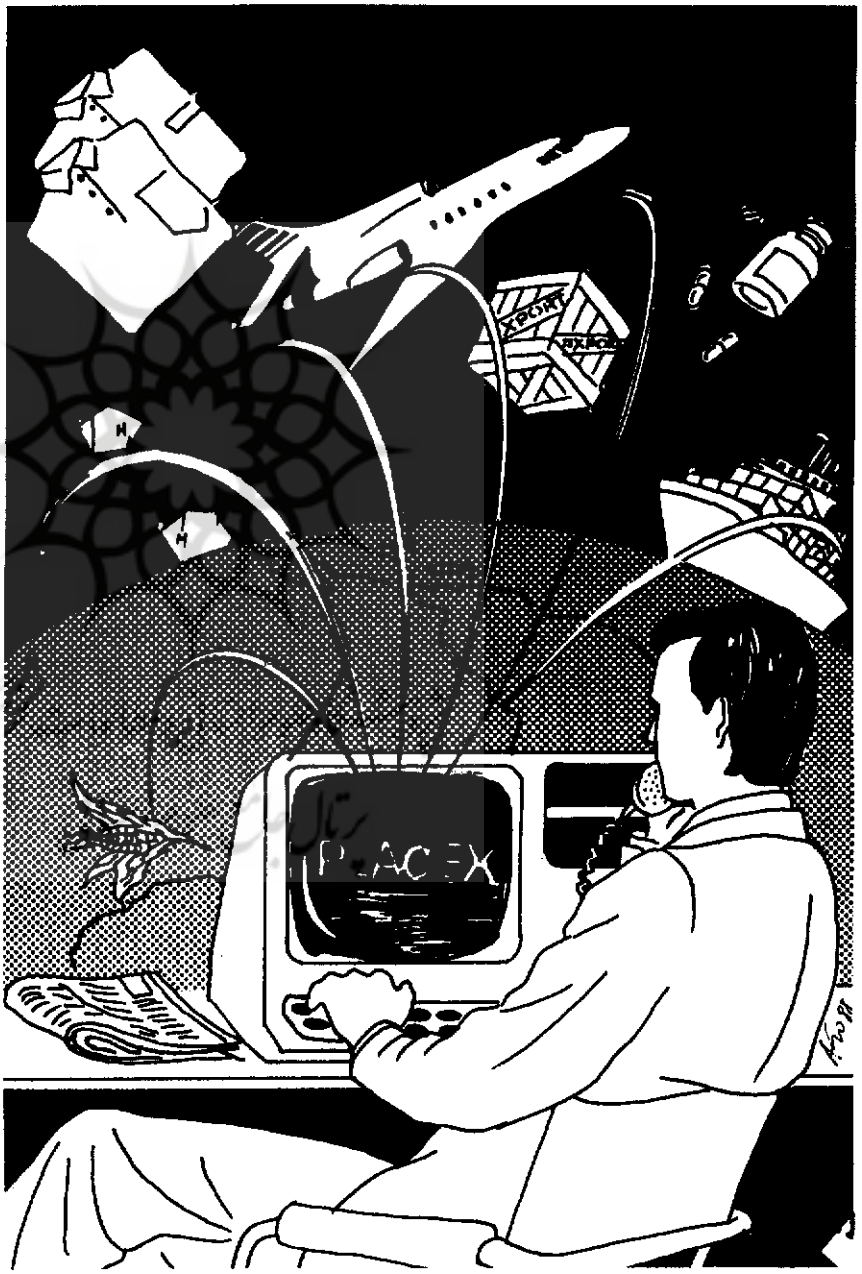
پول الکترونیکی

بخش سوم

مهندس سید مجید مؤمنی

Email: magidmomeni@Yahoo. com



▲ یکی از مزایای پول الکترونیکی، قابلیت انتقال روی شبکه‌های کامپیوتری و خطوط انتقال است.

اشاره

در شماره‌های قبل گفتیم که گسترش فن‌آوری اطلاعات موجب ایجاد موج جدیدی از تغییر در تمام امور جوامع شده و تحولات اساسی رادر جهان آتی رقم خواهد زد. یکی از این تحولات مهم، تغییر تجارت از حالت سنتی به حالت الکترونیکی می‌باشد. در نتیجه، داد و ستدها از طریق رایانه‌های شخصی و حتی در فواصل دور بدون مراجعه به فروشگاه و یا بانک صورت می‌پذیرد.

در تجارت الکترونیکی، به ابزارهای خاص برای پرداخت مالی نیاز می‌باشد. لذا روش‌های جدیدی به نام پرداخت الکترونیکی بوجود آمده است. هدف این روش‌ها، پرداخت وجوه معامله به صورت امن، سریع و بدون حضور فیزیکی طرفین معامله در مؤسسات مالی مانند بانک می‌باشد. مرسوم‌ترین نوع پرداخت‌های الکترونیکی، استفاده از کارت‌های اعتباری است.

همچنین، اشاره شد که پول جدیدی به نام پول الکترونیکی در حال تکوین است. این نوع پول، در واقع، مجموعه شماره‌ها و یا اعدادی است که با امضای دیجیتالی ناشر آن، به عنوان پول به رسمیت شناخته می‌شود.

اسکناس‌های فعلی، شامل یک شماره و امضای ناشر آن بر روی یک برگ کاغذ می‌باشند و ناشر آن هم پرداخت وجه آنها راتضمین کرده است. در پول الکترونیکی محمل فیزیکی این شماره و امضا، تغییر کرده و به جای ثبت روی کاغذ، روی رایانه ثبت می‌شود.

بعضی افراد ممکن است با شنیدن عبارت «پول الکترونیکی» آن را همان کارت‌های بانکی فرض کنند. باید یادآوری کرد که پول الکترونیکی با کارت‌های بانکی تفاوت داشته و در واقع، نسل جدیدی از پول است که ادعای جایگزینی نسل‌های قبلی پول را دارد. در اینجا لازم است برای روشنتر شدن موضوع مقایسه‌ای را بین انواع سیستم‌های پولی موجود انجام دهیم.

مقایسه

سیستم‌های پولی مختلف، پول نقد، چک‌های بانکی، کارت‌های اعتباری و پول الکترونیک را می‌توان از سیستم‌های پولی عصر حاضر دانست و مقایسه بین آنها را می‌توان از طریق تشریح مزایا و معایب هر یک انجام داد که اینک به برخی از آنها اشاره می‌شود:[1]

پول نقد

الف-مزایا:

۱- در استفاده از پول نقد، نیازی به سخت‌افزار و یا وسیله‌ای خاص نمی‌باشد.
۲- پرداخت واقعی خیلی آسان است.
۳- جعل و تقلب در آن آسانتر کشف می‌شود.
۴- ریسک‌های سیستماتیک کمتری دارد.
۵- اطلاعات شخصی طرفین داد و ستد در جایی ثبت نمی‌شود.
۶- پول نقد برای تمام افراد جامعه در تمام محل‌های یک کشور پذیرفته شده است و در دسترس و قابل استفاده می‌باشد.
۷- این نوع پول برای اندوختن و جمع‌آوری مناسب است.

ب-معایب:

۱- پول نقد ممکن است گم و یا دزدیده شود.
۲- حمل پول نقد مشکل و هزینه دارد.
۳- تبدیل آن به پول‌های رایج دیگر کشورها (ارزها) ممکن است با دشواری‌هایی همراه باشد.
۴- با توجه به پیشرفت روزافزون صنایع چاپ، تقلب در اسکناس راحتتر انجام می‌شود.
۵- در معاملات غیرقانونی از پول نقد بیشتر استفاده می‌شود و در نتیجه، کمتر قابل ردیابی است.
۶- به علت شرایط نامناسب نگهداری اسکناس و مسکوک و گردش آن در جامعه، ممکن است آنها کثیف شوند و از نظر بهداشتی هم بیماری‌هایی را منتقل کنند.

چک‌های بانکی

الف-مزایا:

۱- برای انجام معامله نیازی به حمل پول نمی‌باشد.
۲- پرداخت به وسیله چک‌های بانکی می‌تواند به تعویق افتد.
۳- امنیت بیشتری را در داد و ستد فراهم می‌کند.

ب-معایب:

۱- گمنامی و حفظ اطلاعات شخصی در چک‌های بانکی وجود ندارد، چراکه وصول‌کننده چک باید اطلاعات شخصی خود را ثبت کند.
۲- پرداخت به وسیله چک‌های بانکی با هزینه‌های نقدی و یا غیرنقدی مانند صرف وقت همراه است.
۳- برای پرداخت‌های کوچک، استفاده از چک هزینه بیشتری داشته و به صرفه نیست.

کارت‌های اعتباری

مزایا:

۱- سهولت در هنگام استفاده.

○ یک جنبه مهم از آسیب‌پذیری محصولات پول الکترونیکی آنست که آنها برای کاربردهای فروش گسترده طراحی شده‌اند.

۲- امکان استفاده بین‌المللی.
۳- امکان توزیع به طور گسترده در جامعه.
۴- به تعویق انداختن پرداخت.

معایب:

۱- وجود خطرات امنیتی برای مشتریان - صادرکننده و یا بازرگان.
۲- پرداخت با هزینه‌ای همراه است و در نتیجه، برای پرداخت‌های ریز، گران تمام می‌شود.
۳- فقط امکان خرید از فروشنده‌هایی وجود دارد که در مؤسسه‌های اعتباری (که مشتری کارت‌های آنها را دارد) ثبت نام کرده باشند.
۴- تجهیزات مورد استفاده گران بوده و هزینه راه‌اندازی اولیه این سیستم زیاد است.

○ در سال ۱۹۹۹ سهم پرداخت‌های نقدی در میان انواع روش‌های پرداخت همزمان به صفر رسیده است.

پول الکترونیکی

مزایا:

۱- امکان خرید از فواصل دور و پرداخت‌های بدون حضور فیزیکی.
۲- قابلیت انتقال روی شبکه‌های کامپیوتری و خطوط انتقال، مانند تلفن.
۳- امکان ذخیره در رایانه‌های شخصی و کارت‌های هوشمند.
۴- قابلیت بار کردن از شبکه‌های باز، مانند اینترنت.
۵- حمل ارزان به تمام نقاط دنیا.
۶- در تبدیل آنها به ارزهای مختلف مشکلی وجود ندارد.
۷- در مقایسه با اسکناس و مسکوک تمیزتر و بهداشتی‌تر است.
۸- قابلیت برنامه‌ریزی در شرایط مختلف، از جمله پرداخت‌های ریز و واحدهای پولی غیرمرسوم.

ب:معایب:

۱- استفاده از پول الکترونیکی نیاز به سخت‌افزار دارد.
۲- کاربران پول الکترونیکی نیاز به آموزش دارند و در نتیجه، تمام اقشار جامعه به سهولت نمی‌توانند از آن استفاده کنند.
۳- کشف تقلب از سوی کاربران مشکل است.
۴- ایجاد امنیت در این سیستم‌گران تمام شده و با اصل گمنام بودن فرد تقابل دارد.
۵- پول الکترونیکی برای جمع‌آوری و نگهداری، در شرایط حاضر، مناسب نیست.
۶- حجم کم و سرعت انتقال زیاد پول الکترونیکی برای استفاده در معاملات نامشروع به عنوان یک مزیت محسوب می‌شود.

مقایسه آماری

همانطور که اشاره شد، تجارت الکترونیکی موجب تغییر شکل پول شده است. تاکنون آمارهای مختلفی راجع به حجم این نوع تجارت در مراجع مختلف دیده می‌شود. به عنوان مثال، طبق گزارش خزانه‌داری کل انگلیس، کل تجارت الکترونیکی به وسیله کارت‌های اعتباری و پول‌های الکترونیکی ودیجیتالی که در سال ۱۹۹۸ انجام شده، بالغ بر ۸۰ میلیارد دلار بوده است و پیش‌بینی می‌شود که این رقم تا سال ۲۰۰۳ به ۳۲۰۰ میلیارد دلار برسد.[۲] کشورهای اروپایی نیز برنامه‌ریزی کرده‌اند که از سال ۱۹۹۸ تا ۲۰۰۴ با رشد سالانه ۱۴۰ درصد سهم خود را در تجارت الکترونیکی تا مبلغ ۱۶۰۰ میلیارد دلار، یعنی در سطح ۶/۳ درصد از کل تجارت در جهان برسانند.[۳]

جدول شماره یک

سهم انواع پرداخت‌های همزمان در کشورهای اروپایی در سال ۱۹۹۹

کشور	اعتبار انتقال‌بدهی	کارت اعتباری	چک	پول الکترونیکی	نقدی	سایر
معاملات داخلی						
آلمان	۳۳/۶	۲۲/۴			۴۲/۱	۱/۸
بلژیک	۵/۶	۷۷/۸			۱۶/۷	
فرانسه		۷۴/۳	۲۰/۰	۵/۷		
انگلیس		۱۰۰/۰				
اسپانیا		۸۵/۸			۱۱/۴	۲/۹
هلند	۵۰/۰	۸/۳			۳۳/۳	۸/۳
سوئد	۴۰/۰	۲۰/۰			۴۰/۰	
ایتالیا		۱۰۰/۰				
پرتقال		۵۵/۰			۴۰/۰	
معاملات خارجی						
کلیه کشورها	۴/۳	۹۲/۷	۲/۲			۰/۷

Source: Stiftung Warentest (1999)

جدول شماره یک، وضعیت مقایسه‌ای انواع پرداخت‌های همزمان (Online) در کشورهای اروپایی را در سال ۱۹۹۹ نشان می‌دهد. در اینجا سهم هر یک از سیستم‌های پولی به صورت درصد بیان شده است.

همانطور که در جدول شماره یک دیده می‌شود، پرداخت‌های نقدی کمتر از ۴۰ درصد این پرداخت‌ها را شامل می‌شود و حتی در کشورهای فرانسه، انگلیس و ایتالیا سهم پول نقد به صفر رسیده است. در ضمن، کارت‌های اعتباری بیشترین سهم را در پرداخت‌های مربوط به خریدهای همزمان به عهده دارند و سهم آنها در ایتالیا و انگلیس حتی به صددرصد می‌رسد. در ضمن، در فرانسه علاوه بر سهم ۷۴/۳ درصدی کارت‌های اعتباری، پول الکترونیکی ۵/۷ درصد از این پرداخت‌ها را به خود اختصاص داده است.

***

در بخش‌های قبلی گفته شد که برای آنکه پول الکترونیکی بتواند جایگزین پول نقد شود، باید دارای معیارها و خصوصیاتی باشد. یکی از این خصوصیات امنیت آن است.

خطرات امنیتی پول الکترونیکی

هدف از ایجاد سیستم‌های پرداخت الکترونیکی بر روی شبکه‌های عمومی مانند اینترنت، انجام پرداخت‌های الکترونیکی برای کسب کالاهای الکترونیکی، یا گرفتن تعهد برای تحویل کالاهای فیزیکی می‌باشد.

اینترنت رسماً یک شبکه باز (Open Net work) است و در پروتکل ارتباطی آن که مبتنی بر Transmission Control & Internet Protocol (TCP/IP) است، امنیت طراحی نشده است. بنابراین، هر فردی با کمک نرم افزارهای سوء استفاده کنندهٔ موجود، می‌تواند با مشاهدهٔ ترافیک خط، محتویات آن را بخواند.

لذا طبیعی است که نگرانی‌های زیادی در ارتباط با ارسال داده‌های مالی از قبیل شماره کارت اعتباری، شمارهٔ حساب و اطلاعات شخصی بر روی اینترنت وجود داشته باشد. بنابراین، باید برای ارسال امن اطلاعات روش مناسبی اتخاذ شود.

در ارتباط با سیستم‌های پول الکترونیکی، خطراتی وجود دارد که در زیر ضمن اشاره به آنها، معیارهای پیشگیری از آنها نیز بیان می‌شود[۴]

خطرات تقلب

محتمل‌ترین انگیزه برای تقلب‌های مالی، درآمد مالی است. سیستم‌های پول الکترونیکی نیز از این قاعده مستثنا نیستند و این امر می‌تواند با تولید نشانه‌های تقلبی پول الکترونیکی، با اطلاعات یا دستگاه‌های به سرقت رفته از ناشر پول صورت پذیرد. البته ممکن است حمله به یک سیستم پول الکترونیکی، انگیزه‌ای برای درآمد مالی نداشته باشد و بلکه هدف تنها درهم‌شکستن یک سیستم خاص باشد.

یک جنبه مهم از آسیب‌پذیری محصولات پولی الکترونیکی آن است که آنها برای کاربردهای خرده فروشی گسترده طراحی شده‌اند، لذا برای یک حمله کننده، جمع‌آوری اطلاعات و تجزیه و تحلیل ارتباطات و کشف ساختار محصول بعید نیست.

بنابراین، بعضی از تهدیدات عبارتند از:

الف - تکثیر دستگاه‌ها: در سیستم‌های پول الکترونیکی مبتنی بر کارت، روش حمله، می‌تواند خلق دستگاه جدیدی باشد که به وسیله دستگاه‌های دیگر به درستی پذیرفته شود. این دستگاه‌ها می‌توانند یک دستگاه خود پرداز غیر مجاز باشند که اطلاعات کارت مشتری را کشف کنند، یا یک کارت که می‌تواند همانند کارت‌های معتبر کار کند، ولی مبلغ حساب را بیشتر از مقدار واقعی نشان دهد. البته کپی یا تقلب در کارت‌های هوشمند با داشتن تراشه‌های هوشمند پیشرفته به مراتب کمتر خواهد بود.

ب - تغییر یا تکثیر اطلاعات نرم‌افزاری: ممکن است با نفوذ در نرم‌افزارهای یک سیستم یا حتی در یک کارت هوشمند، الگوریتم برنامه‌ها را طوری تغییر داد که ظاهر برنامه از نظر روش‌های حسابداری درست نشان داده شود، ولی در واقع، کلاهبرداری انجام شود.

پ - تغییر پیام‌ها: تلاش یک حمله کننده به سیستم پول الکترونیکی می‌تواند برای گرفتن پیام یا اطلاعات یک دستگاه و جایگزین نمودن آن با یک پیام تغییر یافته (مثلاً جایگزین نمودن یک پول با ارزش کمتر) صورت پذیرد، که این کار ممکن است از طریق جایگزین کردن پست الکترونیکی، یا شبیه سازی یک دستگاه خواننده کارت هوشمند انجام شود.

ت - سرقت: یک روش طبیعی برای تقلب، می‌تواند سرقت وسایل بازرگان یا مشتری و مورد استفاده قرار دادن نشانه‌های مالی ثبت‌شده در آن باشد، البته اطلاعات ذخیره شده روی دستگاه‌ها امکان دارد که از طریق کپی‌های غیرمجاز دزدیده شوند، یا مهاجم، یک برنامه نرم‌افزاری غیر مجاز را به کامپیوتر شخصی مصرف کننده وارد کند تا یادداشت‌های الکترونیکی ذخیره شده، یا در حال مخابره را کپی کرده و از آنها برای اجرای معاملات استفاده کند.

البته باید نیروهای انسانی شاغل در سیستم پول الکترونیکی را هم در نظر گرفت. کارمندان تولید کننده یا نشر دهنده‌های پول الکترونیکی می‌توانند دستگاه‌ها را قبل از اینکه فروخته شوند یا به مشتری داده شوند، سرقت نموده و یا می‌توانند کلیدهای رمزنگاری را بدون اخذ مجوز توزیع کنند. یا کارمند بخش تحقیق و توسعه ممکن است با گرفتن رشوه، اسناد محرمانه و طرح محصول را به مهاجمان بیرونی ارایه دهد.

عدم کارکرد صحیح (Malfunction)

محصولات پول الکترونیکی، ممکن است متحمل ضایعات تصادفی یا از دست دادن اطلاعات ذخیره شده روی دستگاه، یا عدم کارکرد صحیح یک نرم‌افزار کاربردی در عملکردهای امنیتی یا محاسباتی و یا ناتوانی در ارسال پیام گردند. این عدم کارکرد درست، ممکن است از اختلالات الکترونیکی یا فیزیکی در دستگاه، یا از قطع یا انحراف ارسال پیام بین دستگاه‌ها ناشی شود. در ضمن، شاید با نقص موجود در یک دستگاه، قبل از اینکه آشکار شود، بتوان یک کلاهبرداری را انجام داد. در نتیجه، عدم کارکرد صحیح تجهیزات سخت‌افزاری و نرم‌افزاری، ممکن است سبب خساراتی به طرفین معامله شود.

معیارهای امنیتی

با توجه به خطرات مذکور در این بخش، طراحان سیستم‌های پول الکترونیکی تلاش کرده‌اند تا بروز هر گونه تهدید و آسیب احتمالی برای این سیستم‌ها را پیشگیری کنند. معیارهای امنیتی بنا نهاده شده برای سیستم‌های پولی الکترونیکی را می‌توان به معیارهای پیشگیری، تشخیص و یا محدود کردن تقلب تقسیم‌بندی کرد.

الف - معیارهای پیشگیری: برای پیشگیری از تقلب، معیارهای مقاومت سخت‌افزاری، رمزگذاری نرم‌افزاری و مجوزهای همزمان (Online Authorization) مطرح شده‌اند.

طبیعی است که دستگاه‌های الکترونیکی مورد استفاده در محصولات پول الکترونیکی، اولین خط دفاعی در مقابل حملات بیرونی را فراهم می‌سازند. بنابر این، ایجاد امنیت در لایه‌های فیزیکی سخت‌افزاری، همیشه مورد توجه بوده است. به عنوان مثال، در سیستم‌های پول الکترونیکی مبتنی بر کارت‌های هوشمند، فرآیندهای امنیتی در داخل تراشه‌های ریزپردازنده‌ها اجرا می‌شود. این تراشه‌ها، در طی مرحله تولید طوری ساخته می‌شوند که با ایجاد موانع فیزیکی، از خواندن الکتریکی یا نوری و یا تغییر فیزیکی محتویات آنها جلوگیری به عمل آید. در ضمن، سیم‌کشی‌ها و ارتباطات داخلی تراشه‌ها در چند لایه انجام می‌شود، به طوری که برداشتن لایه‌های محافظ روی تراشه بدون خرابی آن ممکن نباشد.

نرم‌افزارها نیز شامل مکانیزم‌هایی برای بازداشتن مصرف کننده از تغییر یا کپی اطلاعات بدون اخذ مجوز می‌باشند. یکی از این مکانیزم‌ها رمزگذاری است که مهمترین بخش ایجاد امنیت و جلوگیری از تقلب در همه سیستم‌های پول الکترونیکی است. تکنیک‌های پیچیده و رمزنگاری، حفاظت منطقی سیستم‌های پول الکترونیکی را با ایجاد اطمینان از محرمانه بودن، اعتبار و درستی دستگاه‌ها و اطلاعات و ارتباطات بکار رفته در معاملات، فراهم می‌سازند.

اخذ مجوزهای همزمان، روش دیگری است که برای هر معامله‌ای در محصولات پول الکترونیکی نرم‌افزاری لازم است. در سیستم‌های کارتی، برای اطمینان از اینکه شخص دارنده کارت، فرد مجاز می‌باشد، یک شمارهٔ شناسایی فردی (Personal Identification Number - PIN) از مشتری درخواست می‌شود. در دیگر سیستم‌های پول الکترونیکی نیز در ابتدا فرآیند شناسایی هویت طرفین انجام می‌شود. بنابراین، همیشه بعد از حصول اطمینان از درستی هویت طرفین، تراکنش‌ها صورت می‌پذیرد.

این مدارک شناسایی افراد طوری برنامه‌ریزی شده‌اند که دستیابی تصادفی یا چک کردن تمام حالات ممکن، برای دستیابی به رمز را مانع می‌شوند.

تکنیک‌های رمزنگاری و روش‌های شناسایی هویت افراد در بخش‌های بعدی تشریح خواهند شد.

ب - معیار تشخیص: سیستم‌های پول الکترونیکی طوری طراحی می‌شوند که بعد از انجام یک تقلب، هویت فرد تشخیص داده شود. به عنوان مثال، اگر شخص، از پول الکترونیکی خود کپی گرفته و آن را مجدداً خرج کند، هویت او آشکار می‌شود.

برای تشخیص تقلب، سیستم‌ها طوری طراحی شده‌اند که مشتری و فروشنده با سیستم مرکزی پول، شامل ناشر پول و یا اپراتور مرکزی در ارتباط باشند تا ضمن رعایت حقوق طرفین معامله، با انجام جعل یا تقلب، آن شخص شناسایی شود.

در ضمن، این سیستم‌ها می‌توانند روش‌های خودکار را بکار برند تا با استفاده از روش‌های نمونه‌گیری آماری از جریان پرداخت‌ها، تراکنش‌های حجیم حاکی از جعل را تشخیص داده و تحلیل و بررسی کنند. استفاده از تکنیک‌های هوش مصنوعی و شبکه‌های عصبی در این روش‌ها می‌تواند مؤثر باشد.

پ - معیار محدودیت: ایجاد محدودیت در مبلغ، یا تاریخ انقضا در مصرف محصولات پول الکترونیکی، یکی از مشخصه‌های امنیتی سیستم‌های پول الکترونیکی است. لذا یک دستگاه تغییر یافته فقط در مدت محدودی برای کلاهبرداری مفید می‌باشد. به عنوان مثال، سیستم‌های کارتی دارای محدودیت در مبلغ یا تعداد تراکنش‌ها برای یک دستگاه خاص می‌باشند.

روش دیگر، ایجاد محدودیت در کارکرد دستگاه‌هاست. به عنوان مثال، اگر فردی چندین بار برای ورود به سیستم‌های کارتی یا پول الکترونیکی تلاش کند، اما با شکست مواجه شود، دستگاه‌ها می‌توانند قفل شوند و دزد را ناامید سازند. در ضمن، کنترل کننده مرکزی، شماره سریال دستگاه مظنون را ثبت می‌کند و به اطلاع دیگر پایانه‌ها می‌رساند تا از انجام تراکنش با آن خودداری ورزند. ■

ادامه دارد

مراجع

1) Godschalk, H. Krueger, M./ Why e-money still fails, chances of e-money within a competitive payment instrument markt/ 26 May 2000.

http://www. berlecon. de/ services/ en/iew3/ abstracts/ godschalk. html

2) http:// www.hmtrea sury. gov. uk/ pub/ html/ Jobs/ gas/ gas68. pdf

3) UNCTAD/ Building Confidence, Electroinc Commerce and Development/ United Nations Conference on Trade and Development/ 2000

http:// www. unctad. org/ ecommerce/ building- pdf

4) Security of Electronic Money/ CPSS Publication/ No.18

http:// www. bis. org/ publ/ cpss18. htm