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

سهولت در کسب وکار مالی با چک الکترونیکی

داریوش آریابرزن، متصدی اموربانکی، بانک اقتصاد نوین، d.aryabarzan@gmail.com

چکیده

با رشد روزافزون خدمات الکترونیکی و نفوذ آن در زندگی روزمره شاهد تبدیل شکل بسیاری از خدمات به خدمت الکترونیکی هستیم. مدت‌ها است که خدمات بانکی به‌صورت الکترونیکی انجام می‌شود و این امر در دسترس‌پذیری خدمات در طول شبانه‌روز، کاهش ترددها و سفرهای شهری،سرعت خدمات و.... داشته است. در حوزه چک نیز آخرین نمونه آن طرح چکاوک بود که از طریق آن چک‌ها بین بانک‌ها به‌صورت تمام الکترونیکی مبادله شده و باعث افزایش سرعت و دقت در گردش چک و وصول آن گردیده است؛ اما هنوز برگ چک در بین مردم وجود داشته و مشابه‌ای در دنیای الکترونیکی برای آن وجود ندارد. اصلی‌ترین پیش‌نیاز برگ چک الکترونیکی را می‌توان زیرساخت کلید عمومی یا به‌اصطلاح عمومی امضای دیجیتال دانست، خوشبختانه مدتی است در بانک مرکزی این زیرساخت تحت عنوان نماد ایجاد گردید و در حال بهره‌برداری است و می‌توان گفت اولین و اصلی‌ترین نیازمندی ایجاد برگ چک الکترونیکی هم‌اکنون در تمام بانک‌های کشور وجود دارد.

در این مقاله به چگونگی اجرای چک الکترونیکی، مزیت‌ها و معایب برگ چک الکترونیکی، پرداخت شده است. هر خدمتی مزیت و معایبی دارد و آنچه باعث بقای آن می‌شود افزونی مزیت‌های آن است. باید دید در برگ چک الکترونیکی چه مزیت‌هایی نسبت به برگ چک کاغذی دارد تا بتوان تصمیم‌گیری صحیح کرد. بر این مبنا مزایای برگ چک کاغذی را می‌توان در سهولت استفاده و نقل‌وانتقال آسان خلاصه کرد. برگ چک کاغذی به‌راحتی توسط صاحب آن قابل حمل‌ونقل بوده و در هر مکان و زمانی قابل استفاده است. درعین‌حال برگ چک کاغذی به‌راحتی بین افراد گردش کرده و به‌نوعی نقش پول مدت‌دار را بازی می‌کند. محدودیت تعداد و عدم امکان ابطال برگه‌های دفترچه قبل از اتمام دفترچه ازجمله معایب برگه چک‌های کاغذی است. در همین حال امکان سرقت برگ چک نیز از دیگر مشکلات استفاده از چک‌های کاغذی است.

بررسی تجارب موفق دنیا نشان می‌دهد، عدم محدودیت تعداد برگ چک، امکان مسدودسازی چک در اولین تخلف، عدم امکان سرقت، مدیریت اعتبار افراد متناسب با تمکن مالی، عدم امکان تغییر در برگ چک الکترونیکی، اعتبارسنجی راحت، صرفه‌جویی در مصرف کاغذ، اطلاع‌رسانی نقل‌وانتقالات چک به صاحب آن ازجمله مهم‌ترین مزایای استفاده از برگ چک‌های الکترونیکی است. در عین حال وابستگی صدور به وجود اینترنت، بزرگ‌ترین مشکل این برگ چک‌ها است.

واژه های کلیدی: خدمات بانکی، چک کاغذی، چک الکترونیکی، امضای دیجیتال

طبقه بندی JEL : M15, O32

Abstract

With the growing growth of electronic services and its influence in everyday life, we are witnessing the transformation of many forms of service into electronic service. For a long time, banking services have been carried out electronically, which has the ability to access day-to-day services, reduce city traffic and travel, speed of service, and so on. In the check area, the latest example was the scheme of the chakavak(Check Image Transfer System), through which checks were exchanged between banks in all electronic ways, which increased the speed and precision of the circulation of the check and its collection, but there was still a check list among the people and There is no similarity in the electronic world. The main prerequisite for the electronic check list is the public key or the so-called public digital signing. Fortunately, in the central bank, this infrastructure has been created under the name of the symbol and is in operation, And it can be said that the first and most important requirement for creating electronic check list is now in all banks of the country.

In this article, how electronic checks have been implemented, the advantages and disadvantages of electronic checking. What should be seen in the electronic checkout paper, what are the advantages of a paper check sheet to make the right decision. On this basis, the advantages of a paper check can be summarized in ease of use and easy transfer. The paper check sheet is easily accessible by the owner and can be used at any time and place. Meanwhile, a sheet of paper check is freely circulating between people and sometimes plays a long-term money role. Limitation of the number and impossibility of cancellation of the banknote sheets before the completion of the notebook is one of the disadvantages of a paper check paper. Meanwhile, the possibility of theft of leaf checks is another problem with the use of paper checks.

A review of the world's best practices shows that there is no limitation on the number of check sheets, the possibility of blocking the check at the first violation, the inability to steal, managing the credibility of the individuals in proportion to the financial compensation, the impossibility of changing the electronic check sheet, convenient validation, saving paper consumption, information of Transmission to the owner of the check is One of the most important benefits of the use of electronic checks. At the same time, the dependence of issuance on the existence of the Internet is the biggest problem with these checks.

Keywords: banking services, Paper check, Electronic check, digital signature

JEL Classification: M15, O32

مقدمه

توسعه فناوری اطلاعات و ارتباطات و گسترش آن به بازارهای پولی و مالی، کار را برای مشتریان بانک‌ها آسان‌تر و همچنین روش‌های بانکداری را دچار دگرگونی کرده است . آمار چک های برگشتی روز به روز بالاتر می‌رود وکسب و کار ورونق اقتصادی را دچار مشکل کرده است . امروزه مشتریان بانک ها به دنبال صرفه جویی در وقت و هزینه شان هستند ، ترافیک شهری ، شلوغی بانک ها و صرفه‌جویی در مصرف کاغذ ، انرژی ، و کاهش هزینه‌های بانک‌ها ، از مهمترین انگیزه‌ها برای بررسی سیستم پرداخت چک الکترونیکی می‌باشد. چک الکترونیکی ابزاری قدرتمند در جهت صرفه‌جویی در مصرف کاغذ ، حفظ محیط زیست ، صرفه جویی در وقت شهروندان ، سهولت در کسب و کار مالی ، کاهش هزینه بانک‌ها و همچنین کاهش چک‌های برگشتی می باشد . در این مقاله سعی شده است به طور مختصر و مفید عملکرد چک الکترونیکی بررسی شود و همچنین توضیح داده شده است که مشتریان برای اخذ دسته چک جدید دیگر نیازی به حضور در بانک‌ها را ندارند(فقط دفعه اول صدور دسته چک حضور مشتری الزامی می باشد) ، همچنین چک الکترونیکی به مشتری امکان می‌دهد از منزل یا دفتر کارش خدمات درخواستی خود را از سامانه الکترونیکی بانک عامل مورد نظرش دریافت کند ؛ در نتیجه صرفه‌جویی‌های بسیاری در این خصوص انجام می‌شود . در واقع چک الکترونیکی[۱] یک ابزار نوین پرداخت است که از امنیت ، سرعت ودقت و فرایند بازدهی تمام تراکنش‌های الکترونیکی توام با زیرساخت قانونی گسترش‌یافته صحیح برخوردار بوده و جایگزین خوبی برای چک‌های کاغذی در تجارت است . مشتریان برای استفاده از چک الکترونیکی نیاز به کلید عمومی[۲] و کلید خصوصی[۳] دارند(که از بانک اخذ می کنند) و همچنین نیاز به تایید طرف مقابل . همچنین موسسه ثالثی(مؤسسه ی عامل[۴]) هم می‌تواند وجود داشته باشد که در صورت عدم موجودی کافی در حساب جاری مشتری خوش حساب(به دلایل گوناگون که مشتری خوش حساب نتوانسته موجودی حساب خود را تامین کند)،چک او را نقد کند.در ادامه به این مطالب پرداخته می‌شود. در این مقاله به بررسی چگونگی اجرای چک الکترونیکی می‌پردازیم هدفمان کمک به سهولت در کسب و کار مالی و رونق چرخه ی اقتصادی با سریع تر کردن نقل وانتقالات مالی به وسیله چک الکترونیکی می باشد.

۱- ادبیات موضوع

چک الکترونیکی یا چک اینترنتی ، نخستین بار در مؤسسه علوم اطلاعات دانشگاه کالیفرنیای جنوبی توسعه وتکامل یافت[۵].در آغاز ، بانکداران نمی‌دانستند که چگونه چک‌های کاغذی را برای وصول در تاریخ سررسید ، از سایر بانک ها جمع آوری کنند وبرای این کار ، تحصیلدارانشان را به بانک های دیگر می‌فرستادند و این امر علاوه بر اتلاف وقت زیاد ، از نظر امنیتی نیز نگران کننده بود. از این رو چک های کاغذی که انتخاب میلیون ها نفر در جهان هست ، به سمت الکترونیکی شدن پیش یافت. گرچه در آغاز کار بازرگانان در مقابل چک های الکترونیکی مقاومت نشان می‌دادند ، ولی بعد ها با آگاهی از

---

[۱] Electronic Check

[۲] Public key

[۳] Private key

[۴] Factor company

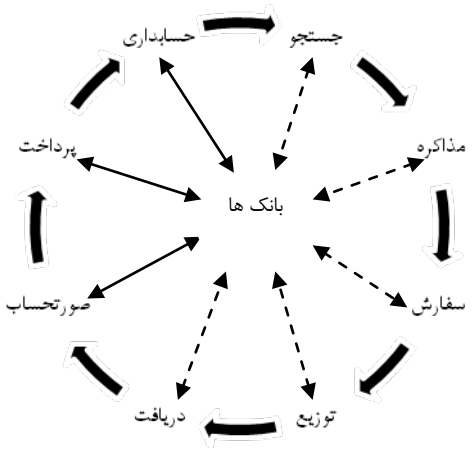
[۵] برای مطالعه بیشتر به منبع زیر رجوع شود:

-Dani, A.Rand Krishna .P.R, "An E-check Framework for Electronic Payment Systems in the Web Based Environment", EC-Web 2001, Springer-Vela LNCS 2115, 2001.

مزایای آن و اینکه چک های الکترونیکی همانند چک های کاغذی معاملات را پوشش می دادند واز قوانین چک کاغذی پیروی می‌کردند، به آن روی آوردند.

این چک که مبتنی بر اینترنت است،برای اولین بار در وزارت خزانه داری ایالات متحده آمریکا به کار گرفته شد.چک الکترونیکی به مفهوم پیشرفته تر آن در سال ۱۹۹۵ توسط شورای چک الکترونیکی[۱] به وجود آمد که حاصل تلاش های کمیته چک الکترونیکی بود.

در سیستم های پرداخت الکترونیکی[۲] ، امنیت جایگاه ویژه ای دارد ، که مستلزم حضور مرجع صدور گواهی است که طی برنامه سوم توسعه اقتصادی ، اجتماعی و فرهنگی جمهوری اسلامی ایران ، با تدوین نظام ملی تایید هویت(CA



شکل۱-۱ چرخه ی تجارت الکترونیکی

در چک‌های کاغذی، با نوشتن مبلغ چک[۱]، تاریخ چک و نام شخص به بانک عامل (بانک صاحب حساب چک) اجازه‌می‌دهید مبلغ نوشته شده را در تاریخ سررسید چک به شخص مورد نظر انتقال دهد.

در چک‌های الکترونیکی شما تنها مرحله اول را انجام می‌دهید. یعنی تنها چک را می‌نویسید و کارهای دیگر به صورت سیستمی انجام می‌شود ، حتی نوشتن چک نیز نیاز به کاغذ و دسته‌چک ندارد. چک الکترونیکی روش پرداختی الکترونیکی است که به واسطه انجام تراکنش پرداخت از طریق اتاق‌های پایاپای اتوماتیک(ACH[۲]) مورد استفاده مشتریان قرار می‌گیرد. اطلاعات این تراکنش شامل مبلغ و اطلاعات بانک پشتیبانی صاحب حساب است؛ همان اطلاعاتی که روی چک‌های کاغذی نوشته می‌شود ، به‌صورت خودکار به چک‌های الکترونیکی تبدیل می‌شود. همچنین باید تاکید کرد چک‌های الکترونیکی با همان چارچوب قانونی چک‌های کاغذی پایه‌ریزی می‌شوند و قابلیت پیوند به اطلاعات نامحدود و معاوضه سریع میان سایر بخش‌ها را دارند و می‌توانند در هر تراکنش مشابه چک‌های کاغذی استفاده شوند. استفاده ازچک‌های الکترونیکی ویژگی‌های مهمی دارند؛ آنها خدمات گوناگونی را عرضه کرده و موجب می‌شوند تراکنش‌های بانکی با امنیت کافی در اینترنت به کار گرفته شوند ، در بستر نامحدود ولی کنترل‌شده اطلاعات، صحت خود را حفظ می‌کنند. به این ترتیب تقلب‌های ایجادشده روی چک‌ها از بین می‌رود و تأیید خودکار محتویات و صحت چک‌ها امکان‌پذیر می‌شود. افزایش قابلیت‌هایی مانند فعال کردن تاریخ پرداخت، افزایش سرعت و کاهش زمان انتقال وجوه از یک نقطه به نقطه‌ای دیگر و استفاده از چک الکترونیکی به جای پول موجب افزایش امنیت در مقابل سرقت و از میان رفتن پول نقد می‌شود، سالانه مبلغ قابل توجهی هزینه صرف چاپ اسکناس می‌شود که با استفاده از چک‌های الکترونیکی، هزینه‌های چاپ اسکناس کاهش می‌یابد.

استفاده از چک الکترونیکی همچنین موجب می‌شود که دسترسی به وجوه با سرعت و در هر نقطه امکان‌پذیر باشد. همچنین از انتقال پول نقد جلوگیری کرده و حجم مسافرت‌های درون‌شهری به منظور دریافت و پرداخت‌های بانکی را کاهش می‌دهد و از این راه موجب کاهش هزینه‌های فردی و اجتماعی می‌شود.

---

[۱] Amount

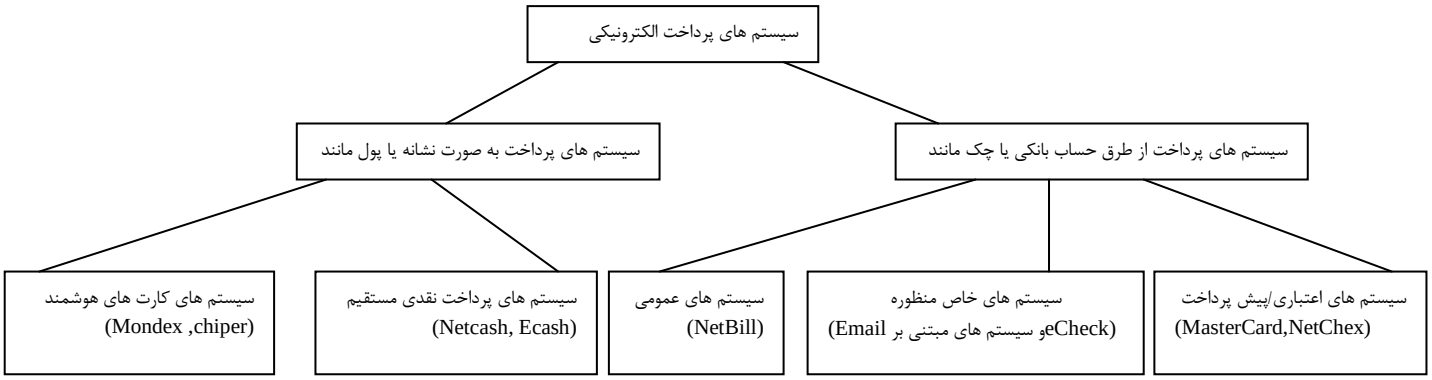
[۲] Automated Clearing House

چک‌های الکترونیکی باعث تسهیل در امور پرداخت و دریافت وجوه نقد شده و از راه گسترش و توسعه آن‌ها رغبت بانک‌ها به بانکداری الکترونیکی افزایش پیدا می‌کند. چک‌های الکترونیکی می‌توانند امنیت[1] پرداخت‌ها را نه تنها در پرداخت‌های جزیی محلی بلکه در سراسر سطح اینترنت برقرار کنند. چک الکترونیکی در اختیار مشتری است نه بانک ، و قابل استفاده برای تمام دارندگان حساب از کوچک و بزرگ است. با استفاده از این چک‌ها علاوه بر جلوگیری از جعل چک، اعتبارسنجی جامع و کامل‌تر متقاضیان در زمان صدور هر برگه چک نیز انجام خواهد شد. در حال حاضر چک‌های الکترونیکی ریسک فرایند چک‌های معمولی را تا حد زیادی کاهش داده و فرایند پرداخت را تا حد زیادی کنترل می‌کنند. این شیوه ی پرداخت ، چک‌های کاغذی را به‌صورت اتوماتیک به یک روش پرداخت الکترونیکی غیرحضوری تبدیل می‌کند. چک های الکترونیکی در جایی که سایر راه‌حل‌های پرداخت الکترونیکی با میزان ریسک بالا یا نامناسب باشند، امن‌ترین ابزار پرداخت هستند.

درعصر فناوری و تجارت الکترونیک، اسناد تجاری الکترونیکی جایگزین مناسبی برای اسناد سنتی(کاغذی) می‌باشد،از این رو چک های الکترونیکی از نمونه های موفق سندهای تجارت الکترونیکی می‌باشد که به نظر می‌رسد استفاده از آن در ایران با استقبال فراوان روبرو شود ، به ویژه اینکه طبق چشم انداز بیست ساله،ایران باید از لحاظ تجارت الکترونیکی رتبه نخست در منطقه خاورمیانه باشد ، موضوع چک الکترونیکی از اهمیت زیادی برخوردار می باشد .

بانک مرکزی ایران در راستای کاهش چک‌های برگشتی، در کنار تکمیل زیرساخت پردازش و پذیرش الکترونیکی چک ، پیاده‌سازی کامل سامانه‌های نظارتی مرتبط نظیر سامانه چک برگشتی، سامانه مرکز کنترل و نظارت اعتباری (مکنا)[2] و به‌خصوص سامانه صدور یکپارچه الکترونیکی دسته‌چک (صیاد) را با هدف ایجاد زمینه نظارت مؤثر بر سازوکار صدور دسته چک در دستور کار قرار داده است.

شکل ۱-۲ طبقه بندی سیستم های پرداخت الکترونیکی از نظر نحوه‌ی انتقال را نشان می‌دهد.



شکل ۱- ۲ طبقه بندی سیستم های پرداخت الکترونیکی از نظر نحوه‌ی انتقال

[1] Security

[2] وظیفه سنجش اعتبار مشتری قبل از صدور کارت اعتباری و دریافت گزارشهای اعتباری از بانک را بر عهده دارد، بانک مرکزی بر این مرکز نظارت کامل دارد.

۲-روش تحقیق

چک چیست؟ برگه تاریخ دار و با ارزش مالی ،که برای خرید در حال و پرداخت در آینده استفاده می‌شود ، بخش‌هایی که در برگ چک وجود دارندکه برخی ازآن ها جاهای خالی تعبیه شده‌ای در چک هستند که باید از سوی نویسنده کامل شود عبارتند از : مبلغ چک ، شماره حساب جاری ، تاریخ پرداخت ، امضای صاحب حساب و شماره برگه چک.

چک الکترونیکی چیست؟ این مفهوم طی پروژه ای از FSTC [۱] گرفته شده است.این شرکت داری ۱۰۰ عضو است که شامل تعدادی از بانک های بزرگ،دانشگاه ها ولابراتور های تحقیقاتی است. چک الکترونیکی یک ابزار جدید پرداخت متشکل از امنیت وسرعت بوده و قابلیت جایگزینی با چک های کاغذی در فرآیندهای تجاری را دارد.

چک الکترونیکی در واقع یکی از شیوه های پرداخت الکترونیکی است[۲] که به دو نوع چک اصلی الکترونیکی و چک جایگزین الکترونیکی تقسیم می شود.چک اصلی الکترونیکی نوعی از سند تجاری الکترونیکی می باشد که با استفاده از اینترنت،به صورت تمام الکترونیکی طراحی شده ودارای تمام خصوصیات چک کاغذی و فاقد معایب آن می باشد و در صدور آن تمام ضرایب امنیتی رعایت شده است. چک جایگزین چک الکترونیکی همان اسکن کردن چک سنتی و ارسال برای بانک مقصد می‌باشد(سامانه چکاوک)که هم اکنون در بانک های کشور ما اجرایی شده است.در واقع چک الکترونیکی نسخه ی مجازی چک کاغذی می‌باشد.چک‌های الکترونیکی همچون چک‌های کاغذی،دارای الزام قانونی برای پرداخت هستند و به جای امضاهای دستی،از امضاهای دیجیتالی[۳] استفاده می‌شود.با الکترونیکی شدن چک و استفاده از امضاها و سندهای دیجیتالی[۴]،امکان بررسی وجود وجه کافی در حساب شخص صادر کننده چک وجود دارد ، همچنین قطعیت پرداخت شدن آن نیز معلوم و تضمین می‌شود ، بدون آنکه بانک دریافت کننده‌ی چک ضرری کند ، لذا از این رو نسبت به چک کاغذی در جایگاه بالاتری قرار می‌گیرد.چک‌های الکترونیکی از همان جریان پرداخت و پایاپای چک کاغذی پیروی می‌کند ، بنابراین بانک ها با سرمایه گذاری کمی می‌توانند این فناوری جدید را عرضه کنند ، علاوه بر آن سیستم چک الکترونیکی می‌تواند با ادغام با سیستم پایاپای بانکی ، ضمن برخورداری از هزینه کمتر پردازش ، بر سهولت ، صحت و سرعت تسویه‌ی حساب‌های بانکی بیفزاید . لذا بانک ها از اینکه نقش خود را همچنان در تراکنش های مالی حفظ خواهند کرد ، علاقه‌مند به چک الکترونیکی خواهند بود.فروشنده‌ها هم به دلیل صرفه جویی در هزینه‌ها،زمان و کاهش برگشت چک‌ها به چک الکترونیکی علاقه‌مند خواهند بود.

کنسرسیوم فناوری خدمات مالی(FSTC) چهار سناریو مطابق شکل ۲-۲ برای پردازش چک های الکترونیکی بیان می‌کند.

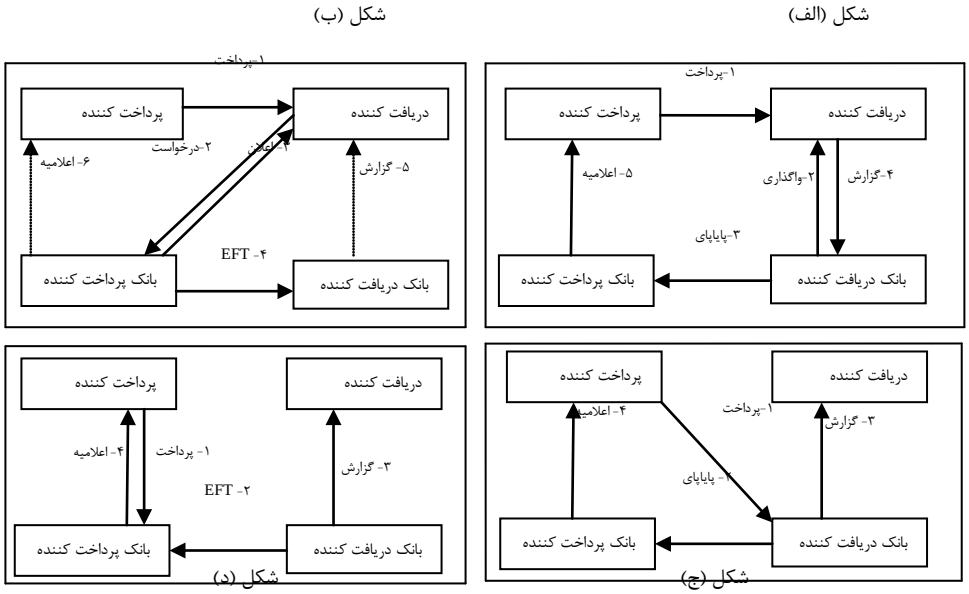
---

[۱] شرکت سرویس های نوین مالی(Financial Services Technology Consortiurn)

[۲] Electronic Payment Method

[۳] digital signature - یک امضای دیجیتالی (با گواهی دیجیتالی اشتباه گرفته نشود) یک روش ریاضی است که برای تأیید صحت و یکپارچگی پیام در نرم افزار یا سند دیجیتالی استفاده می شود.

[۴] Digital document



شکل۲-۱ سناریو های FSTC برای پردازش چک های الکترونیکی

در حالت(الف)،چک الکترونیکی به صورت سند دیجیتالی است که توسط پرداخت کننده(صادر کننده چک) ، نوشته و امضای دیجیتالی می‌شود وبرای دریافت کننده(ذینفع) ارسال می شود . دریافت کننده نیز چک را با امضای دیجیتال خود پشت نویسی می‌کند و به بانکی که خود در آن حساب دارد واگذار می‌نماید تا از طریق سیستم پایاپای تسویه شود . هر یک از کاربران و بانک‌ها سندهای دیجیتالی برای اثبات صحت امضای خود دارند بانک امضای دیجیتالی روی چک را با کلید عمومی پرداخت کننده(صادر کننده چک) بررسی‌می‌کند. کلید عمومی پرداخت کننده همراه با سند دیجیتالی پرداخت کننده به بانک مقصد ارسال می‌شود.

حالت (ب)زمانی استفاده می‌شود که بانک دریافت کننده،چک الکترونیکی را حمایت نمی‌کند و دریافت کننده(ذینفع)،چک را مستقیم به بانک پرداخت کننده(بانک صاحب حساب) می‌فرستد.

حالت (ج) وقتی استفاده می‌شود که تعداد چک ها برای واگذاری زیاد باشد ، بدین صورت که دریافت کننده(ذینفع) یک حساب خاص معروف به صندوق پرداخت[۱] در بانک خود افتتاح می‌کند و بانک با این حساب چک های الکترونیکی دریافت کننده را می‌پذیرد و بعد از دریافت چک ها توسط بانک بقیه مراحل مانند حالت(الف) هست .

حالت (د) همان روش پرداخت بستانکار / بدهکار می‌باشد ، بدین صورت که پرداخت کننده(صادر کننده چک) ، چک الکترونیکی را به بانک خود می‌فرستد ، سپس بانک حساب دریافت کننده را بستانکار می‌کند .

چک های الکترونیکی به واسطه ی FSML[۲] و امضاهای دیجیتالی ، در زمره ی امن ترین ابزار های پرداخت هستند و از تکنیک های امنیت هویت شناسی[۳] ، رمز نگاری کلید عمومی[۱] ، امضاهای دیجیتالی،تشخیص موارد تکراری بودن و رمز

---

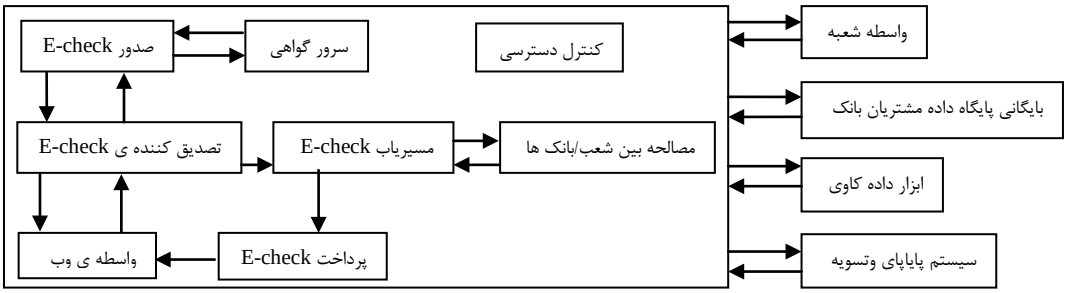
[۱] lock box

[۲] (Financial Services Markup Language) برای حمایت ازساختار های داده ای و امضاهای دیجیتالی مورد نیاز برای چک های الکترونیکی طراحی شد و در آن ،ساختار واقلام داده ای سند به صورت بلوک هایی برای چک های الکترونیکی با برچسب هایی از هم مجزا می شوند.

[۳] Authentication

گذاری[۲] بهره مند هستند.ویژگی‌های امنیتی چک الکترونیکی ، بانک ها را قادر به تصدیق و پردازش خودکار می‌کند و به کاربران چک‌های الکترونیکی توانایی حفاظتی بیشتری در برابر تقلب چک می‌دهد.امضاهای دیجیتالی ثابت می‌کنند که سفارش پرداخت را فقط و فقط شخص پرداخت کننده(صادر کننده چک) داده است و با اطمینان دادن از جامعیت پیام ، هویت شناسی ونفی انکار ، چک الکترونیکی را دربرابر تقلب امن می‌کنند . هم اکنون بانک ها برای بررسی اصلی یا تکراری بودن چک ها بررسی های دقیقی را انجام می‌دهند . این موضوع در مورد چک های الکترونیکی کاملاًجدی انجام می‌شود،به طوری‌که قابلیت های بالاتری برای پیشگیری وشناسایی موارد تکراری جعلی یا اشتباهی ارایه می‌کند.برای امن کردن کلید محرمانه ی امضای دیجیتال وجلوگیری از سوء استفاده از آن،از کارت هوشمند[۳] دسته چک الکترونیکی استفاده می شود . کلید محرمانه‌ی امضا کردن فقط از درون کارت هوشمند توسط الگوریتم های رمزنگاری[۴] که مطابق استاندارد های صنعت بانکداری است ، تولید و استفاده می‌شود .

برای جلوگیری از سرقت کلید محرمانه‌ی امضا کردن از طریق ارتباط شبکه ای کامپیوتر ، این کلید هرگز به کامپیوتر امضا کننده منتقل و افشا نمی‌شود . دسته چک الکترونیکی به طور خودکار هر چک را به منظور اطمینان از یکتایی چک‌ها امضا می‌کند و این در سیستم ثبت می‌شود تا در مواردی که امضاء ، پشت نویسی یا واگذاری چک دچار مشکل می‌شود ، به کمک گرفته شود.استفاده از چک الکترونیکی با ورود یک PIN[۵] توسط امضاء کننده کنترل می‌شود . این کار به دریافت کنندگان(ذینفعان) و بانک اطمینان می‌دهد که پرداخت کنندگان(صاحبان چک) قانونی،روی کلید های محرمانه خود مالکیت وکنترل دارند.



شکل ۲-۳ معماری سیستم E-check

---

[۱] Public Key Cryptography

[۲] encryption

[۳] کارت پلاستیکی حاوی یک تراشه ی کامپیوتری است که مقادیر زیادی از اطلاعات را نگه می دارد و برخی پردازش ها را انجام می دهد ودر مقابل تغییرات خیلی مقاوم است،کارت های هوشمند برای تامین حافظه ی امن کلید های خصوصی امضا و برای ایجاد و صحت سنجی امضاهای دیجیتالی یا چک های الکترونیکی مناسب هستند

[۴] جهت ایجاد امنیت در تبادل اطلاعات با فراهم آوردن خدمت‌های امنیتی مختلف از قبیل اطمینان از یکپارچگی یا دست نخوردگی و حفظ محرمانگی اطلاعات،انکارناپذیری وکنترل دسترسی به منابع اطلاعاتی طراحی شده اند

[۵] Personal Identification Number

سرورهای چک الکترونیکی بانک همچنین پایگاه داده[۱] مستقلی از کلیدهای عمومی امضاها را نگه می‌دارند ، به طوری که همیشه آخرین روابط کلیدها با حساب ها و امضاکنندگان در آن وجود دارد .

اجزای معماری چک های الکترونیکی شامل : پرداخت کننده(صاحب چک) ، دریافت کننده(ذینفع) ، بانک پرداخت کننده ، بانک دریافت کننده و اتاق پایاپای می‌باشد . دفترچه چک های (دسته چک)الکترونیکی که توسط بانک صادر می‌شود روی یک کارت هوشمند بارگذاری می‌شود . یک PIN نیز برای باز کردن قفل روی کارت هوشمند توسط بانک به مشتری داده می‌شود که می‌تواند بعداً آن را تغییر دهد . موقع نوشتن چک ، مشتری (صاحب چک)باید قفل کارت هوشمند را با PIN باز کند . با استفاده از زوج کلید های عمومی وخصوصی در کارت هوشمند ، چک الکترونیکی می تواند به صورت خارج از شبکه(Off-Line) ایجاد و امضا شود . بدین ترتیب امنیت مناسبی فراهم می‌شود . همچنین این سیستم به مفقود شدن چک های الکترونیکی نیز اهمیت می دهد ، چون اگر کارت هوشمند گم شود ، پرداخت کننده می‌تواند برای باقیمانده چک ها در خواست توقف پرداخت به بانک بدهد و درخواست دفترچه چک(دسته چک)الکترونیکی جدید بدهد . برخلاف کارت اعتباری و پول الکترونیکی که مبلغ محدودی را می توان توسط آن ها انتقال داد،در چک الکترونیکی محدودیتی نیست وهمین ویژگی،آن را برای پرداخت های بزرگ شرکت ها و دولت مناسب می‌کند.ویژگی پرداخت از حساب بانکی در چک های الکترونیکی،مزیت آن و در راستای کمک به بهبود نقدینگی است.در مورد کارت های هوشمندِ پول الکترونیکی،مفقود شدن کارت برابر با مفقود شدن پول است،درحالیکه در مورد چک های الکترونیکی،پول در بانک است.

تمام تلاش ها و برنامه ریزی ها باید در جهت جلب اطمینان و اعتماد کامل مردم باشد و بهترین وسیله برای اعمال چنین سیاستی حمایت کامل حقوقی و جزایی از چک است. از طرف دیگر ، سیستم پرداختی در مورد چک سنتی به گونه ای است که کاستی های آن ، مشکلاتی را در نظام اقتصادی به دنبال دارد.در مورد قانون چک،اخیراً ایراداتی برآن مطرح شده است که از جمله ی این مورد ، ضرورت ردپای چک است.مشکلات به قرار زیر است:

(الف) انتقال پول به شخص ثالث از طریق((صدور چک در وجه حامل))با توجه به ویژگی های امضاهای دیجیتالی و ویژگی های چک الکترونیکی ، به دلیل ثبت اطلاعات چک الکترونیکی در تمام مراحل صدور یا وصول ، این مشکل منتفی می‌شود

(ب)لازم است امضای ظهرنویس توسط یکی از بانک های رسمی یا یکی از دفاتر اسناد رسمی مورد گواهی قرار گیرد ، تا از یک طرف از انتقال پول از طریق صدور چک به نام مستعار و یا ظهرنویسی جعلی جلوگیری شود و از طرف دیگر ، از طرف دیگر،گیرندگان چک به واریز چک های وصولی به حساب جاری خود از طریق صدور چک شخصی- از این طریق،ایجاد رد پا- تشویق شوند ، گواهی دیجیتالیِ[۲] کلید عمومی امضاء ، این مشکل را نیز حل می‌کند.

(ج)بانک ها به ارسال اصل چک های کارسازی شده یا رونوشت پشت و روی برابر اصل شده ی چک های کارسازی شده برای صاحب حساب ، مکلف گردند با توجه به مواردی که برای حل مشکل مورد (الف) بیان شد،مورد (ج) نیز حل می‌شود.

(د)تلاش دولت در جهت حفظ حقوق و منافع گیرندگان چک ، جهت آگاه کردن گیرندگان چک از میزان اعتبار صادر کنندگان چک ، قبل از انجام معامله باشد . با بدون وقفه شدن ارتباطات طرفین با یکدیگر و با بانک هایشان ، این مورد نیز حل می‌شود.

---

[۱] Date Base

[۲] Digital Certificate

(ه)برای اطلاع دریافت کنندگان چک در خصوص اعتبار صادر کنندگان چک ، پیشنهاد شده است که موسسات خصوصی تایید کننده‌ی چک تاسیس گردد .گواهی‌های دیجیتالی[۱] صادره از سوی مرجع صدور گواهی دیجیتالی ، این مشکل را نیز حل می-کند .

گواهی‌های دیجیتالی همواره همراه چک الکترونیکی هستند و در هرکدام از مراحل چرخه ی زندگی چک ، بررسی های لازم قابل انجام هستند.

برای مشتریان بر اساس در جه ای از اعتبارشان شرایطی را می‌توان برقرار کرد که چک های برگشتی آن ها از طرف شرکت ثالثی موسوم به مؤسسه ی عامل[۲](که نقش آن در دنیای فیزیکی،خریدن چک های برگشتی به کسری از قیمت است[۳])، پرداخت شوند و در عوض مشتریان متحمل درصد هزینه‌ی بیشتری برای پردازش چک های آینده اش باشند . بدین طریق ضمن حفظ اسرار مالی مشتریان، امکان پرداخت شدن چک های مشتریان خوش اعتبار که به طور ناخواسته و به دلیل اشتباه برگشت خورده است ، فراهم می‌گردد. چنانچه شرکت ثالث ، چک آن‌ها را پرداخت نکند ، در این صورت ، برگشتی بودن چک اعلام می گردد.

۲-۱فرآیند پرداخت چک الکترونیکی

برای ایجاد سیستم چک الکترونیکی،باید مواردی را در نظر گرفت؛ از جمله اینکه پرداخت کننده ،گیرنده و بانک ها باید دارای گواهی دیجیتال و دو کلید (کلید عمومی و کلید خصوصی)باشند. هر دو طرف صادر کننده وگیرنده چک دارای کلید عمومی هستند و علاوه بر آن ، هر دو یک کلید خصوصی نیز دارند که طرف دیگر از آن بی اطلاع است . برای صدور چک الکترونیکی مطمئن ، معمولاً گواهی الکترونیکی نیز لازم است ، گواهی الکترونیکی شامل داده های الکترونیکی است،که حاوی اطلاعاتی در زمینه: مرکز صادر کننده گواهی ، مالک گواهی ، تاریخ صدور ، انقضای کلید عمومی مالک و یک شماره ی سریال که توسط مرکز میانی تولید شده است؛ به گونه ای که هر شخصی می تواند به صحت ارتباط کلید عمومی و مالک آن اعتماد کند. در صورت استفاده از سیستم چک الکترونیکی ، اصولا امکان صدور چک بلامحل وجود ندارد.

به طور خلاصه ، مراحل پرداخت چک الکترونیکی بدین ترتیب است: ۱- مشتری یک چک الکترونیکی را در رایانه می-نویسد ۲- مشتری چک الکترونیکی را امضا می‌کند ۳- مشتری چک الکترونیکی را به سیستم فروشنده می‌فرستد۴- فروشنده پس از دریافت چک الکترونیکی ، امضا را تأیید نموده و ظهرنویسی می کند ۵- چک ظهرنویسی شده به سیستم فروشنده فرستاده می‌شود ۶- بانک امضا را تأیید نموده و وجه چک الکترونیکی را به حساب فروشنده واریز می‌کند ۷- چک الکترونیکی با فرستادن به بانک مشتری تسویه می‌شود ۸- بانک مبلغی را از حساب مشتری بستانکار می‌کند. (مورد اخیر معمولا زمانی است که فروشنده نمی‌خواهد وجه بلافاصله به حسابش انتقال یابد ، بلکه می‌خواهد، بانک وجه مندرج در چک را از حساب صادرکننده یا مشتری غیرقابل برداشت نموده، تا بتواند به هر کس که می خواهد انتقال داده و ظهرنویسی نماید).

---

[۱] گواهی دیجیتال‌که به منظور احراز هویت کاربر می باشد،همان شناسنامه ای است که هویت واقعی شما را به صورت مجازی و برای کسب و کار الکترونیکی تعیین می‌کند وکاربرد آن در حقیقت استفاده از امضای الکترونیکی و رمز نگاری اطلاعات است.

[۲] Factor Company

[۳] در ماده ۲۳۹ قانون تجارت،می توان به نوعی نقش شخص ثالث یا شرخر را مشاهده کرد: هرگاه براتی نکول شد واعتراض به عمل آمد شخص ثالثی می-تواند آن را به نام برات دهنده یا یکی از ظهرنویس‌ها قبول کند-قبولی شخص ثالث باید در اعتراض نامه قید شود و به امضاء او برسد

۳-یافته ها ونتایج:

۳-۱سیستم پیشنهادی ما :پروتکل پرداخت چک الکترونیکی آفلاین[۱] ناشناس[۲]

ما یک‌پروتکل‌پرداخت الکترونیکی چک آفلاین ارائه می‌دهیم که ناشناس بودن پرداخت کننده را نسبت به دریافت‌کننده بیان می‌کند. در پروتکل ما سناریوی سیستم پرداخت چک را می‌پذیریم: ما از مراحل کلی فرآیند پرداخت چک پیروی می-کنیم، با رعایت تمام نیازمندی‌ها / جنبه های آن یا حداقل اهداف امنیتی و عملیاتی پشت سر آنها با توجه دقیق به مشخصات چک الکترونیکی، و همچنین ناشناس بودن پرداخت کننده . در پروتکل ما، دریافت‌کننده قادرخواهد بود تا صحت و اعتبار اولیه یک چک الکترونیکی را با تضمین‌هایی به منظور اعتمادو قبول پرداخت بدون تأثیر ناشناس بودن پرداخت کننده تأیید کند. به منظور تشویق دریافت کنندگان به‌قبول چنین سیستمی، ما جنبه های تأیید و امنیتی مختلفی را ارائه می دهیم که منجر به پرداخت‌چک الکترونیکی با اعتماد و اطمینان در رابطه با ناشناس بودن پرداخت کننده می‌شود.

فرض کنیم که ارتباطات ایمن از محرمانه بودن معاملات حمایت می‌کنند، به طوری که هیچکس نمی‌تواند به داده‌ها دسترسی داشته باشد.

نمادها:

□@: کانال های ارتباطی ناشناس و ایمن را نشان می دهد که پرداخت کننده می تواند به طور ایمن و ناشناس پیام را دریافت و ارسال کند.

U: حد بالای مبلغ پولی که مجاز به صدور مجوز می‌شود، از جمله U□ M

اختصارات:

GM: مدیر گروه (بانک، یک یا مجموعه ای از اشخاص).

DB: پایگاه داده، سوابق که در آن همه مشتریان بانک ذخیره می شود (محلی و امن).

Gverif: روند تأیید امضای گروه.

Look: اطلاعات محرمانه چک الکترونیکی را بررسی می‌کند.

Sub: فرآیندی که در آن ما یک مورد را در مجموعه‌ای از موارد مورد بررسی قرار می دهیم

مثلا Sub({دوشنبه، یکشنبه، دوشنبه، ...، پنجشنبه}) = true

OPEN: فرآیند بررسی امضای گروهی که در آن امضای گروه توسط GM برای شناسایی امضا کننده بررسی می‌شود.

Unforg: یک فرآیند برای اطمینان از اینکه چک الکترونیکی جعلی هست.

Valid: یک فرایند که در آن بانک اعتبار چک الکترونیکی را با بررسی مقدار وجه موجود در چک الکترونیکی، تأیید می‌کند.

Execute: فرآیند اجرای چک الکترونیکی(انتقال از سپرده پرداخت‌کننده به سپرده دریافت‌کننده).

Return: روندی است که اگر چک الکترونیکی نامعتبر باشد هویت پرداخت‌کننده توسط بانک مشخص می‌شود واز طریق بانک پرداخت کننده به دریافت‌کننده ارسال می‌شود.

پرداخت چک الکترونیکی آفلاین ناشناس

مانند چک های سنتی،پرداخت چک در مرحله نهایی انجام می‌شود، زمانی که پول در حساب بانکی دریافت کننده ذخیره می شود، در حالی که ابزار الکترونیکی چک الکترونیکی به عنوان ضمانتی برای پرداخت کننده استفاده می شود تا دریافت کننده مطمئن شود که این سیستم وجه را پرداخت خواهد کرد، یا حداقل هویت پرداخت کننده در مورد کمبود وجه یا جعل نشان داده خواهد شد. در ارتباطات ما رمزنگاری کلید عمومی[1] را به منظور اعمال محرمانه بودن معاملات اعمال می‌کنیم تا اطلاعات از هر نوع دسترسی غیرمجاز محافظت شود. علاوه بر این ، ما فرض می‌کنیم که هر دو پرداخت کننده وگیرنده سفارشاتی را دریافت می‌کنند (به عنوان مثال چک الکترونیکی یا سفارش خرید) ، یا هیچ کدام از آنها هیچ سفارشی را دریافت نمی‌کنند. در این پروتکل شواهد کافی در حین اجرای آن جمع آوری می‌شود،تا در صورتی که یک طرف به تعهدات خود عمل نکند،مورد پیگرد قانونی قرارگیرد. برای روشن شدن این موضوع،مراحل پروتکل پیشنهاد شده را به سه روش اصلی طبقه بندی می‌کنیم:

CLOSE
VERIFY
FOUND

FOUND : در این مرحله پرداخت کننده فرآیند پرداخت را پیدا می کند.

مرحله ۱: پرداخت کننده برای اولین بار توضیح سفارش خرید خود را(P_{desc})از طریق کانال ارتباطی ناشناس و امن برای دریافت‌کننده ارسال می‌کند. در مرحله بعد، دریافت‌کننده یک شماره سفارش(O_{id}) را که یک شماره منحصر به فرد توسط دریافت‌کننده برای هر خرید جدید است و به P_{desc} مرتبط است همراه با مبلغ پرداخت (M)و شناسه شماره حساب دریافت کننده (I_D)که بعداً در پرداخت چک الکترونیکی مشخص می‌کند.

[1] Public-key cryptography- قابل استفاده در امضای دیجیتال

Payer @□ payee: P_{desc}
Payee @□ Payer: O_{id}, M, I_D

مرحله ۲: پرداخت کننده،چک الکترونیکی(Ch_e)را با اطلاعات لازم (موافقت شده) برای دریافت‌کننده، مانند شناسه پرداخت کننده(I_D)، شماره سفارش خرید(O_{id})، پرداخت مبلغ (M)و زمان پرداخت / تاریخ (T)، پر می‌کند. سپس پرداخت کننده با استفاده از امضای B_{Gsig} گروه بانکی، Hash را امضا(تأیید)می کند. پس از آن، پرداخت کننده چک الکترونیکی را با نامه‌ای که Hash در آن امضاء(S)شده است از طریق کانال ارتباطی ناشناس و امن برای دریافت‌کننده ارسال می‌کند.

Payer: H (Ch_e) h, where Ch_e = (I_D, O_{id}, M, T),
B_{Gsig} (h) S
Payer @□ Payee: (Ch_e , S)

VERIFY :در این مرحله، دریافت‌کننده اعتبار چک الکترونیکی را تأیید و صحت آن را ارزیابی می‌کند وتصمیم می‌گیرد که آیا آن را تایید کند یا نه؟

مرحله ۳: دریافت‌کننده به نوبه خود، پیام را رمزگشایی می‌کند؛ H(Ch_e)وتأیید امضای Hash را با توجه به h تأییدمی کند (Hash (S)) و همچنین زمان تایید / تاریخ T را با دوره تأیید اعتبار امضا گروه(Tp)مقایسه می کند.

Payee:H (Ch_e) h,
Gverif (S), w.r.t (h).
Look (I_D, O_{id}, M).
Sub (T, T_p).

مرحله ۴: بعد از اینکه چک الکترونیکی اولیه تأیید شد، اگر دریافت کننده مطمئن باشد که چک الکترونیکی درست و تضمین شده است، موافقت خود را (A) اعلام می‌کند و پرداخت کننده، سفارش خود را از طریق کانال ارتباطی امن و ناشناس دریافت می‌کند.

CLOSE : در این مرحله وصول چک(در مرحله واگذاری چک به حساب دریافت‌کننده) با استفاده از روش های الکترونیکی اعمال می‌شود. یا با انتقال موفقیت آمیز پول به حساب دریافت کننده یا بازگشت چک الکترونیکی همراه با نمایش هویت پرداخت کننده به پایان می‌رسد.

مرحله ۵: واگذاری چک الکترونیکی به سپرده های دریافت کننده (Ch_e، S، A). سپس چک الکترونیکی از طریق روش وصول دقیقاً مانند چک های سنتی وصول می‌شود.

Payee □ (payee) bank: (Ch_e , S, A)

مرحله ۶: در مرحله وصول چک الکترونیکی، بانک پرداخت کننده اعتبار اولیه را که درمرحله ۳ انجام می‌شودرا مجدداً تأیید می‌کند. اگر تأیید نشود، بانک پس از اتمام آن فرآیند تأیید را متوقف می‌کند و چک الکترونیکی را بازمی‌گرداند، اما بدون شناسه پرداخت کننده، از آنجایی که پرداخت کننده درچک الکترونیکی تأیید شده است و در نتیجه، مسئولیت پذیری درباره چک الکترونیکی را رد می کند.

مرحله ۷: بانک پرداخت کننده همیشه امضای گروه را برای شناسایی امضا کننده تأیید می‌کند و بنابراین می تواند اعتبار چک الکترونیکی را تأیید کند.

مرحله ۸: بانک اطلاعات پایگاه داده(DB) خود را چک می‌کند تا ببیند که قبل از اجرای چک الکترونیکی چه اتفاقی افتاده است. اگر آن را با همان O_{id} یافت، پس پرداخت کننده متقلب است، زیرا او کسی است که O_{id} را صادر کرده است (که O_{id}

یکتاست) و او نباید دو بار از این O_{id} استفاده کند. در این صورت بانک از اجرای چک الکترونیکی صرف نظر می‌کند،در غیر این صورت، بانک مقدار پول را در حساب پرداخت کننده بررسی می‌کند؛ در صورتی که کافی باشد،فرآیند وصول چک الکترونیکی اجرا می‌شود، در غیر این صورت اگر کمتر از M باشد (به این معنی که موجودی ناکافی است)، پس از آن نمی-توان چک الکترونیکی را اجرا کرد، و بانک چک را با تأیید هویت پرداخت کننده به بانک دریافت کننده وبه نوبه خود به دریافت‌کننده بازگشت می‌دهد.دریافت کننده می‌تواند اقدام قانونی علیه پرداخت‌کننده را با استفاده ازچک الکترونیکی ،که فریب را در معامله ثابت کرده است،آغاز کند.

تضمین بانک پرداخت‌کننده:

$H(Ch_e)$ h,
Gverif (S), w.r.t (h).
Look (I_D, O_{id}, M).
Sub (T, T_p).
OPEN (B_{Gsig}): Identify the payer I
Unforg (Ch_e, O_{id}): If in DB $Ch_{e(1)} = Ch_{e(2)}$ $O_{id(1)} \square O_{id(2)}$

پرداخت کننده یک فریبکار است:

Valid (M): account $\square$M execute (Ch_e).
If account < M Return (Che , I).

در طراحی پروتکل چک الکترویکی آفلاین ناشناس ، تمام اجزا مرتبط باید با تمام زیرمجموعه های لازم تجهیز شوند. هر دو بانک پرداخت‌کننده و دریافت‌کننده باید چنین سیستم پرداخت الکترونیکی را پشتیبانی کنند. بانک پرداخت‌کننده می تواند یک وب سایت امن با استفاده از زیرساخت کلید عمومی برای مشتریان خود داشته باشد که از طریق آن‌پرداخت‌کننده‌ها بتوانند چک‌های الکترونیکی را صادر کنند. از یک طرف، پرداخت‌کننده و دریافت‌کننده باید ظرفیت ارسال و دریافت ایمیل داشته باشند. بانک فرستنده باید یک سیستم (به عنوان مثال پایگاه داده) داشته باشد، که در آن تمام معاملات الکترونیکی مشتریان در آن ثبت شود. با این وجود ما فرض می‌کنیم که سیستم پرداخت چک الکترونیکی پیشنهادی ما نیز با یک چارچوب قانونی مانند پرداخت های چک سنتی، در صورت ورشکستگی یا برگشت چک الکترونیکی، پشتیبانی می شود.

۳-۲تحلیل روش پیشنهادی:

این پروتکل مفاهیم چک سنتی با چک الکترونیکی را ترکیب می‌کند. در تجزیه و تحلیل پروتکل، ما ویژگی‌های چک سنتی را به ویژگی های پرداخت چک الکترونیکی آفلاین ناشناس ارتباط می‌دهیم و در مورد امنیت، حریم خصوصی و ویژگی‌های عملکردی آن بحث می‌کنیم. در چک‌کاغذی، اطلاعات اجباری وجود دارد که باید ارائه شود، در غیر این صورت پرداخت نمی-تواند پذیرفته شود. این اطلاعات (نام بانک، آدرس ، مبلغ پرداخت، تاریخ زمان بندی، نام گیرنده و شماره چک، نام، آدرس، امضا و شماره حساب پرداخت کننده) است. در جدول ۱ به طور خلاصه اهمیت و تاثیر این اطلاعات را بر ناشناس بودن پرداخت کننده و اعتماد و پذیرش پروتکل ارزیابی می کنیم.

تأیید، اعتماد و پذیرش	پرداخت کننده ناشناس	
اهمیت غیر مستقیم	بدون تأثیر و بدون تغییر	نام، آدرس بانک
با اهمیت	بدون تأثیر و	مبلغ‌پرداخت،تاریخ‌زمان‌بندی،نام‌گیرنده

	تغییرات جزئی	وشماره چک
مهم است (با حفظ اهداف، ناشناس بودن پرداخت کننده جایگزین می شود).	تأثیر بالا	نام،آدرس، امضا وشماره‌حساب پرداخت کننده

جدول ۳-۱ اهمیت و تاثیر اطلاعات بر ناشناس بودن پرداخت کننده و اعتماد و پذیرش در پروتکل چک الکترونیکی آفلاین ناشناس

۳-۲-۱تحلیل و بررسی امنیت و حریم خصوصی پروتکل

نام بانک پرداخت کننده،آدرس، اطلاعاتی هستند که در بانک پرداخت کننده وجود دارد که از طریق آن بانک واسطه(اتاق وصول) می‌تواند چک الکترونیک را شناسایی کند و وارد فرآیند وصول شود. در پروتکل ما ،امضای گروه بانک می‌تواند از طریق کلید عمومی امضای گروه، مشخص کند که کدام گروه امضاء متعلق به پرداخت‌کننده است وبه عنوان یک مزیت اضافی ،چک الکترونیکی را تأیید می‌کند.

در پروتکل پیشنهادی از طرح امضای امن گروه استفاده می‌کنیم و فرض می‌کنیم که آن را ایمن وتمام خواسته های ادعایی خودرا، تضمین می‌کنیم.با داشتن مالکیت زمان بندی شده عضویت ، هنگامی که پرداخت کننده به بانک می‌پیوندد ، مدیر گروه(که بانک مورد نظر ما می‌باشد) ، به یک پرداخت کننده یک کلید امضای گروه معتبر در یک دوره زمانی(T_P) می‌دهد،که نشان می‌دهد عضویت بانکی پرداخت کننده در این دوره زمانی و درقبال یک حساب معتبر،بدون ارائه اطلاعات در مورد مبلغ موجودپول با شماره حساب خود،معتبر است.این بانک به صورت دوره‌ای کلیدهای امضای جدید را در پایان هر دوره زمانی بروزرسانی می‌کند.همچنین بانک دارای توانایی با خواص ابطال پذیری عمومی برگشت‌پذیر،که برای حذف یک گروه کلید امضا در یک دوره(j) آغاز می‌شود،می باشد.به عنوان مثال از در زمانی که پرداخت کننده حساب معتبری در بانک دیگر ندارد،شروع می‌شود به طوری که امضاء را بعد از نامعتبر شدن می‌توان چک کرد که آیا لغو شده است یا نه؟ با استفاده از این ویژگی، زمانی که پرداخت کننده چک الکترونیکی را با تاریخ T در مدت زمان T_p امضاء می‌کند،دریافت‌کننده مطمئن خواهد شد که بانک پرداخت کننده با امضای معتبر در چک الکترونیکی موافقت می‌کند و به طور منطقی گواهی چک الکترونیکی را در دروه زمانی معتبر، با توجه به ویژگی امنیتی قوی آن صادر می‌کند. این واقعیت ویژگی امضای گواهی چک الکترونیکی را فراهم می‌کند.

بدون اطلاعات ضروری (نام، آدرس،امضا و شماره حساب)، در چک کاغذی،دریافت‌کننده پرداخت را قبول نمی‌کند.این کاملاً مخالف هدف اصلی پروتکل ماست، بنابراین ما این اطلاعات را با چیزهایی جایگزین می‌کنیم که اعتماد و اطمینان را حفظ می‌کند.همانطور که در پروتکل ما توافق شده است GMهویت پرداخت کننده را با فرض احتمالی اختلاف نظر یا فریب نشان می‌دهد.

هنگامی که بانک چک الکترونیکی را دریافت می‌کند،آن را به طرف امضاء کننده وصل می‌کند وسپس اعتبار آن را بررسی می‌کند.دراین صورت پرداخت کننده نیازی به شماره حساب خود یا هیچ اطلاعات شخصی(به عنوان مثال آدرس،نام و ...)ندارد. دریافت‌کننده می‌تواند چک الکترونیکی را به امضای خود وصل کند و به این ترتیب هویت امضاء کننده را در مورد فریب مشخص می‌کند.این مزایا از ناشناس بودن پرداخت کننده بر گیرنده پشتیبانی می‌کند.به علت عدم ارتباط امضای گروه، از آنجا که اطلاعات خصوصی پرداخت کننده هیچ اطلاعات قابل تکرار مانند شماره حساب ندارد،پروتکل ما از قطع ارتباط چک الکترونیکی پشتیبانی می‌کند. برخلاف چک کاغذی، با امضای گروه، پرداخت کننده نمی‌تواند امضا را جعل کند یا به نمایندگی از گروهی که متعلق به آن نیست،امضاءکند. همچنین، به وسیله ویژگی های مستحکم و پیوسته، هیچ یک از دو عضو یا بیشتر از اعضای گروه نمی‌توانند امضای گروه را بدون اینکه بانک حداقل یکی از آن‌ها را شناسایی کند،جعل کنند(در مورد حساب های مشترک). با این حال،ویژگی‌هایی مانع شونده، خصوصیات غیر قابل جعل پذیری را فراهم می‌کند. هر عضو

گروه (یا زیرمجموعه) یک کلید عمومی امضای خاص گروه دارد، که هیچکس نمی‌تواند از آن استفاده کند، بلکه فقط صاحب آن می‌تواند از آن استفاده کند.(فرض می شود که از هر حمله هم محافظت می شود)، بنابراین پرداخت کننده نمی‌تواند امضای‌چک الکترونیکی را رد کند، و بدین ترتیب خصوصیات عدم انکار را پشتیبانی می‌کند.

در مرحله ۱ پروتکل، دریافت‌کننده درخواست پرداخت‌کننده برای‌سفارش خرید با شماره سفارش منحصر به فرد را جواب می‌دهد این شماره منحصر به فرد از ویژگی غیرقابل کپی بودن پشتیبانی می‌کند، از زمانی که دریافت‌کننده، هنگام تأیید چک الکترونیکی، موافقت خود را(A)بدون بررسی شماره O_{id} ،(که این شماره قبلاً هرگز استفاده نشده باشد) نمی‌دهد(مرحله ۳). بنابراین تنها فرد مقصر دراینکه یک چک الکترونیکی تکراری باشد یا نه، دریافت‌کننده است و تشخیص جعل هنگامی که بانک،بانک اطلاعاتی خود را بررسی می کند، آسان می‌شود ، به طور مشابه، پرداخت کننده نمی‌تواند چک الکترونیکی را کپی کند زیرا او مجبور است شماره منحصر به فرد سفارش خرید را ضمیمه کند،که این ویژگی منحصر به فرد بودن چک الکترونیکی را قبل از تأیید دریافت کننده نشان می‌دهد.

در مرحله ۲، پرداخت کننده از یک تابعHash یک طرفه برای رمزگذاری چک الکترونیکی استفاده می‌کند قبل از امضای آن با امضای گروه بانک، و نامهHash امضا شده همراه با چک الکترونیکی اصلی را برای دریافت کننده ارسال می کند،با این کار، دریافت‌کننده می‌تواند تأیید کند که مقدارHash مجاز،همان مقدار Hash اصلی چک الکترونیکی است که آن را قبول می-کندوبا اطلاعات مربوط به آن موافق است. بنابراین دریافت کننده و پرداخت‌کننده و بانک می‌توانند مطمئن باشند، که چک الکترونیکی را نمی‌توان بعداً تغییر داد یا جایگزین کرد،در طول مراحل کلی پروتکل،همانطور که مقدار Hash امضاءشده از چک الکترونیکی تأیید شده است،بنابراین عملکرد یک Hash یکپارچه،تضمین یکپارچگی چک الکترونیکی را فراهم می‌کند.

۳-۲-۲تجزیه و تحلیل عملکرد

در چک کاغذی، مبلغ پرداخت، تاریخ زمان بندی و نام گیرنده، اطلاعات مورد توافق هر دو طرف برای پردازش پرداخت است. با این همه، بانک می تواند اعتبار چک را تأیید کند؛پس دریافت‌کننده را شناسایی و در نتیجه مبلغ پول به بانک خود را بعد از تاریخ زمانبندی انتقال می دهد. در پروتکل ما این اطلاعات در تأیید اعتبار اولیه چک الکترونیکی توسط دریافت-کننده و بعد ازتأیید اعتبار آن توسط بانک هم همان (در واقع بیشتر) ارزش را دارد،به عنوان یک نتیجه منطقی می توانیم قابل اطمینان بودن چک الکترونیکی را ببینیم.دریافت‌کننده می‌تواند به راحتی اعتبار اولیه چک الکترونیکی را بدون نیاز به ارتباط با بانک بررسی کند. باصدور گواهینامه ویژگی‌های امنیت و ویژگی‌های اولیه کاربردی،چک الکترونیکی صحت ویژگی‌ها را تأیید می‌کند.

در سناریوی طبیعی پروتکل(به عنوان مثال فریب)، بانک به طور منطقی با اجرای امضای چک الکترونیکی با امضای گروه معتبر موافقت می‌کند و آن را می‌پذیرد (کلید امضای عضو گروه معتبر که در وهله اول توسط بانک به وی پرداخت می‌شود) . همانطور که می‌توانیم از بحث فوق بیان کنیم،دریافت‌کننده نیازبه ارتباط با بانک را ندارد ،نه برای تأیید اعتبار اولیه چک الکترونیکی و نه در هر مرحله از پروتکل، اما وقتی که چک الکترونیکی را که ممکن است بعداً اجرا شود، واگذار می‌شود، و این باعث می‌شود پرداخت چک الکترونیکی به صورت آفلاین باشد،علاوه بر این، با تمام تضمین هایی که به دریافت‌کننده از امنیت ، خصوصیات و ویژگی های عملکرد، داده شده است، دریافت‌کننده ،با چک الکترونیکی به عنوان یک ابزار تضمین شده، موافقت خواهد کرد.

پرداخت چک‌های الکترونیکی را می‌توان در یک زمان بندی T در مدت زمان اعتبار گروه Tp، مبلغ درخواستی را در فواصل منظم،در مدت زمان اعتبار در یک سری ازچک‌های الکترونیکی مرتبط انجام داد. هر چک الکترونیکی دارای زمان بندی

متفاوت است اما دارای همان شماره سفارش منحصر به فرد است که به دو قسمت تقسیم شده است. بخش اول که ثابت شده است،شماره سفارش خرید منحصر به فرد را نشان می دهد، وبخش دوم نشان دهنده شماره بخش پرداخت،x از n، جایی که n تعداد قطعات پرداخت است، ۱ ä n □ x (به عنوان مثال ۳ از ۵ نشان دهنده پرداخت سوم چک الکترونیکی از پنجمین چک الکترونیکی است). همچنین مقدار پول M می تواند متفاوت باشد به طوری که هر چک الکترونیکی با آن مشخص می شود:

$Ch_e\_n = (I_D, O_{id\_n1}, m_n, T_n)$, 1□n □z,

ما داریم

۵- منابع

[۱] امنیت در بانکداری اینترنتی، انتشارات: دانشگاه صنعتی خواجه‌نصیرالدین طوسی، مؤلفان:دکتر شهریار محمدی زینب زارع‌حسینی

[۲] زیر ساخت کلید عمومی(PKI):مفاهیم ،کاربردها و کاربری امضای دیجیتال،جعفر محمودی

[۳]سند جامع پروفایلهای زیرساخت کلید عمومی کشور ، مرکز دولتی صدور گواهی الکترونیکی ریشه،بازنگری ۳,۱،قابل دسترس درhttp://www.rca.gov.ir

[۴] سیستمهای پرداخت الکترونیکی در ایران، فرامرز فردی -کارشناس فنی غلامرضا وطنیان عضو هیات علمی دانشگاه آزاد اسلامی، قابل دسترس در ماهنامه داخلی بانک اقتصادنوین، شماره چهلم - خردادماه ۱۳۹۱

[۵] مرکز توسعه تجارت الکترونیکی،آزمایشگاه ارزیابی تجهیزات زیرساخت کلید عمومی،قابل دسترس در http://www.ecommerce.gov.ir

[1]Bank Systems & Technology Available at:http://www.banktech.com/channels/fstc-to-market-e-check-technology.

[2] Chaum D. and van Heyst E., "Group signatures", in Proceding of Advances in Cryptology EUROCRYPT '91, D.W. Davies (Ed.), Springer-Verlag, pp. 257-265

[3]Chaum D., Den Boer B.,van Heyst E., Mjølsnes S., Steenbeek A., "Efficient Offline Electronic Checks, Advances in Cryptology," in Proceeding Eurocrypt '89, LNCS 434, SpringerVerlag, 294-301.

[4] Differences Between E-Checks & Paper Checks Available at: http://smallbusiness.chron.com/differences-between-echecks-paper-checks-39153.html.

[5] Electronic Check Available at: https://www.investopedia.com/terms/e/electroniccheck.asp.

[6] Electronic Check Process Diagram Available at: https://www.authorize.net/resources/echeckdiagram.

[7] Electronic Check Services Using the Simple Order API October 2016 Available at: http://apps.cybersource.com/library/documentation/dev_guides/EChecks_SO_API/Electronic_Checks_SO_API.pdf.

[8] Electronic Commerce and Web Technologies Second International Conference, EC-Web 2001 Munich, Germany, September 4-6, 2001 Proceedings.

[9] Hirose S. and Yoshida S., "A one-way hash function based on a two-dimensional cellular automaton", in the proceeding of The 20th Symposium on Information Theory and Its Applications (SITA97), Matsuyama, Japan, Dec. 1997, Proc. vol. 1, pp. 213-216.

[10] Implementing US Bank's eCheck. Available at https://www.sbctc.edu/resources/documents/colleges-staff/it-support/fms/eCheck-Implement.pdf

[11]iPayX Secure ePayment solutions Available at: http://www.ipayx.com/tags/echeck.

[12] Low S.H., .Maxemchuk N.F., and Paul S., پ Anonymous Credit Cards,پin th

[13] Merkle R.C., "A fast software one-way hash function," Journal of Cryptology, 3(1):43--58, 1990

[14] Park S.J., Lee I.S., and Won D.H., "A practical group signature," in Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, pages 127--133, Jan. 1995
[15] Shields C. and Levine B.N., "A Protocol for Anonymous Communications Over Internet," in Proceeding of 7th ACM Conference on Computer and Communication Security, November 2000.
[16] The Electronic Check Architecture Milton M. Anderson Available at :http://echeck.org/files/ArchitectualOverview.pdf.
[17] What Is a Lockbox Payment?Learn the benefits of this payment process Available at: https://www.thebalance.com/what-is-a-lockbox-payment-315203.
proceeding of .2nd ACM Conf. Computer and Communication Security, ACM Press, New York, 1994, pp. 108-117