Journal of Electronical & Cyber Defence
Vol. 9, No. 2, 2021, Serial No. 34

The Design of a Blockchain-based Electronic Payment Protocol Preserving User Anonymity

Z. Hatefi, M. Bayat*, N. Hamian

*Shhed University

(Received: 26/08/2020, Accepted: 11/01/2021)

ABSTRACT

The security of electronic payment systems has become prominent with the increase in demand. Protection against double spending, tracing malicious users, user anonymity and privacy-preserving are important secure goals of any electronic payment system. To achieve these goals, blockchain technology is useful. The blockchain technology can solve many issues, such as bottlenecks, delays and operational risks that exist in the financial industry, but blockchain-based electronic payment systems cannot punish or trace malicious users without using a trusted third party (TTP). In this article, we present a blockchain-based electronic payment scheme to protect the anonymity and privacy of honest users, and also trace and punish malicious users with no need of a TTP. We have used a fair blind digital signature scheme and a secret sharing scheme for this purpose. In our proposed method, the users also employ pseudonyms to maintain anonymity and as these pseudonyms are generated by pre-computations, the proposed scheme has a good performance.

Keywords: Blockchain, Electronic Payment, Anonymity, Conditional Privacy, Traceability, Revocation

* Corresponding Author Email: mbayat@shahed.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۲، تابستان ۱۴۰۰، ص ۱۰۰-۸۵

علمی – پژوهشی

طراحی یک پروتکل پرداخت الکترونیکی مبتنی بر زنجیره‌قالب با حفظ گمنامی کاربران

زهرا هاتفی[۱]، مجید بیات[۲*]، نگین حامیان[۱]

۱ و ۳- کارشناس‌ارشد مخابرات امن و رمزنگاری، گروه مخابرات، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

۲- استادیار گروه کامپیوتر، دانشگاه شاهد، تهران، ایران

(دریافت: ۱۳۹۹/۰۶/۰۵، پذیرش: ۱۳۹۹/۱۰/۲۲)

چکیده

با افزایش تقاضا، سامانه‌های پرداخت الکترونیک مورد توجه قرار گرفته‌اند. محافظت در برابر خرج مضاعف، ردیابی کاربران مخرب، گمنامی کاربران و حفظ حریم خصوصی آن‌ها از جمله اهداف مهم هر سیستم پرداخت الکترونیکی می‌باشد. برای رسیدن به این اهداف، فناوری زنجیره‌قالب بسیار مفید می‌باشد، فناوری زنجیره‌قالب می‌تواند بسیاری از تنگناها، تاخیر و خطرات عملیاتی را که در صنعت مالی وجود دارند را حل کند؛ اما سامانه‌های پرداخت الکترونیک مبتنی بر زنجیره‌قالب توانایی تنبیه و یا ردیابی کاربران مخرب بدون استفاده از شخص سوم قابل اعتماد را ندارند. در این مقاله، ما یک طرح پرداخت الکترونیک مبتنی بر زنجیره‌قالب را ارئه می‌دهیم که علاوه بر قابلیت حفظ گمنامی و حریم خصوصی کاربران صادق، در صورت لزوم قادر به ردیابی و تنبیه کاربران مخرب بدون نیاز به استفاده از شخص سوم قابل اعتماد، نیز می‌باشد. برای این منظور از یک امضای کور عادلانه و یک طرح تسهیم راز استفاده کرده‌ایم. همچنین در این طرح برای حفظ گمنامی، کاربران از نام‌های مستعار استفاده می‌کنند و از آن جایی که نام‌های مستعار به‌صورت پیش محاسبه، تولید می‌شوند، طرح پیشنهادی دارای عملکرد مطلوبی است.

کلید واژه‌ها: زنجیره‌قالب، پرداخت الکترونیک، گمنامی، حریم خصوصی مشروط، ردیابی، لغو عضویت

۱- مقدمه

معاملات مالی برای اقتصاد ملی و جهانی پایه و اساس است. سامانه‌های مالی جهانی هر روز هزار میلیارد دلار به مشتریان می‌پردازند. حریم خصوصی داده یک جنبه ضروری در تراکنش‌های مالی است زیرا مشتریان به حریم خصوصی داده‌شان اهمیت می‌دهند [۱].

پنج الزام مهم برای سامانه کامل پول نقد الکترونیکی وجود دارد. آنها عبارتند از: (۱) احراز اصالت متقابل، (۲) قابل اطمینان بودن، (۳) گمنامی، (۴) انکارناپذیری و (۵) ردیابی. "احراز اصالت متقابل" به این معنی است که دو طرف می‌توانند به‌طور صحیح یکدیگر را تائید کنند. "قابلیت اطمینان" اشاره می‌کند که می‌تواند اطمینان حاصل شود صحت و یکپارچگی پیام‌های ارسال شده توسط طرف دیگر تعیین شده است. در ویژگی "گمنامی" باید دو مورد متفاوت در نظر گرفته شود: (۱) ناشناس بودن پرداخت‌کنندگان و (۲) ناشناس بودن دریافت‌کنندگان. "انکارناپذیری" و در نهایت "ردیابی" نیز به این معنی است که می‌توان هویت کاربر مخرب را آشکار کرد [۲].

بررسی دارایی، نگهداری سوابق، حریم خصوصی داده و هزینه‌های معامله چند حوزه از حوزه تراکنش مالی هستند.

پیشرفت‌های فن‌آورانه گذشته جایگزین‌هایی را در نظر گرفت که در نتیجه میزان رقابت را تشدید می‌کرد. به‌عنوان مثال، محصولات مالی اینترنتی به سهم بازار موسسات مالی سنتی تجاوز کرده‌است. به منظور برآورده کردن نیازهای مشتری، بخش مالی باید از طریق به‌کارگیری فناوری‌های جدید به‌طور مداوم نوآوری داشته باشد. از این رو، فناوری زنجیره‌قالب به‌عنوان یک فناوری نوین در زمینه‌های مالی شناخته شده است

فناوری زنجیره‌قالب توسط ناکاماتو [۳] برای دور زدن فعالان واسطه مانند موسسات مالی با اجازه دادن به تراکنش‌های همتا به همتا معرفی شد. برای رسیدن به این هدف، ناکاماتو یک دفتر توزیع همتا به همتا را پیشنهاد کرد. بدین ترتیب، پرداخت‌کننده و دریافت‌کننده می‌توانند مستقیما بر روی شبکه، با استفاده از سازوکارهای رمزگذاری و توافق عمومی تبادل نظر کنند [۴].

زنجیره‌قالب به‌عنوان یک معماری امن، قابل اعتماد و غیرمتمرکز، برای ایجاد طرح‌های پرداخت امن استفاده می‌شود

* رایانامه نویسنده مسئول: mbayat@shahed.ac.ir

که می‌تواند به اقتصاد و جوامع بدون شخص سوم قابل اعتماد کمک کند. با توجه به اهمیت گمنامی و حفظ حریم خصوصی در پروتکل‌های پرداخت، این مسائل امروزه بسیار مورد توجه قرار گرفته است.

یکی از اهداف اساسی هر سامانه پرداخت، محافظت در برابر هزینه‌های مضاعف است. به عبارت دیگر، سامانه باید قادر به ردیابی کسانی باشد که صاحب پول هستند و تنها باید به کسی که صاحب پول است اجازه دهد که آن را یک‌بار و نه بیش از یک‌بار خریداری کند. فن‌آوری زنجیره‌قالب، مساله هزینه دوگانه را از طریق یک مکانیزم اجماع حل می‌کند.

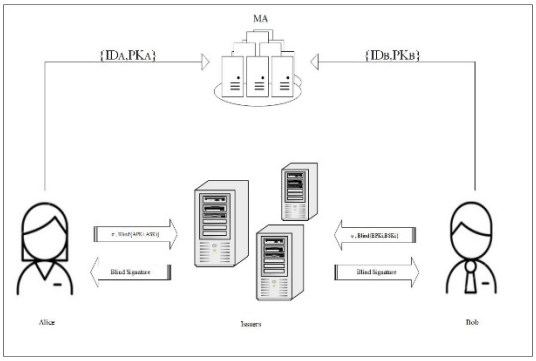
در این مقاله، یک طرح پرداخت الکترونیک مبتنی بر زنجیره‌قالب ارائه شده است؛ که در آن علاوه بر حفظ گمنامی و حریم خصوصی افراد، در مواقع لزوم و با استفاده از اجماع می‌توان کاربر مخرب را ردیابی کرد و عضویت وی را لغو کرد. برای رسیدن به این دستاورد از امضای کور عادلانه و تسهیم راز و همچنین فناوری زنجیره‌قالب استفاده شده است.

۱-۱- نوآوری مقاله

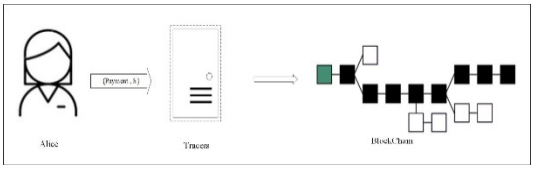
در این مقاله، یک پروتکل پرداخت الکترونیکی مبتنی بر زنجیره‌قالب معرفی شده است. در این طرح، گمنامی کاربران صادق با استفاده از نام مستعار حفظ می‌شود. برای رسیدن به ویژگی‌های مورد نیاز یک طرح پرداخت الکترونیک امن و حفظ حریم خصوصی از امضای کور عادلانه و تسهیم راز استفاده شده است. این طرح دارای مزایای زیر می‌باشد:

۱) در این کار امکان ردیابی کاربران مخرب با کمک t تا از n رديابان وجود دارد. بنابراین دارای ویژگی حریم خصوصی مشروط می‌باشد.
۲) محاسبات نام مستعار کاربران به‌صورت پیش محاسبه انجام می‌شود؛ بنابراین این طرح دارای عملکرد بهتری می‌باشد.
۳) برخلاف طرح‌های قبلی، نیاز به اعتماد کامل به یک سرور خاص وجود ندارد و سرور اصلی هم نمی‌تواند به تنهایی ارتباطی بین نام‌های مستعار و هویت واقعی کاربران پیدا کند.
۴) امکان لغو عضویت کاربران مخرب از شبکه و آشکار کردن هویت آن‌ها وجود دارد.
۵) امنیت این طرح نیز با استفاده از نرم‌افزار پرووریف اثبات شده است.

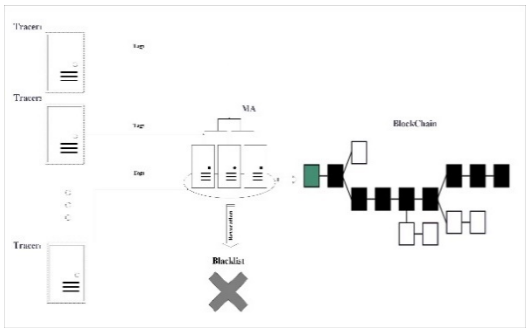
همان‌طور که در شکل (۱- الف) تا (۱- ج) نشان داده شده است، این طرح شامل چهار مرحله‌ی ثبت‌نام و تولید کلید، تولید کلیدهای کوتاه‌مدت، پرداخت الکترونیک و ردیابی می‌باشد.



الف



ب



ج

شکل (۱): الف) مرحله ثبت‌نام اولیه و تولید کلید، ب): مرحله پرداخت الکترونیکی، ج) مرحله ردیابی.

۱-۲- سازماندهی مقاله

در ادامه کارهای پیشین را مورد بررسی قرار خواهیم داد. در بخش سوم به تعریف مقدمات مورد نیاز خواهیم پرداخت. جزئیات طرح پیشنهادی در بخش چهارم آورده شده است، همچنین در این بخش به بررسی ویژگی‌های طرح پیشنهادی می‌پردازیم. امنیت طرح با استفاده از نرم‌افزار پرووریف مورد تجزیه و تحلیل قرار گرفته است که در بخش پنجم به آن می‌پردازیم. در نهایت نیز در بخش ششم نتیجه گیری ارائه گردیده است.

۲- کارهای مرتبط

روش‌های پرداخت سنتی، مانند کارت‌های اعتباری و انتقال پی پال[۱]، نیازمند ارتباط با اشخاص ثالث متعددی هستند. این ارتباط، اطلاعات پرداخت ذخیره شده را با سازمان‌های متعدد، که

[۱] Pay pal

می‌تواند بدون رضایت و یا تمایل کاربران باشد، به اشتراک می‌گذارد.

در مقاله [۵]، با استفاده از امضای دیجیتال و روش‌های شبه هویت[۱] (استفاده از نام مستعار)، یک طرح کیف پول تلفن همراه ارائه شده است. همچنین از سرور ابر و تائید برون سپاری امن استفاده شده است. در طرح پیشنهادی مقاله [۵] از یک سرور قابل اعتماد استفاده شده است که به تمام اطلاعات محرمانه کاربران دسترسی دارد و در صورت لزوم می‌تواند کاربران مخرب را ردیابی کند و بنابراین از گمنامی بالایی برخوردار نمی‌باشد.

در مقاله [۶] یک سامانه پرداخت الکترونیکی مشروط جدید و کارآمد مبتنی بر طرح امضای کور چن و همکاران پیشنهاد شده است. همچنین یک سامانه پرداخت الکترونیکی مشروط با قابلیت انتقال است که امکان انتقال ارز را به‌صورت ناشناس به دیگری توسط زنجیره‌ای از پرداخت کنندگان فراهم می‌کند. اما نیاز به اعتماد به یک شخص سوم مورد اعتماد دارد.

در مقاله [۷]، با استفاده از طرح روی زنجیره‌قالب[۲] یک روش استاندارد انتقال بیت‌کوین را معرفی کرده‌اند؛ یعنی از زنجیره‌قالب بیت‌کوین استفاده می‌شود. این طرح چهار تراکنش را در سه بلوک تائید می‌کند (حدود ۳۰ دقیقه). این پروتکل در زمان‌های مختلف اجرا می‌شود و در هر زمان گمنام می‌باشد. به‌عبارت‌دیگر، تا زمانی‌که زنجیره‌قالب عمومی مجموعه‌ای از پرداخت کنندگان و دریافت کنندگان وجه را در طی یک دوره نشان می‌دهد، هیچ‌کس نمی‌تواند بگوید که چه کسی به چه شخص دیگری وجه پرداخت کرده است. برای انجام این کار، یک واسطه‌ی غیرقابل اعتماد (احتمالاً بدکار) I را بین تمام پرداخت کنندگان و دریافت کنندگان وجه، معرفی می‌کنند. همچنین در این مقاله یک طرح خارج از زنجیره‌قالب[۳] نیز پیشنهاد شده است که از یک شبکه کانال‌های ریزپرداخت استفاده می‌کند؛ در این طرح تراکنش‌ها خارج از زنجیره‌قالب هستند و بنابراین سرعت بالایی دارند. طرح خارج از زنجیره‌قالب، زمانی مجموعه گمنامی در یک دوره را به ارمغان می‌آورد که واسط صادق اما کنجکاو باشد. اما در طرح روی زنجیره‌قالب مدت زمان پرداخت بسیار طولانی است و در طرح خارج از زنجیره‌قالب به دلیل اینکه برخی از معاملات خارج از زنجیره‌قالب انجام می‌شوند احتمال حمله خرج مضاعف[۴] بیشتر است. همچنین در هر دو طرح در هربار انجام عملیات پرداخت هر دو کاربر فروشنده و خریدار نیاز به برقراری ارتباط با واسط دارند. همچنین قابلیت ردیابی کاربران مخرب وجود ندارد.

[۲] Pseudo-identity
[۳] On blockchain
[۴] Off blockchain
[۱] Double spending

در مقاله [۸] یک سیستم پرداخت الکترونیک بر اساس زنجیره‌قالب ارائه داده شده است که شامل ویژگی‌هایی از قبیل امنیت، حریم خصوصی و پرداخت‌های خارج از زنجیره‌ای می‌باشد. این طرح براساس اولویت‌های رمزنگاری موجود، یعنی تابع یک طرفه و امضای دیجیتال، و سیستم زنجیره‌قالب می‌باشد. اما در آن ردیابی کاربران مخرب امکان‌پذیر نیست و همچنین ویژگی ارتباط ناپذیری را دارا نمی‌باشد که باعث ضعیف شدن گمنامی کاربران می‌شود.

در مقاله [۹]، یک حریم خصوصی مبتنی بر زنجیره‌قالب برای حفظ ساز و کار پرداخت برای شبکه‌های V2G[۵] ارائه‌داده شده است، که اشتراک گذاری داده‌ها را با حفظ اطلاعات کاربران ارائه می‌دهد. این مکانیزم یک فرایند ثبت‌نام و نگهداری داده‌ها را ارائه می‌دهد که براساس روش زنجیره‌قالب است که گمنامی اطلاعات پرداخت کاربران را تضمین می‌کند. طراحی بر اساس هایپرلجر[۶] به منظور ارزیابی امکان سنجی و اثربخشی آن انجام‌شده است. اما در این طرح از یک نهاد ایمن استفاده شده است که به تمام اطلاعات کاربران و معاملات پرداخت آن‌ها دسترسی دارد.

۳- پیش‌نیازها

در این بخش پیش‌نیازهای مورد استفاده در طرح پیشنهادی را که شامل تعریف زنجیره‌قالب، ساختار زنجیره‌قالب، امضای کور عادلانه و تسهیم راز را بیان می‌کنیم.

۳-۱- تعریف زنجیره‌قالب

زنجیره‌قالب (که با عنوان پروتکل اعتماد شناخته می‌شود.) یک مفهمومی است که هدف آن غیرمتمرکز سازی به‌عنوان یک اقدام امنیتی است و دارای یک تابع برای ایجاد یک شاخص جهانی برای همه‌ی معاملاتی که در یک شبکه داده رخ می‌دهد، است و آن‌ها را غیرقابل تغییر می‌کند.

ناکاموتو[۷] (نام مستعار توسعه دهنده‌ی بیت کوین) زنجیره‌قالب را به‌عنوان یک روش قابل اعتماد و غیرقابل تغییر تعریف کرده است که امنیت را به معاملات الکترونیکی ارائه می‌دهد، که به‌عنوان یک دفتر کل توزیع شده ارائه می‌شود. در اصل زنجیره‌قالب نوآوری اصلی معرفی شده توسط بیت کوین است[۱۰].

به بیان ساده، زنجیره‌قالب یک ساختار داده‌ای است که معاملات را به‌صورت مرتب ذخیره می‌کند و با بلوک قبلی ارتباط

[۲] Vehicle to Grid
[۳] Hyperledger
[۴] Nakamato

دارد. این ساختار به دو بخش سرآیند[۱] و معاملات تقسیم می‌شود و اطلاعات دقیق معاملات در آن ذخیره می‌شود. بنابراین می‌توان یک معامله را با آدرس مبدأ و مقصد آن مرتبط ساخت. همچنین هر بلوک یک شناسه منحصر به فرد نیز دارد.

این فناوری برای احراز اصالت، اختیار دادن و رسیدگی به داده‌های تولیدشده توسط دستگاه‌ها مورد استفاده قرار می‌گیرد. همچنین به دلیل ماهیت غیرمتمرکز آن، نیاز به اعتماد به شخص سوم را از بین می‌برد و نقطه شکست[۲] ندارد [۱۰].

زنجیره‌قالب را می‌توان به دو صورت جزئی و کلی تعریف کرد. زنجیره‌قالب جزئی، نوعی از ساختار داده است که در آن بلوک داده به‌عنوان یک زنجیره به یکدیگر متصل هستند. زنجیره‌قالب کلی یک زیرساخت غیرمتمرکز است که بر پایه زنجیره قالب‌های داده، ذخیره‌سازی بلوک‌ها و نرم‌افزارهای پشتیبان است.

زنجیره‌قالب دارای ویژگی‌های متفاوت زیر است که باعث منحصربه‌فرد بودن و مورد توجه قرار گرفتن این فناوری می‌شود[۱۱]:

۱- غیر متمرکز بودن
۲- بازبودن[۳]
۳- غیرقابل تغییر بودن

۳-۲- ساختار زنجیره‌قالب

زنجیره‌قالب از تعدادی بلوک تشکیل شده است، هر بلوک شامل دو قسمت سرآیند بلوک و بدنه اصلی بلوک می‌باشد. سرآیند بلوک شامل شماره فعلی بلوک، مقدار هش بلوک قبلی، مهر زمانی[۴] و عدد تصادفی است.

بدنه‌ی بلوک شامل داده‌های تراکنش در شبکه‌ی فعلی است که در قالب یک درخت مرکل[۵] ضبط می‌شود. سرآیند بلوک حاوی مقدار هش بلوک قبلی است و به بلوک بعدی وصل می‌شود؛ بنابراین هر بلوک در زنجیره‌قالب با هم مرتبط هستند و یک زنجیره‌ی یکپارچه را تشکیل می‌دهند.

الزام گمنامی به این دلیل است که هویت‌های واقعی A و B توسط گره های شبکه آشکار نشوند. یکی دیگر از خصوصیات مهم زنجیره‌قالب این است که آدرس کاربران توسط شبکه تعیین نمی‌شود. زیرا کلید عمومی و خصوصی به‌طور پیوسته با یکدیگر مرتبط هستند و آن‌ها در دستگاه کاربران تولید می‌شوند.

[۵] Header
[۶] Single point of failure
[۷] Openness
[۸] Time stamp
[۱] Merkle tree

۳-۲-۱- امنیت زنجیره‌قالب

امنیت و حریم خصوصی اصول اساسی هر سیستم اطلاعاتی هستند. ما به ایمنی به‌عنوان ترکیبی از یکپارچگی، دسترسی و محرمانگی اشاره می‌کنیم.

فناوری زنجیره‌قالب دو مشکل دیرینه پول دیجیتال را حل می‌کند، یکی مشکل خرج مضاعف و دیگری مشکل حمله بیزانس [۱۲]. زنجیره‌قالب مشکل اول را با استفاده از روش اجماع از طریق سند کار[۶] حل کرده است و مشکل دوم را نیز با استفاده از امضای دیجیتال و الگوریتم اجماع حل کرده است [۱۳].

به‌طور معمول می‌توان امنیت را با استفاده از ترکیبی از احراز اصالت، مجوز و شناسایی به‌دست آورد. این مفاهیم در ادامه تعریف شده‌اند [۱۴]:

۱) احراز اصالت: به دنبال هویت فردی است که یک عمل خاص را در یک سیستم انجام می‌دهد. زنجیره‌قالب این عمل را تضمین می‌کند، زیرا تنها کاربرانی که کلید خصوصی دارند می‌توانند معاملات را انجام دهند.
۲) انکارناپذیری: تضمین می‌کند که فرد نمی‌تواند یک عمل را در یک سیستم انکار کند. زنجیره‌قالب این ویژگی را نیز تضمین می‌کند.
۳) گمنامی: ما باید دو مورد متفاوت را در نظر بگیریم: ناشناس بودن پرداخت‌کنندگان و ناشناس بودن دریافت‌کنندگان (این با سامانه‌های سنتی پول الکترونیکی متفاوت است). ناشناس بودن پرداخت کنندگان بدان معنی است که نمی‌توان ارز منتقل شده را با هویت یک پرداخت‌کننده صادق مرتبط کرد. بنابراین، ما دشمن A را به‌عنوان یک بانک تبانی، دریافت‌کننده و ناشر در نظر می‌گیریم. A می‌تواند کلیدهای خصوصی و عمومی بانک را ایجاد کند و در پرس و جوها درگیر شود، جایی که A پروتکل تولید پرداخت را با کاربران مختلف اجرا می‌کند. سپس A با یک انتقال مشروط چالش درگیر می‌شود، جایی که با کاربر واقعی یا شبیه ساز بدون دسترسی به اطلاعات کاربر ارتباط برقرار می‌کند. گمنامی پرداخت‌کننده این است که احتمال تمایز بین پرداخت‌کننده واقعی و شبیه ساز ناچیز است.

برای ناشناس بودن دریافت کنندگان، A می‌تواند بانک تبانی با پرداخت‌کنندگان باشد. در این حالت، A قادر به ایجاد کلید بانک، ایجاد کاربران و انتشار ارز

[۲] POW:proof of work

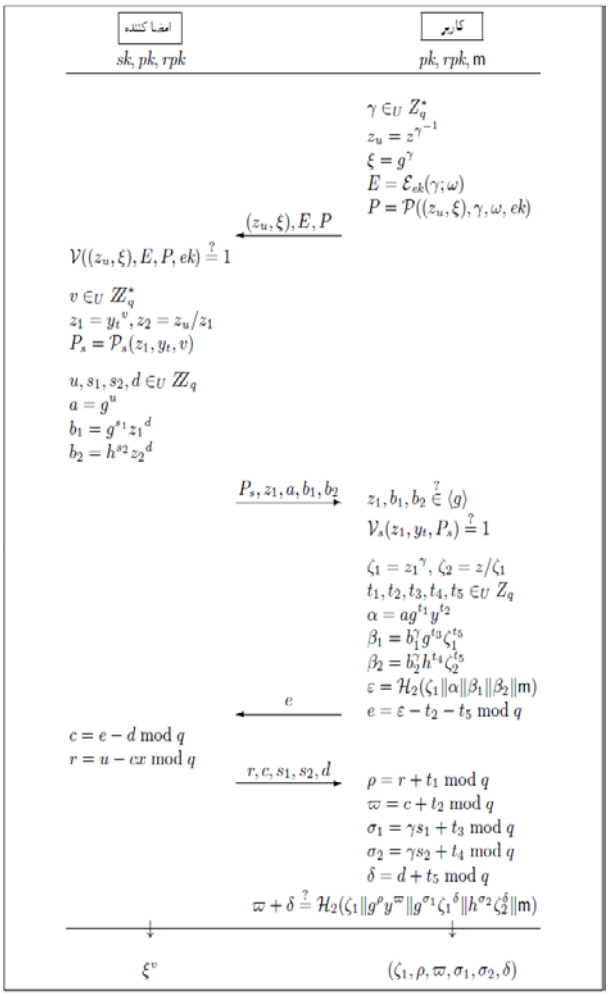
خواهد بود. به‌طور مشابه، ناشناس بودن پرداخت‌کننده این است که احتمال تمایز A در بین پرداخت‌کننده واقعی و شبیه‌ساز در طول پروتکل انتقال مشروط و پروتکل پرداخت نقدی قابل اغماض باشد.

۴) عدم خرج مضاعف: در این حالت، طرف مقابل A نماینده پرداخت‌کننده‌ای است که احتمالاً در یک ائتلاف با یک یا چند شخص متقاضی قرار دارد. فرض کنید که می‌توانید هر بار که بخواهید در پروتکل‌های تولید پرداخت، انتقال مشروط و پرداخت پول پرداخت کنید، می‌گوییم A در صورت برنده شدن در این بازی اگر بانک دو درخواست پول نقد با همان پرداخت را بپذیرد بدون اینکه بتواند هویت A را بازیابی کند. خاصیت عدم خرج مضاعف بدان معنی است که هر شخصی فقط با یک احتمال ناچیز می‌تواند در این بازی پیروز شود.

۳-۳- طرح امضای کور عادلانه

یک طرح امضای کور عادلانه (FBSS[۱]) [۱۵] برای تائید صحت و ناشناس بودن کاربران صحیح و جلوگیری از سوء استفاده از ناشناس بودن کاربران مخرب طراحی شده است. FBSS شامل سه نوع کاربر است: کاربر، امضا کننده و ردیاب. امضا کننده جفت کلید عمومی و خصوصی (PK، SK) را نگه می‌دارد و ردیاب یک کلید ردیابی محرمانه SK_T را نگه می‌دارد. برای امضای پیام m، کاربر برای اولین بار با استفاده از یک عامل کور انتخاب شده توسط خودش، را کور می‌کند و کورشده m را به امضاکننده (یعنی صادرکننده پیام) ارسال می‌کند. سپس امضاءکننده کور شده m را امضا می‌کند. کاربر با استفاده از PK می‌تواند اعتبار امضای کور عادلانه را تائید کند. اگر امضای کور عادلانه معتبر باشد، کاربر می‌تواند با استفاده از فاکتور کور، امضا را از امضای کور عادلانه استخراج کند. FBSS امن است اگر امضا کننده نتواند یک نشست صادرکننده را با یک جفت امضا پیام پیوند دهد. با این حال، ردیاب با SK_T می‌تواند کور بودن طرح را با پیوند یک نشست صادرکننده با یک جفت امضا پیام، لغو کند. FBSS برای امضای شبه گمنام یا کلیدهای عمومی کوتاه مدت کاربران استفاده می‌شود [۱۶].

الگوریتم امضای کور عادلانه FBSS در شکل (۲) نشان داده شده است.



شکل (۲): الگوریتم امضای کور عادلانه.

۴-۳- تسهیم راز

طرح تسهیم راز (t، n) قادر است مقدار مخفی S را به n تعداد سهام S1، S2، ...، Sn توزیع کند. سپس S را می‌توان از تعداد t سهام بازسازی کرد. امنیت طرح تسهیم راز تضمین می‌کند که **S** از تعداد کمتری از سهام قابل بازیابی نیست. در یک FBSS، اگر از یک ردیاب برای ردیابی هویت واقعی یک کاربر استفاده شود، سامانه ممکن است مورد سوء استفاده قرار گیرد. برای حل این مشکل، می‌توان از یک طرح تسهیم راز (t، n) بدون یک شخص سوم مورد اعتماد [۱۷] برای تولید کلید مخفی ردیاب SK_T^i استفاده کرد. هر ردیاب با سهم خود، می‌تواند یک برچسب جزئی تولید کند. یک نهاد که t تا از n برچسب ردیابی جزئی را دارا باشد، می‌تواند هویت واقعی یک کاربر را پیدا کند. با این حال، نهاد (و همچنین ردیاب‌ها) نمی‌تواند کلید ردیابی SK_T را از برچسب‌ها بازسازی کند[۱۶].

[۲] Fair Blind Signature Scheme

۴- طرح پیشنهادی

در این بخش ابتدا شرح اولیه طرح پیشنهادی بیان می‌شود. سپس به جزئیات طرح پیشنهادی خواهیم پرداخت.

طرح پیشنهادی، یک طرح پرداخت الکترونیک مبتنی بر زنجیره‌قالب می‌باشد؛ با استفاده از فناوری زنجیره‌قالب توانسته‌ایم ویژگی‌هایی نظیر شفافیت، گمنامی، حریم خصوصی مشروط و غیره را به ارمغان بیاوریم، که در بخش تجزیه و تحلیل امنیتی با جزئیات بیشتری شرح داده شده است.

این طرح شامل چندین موجودیت می‌باشد که عبارتند از: کاربران که شامل دو هویت فروشنده وخریدار می‌باشند، سرور *MA*، صادر کنندگان و ردیاب‌ها.

۱. *MA*: برای ارتباط بین کلید عمومی و هویت واقعی
۲. صادرکنندگان: برای صدور گواهینامه‌های موقت و امضای کلیدهای کوتاه مدت کاربر و هر کدام دارای یک زوج کلید عمومی و خصوصی می‌باشند.
۳. ردیاب‌ها: برای ردیابی کاربران مخرب می‌باشند و هر کدام یک مقدار مخفی انتخاب می‌کنند، همچنین تولید بلوک جدید در زنجیره‌قالب بر عهده ردیاب‌ها می‌باشد.
۴. فروشنده و خریدار: هر کاربر هویت واقعی خود، کلید خصوصی اصلی و کلید عمومی مربوطه را دارد. اطلاعات محرمانه هر کاربر به‌صورت زیر است که در آن آلیس به‌عنوان خریدار و باب به‌عنوان فروشنده شناخته می‌شود.

$$(ID_A, PK_A, SK_A) \rightarrow \text{Alice} \quad (۱)$$

$$(ID_B, PK_B, SK_B) \rightarrow \text{Bob} \quad (۲)$$

طرح پیشنهادی شامل سه مرحله‌ی (۱) ثبت‌نام اولیه و تولید کلیدهای کوتاه‌مدت (۲) پرداخت الکترونیک و (۳) ردیابی می‌باشد.

در طرح پرداخت الکترونیک پیشنهادی، در مراحل ثبت‌نام اولیه و تولید کلیدهای کوتاه‌مدت، ابتدا فروشنده (باب) و خریدار (آلیس) کلیدهای عمومی خود به همراه هویت واقعی خود را از طریق کانال امن برای *MA* ارسال می‌کنند و *MA* اطلاعات دریافتی را ذخیره می‌کند. بنابراین، تنها *MA* از هویت واقعی کاربران آگاه است. سپس هر یک از کاربران مجموعه‌ای از کلیدهای خصوصی و عمومی متناظر کوتاه‌مدت تولید می‌کند و سپس با استفاده از طرح امضای کور عادلانه آن‌ها را کور و سپس امضا می‌کند و برای صادرکنندگان ارسال می‌کند. سپس صادرکنندگان مقادیر کورشده دریافتی را امضا می‌کنند و به کاربر بر می‌گردانند. کاربر نیز ابتدا صحت امضای کور دریافتی را بررسی می‌کند و سپس با استفاده از عامل کورسازی، مجموعه کلیدهای خصوصی و عمومی کوتاه‌مدت که توسط صادرکننده تأیید شده‌اند را بازیابی می‌کند. در نهایت، صادرکنندگان متناظر با مقادیر کورشده هر کاربر یک مقدار تولید می‌کنند و آن‌ها را در زنجیره‌قالب ذخیره می‌کنند.

در مرحله پرداخت طرح پیشنهادی، آلیس معامله پرداخت خود را می‌سازد و آن را با استفاده از امضای *ECDSA* [۱۸]، امضا می‌کند. سپس معامله پرداخت را برای ردیاب‌ها ارسال می‌کند. ردیاب‌ها نیز ابتدا معامله پرداخت را بررسی می‌کنند و در صورت صحت معامله و تأیید امضای آلیس، آن را در زنجیره‌قالب ذخیره می‌کنند.

مرحله آخر، مرحله ردیابی می‌باشد که تنها زمانی که ردیاب‌ها با یک کاربر مخرب مواجه شوند به این مرحله مراجعه می‌کنند. کلید ردیابی مخفی مربوط به امضای کور FBSS با استفاده از یک طرح تسهیم راز بدون شخص سوم قابل اعتماد بین ردیاب‌ها به اشتراک گذاشته می‌شود. یک فروشنده مخرب کسی است که پس از ثبت پرداخت در زنجیره‌قالب کالا را به خریدار تحویل ندهد و یک خریدار مخرب کسی است که پولی را دو بار خرج کند و یا تبانی انجام دهد. بنابراین، ردیاب‌ها با شناسایی کاربر مخرب شروع به تولید یک مقدار می‌کنند و آن را برای *MA* ارسال می‌کنند. حال اگر n ردیاب رای به مخرب بودن کاربر دهند و n مقدار تولیدی به‌دست *MA* برسد، سرور *MA* می‌تواند با استفاده از طرح تسهیم راز به هویت واقعی کاربر مخرب دست پیدا می‌کند. پس از رسیدن به هویت واقعی کاربر معامله جریمه را تشکیل می‌دهد و در زنجیره‌قالب ثبت می‌کند و در صورتی که کاربر مخرب معامله جریمه دیگری داشته باشد، *MA* هویت واقعی او را در لیست سیاه اضافه می‌کند و آن را در بلوک زنجیره‌قالب ثبت می‌کند.

در طرح پیشنهادی حتی *MA* در طول اجرای پرداخت از هویت واقعی کاربرانی که پرداخت را انجام می‌دهند، اطلاعی ندارد و تنها با کمک n ردیاب می‌تواند کاربر مخرب را ردیابی کند. جدول (۱) نشان‌دهنده متغیرهای استفاده شده در طرح پیشنهادی می‌باشد.

جدول (۱): معرفی متغیرهای موجود در طرح پیشنهادی.

نام متغیر	تعریف
IDA	هویت واقعی خریدار (آلیس)
PKA	کلید عمومی خریدار (آلیس)
$\{APK_i , ASK_i\} i \in \{1, \dots, l\}$	مجموعه کلیدهای عمومی و خصوصی کوتاه‌مدت خریدار (آلیس)
IDB	هویت واقعی فروشنده (باب)
PKB	کلید عمومی فروشنده (باب)
$\{BPK_i , BSK_i\} i \in \{1, \dots, l\}$	مجموعه کلیدهای عمومی و خصوصی کوتاه‌مدت فروشنده (باب)
Ti	شماره معامله پرداخت
AmountTi	مبلغ قابل پرداخت
Cre APKi	گواهینامه کوتاه‌مدت خریدار (آلیس)
Cre Bpki	گواهینامه کوتاه‌مدت فروشنده (باب)
Tagi	مقدار تولیدی توسط ردیاب‌ها

مرحله ثبت‌نام و تولید کلیدهای کوتاه‌مدت:

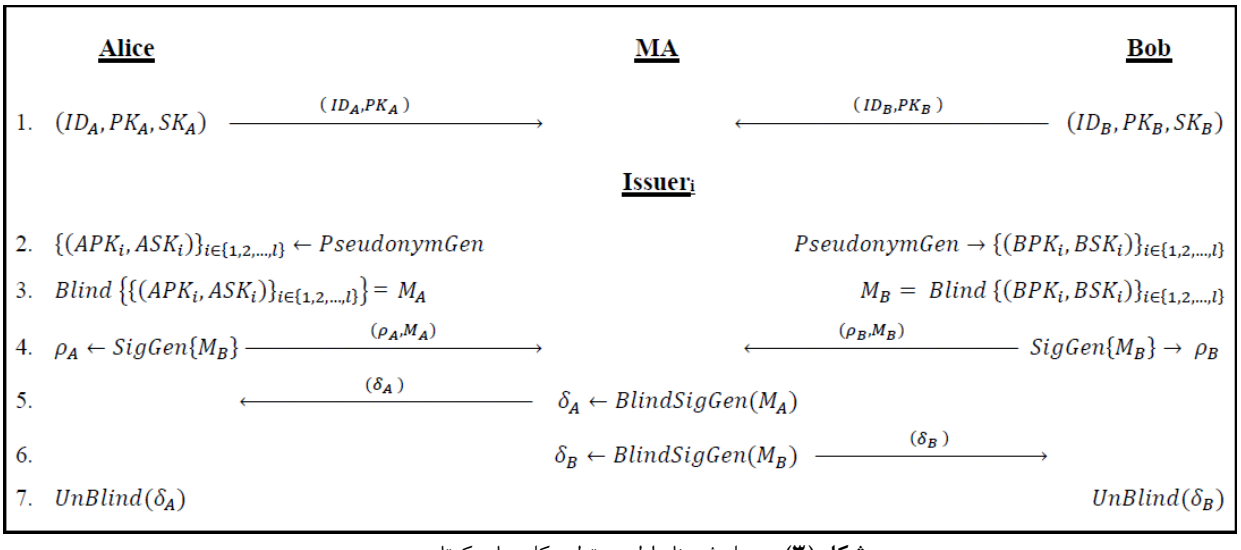
آلیس مقدارهای ID_A و PK_A را برای *MA* ارسال می‌کند. آلیس مجموعه‌ای از کلیدهای عمومی و خصوصی را تولید می‌کند:

$$\{APK_i , ASK_i\} i \in \{1, \dots, l\} \quad (۳)$$

حال آلیس از کلیدهای عمومی کوتاه‌مدت خود به‌عنوان نام مستعار استفاده می‌کند و مجموعه کلیدهای کوتاه‌مدت خود را کور می‌کند و آن را برای صادرکننده به همراه امضای $\boldsymbol{\sigma}$ بر روی داده‌های کور ارسال می‌کند. (از طرح امضای کور عادلانه *(FBSS)*) صادرکننده امضا را بررسی می‌کند و سپس کلیدهای عمومی را امضا می‌کند و برای آلیس ارسال می‌کند. آلیس نیز پس از بررسی امضا آن را کور می‌کند و از آن برای تولید گواهینامه‌های کوتاه‌مدت استفاده می‌کند:

$$cer_{APK_i} \quad (۴)$$

امضای FBSS برای تأیید صحت و گمنامی کاربران صادق و جلوگیری از سوءاستفاده کاربران مخرب طراحی شده است. در امضای FBSS سه نوع موجودیت وجود دارد که شامل کاربران، امضا کننده و ردیاب می‌باشد. ردیاب با استفاده از کلید خصوصی خود (SK_T) قادر به آشکار کردن هویت کاربر است. اما اگر از یک ردیاب برای ردیابی هویت واقعی یک کاربر استفاده شود، سیستم ممکن است مورد سوء استفاده قرار گیرد برای حل این مشکل، ما می‌توانیم از یک طرح تسهیم راز بدون یک شخص سوم مورد اعتماد برای تولید کلید مخفی ردیاب SK^i_T استفاده کنیم.



شکل (۳): مرحله ثبت‌نام اولیه و تولید کلیدهای کوتاه مدت.

صادرکننده نیز یک هویت نشست منحصربه‌فرد S_{id} را ایجاد می‌کند و (S_{id} , pk) را در یک زنجیره‌قالب جداگانه که بلوک‌های آن شامل S_{id} و امضای مربوطه می‌باشد، ذخیره می‌کند.

تمام مراحل فوق برای باب نیز تکرار می‌شود. شکل (۳) به‌طور مختصر این مرحله را نشان می‌دهد.

- مرحله پرداخت:

آلیس معامله پرداخت زیر را تولید می‌کند:

$$payment = (T_i, Amount_{T_i}, BPK_i, cer_{APK_i}) \quad (۵)$$

سپس معامله پرداخت فوق را امضا می‌کند. سپس آن را به همراه معامله پرداخت برای ردیاب‌ها ارسال می‌کند.

$$Sig_{ASKi}(payment) \quad (۶)$$

ردیاب‌ها ابتدا امضا و تراکنش را بررسی می‌کنند و به‌عنوان ماینر، پرداخت را در زنجیره‌قالب ذخیره می‌کنند. بخش‌های مختلف این مرحله در شکل (۴) نشان داده شده است.

- مرحله ردیابی:

به این مرحله تنها زمانی مراجعه می‌شود که ردیاب‌ها در مرحله تائید امضا با خطا مواجه شوند و یا با یک فرد بدخواه مواجه شوند. آنگاه با استفاده از کلید عمومی کوتاه مدت و اعتبار نامه کوتاه مدت آلیس و همچنین کلید مخفی ردیابی مربوط به خود (SK^i_T) یک برچسب درست می‌کنند و آن را برای MA ارسال می‌کنند. اگر t تا برچسب به MA برسد آنگاه MA می‌تواند کلید ردیابی مخفی امضای کور FBSS را با استفاده از تسهیم راز بازیابی کند و از طریق آن به نشست مربوط به امضای کور انجام‌شده بر روی نام‌های مستعار دست‌یابی پیدا می‌کند و می‌تواند کلید عمومی واقعی کاربر مخرب را پیدا کرده و هویت وی برای MA آشکار شود.

حال MA بررسی می‌کند اگر برای بار اول فرد به‌عنوان بدخواه شناخته شده باشد آنگاه فرد را جریمه می‌کند و معامله پرداخت جریمه (مبلغی ارز را از حساب کاربر بدخواه به حساب خود انتقال می‌دهد.) را در زنجیره‌قالب قرار می‌دهد؛ اگر بار دوم فرد باشد که به‌عنوان بدخواه شناخته می‌شود و اگر جریمه را پرداخت نکرده باشد آنگاه MA می تواند هویت واقعی فرد را آشکار کند و آن را به لیست سیاه اضافه کند.

Alice		Tracer	Blockchain
1.	$\mathbb{G}, P$		
2.	$Payment = (T_i \parallel Amount_{T_i} \parallel BPK_i \parallel Cre_{BPK_i})$		
3.	$k \in \{1, \dots, n-1\}$		
4.	$k.P = (x, y)$		
5.	$r = x \bmod n$		
6.	$\sigma = k^{-1}(h(Payment) + ASK_i.r)$	$\xrightarrow{\{r,\sigma,Payment\}}$	$w = \sigma^{-1} \bmod n$
7.			$u_1 = h(Payment).w \bmod n$
8.			$u_2 = r.w \bmod n$
9.			$(x, y) = u_1.P + u_2.APK_i$
10.			$r =? x \bmod n \xrightarrow{\{\sigma,Payment\}}$

شکل (۴): مرحله پرداخت الکترونیک.

۴-۱- ویژگی‌های پروتکل

۱. احراز اصالت متقابل: از آنجایی که برای هر فرد چندین گواهینامه موقت تولید می‌شود، بنابراین، کاربران می‌توانند با استفاده از گواهینامه موقت طرف مقابل، یکدیگر را تائید کنند.

۲. قابلیت اطمینان: از آنجایی که پس از تشکیل معامله پرداخت، پرداخت‌کننده آن را امضا می‌کند و گواهینامه موقت وی نیز در معامله وجود دارد، بنابراین، اطمینان از صحت و یکپارچگی پرداخت حاصل می‌شود.

۳. جعل ناپذیری: به‌دلیل ویژگی جعل ناپذیری امضا ECDSA، بنابراین، هیچ‌کسی قادر به خرج کردن ارز کس دیگری نمی‌باشد.
۴. ردیابی: به‌دلیل ویژگی ردیابی امضای FBSS، اگر کاربری بخواهد ارزی را دو بار مصرف کند می‌توان آن را ردیابی کرد و مجازات کرد.
۵. عدم نیاز به اعتماد به یک سرور: از آنجایی که MA تنها کلید عمومی و هویت واقعی افراد را دارا می‌باشد و نمی‌تواند به‌تنهایی ارتباطی بین نام‌های مستعار و هویت واقعی پیدا کند، بنابراین، در صورت ناصادق بودن او نیز مشکلی ایجاد نمی‌شود.
۶. عدم ارتباط پذیری: به‌دلیل ویژگی ارتباط ناپذیری امضا FBSS، حتی MA یا صادرکنندگان نیز نمی‌تواند ارتباطی بین هویت واقعی کاربر و نام‌های مستعار او پیدا کند و حداقل به t ردیاب برای آشکار کردن هویت واقعی فرد نیاز است.
۷. گمنامی: به‌دلیل اینکه در هر معامله پرداخت از یک نام مستعار جدید و یک گواهینامه موقت جدید استفاده می‌شود و به‌دلیل وجود امضا FBSS نمی‌توان ارتباطی بین هویت واقعی و نام مستعار کاربر پیدا کرد، بنابراین، این طرح دارای سطح مطلوبی از گمنامی می‌باشد و دارای حریم خصوصی مشروط می‌باشد.
۸. حریم خصوصی مشروط: با توجه به اینکه کاربران برای انجام معاملات از نام مستعار استفاده می‌کنند، گمنامی کاربران صادق حفظ می‌شود. اما از آنجایی که در مواقع لزوم و در هنگام مواجه با کاربر مخرب، با کمک t ردیاب، MA می‌تواند هویت کاربر مخرب را با استفاده از تسهیم راز بدون شخص سوم قابل اعتماد فاش کند؛ بنابراین طرح پیشنهادی دارای حریم خصوصی مشروط می‌باشد.
۹. لغو عضویت: از آنجایی که این طرح دارای حریم خصوصی مشروط و قابلیت ردیابی می‌باشد در صورتی که یک کاربر مخرب باشد و t تا از n ردیاب رأی به مخرب بودن فرد دهند، می‌توان نام‌های مستعار فرد را لغو کرد و از شبکه خارج کرد.
۱۰. شفافیت: به‌دلیل استفاده از زنجیره‌قالب، تمام پرداخت‌ها به‌صورت شفاف برای همگان در دسترس است.
۱۱. ثبت رکوردها: تمام تراکنش‌ها در دفترکل زنجیره‌قالب ذخیره می‌شوند و برای همه در دسترس می‌باشد.
۱۲. سر بار محاسباتی: به‌دلیل اینکه مرحله تولید نام‌های مستعار با صورت پیش محاسبه می‌باشد و پس از یک‌بار تولید به‌صورت طولانی‌مدت قابل استفاده است، بنابراین، سربار زیادی به ایجاد معامله وارد نمی‌کند. در مرحله تشکیل معامله نیز فقط نیاز به یک امضای ECDSA دارد و از آن جایی که مرحله تأیید آن نیز نیاز به محاسبات زوج دو خطی[۱] ندارد، بنابراین، پروتکل دارای سربار محاسباتی کمی می‌باشد.
۱۳. هزینه معاملات: هزینه معاملات تنها یک مقدار بسیار کمی است که برای کارمزد در نظر گرفته شده است و استفاده از زنجیره‌قالب باعث کاهش هزینه‌های معاملات شده است.

۴-۲- اثبات امنیتی

برای اثبات امنیت طرح پیشنهادی پرداخت الکترونیکی مبتنی بر زنجیره‌قالب از دو مدل امنیتی مبتنی بر مدل ارائه‌شده در مقاله [۸] استفاده می‌کنیم؛ در مدل اول، فرض می‌شود که یک مهاجم خارجی وجود دارد که می‌خواهد ارز کاربر دیگر را خرج کند، به‌عبارت‌دیگر مهاجم می‌خواهد امضای مرحله پرداخت را جعل کند. فرض می‌شود که زنجیره‌قالب امن است و مهاجم به کلید خصوصی اصلی و کوتاه‌مدت کاربران دسترسی ندارد. از طرف دیگر فرض می‌شود که مهاجم می‌تواند تعدادی معامله پرداخت تولید کند و درخواست تأیید و امضای آن‌ها را بدهد.

مدل امنیتی اول طرح پیشنهادی، از طریق بازی امنیتی زیر بین مهاجم A_1 و چالشگر C_1 انجام می‌شود که هر دو آن‌ها پارامتر امنیتی $\lambda \in N$ *را به‌عنوان* ورودی دریافت می‌کنند.

- مقداردهی اولیه: چالشگر C مرحله ثبت‌نام و تولید کلیدهای کوتاه‌مدت را اجرا می‌کند و کلیدهای خصوصی و عمومی کوتاه‌مدت $\{Ask_i ، Apk_i\}$ را تولید می‌کند، سپس C کلیدهای خصوصی کوتاه‌مدت $\{Ask_i\}$ را نگه می‌دارد، اما کلیدهای عمومی کوتاه‌مدت $\{Apk_i\}$ را برای مهاجم A_1 ارسال می‌کند.
- درخواست‌ها: مهاجم A_1 می‌تواند درخواست تعدادی امضا به چالشگر C_1 بدهد. به‌عبارت‌دیگر مهاجم A_1 یک فهرستی از معاملات پرداخت را برای چالشگر C_1

[۱] Pairing

ارسال می‌کند و از او می‌خواهد تا امضای معادل آن‌ها را ارسال کند.

- چالش:چالشگر C_1 امضای مربوط به هر معامله پرداخت و کلید عمومی کوتاه‌مدت ارسال‌شده را با استفاده از الگوریتم امضا $\sigma_k \rightarrow Sign_{TSK_i}(Payment_k), 1 \leq k \leq t$ تولید می‌کند. سپس چالشگر C_1 امضاهای $\sigma_k, 1 \leq k \leq t$ را برای مهاجم A_1 ارسال می‌کند.
- خروجی: مهاجم A_1 یک جفت $(Payment^*, \sigma^*)$را تولید می‌کند و مهاجم A_1 برنده است اگر $(Payment^*, \sigma^*)$ با هیچ‌یک از $(Payment_k, \sigma_k), 1 \leq k \leq t$ برابر نباشد و $Verify_{TPKi}(Payment^*, \sigma^*) = Valid$ باشد.

احتمال موفقیت مهاجم A_1 در بازی فوق با تابع $\mathbf{AdvA1}(\boldsymbol{\lambda})$ تعریف می‌شود. طرح پرداخت الکترونیک مبتنی بر زنجیره‌قالب در برابر مهاجم A_1 امن است اگر مقدار $\mathbf{AdvA1}(\boldsymbol{\lambda})$ قابل اغماض باشد.

تئوری ۱: طرح پیشنهادی پرداخت الکترونیک مبتنی بر زنجیره‌قالب دارای امنیت در برابر خرج کردن ارز کاربر دیگر می‌باشد،اگر الگوریتم امضای دیجیتال **ECDSA** جعل‌ناپذیر باشد.

اثبات: فرض می‌کنیم که یک مهاجم زمان چندجمله‌ای A_1 وجود دارد که می‌تواند ارز کاربر دیگر را خرج کند. ما یک الگوریتم B_1 طراحی کردیم که دارای احتمال غیرقابل اغماض برای شکستن جعل‌ناپذیری امضای دیجیتال با کمک الگوریتم A_1 می‌باشد. الگوریتم B_1 به‌عنوان مهاجم برای طرح امضای دیجیتال اصلی و به‌عنوان چالشگر برای سیستم پرداخت الکترونیک مبتنی بر زنجیره‌قالب عمل می‌کند. شبیه‌سازی به‌صورت زیر اجرا می‌شود:

- مقداردهی اولیه: الگوریتم کلید عمومی Pk مربوط به طرح امضای دیجیتال ECDSA توسط چالشگر اجرا می‌شود و کلید عمومی را به مهاجم A_1 می‌دهد.
- درخواست: مهاجم A_1 فهرستی از اطلاعات شامل معاملات پرداخت و کلیدهای عمومی کوتاه‌مدت را به الگوریتم B_1 ارسال می‌کند. الگوریتم B_1 این اطلاعات را به طرح امضای دیجیتال اصلی ارسال می‌کند.
- چالش: پس از دریافت امضاشده اطلاعات $\sigma_k \rightarrow Sign_{TSK_i}(Payment_k), 1 \leq k \leq t$ از طرح امضای دیجیتال، الگوریتم B_1، آن‌ها را برای مهاجم A_1 ارسال می‌کند.
- خروجی: خروجی مهاجم A_1 زوج $(Payment^*, \sigma^*)$ است که با احتمال غیرقابل اغماض برابر با هیچ‌یک از زوج‌های $(Payment_k, \sigma_k), 1 \leq k \leq t$ نمی‌باشد و $Verify_{TPK_i}(Payment^*, \sigma^*) = Valid$ باشد. الگوریتم همچنین جفت $(Payment^*, \sigma^*)$ را به‌عنوان امضای خود به چالشگر طرح امضای دیجیتال بازمی‌گرداند.

بنابراین، اگر مهاجم A_1 با احتمال غیرقابل اغماض بتواند ارز کاربر دیگری را خرج کند، الگوریتم B_1 می‌تواند ویژگی جعل‌ناپذیری امضای دیجیتال را با احتمال غیرقابل اغماض شکست دهد. با این حال، از آن‌جایی که در طرح پیشنهادی در مرحله پرداخت از امضای ECDSA استفاده شده است که دارای خاصیت جعل‌ناپذیری [۱۸] است، بنابراین، طرح پیشنهادی در برابر مهاجم A_1 امن است.

در مدل امنیتی دوم فرض می‌شود که مهاجم به‌عنوان یک MA بدخواه عمل می‌کند که می‌خواهد با استفاده از نام مستعار یک کاربر به هویت واقعی کاربر برسد و گمنامی فرد را نقض کند. به‌عبارت‌دیگر، مهاجم می‌خواهد خاصیت کورد بودن امضا را از بین ببرد.

مدل امنیتی دوم طرح پیشنهادی، از طریق یک بازی امنیتی بین مهاجم A_2 و چالشگر C_2 انجام می‌شود که هر دو آن‌ها پارامتر امنیتی $\boldsymbol{\lambda} \in \boldsymbol{N}$ را به‌عنوان ورودی دریافت می‌کنند.

- مقداردهی اولیه: چالشگر C_2 مرحله ثبت‌نام اولیه و تولید کلید را اجرا می‌کند و کلید خصوصی عمومی (s_k, p_k) را تولید می‌کند. سپس C_2 کلید خصوصی را نگه می‌دارد اما کلید عمومی را برای مهاجم A_2 ارسال می‌کند.$(\forall \{PK, SK\} \leftarrow Key\ Gen\ (1^{\lambda}))$
- درخواست: مهاجم می‌تواند تعدادی از نام‌های مستعار را تولید می‌کند و درخواست هویت واقعی متناظر با آن‌ها را می‌دهد.
- چالش: چالشگر C_2 هویت واقعی مربوط به نام‌های مستعار تولیدشده توسط مهاجم را تولید و برای مهاجم A_2 ارسال می‌کند.
- خروجی: خروجی مهاجم A_2 هویت واقعی مربوط به یک نام مستعار مشخص (PK_i^*, ID_i^*)می‌باشد و برای چالشگر C_2 ارسال می‌کند.

احتمال موفقیت مهاجم A_2 در بازی فوق با تابع $Adv_{A2}(\lambda)$ تعریف می‌شود. طرح پرداخت الکترونیک مبتنی بر زنجیره‌قالب در برابر مهاجم A_2 امن است اگر مقدار $Adv_{A2}(\lambda)$ قابل اغماض باشد.

تئوری ۱: طرح پرداخت الکترونیکی مبتنی بر زنجیره‌قالب امن است اگر امضای کور استفاده شده در مرحله ثبت‌نام اولیه و تولید کلیدهای کوتاه‌مدت دارای خاصیت کور بودن باشد.

اثبات: فرض می‌کنیم که یک مهاجم زمان چندجمله‌ای A_2 وجود دارد که می‌تواند ارز کاربر دیگر را خرج کند. ما یک الگوریتم B_2 طراحی کردیم که دارای احتمال غیرقابل اغماض برای شکستن خاصیت کور بودن امضای کور با کمک الگوریتم A_2 می‌باشد. الگوریتم B_2 به‌عنوان مهاجم برای طرح امضای کور اصلی و به‌عنوان چالشگر برای سیستم پرداخت الکترونیک مبتنی بر زنجیره‌قالب عمل می‌کند. شبیه‌سازی به‌صورت زیر اجرا می‌شود:

- مقداردهی اولیه: الگوریتم کلید عمومی Pk مربوط به طرح امضای کور عادلانه FBSS توسط چالشگر C_2 اجرا می‌شود و کلید عمومی را به مهاجم A_2 می‌دهد.
- درخواست: مهاجم A_2 فهرستی از نام‌های مستعار را به الگوریتم B_2 ارسال می‌کند. الگوریتم B_2 این اطلاعات را به طرح امضای کور عادلانه اصلی ارسال می‌کند.
- چالش: پس از دریافت هویت واقعی مربوط به نام‌های مستعار از طرح امضای کور عادلانه، الگوریتم B_2 ، آن‌ها را برای مهاجم A_2 ارسال می‌کند.
- خروجی: خروجی مهاجم A_2 ، هویت واقعی متناظر با یک نام مستعار مشخص (PK_i^*, ID^*)می‌باشد که با احتمال غیرقابل اغماض برابر با هیچ‌یک از نام‌های مستعار درخواست‌شده نمی‌باشد. الگوریتم همچنین جفت (PK_i^*, ID^*) را به‌عنوان خروجی خود به چالشگر طرح امضای کور بازمی‌گرداند.

بنابراین اگر مهاجم A_2 با احتمال غیرقابل اغماض بتواند هویت یک کاربر صادق را آشکار کند، الگوریتم B_2 می‌تواند ویژگی کور بودن امضای کور را با احتمال غیرقابل اغماض شکست دهد. با این حال، از آن‌جایی که در طرح پیشنهادی در مرحله ثبت‌نام اولیه و تولید کلیدهای کوتاه‌مدت از امضای FBSS استفاده شده است که دارای خاصیت کور بودن [۱۵]، است، بنابراین، طرح پیشنهادی در برابر مهاجم A_2 امن است.

۵-تجزیه و تحلیل طرح پیشنهادی با استفاده از نرم‌افزار پروریف

پروریف یک ابزار برای تجزیه و تحلیل خودکار پروتکل‌های رمزنگاری است. این نرم‌افزار از سامانه‌های رمزنگاری شامل: رمزگذاری متقارن و نامتقارن، امضاهای دیجیتال، توابع چکیده‌ساز و اثبات دانایی صفر پشتیبانی می‌کند. پروریف قادر به اثبات ویژگی‌های دستیابی، ادعاهای متقابل و همبستگی مشاهداتی می‌باشد. این قابلیت‌ها به‌ویژه برای امنیت رایانه مفید هستند، زیرا آنها اجازه تجزیه و تحلیل خصوصیات پنهان‌کاری و احراز اصالت را می‌دهند. علاوه بر این، خواص در حال ظهور مانند حفظ حریم خصوصی، قابلیت ردیابی و قابل اطمینان بودن نیز می‌تواند مورد توجه قرار گیرد. علاوه‌بر این، این ابزار قادر به بازسازی حمله می‌باشد: هنگامی‌که یک ویژگی را نمی‌توان ثابت کرد، پروریف تلاش می‌کند تا یک ردیابی اجرایی که ویژگی مورد نظر را جعل می‌کند، بازسازی کند [۱۹].

محرمانگی هویت واقعی کاربران و احراز هویت کاربران با استفاده از نام مستعار آن‌ها در پروتکل پرداخت الکترونیک عادلانه مبتنی‌بر زنجیره‌قالب با استفاده از نرم‌افزار پروریف تحلیل گردیده است. همان‌طور که در تصویر نشان داده شده است، محرمانگی هویت واقعی کاربران و احراز هویت آن‌ها در طرح پیشنهادی به‌درستی انجام می‌شود.

شبیه‌سازی با استفاده از نرم‌افزار پروریف شامل چندین قسمت راه‌اندازی سامانه، زیر فرآیند پرداخت‌کننده و دریافت‌کننده، زیرفرآیند MA، زیر فرآیند مربوط به صادرکننده، زیر فرآیندهای مربوط به ردیاب‌ها، زیرفرآیند زنجیره‌قالب، ادعاها و در نهایت شروع فرآیند می‌باشد. در ادامه کدهای مربوط به هر قسمت آورده شده است.

۵-۱- قسمت راه‌اندازی سامانه

راه‌اندازی سامانه بخش ابتدایی دستورات می‌باشد که در آن باید توابع و کانال‌های مورد نیاز تعریف شود؛ همچنین نوع کلیدها و مقادیر یک‌بارمصرف نیز در این بخش تعریف می‌شوند. همان‌طور که در شکل (۵) نشان داده شده است در این بخش دو کانال تعریف شده است که یکی کانال امن و دیگری عمومی می‌باشد. همچنین توابه منحنی بیضوی، امضای دیجیتال، تابع چکیده‌ساز و بقیه توابع نیز در این بخش معرفی شده‌اند.

```
1  free c: channel.
2  free s: channel [private].
3  type pkey.
4  type skey.
5  type G.
6  type nonce.
7  type timestamp.
8  fun exp(G, bitstring): bitstring.
9  fun exp1(bitstring, bitstring): bitstring.
10 fun cerGeneration(bitstring): bitstring.
11 fun ECC(bitstring, bitstring): bitstring.
12 fun ECC1(bitstring, pkey): bitstring.
13 fun SecretShare(bitstring): bitstring.
14 fun h(bitstring, bitstring): bitstring.
15 fun h1(bitstring): bitstring.
16 fun Multiplication1(bitstring, bitstring): bitstring.
17 fun Multiplication(bitstring, bitstring, bitstring, bitstring, bitstring, bitstring, bitstring): bitstring.
18 fun division(bitstring, bitstring): bitstring.
19 fun Blindsignature(bitstring): bitstring.
20 fun TAG(pkey, bitstring): bitstring.
21 fun recover(bitstring, bitstring): bitstring.
22 fun invers(bitstring): bitstring.
23 fun sum(bitstring, bitstring): bitstring.
24 fun sign1(bitstring, bitstring): bitstring.
```

شکل (۵): قسمت راه‌اندازی سامانه در نرم‌افزار پرووریف

```
48 let Alice(PKA: pkey, SKA: skey, IDA: bitstring, P: bitstring, q: bitstring, g: G, BPK1: bitstring) =
49       (*Initialization phase*)
50        out (s, (IDA, PKA));
51        new APk1: bitstring;
52        new APk2: bitstring;
53        new APk3: bitstring;
54        new ASK1: bitstring;
55        new ASK2: bitstring;
56        new ASK3: bitstring;
57        new z: bitstring;
58        let Z = exp(g, z) in
59        let Y = Multiplication(Z, APk1, APk2, APk3, ASK1, ASK2, ASK3) in
60        out (c, Y);
61        in (c, BS: bitstring);
62  let creAPK1 = cerGeneration(BS) in
63       (*payment*)
64       new T1: bitstring;
65       new AmountT1: bitstring;
66       let payment = (T1, AmountT1, BPK1, creAPK1) in
67       new k: bitstring;
68       let (x: bitstring, y: bitstring) = ECC(k, P) in
69       let r = x in
70       let K = invers(k) in
71       let B = Multiplication1(ASK1, r) in
72       let H = sum(h1(payment), B) in
73       let S = Multiplication1(K, H) in
74       out (c, (S, r, payment)).
```

شکل (۶): قسمت پرداخت‌کننده در نرم‌افزار پرووریف.

۵-۲- قسمت پرداخت‌کننده و دریافت‌کننده

شکل (۶) کدهای مربوط به پرداخت‌کننده در نرم‌افزار پرووریف در دو مرحله ثبت‌نام اولیه و پرداخت نشان می‌دهد. خطوط ۵۱ تا ۵۶ مربوط به تولید نام‌های مستعار توسط پرداخت‌کننده می‌باشد. سپس نام‌های مستعار تولیدی را کور می‌کند. پس از رسیدن به نام‌های مستعار وارد مرحله پرداخت می‌شود. خطوط ۶۴ تا ۷۴ مربوط به مرحله پرداخت می‌باشد.

شکل (۷) نیز کدهای مربوط به دریافت‌کننده وجه را نشان می‌دهد. دستورات این بخش مربوط به تولید نام‌های مستعار و کور کردن آن‌ها توسط دریافت‌کننده می‌باشد.

۵-۳- قسمت مربوط به MA

شکل (۸) دستورات مربوط به MA در دو مرحله ثبت‌نام اولیه و ردیابی می‌باشد. خطوط ۸۸ و ۸۹ مربوط به دریافت کلید عمومی

و هویت واقعی دریافت‌کننده و پرداخت‌کننده از طریق کانال امن در محله ثبت‌نام اولیه می‌باشد. خطوط ۹۱ و ۹۲ مربوط به دریافت برچسب تولیدشده توسط ردیاب‌ها می‌باشد. سپس MA شروع به بازیابی هویت واقعی کاربر مخرب می‌کند.

```
75  let Bob(PKB: pkey, SKB: skey, IDB: bitstring, P: bitstring, q: bitstring, g: G) =
76        (*Initialization phase*)
77        new BPk1: bitstring;
78        new BPk2: bitstring;
79        new BPk3: bitstring;
80        new BSK1: bitstring;
81        new BSK2: bitstring;
82        new BSK3: bitstring;
83  out (s, (IDB, PKB));
84        new zB: bitstring;
85        let ZB = exp(g, zB) in
86            let YB = Multiplication(ZB, BPk1, BPk2, BPk3, BSK1, BSK2, BSK3) in
87        out (c, YB);
88        in (c, BSB: bitstring).
```

شکل(۷): قسمت مربوط به دریافت‌کننده وجه در نرم‌افزار پرووریف.

```
109 let MA(pkm: pkey, skm: skey) =
110       (*Initialization phase*)
111         in (s, (IDA: bitstring, PKA: pkey));
112         in (s, (IDB: bitstring, PKB: pkey));
113       (*tracing*)
114       in (c, tag1: bitstring);
115       in (c, tag2: bitstring);
116       let PKA = recover(tag1, tag2) in
117       out (c, (PKA,IDA));
118     in (c, m: bitstring);
119   in (c, PKA: pkey).
```

شکل (۸): .قسمت مربوط به **MA** در نرم‌افزار پرووریف.

۵-۴- قسمت مربوط به صادرکننده

شکل (۹) دستورات مربوط به یک صادرکننده را نشان می‌دهد. همان‌طور که در خط ۹۶ نشان داده شده است، یک صادرکننده دارای یک جفت کلید عمومی و خصوصی می‌باشد و امضای کور را بر روی نام‌های مستعار کاربران اجرا می‌کند.

```
96  let Issuer(pki: pkey, ski: skey) =
97        (*Initialization phase*)
98        in (c, Y: bitstring);
99        let BS = Blindsignature(Y) in
100       out (c, BS);
101
102       in (c, YB: bitstring);
103       let BSB = Blindsignature(YB) in
104       out (c, BSB).
```

شکل (۹): قسمت مربوط به صادرکننده در نرم‌افزار پرووریف.

۵-۵- قسمت مربوط به ردیاب‌ها

برای شبیه‌سازی با نرم‌افزار پرووریف ما دو ردیاب را در نظر گرفته‌ایم. شکل (۱۰) دستورات مربوط به این دو ردیاب را نشان می‌دهد. ردیاب اول هم در مرحله پرداخت حضور دارد و به‌عنوان یک استخراج‌گر عمل می‌کند و هم در مرحله ردیابی به‌عنوان یک ردیاب برای تولید برچسب حضور دارد (خطوط ۱۰۵ تا۱۱۷). ردیاب دوم نیز تنها در مرحله ردیابی حضور دارد و اقدام به تولید برچسب برای ردیابی کاربر مخرب می‌کند.

۵-۶- قسمت مربوط به زنجیره‌قالب

شکل (۱۱) دستورات مربوط به زنجیره‌قالب در نرم‌افزار پرووریف می‌باشد. در طرح پیشنهادی از زنجیره‌قالب به‌عنوان یک ذخیره‌ساز استفاده شده است. بنابراین تمام پرداخت‌ها را دریافت می‌کند (خط ۱۳۰). همچنین در صورت آشکارسازی هویت واقعی یک کاربر مخرب توسط MA، کلید عمومی واقعی وی در زنجیره‌قالب ثبت می‌شود (خط ۱۳۱).

از آنجایی که از زنجیره‌قالب به‌عنوان یک سرور ذخیره‌ساز استفاده شده است، بنابراین، تمام مواردی که در کد مربوطه به زنجیره‌قالب وارد می‌شود، برای همگان آشکار است. و در زمان نیاز اطلاعات لازم توسط MA از داخل زنجیره‌قالب برداشته می‌شود.

```
let Tracer1(APk1: pkey, APk2: pkey, APK3: pkey, creAPK1: bitstring, P: bitstring) =
(*payment phase*)
          in (c, (S: bitstring, r: bitstring, payment: bitstring));
          let w1 = invers(S) in
          let u1 = Multiplication1(h1(payment), w1) in
          let u2 = Multiplication1(r, w1) in
          let (x1: bitstring, y1: bitstring) = sum(ECC(u1, P), ECC1(u2, APk1)) in
          if r = x1 then
          event userauthenticated(x1);
          out (c, payment);
          (*tracing*)
     let tag1 = TAG(APk1, creAPK1) in
     out (c, tag1).

let Tracer2(APk1: pkey, APk2: pkey, APK3: pkey, creAPK1: bitstring) =
(*tracing*)

     let tag2 = TAG(APk1, creAPK1) in
     out (c, tag2).
```

شکل (۱۰): قسمت مربوط به ردیاب‌ها در نرم‌افزار پرووریف.

۵-۷- قسمت ادعاها

شکل (۱۲) نشان‌دهنده دستورات مربوط به ادعاهای انجام‌شده در طرح پیشنهادی می‌باشد. سه ادعا با استفاده از نرم‌افزار پرووریف مورد تجزیه و تحلیل قرار گرفته است. محرمانگی هویت واقعی پرداخت‌کننده (خط۳۴)، محرمانگی هویت واقعی دریافت‌کننده (خط ۳۵) و احراز اصالت پرداخت‌کننده (خطوط ۳۶ و ۳۷) سه ادعا مورد بررسی قرار گرفته می‌باشند.

```
let Blockchain(APK1: pkey) =
(*payment phase*)

     in (c, m: bitstring);
     in (c, (PKA: pkey, IDA: bitstring));
out(c, m);
out(c, PKA).
```

شکل (۱۱): قسمت مربوط به زنجیره‌قالب.

۵-۸- قسمت پردازش

این قسمت، بخش اصلی دستورات می‌باشد. در این قسمت تمام موجودیت‌ها و اطلاعات اولیه‌ای که دارند تولید و معرفی می‌شود. شکل (۱۳) دستورات مربوط به این قسمت را نشان می‌دهد.

۵-۹- خروجی شبیه‌سازی

شکل (۱۴) نشان‌دهنده خروجی تجزیه و تحلیل با استفاده از نرم‌افزار پرووریف می‌باشد. همان‌طور که مشاهده می‌شود، ادعاهای انجام‌شده مورد تجزیه و تحلیل قرار گرفته‌اند و نرم‌افزار هر سه ادعا را درست اعلام می‌کند.

```
(*Query*)
free r: bitstring [private].
type host.
free x1: bitstring [private].
free IDA: bitstring [private].
free IDB: bitstring [private].
query attacker (IDA).
query attacker (IDB).
event userauthenticated(bitstring).
query event(userauthenticated(r)) ==> inj-event(userauthenticated(x1)).
```

شکل (۱۲): قسمت مربوط به ادعاها در نرم‌افزار پرووریف.

```
process
new g: G;
new P: bitstring;
new q: bitstring;
new IDA: bitstring;
new IDB: bitstring;
new BPK1: bitstring;
new APk1: pkey;
new APk2: pkey;
new APK3: pkey;
new creAPK1: bitstring;
new SKA: skey;
new PKA: pkey;
out(s, PKA);
new SKB: skey;
new PKB: pkey;
out (s, PKB);
new skm: skey;
new pkm: pkey;
out (s, pkm);
new ski: skey;
new pki: pkey;
out(s, pki);
((!Alice(PKA, SKA, IDA, P, q, g, BPK1)) | (!Bob(PKB, SKB, IDB, P, q, g)) | (!MA(pkm, skm)) | (!Issuer(pki, ski))
| (!Tracer1(APk1, APk2, APK3, creAPK1, P)) | (!Tracer2(APk1, APk2, APK3, creAPK1)) | (!Blockchain(APk1)))
```

شکل (۱۳): قسمت پردازش در نرم‌افزار پرووریف.

```
-- Query not attacker(IDA[])
Completing...
Starting query not attacker(IDA[])
RESULT not attacker(IDA[]) is true.
-- Query not attacker(IDB[])
Completing...
Starting query not attacker(IDB[])
RESULT not attacker(IDB[]) is true.
-- Query inj-event(userauthenticated(r[])) ==> inj-event(userauthenticated(x1[]))
Completing...
Starting query inj-event(userauthenticated(r[])) ==> inj-event(userauthenticated(
x1[]))
RESULT inj-event(userauthenticated(r[])) ==> inj-event(userauthenticated(x1[])) i
s true.
neam@ubuntu:~/Downloads/proverif2.00$
```

شکل (۱۴): خروجی نرم‌افزار.

۶- نتیجه‌گیری

در این تحقیق ما یک طرح پرداخت الکترونیک مبتنی‌بر زنجیره‌قالب را ارائه دادیم که با استفاده از فناوری زنجیره‌قالب و استفاده از توابع رمزنگاری به ویژگی‌هایی از قبیل امنیت، حریم خصوصی مشروط، ردیابی و لغو کاربران مخرب، حفظ گمنامی کاربران صادق و اقدامات تشویقی و تنبیهی دست یافتیم. در طرح پیشنهادی، تولید نام‌های مستعار به‌صورت پیش محاسبه می‌باشد؛ بنابراین این طرح دارای عملکرد مناسبی می‌باشد. ما یک ساختار کلی از طرح را بر اساس اولویت‌های رمزنگاری موجود، یعنی امضای کور منصفانه و تسهیم راز، و فناوری زنجیره‌قالب پیشنهاد کردیم

۷- مراجع

[1] N. Radziwill, “Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world,” The Quality Management Journal, vol. 25(1): pp. 64-65, 2018.

[2] J.-S. Chou, et al., “A Novel ID-based Electronic Cash System from Pairings,” IACR Cryptology ePrint Archive, p. 339, 2009.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system, 2008.

[4] Y. Guo and C. Liang, “Blockchain application and outlook in the banking industry,” Financial Innovation, vol. 2(1), p. 24, 2016.

[5] Z. Qin, et al., “A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing,” Computer Standards & Interfaces, vol. 54, pp. 55-60, 2017.

[6] X. Chen, et al., "New and efficient conditional e-payment systems with transferability," Future Generation Computer Systems, vol. 37, pp. 252-258, 2014.

[7] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in International conference on financial cryptography and data security, Springer, 2016.

[8] L. Zhong, et al., "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327-337, 2019.

[9] F. Gao, et al., "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," IEEE Network, vol. 32(6), pp. 184-192, 2018.

[10] E. F. Jesus, et al., "A survey of how to use blockchain to secure internet of things and the stalker attack," Security and Communication Networks, 2018.

[11] P.-Y. Chang, M.-S. Hwang, and C-.C. Yang, "A blockchain-based traceable certification system," in International Conference on Security with Intelligent Computing and Big-data Services, Springer, 2017.

[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem ACM Transactions on Progamming Languages and Syetems," vol. 4, no. 3, pp. 382-401, July 1982.

[13] Yin, W., et al., "An anti-quantum transaction authentication approach in blockchain," IEEE Access, vol. 6, pp. 5393-5401, 2018.

[14] W. Stallings, "Network and internetwork security principles and practice," Prentice Hall Englewood Cliffs, NJ., vol. 1, 1995.

[15] M. Abe and M. Ohkub, "Provably Secure air Blind Signatures with Tight Revocation. inInternational Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001.

[16] L. Zhang, et al., "Blockchain based secure data sharing system for Internet of vehicles: A position paper," Vehicular Communications, vol. 16, pp. 85-93, 2019.

[17] S. K. Langford, "Threshold DSS signatures without a trusted party," in Annual International Cryptology Conference, Springer, 1995.

[18] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International journal of information security, vol. 1(1), pp. 36-63, 2001.

[19] M. H. Kazemi, et al, "A secure three factor authentication scheme for wireless healthcare sensor networks based on elliptic curve," Advanced Defence Sci.& Tech., vol. (1)8, pp. 147-167, 2020. (In Persian)