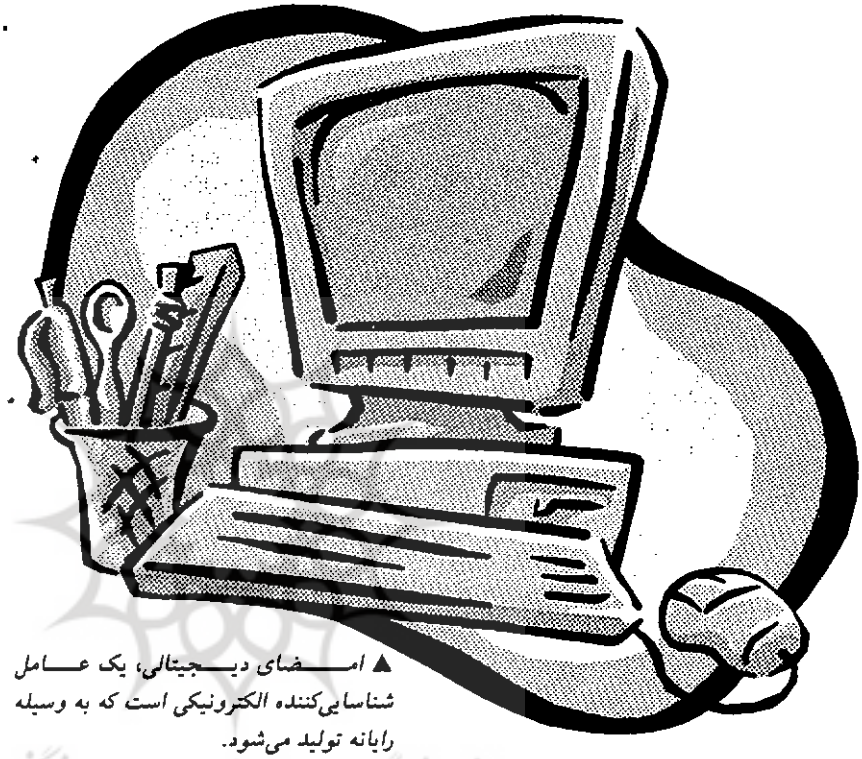
مبانی حقوقی پول الکترونیکی

بخش چهارم

مهندس سید مجید مؤمنی
Email: majidmomeni@ yahoo. com



▲ *امضای دیجیتالی، یک عامل شناسایی‌کننده الکترونیکی است که به وسیله رایانه تولید می‌شود.*

اشاره

در بخش‌های قبلی بیان شد که گسترش تجارت الکترونیکی و پیشرفت فن‌آوری اطلاعات، نیاز به پول جدیدی متناسب با این شرایط، به نام پول الکترونیکی را بوجود آورد، است. در واقع، پول الکترونیکی یک عدد (شامل بیت‌های دیجیتالی) است که بعد از امضای دیجیتالی ناشر آن، با ارزش معینی اعتبار می‌یابد و قابلیت انتشار و مبادله سریع را در شبکه رایانه‌ای دارا می‌باشد. البته با اینکه پول الکترونیکی دوران تکوین خود را می‌گذراند، ولی این نوع پول ادعای جایگزینی اسکناس و مسکوک را دارد. بنابراین، برای این نوع پول خصوصیاتی تعریف شده است. در شماره‌های قبلی، بعضی از معیارهای یک پول الکترونیکی خوب بیان شد؛ امنیت، گمنام بودن کاربر، قابلیت کاربری آسان، حمل آسان، استفاده مستمر، دایمی بودن و قابلیت اطمینان از مهمترین خصوصیات یک پول الکترونیکی خوب می‌باشند که قبلاً تشریح شده‌اند. همچنین، در بخش قبل، با انجام مقایسه‌ای بین سیستم‌های پولی مختلف مانند پول نقد، چک‌های بانکی، کارت‌های اعتباری و پول الکترونیکی به مزایا و معایب هر یک اشاره شد. در ضمن، با توجه به اینکه امنیت پول الکترونیکی از مهمترین خصوصیات آن می‌باشد، معیارهای مورد نیاز امنیتی آن، و روش ایجاد امنیت به وسیله رمزنگاری ذکر شده است.

بدیهی است که با توجه به جدید بودن بحث پول الکترونیکی، ممکن است سوالات متعددی در ذهن خوانندگان محترم بوجود آید. هدف نگارنده آن است که در موضوعاتی که در آینده مطرح می‌شود، به این سوالات و ابهامات پاسخ دهد. لذا از خوانندگان گرامی تقاضا دارد که سوالات و یا نظریات اصلاحی خود را با دفتر مجله و یا پست الکترونیکی فوق مطرح کنند تا در بخش پرسش و پاسخ این سلسله مقالات تشریح شوند.

و اینک ادامه بحث را با جنبه‌های حقوقی پول الکترونیکی پی می‌گیریم.

تاکنون در مبادلات تجاری، به غیر از کالاهایی که مبادله می‌شوند، حجم زیادی از کاغذ برای ثبت اطلاعات تجاری و تضمین شرایط آن، استفاده و رد و بدل می‌شود. در یک معامله تجاری معمولی، طرفین پس از پذیرش شرایط مورد نظر خود، اسنادی را به وسیله امضای دستی تأیید نموده و نگهداری می‌کنند. این اسناد از نظر حقوقی قابل استفاده بوده و متضمن حفظ حقوق طرفین می‌باشند.

یک قرارداد تجاری شامل حداقل اجزای زیر است: ۱- نام، مشخصات و نشانی طرفین قرارداد، ۲- موضوع قرارداد و حدود خدمات، ۳- مدت قرارداد، ۴- مبلغ و نحوهٔ پرداخت. معمولاً در این قسمت از قراردادها نوع و واحد پول مورد نظر برای پرداخت نیز (ریال، دلار،...) مشخص می‌شود، ۵- تعهدات فروشنده، ۶- تعهدات خریدار، ۷- نحوهٔ پرداخت مالیات‌ها، بیمه، عوارض متداول در مورد معامله، ۸- تأخیر در انجام تعهدات و جرایم مربوط به آن، ۹- نحوهٔ حل اختلاف، در این بخش در صورتی که اختلاف در تعبیر و تفسیر و یا اجرای مفاد قرارداد بوجود آید و از طریق مذاکره طرفین حل و فصل نشود، داور مورد نظر تعیین می‌شود، و در صورتی که اختلاف از طریق داوری حل نشود، مرجع قضایی و قوانین و مقررات کشور مورد نظر برای اقامه دعوا تعریف می‌شود. در پایان قرارداد هم طرفین با امضای صفحات آن، اجزای آن را تأیید نموده و مسوولیت‌های خود را متعهد می‌شوند. سازمان ثبت اسناد و دفاتر ثبت اسناد رسمی هم برای تأیید مندرجات سندها بوجود آمده‌اند. لذا طرفین معامله نمی‌توانند در صحت اسناد مزبور تردید کنند.

در استفاده از پول الکترونیکی نیز روابط بین بانک ناشر و کاربر پول الکترونیکی و همچنین مشتری و بازرگان توسط قراردادهایی تعریف می‌شود. تفاوت این قراردادها با قراردادهای معمولی آن است که به صورت الکترونیکی تولید می‌شوند و داده‌های مربوطه از راه دور امضا و مبادله و در فایل‌های رایانه‌ای ذخیره خواهند شد. لذا در محتویات قراردادها چندان تفاوتی با قراردادهای مرسوم وجود ندارد. مهمترین بخش این نوع قراردادهای الکترونیکی، امضای دیجیتالی آن، بررسی صحت امضا و ارسال امن آنها در شبکه می‌باشد.

هنگامی که فردی مشتری یک بانک برای استفاده از پول الکترونیکی می‌شود، قراردادی را به صورت الکترونیکی امضا می‌کند. واضح است که برای استفاده از پول الکترونیکی باید از وسایل و امکانات مخابراتی واسطه استفاده کرد. این امکانات تحت کنترل سیستم‌های مالی نیستند، در ضمن، طرفین

معامله یکدیگر را نمی‌بینند. لذا در قرارداد فیمابین مسایل مهم زیر لحاظ می‌شوند:[۱]

- حفظ اطلاعات شخصی (Privacy): واضح است که اطلاعات شخصی افراد باید از دستبرد و استراق سمع محفوظ باشد. به عنوان مثال، رمز مربوط به شمارهٔ حساب، پول الکترونیکی شخص، مشخصات فردی معامله، اطلاعات مورد معامله و غیره که روی اینترنت ارسال می‌شوند، نباید در اختیار فرد دیگری قرار گیرند. لذا طرفین معامله در قرارداد متعهد به حفظ اسرار شخصی می‌شوند.

- شناسایی طرفین (User Identification): واضح است که در تجارت الکترونیکی، کاربر باید بداند که با چه کسی وارد معامله شده است. لذا طبیعی است که کاربران شبکه و طرفین معامله باید درست شناسایی شوند و قبل از مبادله پول الکترونیکی، باید از عدم جعل هویت طرف مقابل اطمینان حاصل کنند.

- انسجام اطلاعات (Message Integrity): اطلاعات ارسالی بین دو نفر که می‌تواند یک قرارداد الکترونیکی، و یا پول الکترونیکی باشد، باید انسجام اولیه خود را حفظ کند و از مداخله و یا تعرض در بین راه محفوظ باشد. در واقع، یک کاربر، هنگامی که اطلاعاتی را دریافت می‌دارد، باید مطمئن باشد که آنها همان اطلاعاتی هستند که فرستاده شده‌اند. انسجام اطلاعات به وسیله روش‌های امنیتی رمزنگاری و ارسال در شبکه حاصل می‌شود.

- عدم انکار (Non Repudiation): طرفین معامله، وقتی که یک قرارداد و یا مبادله‌ای را بین هم دارند، نباید قادر باشند که قرارداد، پرداخت الکترونیکی و یا اطلاعات دیجیتالی دریافتی را تکذیب کنند. این امر برای انجام تجارت الکترونیکی ضرورت است.

در دنیای مبادلات الکترونیکی، شناسایی طرفین معامله و عدم انکار تعهدات پذیرفته شده توسط امضای دیجیتالی به راحتی انجام می‌شود. لذا در اینگونه معاملات هم شبیه قراردادهای معمولی، قراردادی به صورت متن دیجیتالی تهیه می‌شود و در آن قرارداد مواردی چون موضوع و هدف قرارداد، تعاریف، حوزهٔ فعالیت، استانداردهای تبادل، ایمنی و گواهینامه‌ها، نحوهٔ ارسال و دریافت پیام‌ها، نحوهٔ تشخیص هویت طرف‌های تجاری، نحوهٔ نگهداری اطلاعات و سوابق و ذخیره‌سازی داده‌ها و دیگر تعهدات و قوانین حل اختلاف را مشخص می‌کنند. و در پایان مراتب را به وسیله امضای دیجیتالی تأیید می‌نمایند.

برای جلوگیری از انکار امضاهای دیجیتالی و ثبت امضاها نیز سازمان‌هایی به نام سازمان گواهینامه (Certificate Authorithy) بوجود آمده‌اند. این سازمان‌ها برای افراد گواهینامه دیجیتالی صادر می‌کنند. در این گواهینامه‌ها، هویت فرد معرفی می‌شود و یک جفت کلید عمومی و خصوصی جهت امضای دیجیتالی برای او صادر خواهد شد. این سازمان‌ها کلید خصوصی فرد را منحصراً به او می‌دهند و یک گواهینامه دیجیتالی شامل ۱- اسم و مشخصات فرد، ۲- کلید عمومی فرد، ۳- امضای دیجیتالی سازمان صادرکننده گواهینامه را تولید و در شبکه منتشر می‌کنند. تعداد این سازمان‌های صدور گواهینامه می‌تواند متعدد باشد. به عنوان مثال، آمازون (Amazone) یکی از این سازمان‌ها است، ولی هویت این سازمان‌ها توسط یک مؤسسه قانونی تأیید می‌شود.[۲]

امضای دیجیتالی

یک امضای دیجیتالی به هر نوع عامل

○ مهمترین بخش قراردادهای الکترونیکی، همانا امضای دیجیتالی، بررسی صحت امضاها و ارسال امن آنها در شبکه می‌باشد.

شناسایی کننده الکترونیکی گفته می‌شود که به وسیله رایانه تولید می‌شود و قدرت و تأثیر آن همانند امضای دستی برای گروه استفاده کننده می‌باشد، و برای تأیید یک سند الکترونیکی مانند یک نامه، قرارداد، فرم مالیاتی، تصویر، نقشه و حتی یک وصیت‌نامه که قابل ذخیره در کامپیوتر باشد، بکار می‌رود. در بعضی از کشورها مانند ایالات متحده، اتحادیه اروپا و هند قوانین مربوط به رسمیت یافتن امضای دیجیتالی تصویب شده است و طبق قانون یک امضای دیجیتالی با خصوصیات زیر دارای تأثیر امضای دستی می‌باشد:[۳]

- برای هر فرد یکتاست.
- قابلیت تصدیق و تأیید دارد.
- تنها در کنترل اختصاصی فرد استفاده کننده است.
- امضای دیجیتالی به صورتی به داده‌ها الصاق می‌شود که اگر داده‌ها تغییر کند، امضای دیجیتالی هم غیر معتبر می‌شود.

امضای دیجیتالی توسط نرم‌افزارهای واسطه‌ای انجام می‌شود و اطلاعات قابل مشاهده در یک امضا، نام فرد و شمارهٔ سریال تصدیق او و نام صادرکنندهٔ حق امضا برای او می‌باشند. فن‌آوری امضای دیجیتال امکان انجام عملیات قانونی و تعهدآور را بدون استفاده از کاغذ و در فواصل دور بوجود آورده است. در ضمن، چون در امضای دیجیتالی از روش‌های رمزگذاری استفاده می‌شود، جعل و تقلب در آن به مراتب از امضای دستی مشکل‌تر است.

انواع فن‌آوری امضای دیجیتالی

در این بخش به اختصار به معرفی چند روش ایجاد امضای دیجیتالی می‌پردازیم:[۴]

الف- Bitmaps: در این روش، امضای دستی توسط دستگاه‌های اسکنرو یا دیجیتایزر، اسکن شده و به اسناد دیجیتالی الصاق می‌شود. امنیت این روش پایین است و تغییر اسناد بدون تغییر امضا به راحتی انجام می‌شود. اشکال دیگر این روش آن است که برای اسناد بزرگ، حجم زیادی از حافظه را اشغال می‌کند و سرعت انتقال را کاهش می‌دهد.

ب- Biometric Signature Verification: این سیستم، سرعت و زاویه حرکت و دیگر مشخصات یک امضای دستی را که روی یک دستگاه دیجیتایزر انجام می‌شود، به عنوان نمونه امضا در یک بانک اطلاعاتی نگهداری می‌کند. برای تصدیق امضا به روش مشابه، امضای دستی فرد اخذ و با اطلاعات قبلی امضا مقایسه می‌شود. اشکالات این سیستم، نیاز به هزینهٔ زیاد اولیه برای تجهیزات، بانک‌های اطلاعاتی حجیم و پرهزینه و در ضمن، امکان تغییر اسناد، حتی بعد از امضا می‌باشد.

پ- امضای کلید عمومی (Public Key Infrastructure): این روش رمزنگاری با کلیدهای عمومی و خصوصی است. در این روش نیز یک جفت کلید عمومی و خصوصی برای فرد صادر می‌شود. وقتی که او سندی را با کلید خصوصی خود امضا می‌کند، طرف مقابل با استفاده از کلید عمومی امضا کننده که در شبکه انتشار یافته است، می‌تواند صحت امضا را تصدیق کند.

دارنده کلید خصوصی باید از آن به طور کامل حفاظت کند. بدین منظور، کلید خصوصی در هنگام ذخیره در کامپیوتر توسط نرم‌افزارهایی به رمز در می‌آید. اگر کلید خصوصی یک فرد آشکار شود. در این صورت، امضای صاحب آن ارزشی نداشته و باید گواهینامه امضای دیجیتالی خود را باطل کند و دوباره گواهینامه دیگری را اخذ نماید.

فرض کنید که فردی بخواهد پیام M را با کلید خصوصی خود امضا کند. بدین منظور، توابعی را به نام Ssk برای امضا با استفاده از کلید خصوصی و Vpk برای آشکار کردن امضا با استفاده از کلید عمومی تعریف می‌کند. خاصیت مهم این توابع، یک طرفه (غیرمعکوس‌پذیر) بودن آنها است تا نتوان با انجام عملیات معکوس به کلید خصوصی فرد امضا کننده دسترسی پیدا کرد.

بنابراین، با اعمال تابع Ssk روی پیام M، سند یا پیام به صورت ناخوانا و به نام "M در می‌آید.

$M"=Ssk(M)$

طرف مقابل هم با استفاده از تابع Vpk و اعمال آن روی "M، اصل سند امضا شده را دریافت نموده و امضا آن را تصدیق می‌کند.

$Vpk(M")= Vpk(Ssk(M)=M$

مزیت امضا با کلید عمومی نسبت به دو روش "الف" و "ب" آن است که تصدیق امضا بلافاصله انجام می‌شود، در حالی که این فرآیند در آن دو روش طولانی‌تر است. همچنین، روش اخیر از قابلیت‌های نرم‌افزاری استفاده کرده و دارای درجه اطمینان بالاتری می‌باشد و هزینه آن نسبت به روش‌های قبلی نیز به دلیل عدم استفاده از سخت‌افزار اضافی، کمتر است. در ضمن، این روش به علت وجود یک سازمان واسطه به نام صادرکننده امضای دیجیتالی، طرفین را به طور قانونی از تکذیب احتمالی منع می‌کند.

لازم به تذکر است که کلیدها، یک سری بیت‌های ۰ و یا ۱ پشت سر هم می‌باشند که مجموعاً یک عدد N بیتی را تولید می‌کنند. یک راه کشف کلیدها آن است که عدد مورد نظر را از صفر امتحان کرده و با افزایش یکی یکی آن به کلید مورد نظر رسید. اگر یک عدد دارای n بیت باشد، 2^n حالت مختلف برای امتحان کردن بوجود می‌آید. طبیعی است که هر چه تعداد بیت‌ها بیشتر باشد، تولید حالت‌های مختلف مذکور و رسیدن به کلید، مدت زمان بیشتری طول می‌کشد.

به عنوان مثال، با یک سرمایه‌گذاری یک میلیون دلاری در سخت‌افزار و کامپیوتر، ما می‌توانیم تعداد حالت‌های مختلف یک عدد ۴۰ بیتی (2^{40} حالت مختلف) را در یک ثانیه تولید کنیم. اما هرچه تعداد بیت‌ها بیشتر شود، زمان بیشتری طول می‌کشد. جدول زیر زمان‌های مورد نیاز برای تولید و کشف کلید را با توجه به تعداد بیت‌ها بیان می‌کند.[۴] (در ضمن، منظور از کلیدهای متقارن و غیر متقارن در بخش دوم مقاله با عنوان رمزگذاری متقارن و غیرمتقارن تشریح شده‌اند.)

زمان‌شکستن کلید	تعدادبیت‌های کلیدمتقارن	تعدادبیت‌های کلیدغیرمتقارن
ثانیه	۴۰	۲۷۴
ساعت‌ها	۵۶	۳۸۴
روزها	۶۴	۵۱۲
قرن‌ها	۸۰	۷۶۸
هزاران‌سال	۱۲۸	۲۳۰۸

ت- امضای چشم بسته (Blind Signature): امضای چشم بسته توسط دیوید چام (DavidChaum) از پیشگامان طراحی پول الکترونیکی، به منظور ایجاد گمنامی برای استفاده کنندهٔ پول الکترونیکی ابداع شده است.[۵]

○ کاربران شبکه و طرفین معامله باید قبل از مبادله پول الکترونیکی، از عدم جعل هویت طرف مقابل اطمینان حاصل کنند.

○ قوانین مربوط به رسمیت یافتن امضای دیجیتالی در کشورهایی مانند ایالات متحده، اتحادیه اروپا و هند به تصویب رسیده است.

فرض کنید که فردی از بانک می‌خواهد تا یک پیام M را امضا نماید، بدون آنکه بانک از محتویات آن چیزی بداند. بنابراین، مراحل زیر انجام می‌شود:

۱- فرد پیام M را در یک عدد تصادفی R ضرب (یا ترکیب) می‌کند. حاصل این عمل تولید پیام "M و به صورت ناخوانا می‌باشد.

۲- فرد پیام ناخوانا شدهٔ "M را امضا کرده و حاصل یک عدد مانند S می‌شود که برای فرد بازگردانده می‌شود.

۳- فرد پیام S را بر عدد R تقسیم (عکس ترکیب اولیه) می‌کند، و پیام اولیه M را به صورت امضا شده دریافت می‌دارد.

این تکنیک، شبیه گذاشتن یک کاغذ کاربن‌دار حامل پیام، در یک پاکت است. وقتی که روی پاکت امضا شود، امضا از طریق کاربن به پیام منتقل می‌شود، بدون آن که از محتویات پیام اطلاعی در دست باشد. ■

مراجع

1) Stalder,F." Electronic Money: Preparing the Stage" http:// www. fis. utoronto. ca/ N Stalder/ html/ excash2

۲) سمسارزاده ،غ/ امنیت اطلاعات در شبکه اینترنت/ صندوق بین‌المللی پول/ ۱۳ دسامبر سال ۲۰۰۰

3) EDC" Digital Sigature FAQ" http:// www. sss.org/ ecos/ archived20 pages/ p2000ds. htm

4) Pam,R." Electronic/ Digital Signature Position Paper" , July 1997 httP:// www. State. tn. us/ Finance/ oir/ prd/ ed signat. html

5) Chaum,D." Blind Signature for Untraceable Payments, advances in cryptology." http:// www. inf. usc. br/ custodiot/ papers/ network- security. paper21.pdf