث رمزگذاری می‌کند. مشتری یک کلید خصوصی از شخص ثالث درخواست می کند، اطلاعات پرداخت را از تاجر دریافت می کند، و اطلاعات را با استفاده از کلید خصوصی برای احراز هویت اطلاعات پرداخت رمزگشایی می کند. این یک روش مناسب برای پردازش احراز هویت بین بازرگانان و مشتریان است، اما نیاز به یک جفت کلید برای هر تراکنش دارد که یک کلید خصوصی از طریق شخص ثالث برای مشتری ارسال شود. بطور کلی، فرآیند احراز هویت بین فرستنده و گیرنده به شرح زیر است که در شکل ۲ نشان داده شده است:

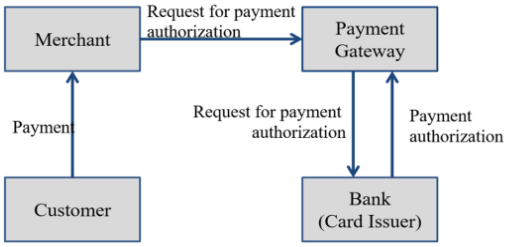
فرستنده پیام را هش می کند. کلید خصوصی فرستنده برای رمزگذاری نتیجه هش شده برای ایجاد کد احراز هویت پیام MAC استفاده می شود. سپس فرستنده پیام و MAC را به گیرنده ارسال می کند. گیرنده پیام ارسال شده را هش می کند تا یک نتیجه هش شده ایجاد کند و MAC دریافتی را با کلید عمومی فرستنده رمزگشایی می کند تا یک MAC رمزگشایی ایجاد کند. در نهایت، نتیجه هش شده و MAC رمزگشایی شده با هم مقایسه می شوند و اگر این دو مقدار یکسان داشته باشند، یکپارچگی پیام و عدم انکار فرستنده ثابت می شود. در اینجا، فرآیندی که توسط فرستنده انجام می‌شود، پیام علامت و فرآیندی که توسط گیرنده انجام می‌شود، پیام تأیید نامیده می‌شود. مطالعه حاضر از یک روش احراز هویت شامل این دو فرآیند استفاده می کند (Kim & Kim, 2022).



شکل ۲. نمودار احراز هویت پیام

مدل پرداخت (PG)

همانطور که در شکل ۳ نشان داده شده است، PG یک سیستم واسطه است که پرداخت های تجارت الکترونیک را مجاز می کند. PG ها بین تاجر و بانک (یا صادرکننده کارت) وجود دارند که به عنوان میان افزار عمل می کنند (Kim & Kim, 2022).



شکل ۳. مدل پرداخت کارت اعتباری معمولی

سیستم پرداخت بدون PG مقاله حاضر استفاده از فناوری بلاک چین را برای ساخت مدلی پیشنهاد می‌کند که نیازی به پیاده‌سازی ماژول‌های ویژگی خارجی ندارد. اگرچه ساختار آن ساده است و نیازی به ماژول های ویژگی خارجی ندارد، اما یکپارچگی و عدم انکار تراکنش بین تاجر و مشتری و بین مشتری و سیستم بلاک چین را تضمین می کند، در نتیجه توسعه کلی سیستم و هزینه های عملیاتی و هزینه های مشتریان را کاهش می دهد (Kim & Kim, 2022).

ساختار سیستم مدل پرداخت پیشنهادی بدون PG

ساختار سیستم

سیستم پرداخت پیشنهادی تجارت الکترونیک بلاک چین شامل تاجر، اپلیکیشن گوشی هوشمند مشتری و سیستم بلاک چین است. شکل ۴ ساختار کلی سیستم را نشان می دهد و روش پردازش پرداخت به شرح زیر است:

(۱) پس از فروش محصولات و خدمات خود، تاجر از مشتری درخواست می کند تا با استفاده از ارز دیجیتال بلاک چین، پرداخت را انجام دهد. این فرآیند با یک خط نقطه چین نشان داده شده است، زیرا تاجر درخواست پرداخت را از طریق یک کد QR نمایش داده شده در مشتری انجام می دهد. مرورگر وب، به جای یک کانال آنلاین جداگانه. در مقابل، درخواست‌هایی که با (۲)، (۳)، (۴)، و (۵) نشان داده شده‌اند، همگی با خطوط ثابت نشان داده می‌شوند زیرا از خطوط مخابراتی جداگانه استفاده می‌کنند.

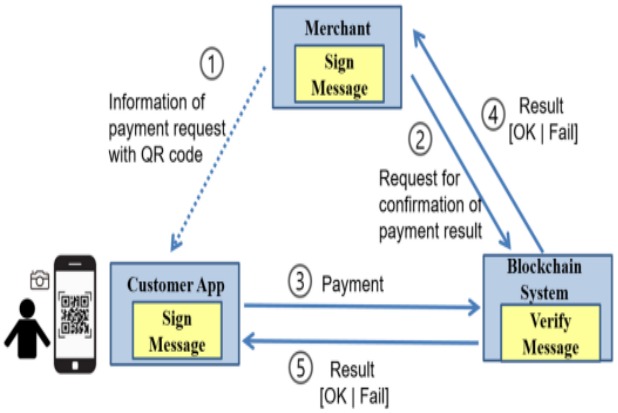
(۲) برای تأیید اینکه آیا مشتری پرداخت را انجام داده است یا خیر، تاجر درخواست تأیید به سیستم زنجیره بلوک می کند.

(۳) پس از خرید محصولات و خدمات از تاجر، مشتری کد QR را اسکن می کند تا قیمت را به تاجر بپردازد. پرداخت مستقیماً به تاجر منتقل نمی شود. یک درخواست پرداخت به سیستم بلاک چین انجام می شود که شامل دفتر کل تراکنش است.

(۴) سیستم بلاک چین مبلغ پرداختی را از حساب مشتری کسر می کند و همان مبلغ را در حساب تاجر جمع می کند. پس از اجرای این انتقال بین حساب ها، سیستم بلاک چین نتایج را به تاجر منتقل می کند. هنگامی که تاجر تایید می

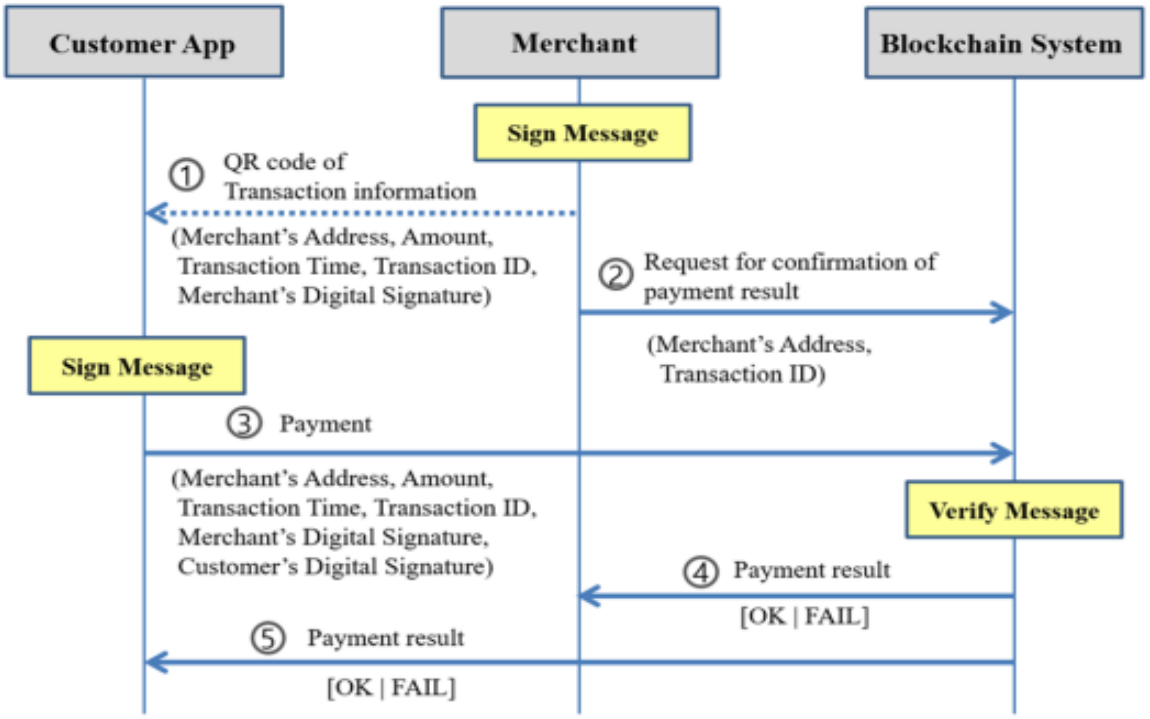
کند که پرداخت انجام شده است، محصول خریداری شده را تحویل می دهد یا شروع به ارائه خدمات خریداری شده به مشتری می کند.

(۵) سیستم بلاک چین همچنین اطلاعات نتیجه پرداخت را به برنامه تلفن هوشمند مشتری منتقل می کند (Kim & Kim, 2022).



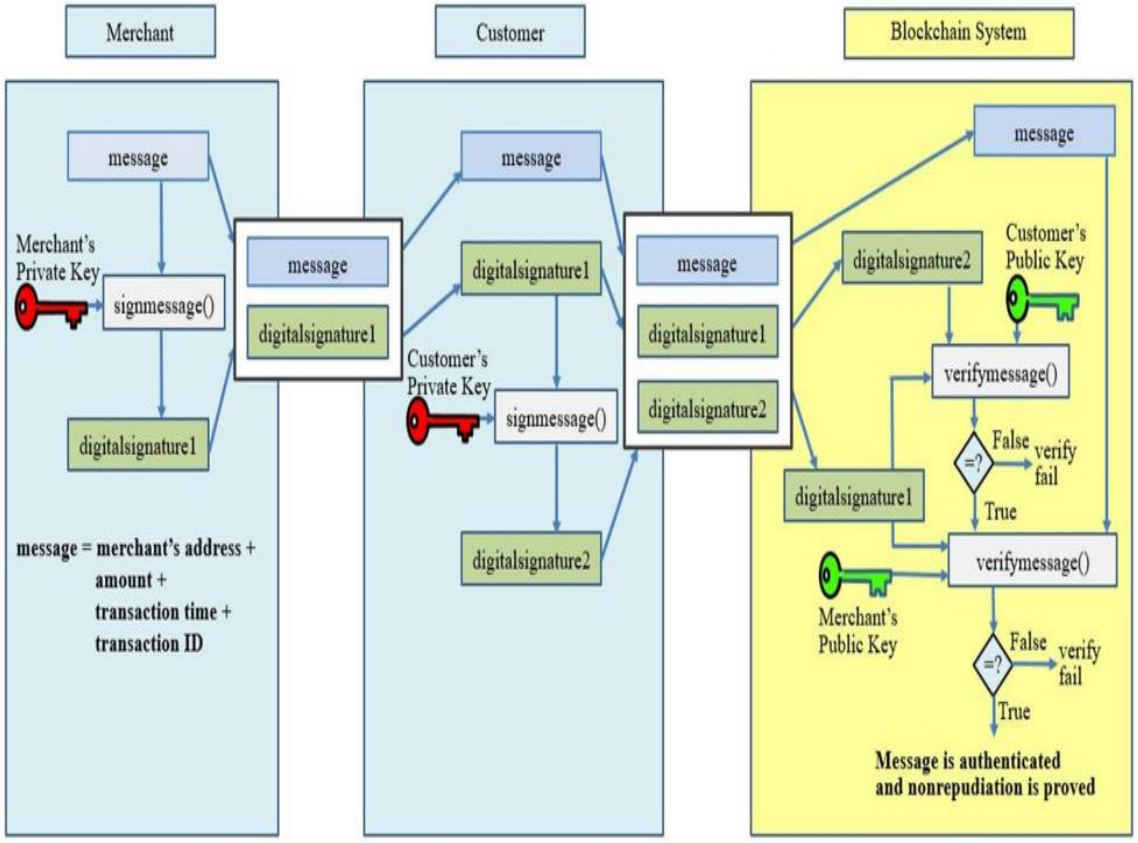
شکل ۴. ساختار احراز هویت

این روشی است که از طریق آن پرداخت در سه مؤلفه تاجر، برنامه تلفن هوشمند مشتری و سیستم بلاک چین تأیید می شود. یک امضای دیجیتال در دستگاه تاجر از طریق فرآیند پیام علامت تولید می‌شود و امضای دیجیتال دیگری با استفاده از عملکرد پیام علامت در برنامه تلفن هوشمند مشتری ایجاد می‌شود. امضای دیجیتالی تاجر و مشتری در سیستم بلاک چین با استفاده از تابع پیام تأیید می شود. شکل ۵ امضای دیجیتال و رویه های تأیید را در فرآیند پرداخت نشان می دهد. پارامترهای منتقل شده بین تاجر، برنامه تلفن هوشمند مشتری و سیستم بلاک چین عبارتند از آدرس، مبلغ، زمان تراکنش، شناسه تراکنش، امضای دیجیتال تاجر، و امضای دیجیتال مشتری. تاجر و مشتری هر کدام کلیدهای عمومی و خصوصی خود را دارند (Kim, & Kim, 2022).



شکل ۵. معماری سیستم پرداخت تجارت الکترونیک بلاکچین

شکل ۶ بلوک دیاگرام زیرسیستم های تاجر، مشتری و بلاک چین را نشان می دهد که اصول فرآیند احراز هویت بلاک چین هستند. زیرسیستم تاجر پیامی حاوی آدرس، مبلغ، زمان تراکنش و شناسه تراکنش تاجر را پیکربندی می‌کند. این پیام با کلید خصوصی تاجر امضا می‌شود تا یک امضای دیجیتال تولید کند که به‌عنوان یک کد QR شامل پنج پارامتر در صفحه مرکز خرید آنلاین تاجر نمایش داده می‌شود. با استفاده از کد QR، مشتری پیام و امضای دیجیتال تاجر (digitalsignature1) را دریافت می کند. امضای دیجیتالی به دست‌آمده ۱ سپس با کلید خصوصی مشتری امضا می‌شود تا امضای دیجیتال مشتری (digitalsignature2) تولید شود. سپس، مشتری پیام و امضای دیجیتالی را که توسط تاجر ارسال می‌شود و امضای دیجیتالی تولید شده توسط مشتری را به سیستم بلاک چین منتقل می‌کند. در نهایت، سیستم بلاک چین پیام (شامل آدرس تاجر، مبلغ، زمان تراکنش و شناسه تراکنش)، digitalsig nature1 و digitalsignature2 را از مشتری دریافت می‌کند. بعد، کلید عمومی مشتری برای تأیید امضای دیجیتال ۱ و امضای دیجیتال ۲ استفاده می شود. هنگامی که نتایج مطابقت دارند، ثابت می‌شود که Digitalsignature1 یکپارچگی دارد و مشتری تنها کسی است که می‌تواند آن را ارسال کند. بعداً، کلید عمومی تاجر برای تأیید امضای دیجیتال ۱ و پیام رسان (شامل آدرس تاجر، مبلغ، زمان تراکنش و شناسه تراکنش) استفاده می‌شود. هنگامی که نتایج مطابقت دارند، ثابت می شود که پیام یکپارچگی دارد و تاجر تنها کسی است که می تواند آن را ارسال کند. یکپارچگی و عدم انکار تراکنش پرداخت از طریق این فرآیند تأیید تضمین می شود (Kim & Kim, 2022).

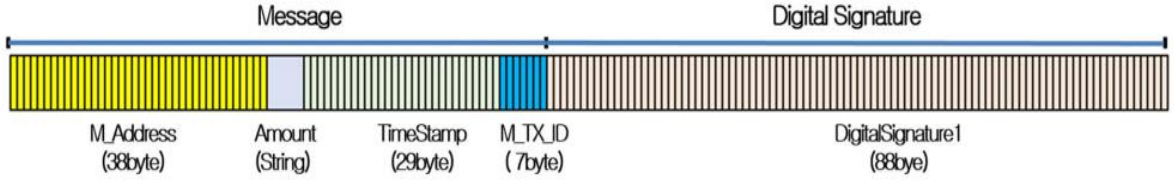

Merchant
Customer
Blockchain System
message
Merchant's Private Key
signmessage()
digitalsignature1
message = merchant's address + amount + transaction time + transaction ID
Customer's Private Key
digitalsignature2
verifymessage()
=?
False
verify fail
True
Merchant's Public Key
Customer's Public Key
Message is authenticated and nonrepudiation is proved

شکل ۶. بلوک دیاگرام زیرسیستم های احراز هویت بلاکچین

زیرسیستم بازرگان

شکل ۷ و جدول ۱ بسته داده تحویل شده از تاجر به مشتری را با استفاده از یک کد QR نمایش داده شده در صفحه مرکز خرید آنلاین نشان می دهد. سپس، مشتری قصد خرید را نشان می‌دهد و مولد تاجر با اتصال مقادیر آدرس، زمان تراکنش و شناسه تراکنش در یک رشته، پیامی را می‌خورد. بعداً، پیام به صورت دیجیتالی با کلید خصوصی تاجر امضا می‌شود و امضای دیجیتالی را ایجاد می‌کند. سپس، تاجر M_Address، Amount، TimeStamp، M_TX_ID، و DigitalSignature1 را به عنوان نمایش می دهد. یک کد QR در صفحه مرکز خرید آنلاین خود. تاجر پیامی با رشته‌ای از M_Address، Amount، TimeStamp و M_TX_ID تولید می‌کند. پیام پیکربندی شده به صورت دیجیتالی با آدرس تاجر (کلید عمومی) برای تولید امضای دیجیتالی امضا می‌شود. الگوریتم امضای دیجیتال تاجر به شرح زیر است:

در شکل ۷، signmessage و verifymessage توابعی هستند که امضای دیجیتال را پردازش می کنند. پیام علامت تابع اصولا باید از یک کلید خصوصی استفاده کند، اما ممکن است برای راحتی از یک کلید عمومی استفاده شود. در واقع، استفاده از کلید عمومی به دلایل امنیتی توصیه می شود، زیرا این کار از افشای کلید خصوصی در منبع برنامه جلوگیری می کند. هنگامی که کلید عمومی به جای کلید خصوصی وارد می شود، تابع به صورت داخلی آن را با a جایگزین می کند. کلید خصوصی برای رمزگذاری در همین حال، verifymessage دارای پارامترهای ورودی آدرس (کلید عمومی)، ماهیت علامت دیجیتال و پیام است. اگر امضای دیجیتال رمزگشایی شده و پیام دارای یک مقدار باشند، "true" برگردانده می شود. در غیر این صورت، "نادرست" برگردانده می شود. DigitalSignature1 پارامتری است که در آن تاجر به صورت دیجیتالی پیام حاوی رشته M_Address، Amount، TimeStamp و M_TX_ID را با استفاده از کلید خصوصی خود امضا می کند (Kim & Kim, 2022).



شکل ۷. فرمت پیام تاجر و امضای دیجیتال

جدول ۱. امضای دیجیتالی تاجر و مولفه پیام

Algorithm 1 Digital Signature by Merchant

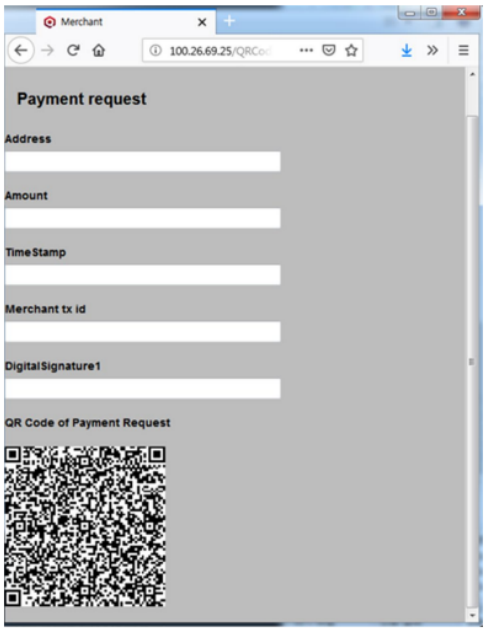
1. message = M_Address + Amount + TimeStamp + M_TX_ID
2. DigitalSignature1 = signmessage(M_Address, message)

Item	Size	Description
M_Address	38 bytes	Merchant's address (public key)
Amount	String	Payment amount
TimeStamp	29 bytes	Payment transaction time (UTC)
M_TX_ID	7 bytes	Merchant's transaction ID
DigitalSignature1	88 bytes	Generated by digitally signing the message with the merchant's private key

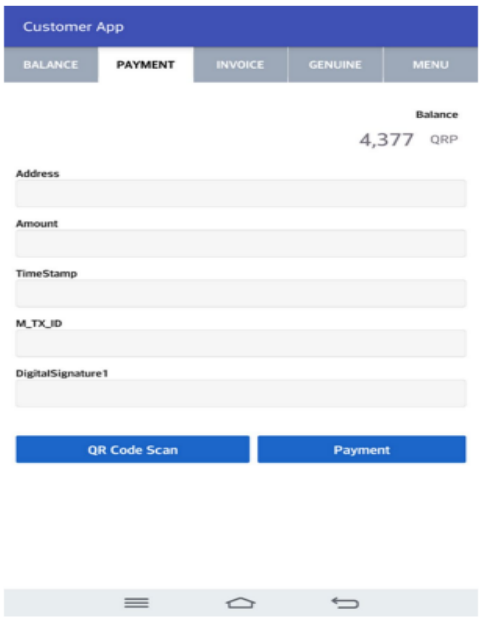
شکل ۸ نشان می دهد صفحه کد QR حاوی پنج نقطه داده پارامتر همانطور که در جدول ۲ نشان داده شده است.

جدول ۲. توابع signmessage و verifymessage

Function	Return value	Description
signmessage()	Digital signature	Returns a digital signature, which proves that the message was approved by the owner of the address or private key DigitalSignature = signmessage([address | private key], message)
verifymessage()	True or false	Verifies that message was approved by the owner of address by checking the digital signature. The result is true or false unless an error occurs [True | False] = verifymessage(address, digitalsignature, message)



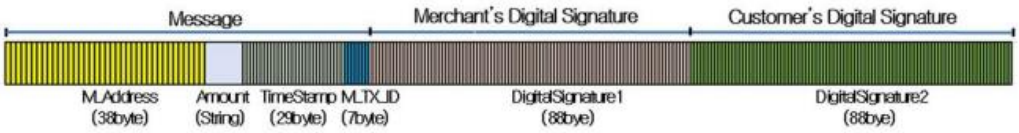
شکل ۹. صفحه کاربری مشتری



شکل ۸. صفحه بازرگان

هنگامی که مشتری برنامه را راه‌اندازی می‌کند و دکمه «QR Code Scan» را انتخاب می‌کند، دوربین تلفن برای اسکن کد QR خواننده در برنامه راه‌اندازی می‌شود. همانطور که در شکل ۹ نشان داده شده است. شکل ۱۰ و جدول ۳، برنامه مشتری امضای دیجیتال ۲ را برای اثبات یکپارچگی و عدم انکار تولید می کند را نشان می دهند.

یعنی Digitalsignature1 تولید شده توسط تاجر دوباره به صورت دیجیتالی با کلید خصوصی مشتری برای تولید Digitalsignauture2 امضا می شود. آدرس مشتری (C_Address)، یک پارامتر ورودی، یک کلید عمومی است که با یک کلید خصوصی در تابع signmessage جایگزین می شود. برنامه مشتری دارای آدرس (کلید عمومی) و یک کلید خصوصی است. الگوریتم ۲ الگوریتم امضای دیجیتال برنامه مشتری همانطور که در جدول ۴ نشان داده شده است. در اینجا، برنامه مشتری M_Address، Amount، TimeS tamp، M_TX_ID، و DigitalSignature1 که توسط کد QR تاجر و DigitalSignature2 تولید شده به دست آمده است، همانطور که در شکل ۱۰ نشان داده شده است، به سیستم بلاک چین ارسال می کند (Kim & Kim, 2022).



شکل ۱۰. فرمت داده پیام و امضای دیجیتال پردازش شده توسط برنامه مشتری

جدول ۴. تنظیمات سخت افزاری و نرم افزاری برای آزمایش

Item	Size	Description
M_Address	38 bytes	Get value from QR code
Amount	String	Get value from QR code
TimeStamp	29 bytes	Get value from QR code
M_TX_ID	7 bytes	Get value from QR code
DigitalSignature1	88 bytes	Get value from QR code
DigitalSignature2	88 bytes	Generated by digitally signing DigitalSignature1 with the customer's private key

جدول۳. امضای دیجیتال پردازش شده توسط برنامه مشتری

Component	Hardware	Software
Merchant	AWS EC2 (m5.large)	Node.js v8.12.0
Customer application	LG G Pad HomeBoy	Android 4.2.2, Android Studio 3.2.1, Java SDK version 28
Blockchain system	AWS EC2 (m5.large)	Node.js, MultiChain 1.0.3

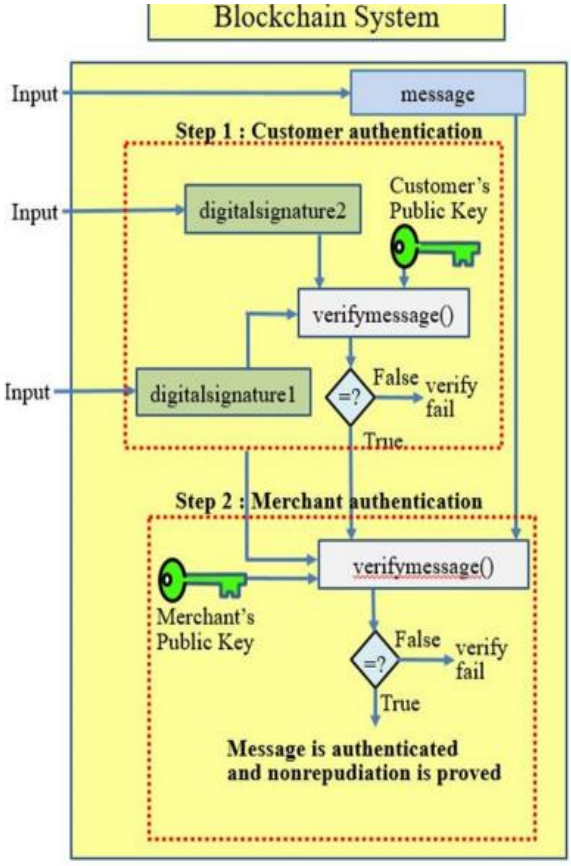
زیرسیستم بلاک چین

همانطور که در شکل ۱۱ نشان داده شده است، سیستم بلاک چین یک فرآیند احراز هویت دو مرحله‌ای را اجرا می‌کند. مرحله اول اجرای تابع تایید برای مشتری است و در مرحله بعد همان فرآیند را برای تاجر دنبال می کند. وقتی نتیجه تأیید پیام «درست» باشد، ثابت می‌شود که پیام‌های ارسال شده توسط مشتری و تاجر یکپارچگی دارند و دو طرف تنها افرادی هستند که می‌توانند پیام‌ها را ارسال کنند، که تضمین می‌کند که مرحله ۱ یک رویه است. که یکپارچگی و عدم انکار اطلاعات درخواست پرداخت از برنامه مشتری را تأیید می کند. در اینجا، digitalsignature2، که توسط برنامه مشتری امضا شده است، با استفاده از تابع verifymessage تأیید می شود. یعنی verifymessage digitalsignature2 را با استفاده از کلید عمومی مشتری رمزگشایی می کند و مقدار حاصل را با Digitalsignature1 مقایسه می کند. هنگامی که مقادیر مطابقت دارند، سیستم "true" را برمی گرداند. در مرحله ۲، یکپارچگی و عدم انکار اطلاعات درخواست پرداخت تاجر احراز هویت می شود. دیجیتال digitalsignature1 امضا شده توسط تاجر با استفاده از تابع verifymessage تایید می شود. یعنیverify message digitalsignature1 را با استفاده از کلید عمومی تاجر رمزگشایی می کند و مقدار حاصل را با پیام مقایسه می کند. هنگامی که مقادیر مطابقت دارند، سیستم "true" را برمی گرداند. در این مورد، پیام شامل M_address، Amount، TimeStamp و M_TX_ID است. هنگامی که دو مرحله احراز هویت پیام با موفقیت اجرا شد، M_TX_ID تاجر برای انتقال نتیجه پرداخت مقایسه می‌شود. علاوه بر این، مقدار زمان و زمان جاری در سیستم زنجیره بلوک را می توان با حملات پخش مجدد بلوک مقایسه کرد. الگوریتم ۳ روش احراز هویت پیام توضیح داده شده در بالا را نشان می دهد (Kim & Kim, 2022).

Algorithm 3 Authentication by Blockchain System

INPUT : M_Address, Amount, TimeStamp, M_TX_ID, DigitalSignature1, DigitalSignature2 from Customer App,
M_Address, M_TX_ID from Merchant

```
1.  message = M_Address + Amount + TimeStamp + M_TX_ID
2.  // Step 1 : Customer authentication
3.  if (verifymessage(C_Address, DigitalSignature2, DigitalSignature1)) {
4.      // Step 2 : Merchant authentication
5.      if (verifymessage(M_Address, DigitalSignature1, message)) {
6.          if (M_Address + M_TX_ID from Merchant ==
7.              M_Address + M_TX_ID from Customer App) {
8.              send OK to Customer App and Merchant
9.          } else {
10.             send FAIL to Customer App and Merchant
11.         }
12.     } else {
13.         send FAIL to Customer App and Merchant
14.     }
15. } else {
16.     send FAIL to Customer App and Merchant
17. }
```



شکل ۱۱. فرآیند احراز هویت پیام دو مرحله ای زیر سیستم بلاک چین

امنیت در سیستم های پرداخت با استفاده از بلاکچین غیرمتمرکز

بررسی روش پیشنهادی (Hyperledger Fabric)

Hyperledger Fabric یک پلتفرم دفتر کل توزیع شده می‌باشد و مشکل وابستگی به شخص ثالث را کاهش و هزینه های مضاعف را حذف می‌کند همچنین یک زیرساخت بلاکچین مجاز غیرمتمرکز و سریعترین بلاکچین مجاز منبع باز است. هک کردن آن امری دشوار و چالش برانگیز است، زیرا از محاسبات ریاضی پیچیده استفاده می‌کند. همچنین معماری آن درجه بالایی از انعطاف پذیری را در اجرا و طراحی فراهم می‌کند. این انعطاف پذیری موجب حفظ حریم خصوصی، مقیاس‌پذیری و سایر ویژگی‌های ضروری می‌شود (Al-Amin et al, 2022).

زیرساخت های معماری

سیستم پیشنهادی از پایه های لینوکس Hyperledger Fabric به عنوان چارچوبی برای این پروژه استفاده کرده و کل معماری بر این اساس طراحی شده است. معماری Hyperledger Fabric به ما امکان می‌دهد یک شبکه خصوصی برای همه سازمان ها ایجاد کنیم. تمام بخش اتوماسیون توسط ChainCode انجام می‌شود. این قرارداد هوشمند Hyperledger Fabric است. یک پایگاه داده مرکزی وجود خواهد داشت که داده ها را تا زمانی که کل فرآیند به پایان می‌رسد حفظ می‌کند، اما برای اطمینان از ایمنی و حفظ حریم خصوصی، سیستم به کسی که فقط توسط خود سیستم به آن دسترسی دارد دسترسی به پایگاه داده و داده ها را نمی

دهد. زیرا فقط داده های بزرگ در اینجا نگهداری می شود و تمام اطلاعات مربوط به آن به بلوک های بلاک چین ارجاع می شود (Al-Amin et al, 2022).

جریان داده در سیستم پیشنهادی

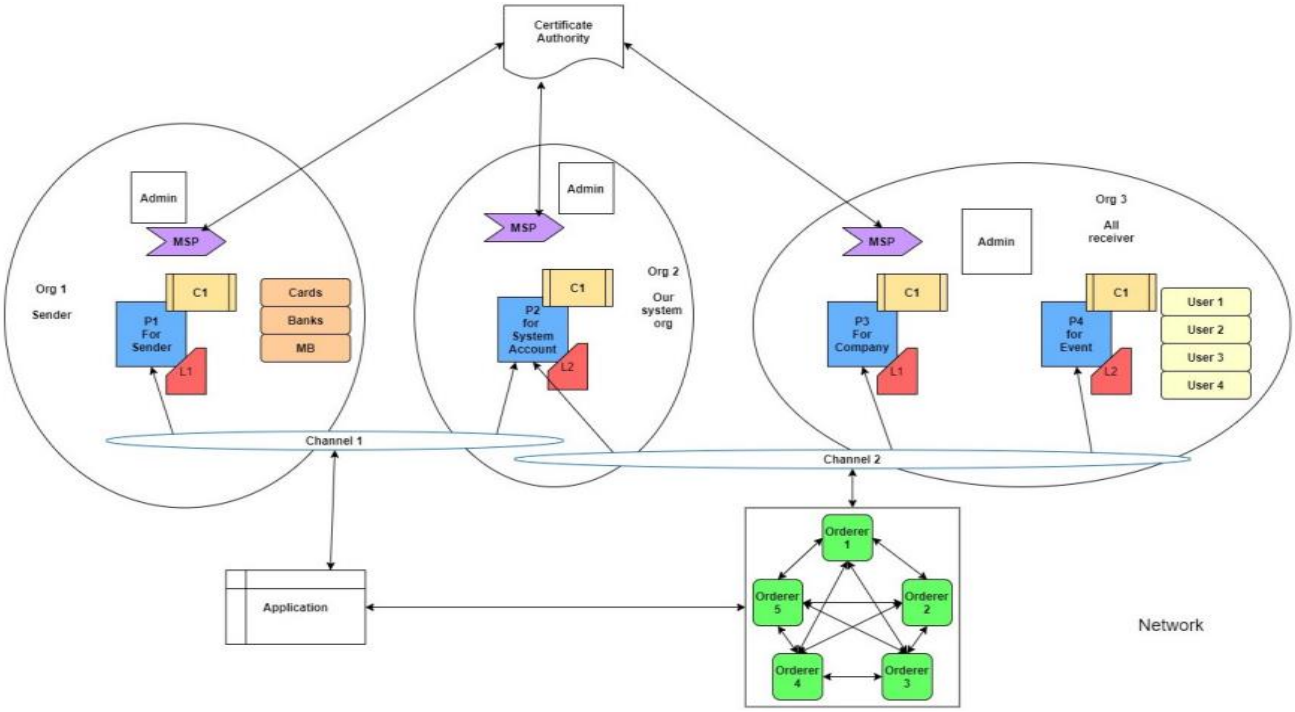
در این سیستم پیشنهادی از Hyperledger Fabric بعنوان چارچوب استفاده شده که در شکل ۱۲ نشان داده شده است. درحالی که طراحی کل معماری را دنبال می‌کنیم، از قرارداد و قوانین یکپارچه Hyperledger پیروی می‌کنیم. در این سیستم دو تراکنش در مقابل هر پرداخت یا ارسال پول انجام می‌شود. اولین مورد انتقال دارایی از مشتری یا فرستنده به بانک ما[1] است. در قسمت دوم سیستم درخواست انتقال از بانک ما به بانک گیرنده را می دهد. جریان تراکنش برای هر دو مرحله تعهد به شرح زیر است:

درخواست تراکنش از برنامه ایجاد می‌شود و این برنامه با استفاده از یک SDK پشتیبانی‌شده، از یکی از همتایان سازمان برای تولید پیشنهاد تراکنش استفاده می‌کند. این پیشنهاد معامله برای همتا ارسال می شود و این همتاها از طریق مرجع گواهی ثبت می شوند. اما مسئولیت همتایان توسط MSP تعریف شده است. این بدان معناست که کدام تراکنش متعلق به کدام همتا است و این مجوزهای تایید کننده و متعهد توسط MSP تعریف می‌شود. در هر peer نیز یک دفتر کل وجود دارد که تمام تراکنش ها در آن ذخیره می‌شوند. هنگامی که تراکنش به همتا منتقل می‌شود، همتا کد زنجیره ای را اجرا می‌کند و تراکنش را تایید می‌کند اما این تراکنش هنوز در دفتر کل ذخیره نشده است. فقط یک پروپوزال تایید اعتبار با علامت معتبر تولید می‌شود و این پیشنهاد توسط برنامه تأیید می‌شود. اگر هر دو پیشنهاد امضا شده از هر دو همتا مطابقت داشته باشند، این پیشنهاد به روز شده را به گره سفارش دهنده ارسال می‌کند (Al-Amin et al, 2022).

در همین حال، از آنجایی که چندین گره سفارش دهنده موجود است، از پروتکل توافق RAFT برای انتخاب اینکه کدام سفارش دهنده بلوک بعدی را انجام دهد استفاده می شود. همچنین، از آنجایی که چندین گره وجود دارد، بنابراین اگر یک گره پایین باشد، بقیه گره ها می‌توانند بلوک را بسازند (Al-Amin et al, 2022).

این گره های سفارش دهنده در یک زمان می‌توانند چندین تراکنش را از برنامه های مختلف بپذیرند و اعتبار این گره ها را بررسی کرده و یک بلوک ایجاد کنند. این بلوک‌ها مجدداً برای همتای تایید کننده ارسال می‌شوند تا تمام تراکنش‌هایی را که با استفاده از همتاهای تایید کننده تأیید شده‌اند بررسی کند. اگر تراکنش‌هایی در بلوکی که قبلاً تایید نشده است باقی بماند، این بلوک به عنوان بلوک نامعتبر در نظر گرفته می‌شود. در غیر این صورت بلوک به عنوان بلوک معتبر در نظر گرفته می شود و در دفتر کل هر همتای شبکه اضافه می شود. (شکل زیر گویای این فرایند است) (Al-Amin et al, 2022).

[1] نکته: در این قسمت برای بیان راحت تر مفاهیم از کلمه "ما" برای شرح عملکرد معماری استفاده شده است.



شکل ۱۲. جریان داده و روند تائید در بلاکچین

بررسی روش پیشنهادی دوم

در معماری پیشنهادی، فرستنده تمام اطلاعات را به ماینر می‌دهد. سپس ماینر تمام اطلاعات را تأیید می‌کند.کار مرجع صدور گواهی (CA) با ماینر تقسیم شده است تا بتواند درخواست های بیشتری را در مقایسه با سیستم های قبلی انجام دهد. اگر سیستم

متوجه شود که شخصی در حال تلاش برای انجام یک تراکنش ناآگاه است، بلافاصله تراکنش را لغو می‌کند، به جای مسدود کردن حساب، آن را در حالت تعلیق قرار می‌دهد (Ahamed et al, 2021).

تعریف الگوریتم

S و R به ترتیب فرستنده و گیرنده تراکنش هستند.

علاوه بر این، ماینرهایی وجود دارند که در واقع تراکنش را تأیید می‌کنند.

Keygen : 1exp φ دریافت ورودی که یک پارامتر امنیتی است و الگوریتم یک جفت کلید عمومی (Pk) و کلید خصوصی (Pr) را برمی‌گرداند.

علامت (Pr, m): یک کلید خصوصی Pr به عنوان ورودی و m می گیرد.

این الگوریتم علامت γ را بر روی m برمی گرداند.

تأیید (γ, Pk): یک امضای ورودی و کلید عمومی Pk می‌گیرد.

الگوریتم true یا false را برمی‌گرداند. این الگوریتم برای تایید تراکنش فراخوانی می‌شود.

BlockchainGen (b, Pk, Pr, n) گرفتن بیت کوین ورودی b، کلید عمومی Pk، کلید خصوصی Pr، n زنجیره. الگوریتم زنجیره ای از n زنجیره را برمی‌گرداند. سپس بلاکچین ایجاد می‌شود و سپس بیت کوین به زنجیره ای از n زنجیره تبدیل می‌شود (Ahamed et al, 2021).

فرآیند تراکنش توسط الگوریتم

فاز ۱ تنظیم عملکرد: CA به عنوان یک شخص ثالث قابل اعتماد در نظر گرفته می‌شود که مسئول مدیریت گواهی کاربران است. در این مدل وظیفه آن ها تولید کلید عمومی برای کاربر است. در اینجا کلید عمومی می تواند ۵۱۲ واحد طول را آدرس دهد و سپس آنها را در یک بلوک ذخیره کند.

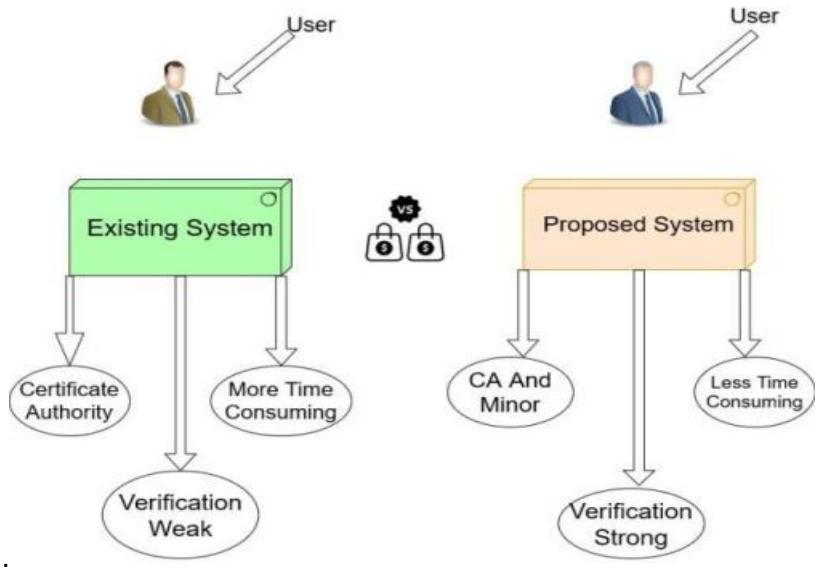
فاز ۲ کاربران معتبر: در این مرحله ماینر کاربران را بر اساس آدرس و مقدار آنها تأیید می‌کند. اگر مقدار بیشتر از ۰ باشد، کاربر معتبر است.

فاز ۳ فرآیند تراکنش: UDS (امضای دیجیتال کاربر) اصطلاحی است که برای تأیید صحت و یکپارچگی تراکنش استفاده می‌شود. برای کاربران ایجاد شده است. ماینرهایی برای بررسی امضای دیجیتال وجود دارد. اگر امضای دیجیتال معتبر باشد، تراکنش انجام می‌شود در غیر این صورت تراکنش را لغو می‌کند.

فاز ۴ به روز رسانی داده ها: اگر کاربران نیاز به به روز رسانی برخی از داده ها داشته باشند، درخواستی را برای به روز رسانی داده ها به ماینر ارسال می‌کنند. سپس ماینر کار را با کمک مرجع گواهی انجام می‌دهد و بلوک را با اطلاعات به روز به روز می‌کند.

فاز ۵ مشاهده همه تراکنش ها: تمام تراکنش های بلاکچین باید توسط ماینرها بررسی شود. بررسی می‌شود که آیا تراکنش بدون کلید عمومی وجود دارد یا خیر. ماینر می‌تواند تراکنش را به صورت ایمن ذخیره کند و می‌تواند تمام تراکنش ها را مشاهده کند.

یک فرآیند تراکنش ایمن و قابل اعتماد پیاده سازی شده است. در اینجا یک فایل JSON وجود دارد که برای نمایش داده های ساخت یافته استفاده می‌شود(Ahamed et al, 2021).



شکل ۱۳. مقایسه بین سیستم فعلی و سیستم ما

نتیجه گیری

با مطالعه این مقاله هنگام پردازش پرداخت کارت اعتباری در تنظیمات تجارت الکترونیک، مشتریان و بازرگانان ملزم به استفاده از سرویس PG هستند. مقاله حاضر یک مدل پرداخت راحت را بدون واسطه تراکنش، مانند گواهی کلید عمومی یا PG پیشنهاد کرد و طرحی را برای تأیید پتانسیل کاربردی آن پیاده‌سازی کرد. آزمایشی برای تأیید اینکه ویژگی‌های بلاک چین مانند کلید عمومی، کلید خصوصی و امضای دیجیتال، می‌توانند برای ساخت یک سیستم پرداخت الکترونیکی کارآمد بدون نیاز به پیاده‌سازی ماژول‌های اضافی مورد استفاده قرار گیرند، انجام شد. در نتیجه، مشخص شد که سیستمی که در آن تاجر، مشتری و زیرسیستم‌های زنجیره بلوکی، هر کدام احراز هویت را اجرا می‌کنند، می‌تواند یکپارچگی و عدم انکار تراکنش‌های پرداخت را تضمین کند. پیشنهادی که در مطالعه حاضر ارائه شده است، انتقال داده بین بازرگانان و مشتریان را با استفاده از کد QR آسان‌تر و راحت‌تر می‌کند، و به این ترتیب، ممکن است به عنوان جایگزینی برای حل مسائل مربوط به هزینه‌های پرداخت برای پردازش تراکنش‌های تجارت الکترونیک عمل کند (Kim & Kim, 2022). در این مقاله مدل هایی مطرح شده است تا تراکنش پرداخت غیر متمرکز ایمن تر، آسان تر و انعطاف پذیر تر باشد. بلاکچین غیر متمرکز این پتانسیل را دارد تا امکان یک تراکنش ایمن و سریع را به کاربران ارائه دهد. تمرکز اصلی این مقاله ها در رابطه با قابلیت اطمینان و تسریع تراکنش در درگاه پرداخت غیرمتمرکز می‌باشد، در مدل های معرفی شده هرکسی می‌تواند تراکنش های خود را با امنیت و سرعت بالاتری انجام دهد.

منابع

Al-Amin, M., Shahrina, K., Hossain, R., Sarker, D., & Meem, S. S. (2022). Decentralized Payment Aggregator: Hyperledger Fabric. International Journal of Advanced Computer Science and Applications, 13(10).

Ahamed, S., Siddika, M., Islam, S., Anika, S., Anjum, A., & Biswas, M. (2021). Bps: Blockchain based decentralized secure and versatile light payment system. Asian Journal of Research in Computer Science, 8(4), 12-20.

Li, X. H. (2021, March). Blockchain-based cross-border E-business payment model. In 2021 2nd International Conference on E-Commerce and Internet Technology (ECIT) (pp. 67-73). IEEE.

Kim, S. I., & Kim, S. H. (2022). E-commerce payment model using blockchain. Journal of Ambient Intelligence and Humanized Computing, 13(3), 1673-1685.

Investigating the blockchain-based payment model and increasing security in payment systems using decentralized blockchain

Fatemeh Kolivand[2]. Master's student, Department of Information Technology Engineering, Faculty of Engineering, Azad University, South Tehran Branch

Faezeh Mojarad. Master's student, Department of Information Technology Engineering, Faculty of Engineering, Azad University, South Tehran Branch

Fatemeh Khodaparast. Professor, Department of Information Technology Engineering, Faculty of Engineering, Azad University, South Tehran Branch

Abstract

With the rapid development of global e-commerce, improving the efficiency and convenience of e-commerce payments becomes increasingly important. Current e-commerce payment systems require a PG payment gateway for credit cards or checks. This entails PG costs, which in turn increases the cost of engaging in e-commerce. Blockchain technology is a distributed ledger that gives participants the opportunity to establish a credit agreement on a set of shared facts without mutual trust, using a cryptographic mechanism and consensus algorithms, etc. The features of blockchain technology's decentralization, continuity, anonymity and auditability, immutability, transparency and natural settlement are actually fully in line with the demand of the electronic payment field. Part of this paper proposes a simple payment model that uses the basic features of digital currencies, such as public key, private key, and digital signature, to eliminate the need for transaction intermediaries such as public key certificates and PG. On the other hand, there are still concerns regarding privacy and security in decentralized blockchain, and another part of this research, Hyperledger Fabric and BPS algorithms to increase security and speed in decentralized blockchain, has been introduced and investigated .

Keywords: Payment Systems, Security, Decentralized Blockchain, Hyperledger Fabric, BPS.

[2] Corresponding Author