پول الکترونیکی

مهندس سید مجید مؤمنی

اشاره

در شماره قبل گفتیم که اگر بخواهیم نسل جدیدی را به تاریخ پول اضافه کنیم، باید از پول الکترونیکی نام ببریم، و بعد این واقعیت را یادآوری کردیم که پیشرفت فن‌آوری اطلاعات، موجب تغییر شکل داد و ستد شده است، و با گسترش تجارت الکترونیکی، پول نیز به‌عنوان وسیله پرداخت، دوران گذار خود را به سمت پول جدید، یعنی پول الکترونیکی می‌گذراند. محققان نیز در تلاش هستند تا با ایجاد پول الکترونیکی ـ به‌صورتیکه تمام خواص پول اسکناس و مسکوک را دارا باشد ـ علاوه‌بر صرفه‌جویی‌های اقتصادی، مزایای دیگر آن مانند سرعت در معاملات، حجم کم و امکان خرید مستقیم از فواصل دور را هم به مردم عرضه کنند. البته بدیهی است که در این صورت، مفاهیم پول ملی نیز تحت‌الشعاع قرار خواهند گرفت.

کلیات

مجموعهٔ اطلاعاتی که باهم و به‌صورت الکترونیکی ارسال می‌شوند، به‌نام «نشانه‌های الکترونیکی[1]» خوانده می‌شوند. درواقع، یک نشانه الکترونیکی، مجموعه‌ای از بیت‌های مرتبط با هم است که از یک سری رسانه‌های فیزیکی[2] برای ذخیره و انتقال استفاده می‌کند.

پول الکترونیکی، نشانه‌های الکترونیکی،

○ مهمترین تفاوت بین پول نقد الکترونیکی با یک سیستم پرداخت الکترونیکی آن است که گر چه هر دو واسطه مبادله می‌باشند، ولی پول نقد الکترونیکی دیگر وظایف پول، همچون ذخیره ارزش را نیز به‌عهده دارد.

(شماره‌هایی) است که با امضای دیجیتالی ناشر آن، به‌عنوان پول به رسمیت شناخته می‌شود. همانطور که یک اسکناس با شمارهٔ مشخص و امضای بانک تضمین کننده اعتبار آن به رسمیت شناخته می‌شود، پول الکترونیکی نیز دارای یک شماره و یک امضای ناشر می‌باشد، با این تفاوت که محمل فیزیکی آن کاغذ نبوده، بلکه یک شبکه الکترونیکی است.

قبل از اشاره به انواع و نحوهٔ تولید پول الکترونیکی، باید به خصوصیات یک پول الکترونیکی خوب اشاره داشت.

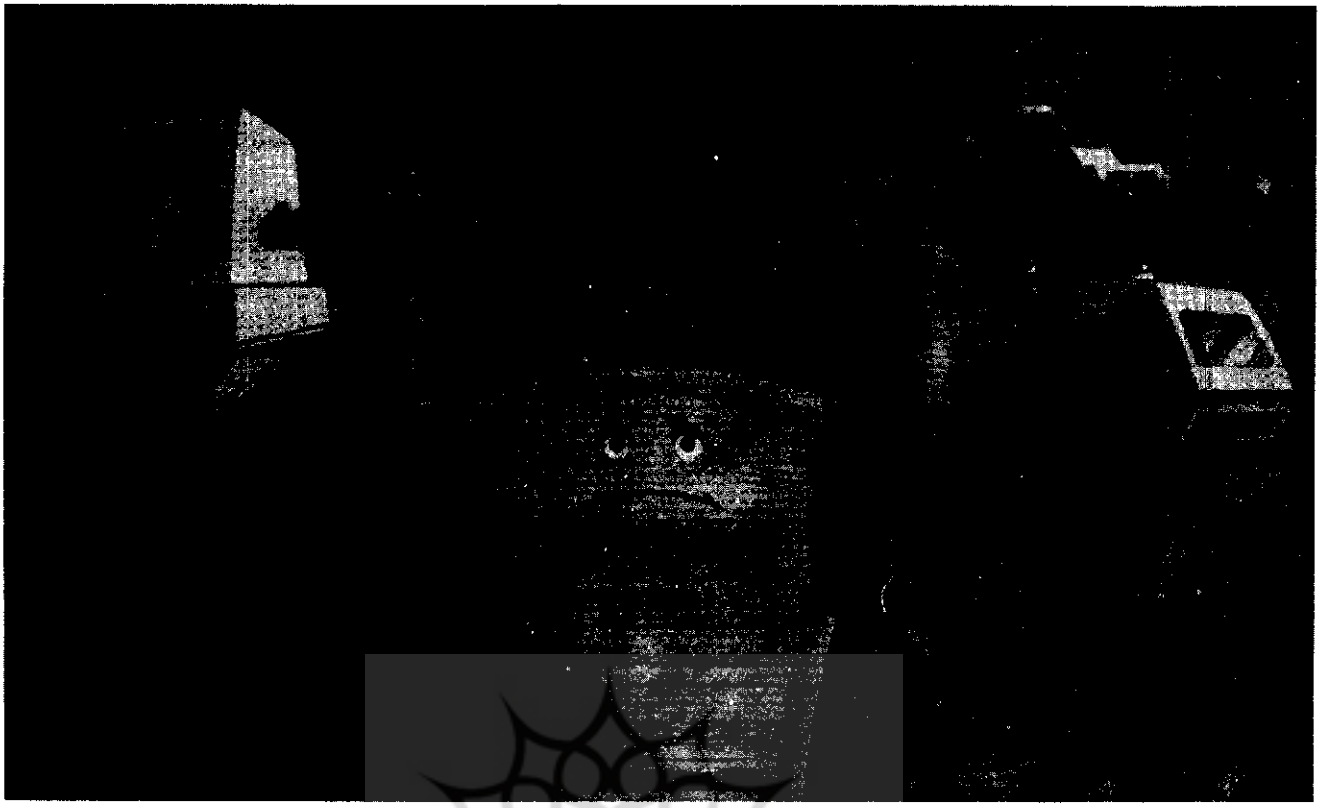
معیارهای یک پول الکترونیکی خوب

محققان معیارهای متعددی را برای بررسی یک پول الکترونیکی مطلوب بیان کرده‌اند که دراین قسمت به برخی از آن‌هااشاره می‌شود:

۱) **امنیت**[3]: نظر اجمالی یک استفاده‌کننده از پول الکترونیکی آن است که سیستم باید به‌طور طبیعی امن باشد. درواقع، ایجاد امنیت وظیفه کاربر نیست. پول الکترونیکی که بین دو نفر انتقال می‌یابد، باید از دزدی، جعل، استراق سمع و مداخله محفوظ باشد. به‌علاوه، این نشانه الکترونیکی نباید امکان کپی، تغییر و یا تولید مجدد را داشته باشد.

۲) **گمنامی**[4]: در معاملات باید حریم شخصی مشتریان محفوظ باشد. بسیاری از مشتریان مایل نیستند که در مبادلات آن‌ها واسطه‌ای وجود داشته باشد و کسی بتواند راجع به داد و ستد آن‌ها اطلاعاتی را کسب نماید، و حتی تاجر نیز نباید بتواند ماهیت خریدار را

○ چون در امضای دیجیتالی از روش‌های رمزگذاری استفاده می‌شود، لذا در صورت رعایت اصول مربوطه، جعل و تقلب در آن به‌مراتب مشکل‌تر از امضای دستی خواهد بود.



▲ *در دنیای تجارت الکترونیک، سازمان‌های معتبری وجود دارند که برای صادرکنندگان و مصرف‌کنندگان پول‌های الکترونیک، گواهینامه دیجیتالی صادر می‌کنند.*

○ پول الکترونیکی که بین دو نفر مبادله می‌شود، باید از عوارضی چون دزدی، جعل، استراق سمع و مداخله به‌دور باشد.

کشف کند. بنابراین، اطلاعاتی همچون چه کسی، چقدر، کجا، چطور، چه وقت و چرا پول را خرج کرده است؟ نباید به‌راحتی قابل کشف و پیگیری باشند.

۳) قابلیت کاربری آسان[5]: در استفاده از پول نقد الکترونیکی، باید سهولت وجود داشته باشد و افراد ـ چه در خرج کردن و چه در گرفتن آن ـ باید راحت باشند. بدیهی است که ساده سازی آن موجب استفاده انبوه شده و استفاده انبوه از آن هم منجر به پذیرش عمومی آن می‌شود. استفاده‌کنندگان از آن نباید متخصص سطح بالایی در رمزنگاری‌های دیجیتالی باشند. درنتیجه، تمام پروتکل‌های ارتباطی بین دو نفر باید بسیار آسان و شفاف برای بکاربردن این نوع پول باشند.

۴) حمل آسان[6]: پول الکترونیکی نباید به محل فیزیکی خاصی وابسته باشد. درحال حاضر، فعالیت‌های تجاری الکترونیکی به شبکه‌های ثابت مانند اینترنت محدود هستند، اما با عمومیت یافتن وب سایت‌ها، باید شرایطی بوجود آید که مشتری و یا کاربر، مالک حتی یک کامپیوتر شخصی هم نباشد، و برای این کار باید امنیت این پول را تأمین و آن را در محلی از شبکه ذخیره کرد، بدون آنکه برای دسترسی به آن از هر ترمینال دلخواه، محدودیتی وجود داشته باشد.

امروزه با گسترش شبکه‌های اینترنتی سیار (موبایل) و همچنین با استفاده از کارت‌های هوشمند، حمل پول الکترونیکی آسان خواهد بود.

۵) استفاده مستمر[7]: همچنانکه یک سکه جاری را می‌توان دست به دست گرداند، پول الکترونیکی نیز باید قابل انتقال به فرد دیگری باشد، بدون اینکه بانک یا فرد دیگری واسطه آن باشد. بدیهی است که استفاده مستمر از پول

○ همزمان با بلوغ تدریجی پول الکترونیکی، مفاهیم پول ملی نیز تحت‌الشعاع قرار خواهند گرفت.

○ یکی از روش‌های مهم برای ایجاد امنیت در پول الکترونیکی، همانا رمزگذاری اطلاعات آن است.

الکترونیکی، ویژگی گمنامی آن را تکمیل می‌کند. در اینصورت، مشتری از یک سکه الکترونیکی استفاده می‌کند، بدون اینکه نیاز به وجود کسی باشد که آن را در جریان انداخته است.

۶) دایمی بودن[8]: مهمترین تفاوت بین پول نقد الکترونیکی با یک سیستم پرداخت الکترونیکی آن است که با اینکه هر دو واسطه مبادله می‌باشند، ولی پول نقد الکترونیکی شامل دیگر وظایف پول، همانند ذخیره ارزش نیز می‌باشد. درنتیجه، این نوع پول نباید محدود به زمان باشد. بنابراین، باید همانند یک پول عادی ارزش خود را داشته باشد تا زمانیکه یا خراب شود و یا ناشر آن را از جریان خارج سازد. هم‌چنین، یک شخص باید بتواند یک نشانهٔ پول الکترونیکی را در محلی امن برای چند سال نگهداری و بعد، از آن استفاده کند.

۷) قابلیت ناپیوستگی[9] **(غیرهمزمانی):**

استفاده از پول معمولی نیازی به‌واسطه ندارد و درهر مکانی قابل استفاده است. در استفاده از پول نقد دیجیتالی نیز نباید به هیچ فرد یا کامپیوتر ثالثی احتیاج باشد. درنتیجه، سیستم پول دیجیتالی نمی‌تواند به تست هایی که معمولاً به‌صورت همزمان[10] انجام می‌شوند، مانند تست‌های اعتبار فرد، همخوانی حساب‌ها وغیره متکی باشد، همچنانکه پول نقد فعلی به آن‌ها نیاز ندارد.

از دیگر خصوصیات یک پول الکترونیکی خوب می‌توان تقسیم‌پذیر بودن، قابلیت اطمینان، کارایی و پذیرش عمومی را هم ذکر کرد.

مشکلات پول الکترونیکی

بدیهی است که استفاده از پول الکترونیکی نیز با مشکلاتی همراه است که به بعضی از آنها اشاره می‌شود:

۸) عدم انکار[11]: فردی که معامله‌ای را به‌صورت الکترونیکی انجام می‌دهد، نباید بتواند آن را منکر شود. در واقع، موضوع عدم انکار در دنیای دیجیتال بسیار سخت‌تر از دنیای معمولی مطرح است. برای تصدیق معاملات الکترونیکی، امضاهای دیجیتالی طراحی شده‌اند. این امضاها باید به‌صورت سرّی نزد صاحب آن نگهداری شوند و درصورتیکه فرد دیگری از آنها سوء استفاده کند، از نظر شناسایی طبیعی و معامله با او صحیح و مشروع است.

۹) خرج مجدد یک پول[12]: یکی از مهمترین و سخت‌ترین مشکلات پول الکترونیکی، خرج مجدد آن است. چون کپی کردن اطلاعات در دنیای دیجیتالی آسان است، لذا مانعی وجود ندارد تا فرد را از کپی کردن از روی سکه خود و استفاده چندین باره از آن باز دارد.

برای جلوگیری از بروز این مشکل، دو راه‌حل پیشنهاد شده است: یکی آنکه، ضرب‌کننده سکه الکترونیکی تمام اطلاعات مربوط به سکه‌های استفاده شده را در رکوردهایی نگهداری کند و پذیرندهٔ سکه نیز قبل از قبول آن، به‌وسیله بانک از عدم استفادهٔ قبلی از آن مطمئن شود. روش دیگر آنست که به‌وسیله یک آلگوریتم ریاضی، درصورتیکه از سکه‌ای دوبار استفاده شد، بعضی از اطلاعات فرد خطاکار آشکار شود، به‌نحوی که بتوان او را شناخت.

۱۰) گم شدن پول[13]: یکی از سطوح پایین گمنامی پول معمولی آن است که اگر پول معمولی گم شود، قابل ردیابی نیست. در پول الکترونیکی نیز به‌دلیل آنکه پول به‌صورت بیت یا بایت‌هایی روی دیسک ذخیره می‌شود، لذا اگر این دیسک خراب شود، این پول درواقع گم شده است.

شایان ذکر است که گم شدن پول الکترونیکی، به‌خاطر حساسیت این نوع پول، بسیار محتمل‌تر از پول رایج است. درضمن، تغییر یک بیت کوچک در پول دیجیتالی می‌تواند حجم زیادی از پول را خراب کند و اطلاعات آن را غیرقابل استفاده نماید.

امنیت پول الکترونیکی

یکی از بحث‌های مهم در سیستم‌های پرداخت الکترونیکی امنیت آنهااست، چرا که شبکه‌هایی مانند اینترنت رسماً یک شبکه باز هستند، لذا طبیعی است که نگرانی‌های زیادی در ارتباط با ارسال داده‌های مالی وجود داشته باشد.

محتمل‌ترین انگیزه برای ارتکاب تقلب‌های مالی،بحث درآمد مالی است. سیستم‌های پول الکترونیکی نیز از این قاعده مستثنا نیستند و این امر می‌تواند با تولید نشانه‌های تقلبی پول الکترونیکی با استفاده از اطلاعات یا دستگاه‌های به سرقت رفته از ناشر پول صورت پذیرد.

تهدید سیستم‌های پول الکترونیکی می‌تواند به‌وسیله تکثیر دستگاه‌ها، تغییر یا تکثیر اطلاعات نرم‌افزاری، تغییر پیام‌های ارسالی، سرقت وسایل سخت‌افزاری و یا اطلاعات نرم‌افزاری و عدم کارکرد صحیح صورت پذیرد.

در طراحی سیستم‌های امنیتی پول الکترونیکی، تلاش می‌شود که به‌وسیله معیارهای پیشگیری مانند معیارهای مقاومت سخت‌افزاری، رمزگذاری نرم‌افزاری، مجوزهای همزمان، و معیارهای تشخیص تقلب، امنیت این پول تأمین شود.

۱) رمزگذاری: از روش‌های مهم در ایجاد امنیت در پول الکترونیکی، رمزگذاری اطلاعات آن است. در این زمینه هدف آنست که در جریان ارسال اطلاعات مربوطه، از وجود محرمانگی و صحت اطلاعات اطمینان حاصل شود و درضمن، گیرنده و فرستنده بتوانند یکدیگر را تصدیق کنند و از ساختگی نبودن و یا عدم انکار در معامله مطمئن شوند.

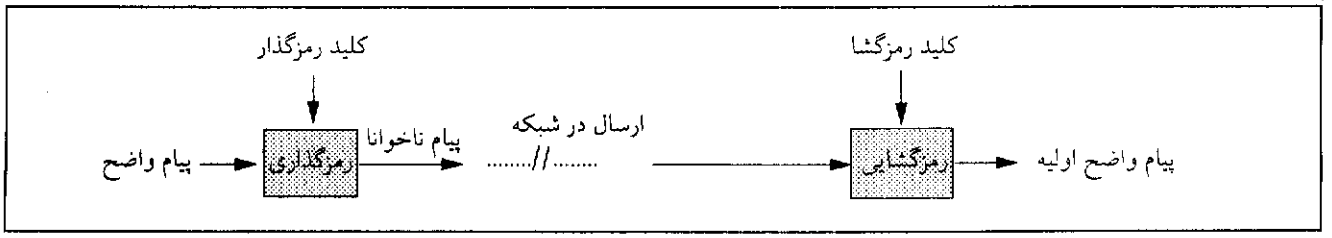
یکی از روش‌های مرسوم رمزگذاری، استفاده از کلید رمزگذار است. در این روش، فرستنده با استفاده از یک کلید رمزگذار، پیام خود را به‌صورت ناخوانا درآورده و از طریق شبکه برای طرف مقابل ارسال می‌کند. گیرنده نیز با استفاده از یک کلید رمزگشا آن پیام را به‌صورت پیام واضح اولیه تبدیل می‌کند. شکل شماره یک این فرآیند را تشریح می‌کند.

رمزگذاری با کلید به دو روش زیر انجام می‌شود:

الف ـ رمزگذاری متقارن[14]: در این روش، فرستنده و گیرنده باهم توافق می‌کنند که از یک کلید سرّی مشترک برای رمزگذاری و رمزگشایی استفاده کنند. بزرگترین مشکل این روش، به‌دست آوردن یک کلید مشترک و ارسال آن از طریق اینترنت می‌باشد. همچنین، سیستم‌های تک کلیدی برای اهداف تصدیق فرستنده و مساله عدم انکار کمکی نمی‌کنند. این مشکلات موجب ابداع یک روش دو کلیدی به‌نام رمزگذاری غیرمتقارن شده است.

ب ـ رمزگذاری غیرمتقارن[15]: در این روش، برای هر شخص یک جفت کلید (عمومی و خصوصی) صادر می‌شود. کلید عمومی در شبکه منتشر است و کلید خصوصی نزد فرد مخفی نگه‌داشته می‌شود. درصورتیکه یک فرد بخواهد پیامی را به گیرنده خاصی بفرستد، ابتدا

شکل شماره یک



کلید عمومی گیرنده را در دایرکتوری شبکه جستجو کرده و پیام خود را به‌وسیله آن به رمز درآورده و برای گیرنده ارسال می‌دارد. گیرنده نیز با استفاده از کلید خصوصی خود می‌تواند پیام را رمزگشایی کند.

۲) امضای دیجیتالی: امضای دیجیتالی، عامل شناسایی کننده الکترونیکی است که برای تأیید اسناد الکترونیکی مانند نامه، قرارداد و غیره بکار می‌رود. امضای دیجیتالی با خصوصیات زیر دارای ویژگی‌های امضای دستی می‌باشد:

- برای هر فرد یکتا است.
- امکان تصدیق و تأیید را دارد.
- در کنترل اختصاصی صاحب آن است.
- بعد از الصاق امضای دیجیتالی به داده‌ها، درصورتیکه داده تغییر کند، امضا هم غیرمعتبر می‌شود.

یکی از روش‌های امضای دیجیتالی، امضای کلید عمومی است که روش آن همانند رمزگذاری غیرمتقارن می‌باشد. درضمن، چون در امضای دیجیتالی از روش‌های رمزگذاری استفاده می‌شود، لذا درصورت رعایت اصول مربوطه، جعل و تقلب در آن به مراتب از امضای دستی مشکل‌تر می‌شود.

۳) گواهینامه دیجیتالی: وقتی که در شبکه اینترنت، دو نفر قصد انجام معامله‌ای را دارند، باید یکدیگر را تصدیق کنند. درضمن، یک فرد باید مطمئن شود که کلید عمومی طرف مقابل، دقیقاً متعلق به اوست. انجام این کار از طریق گواهینامه دیجیتالی صورت می‌پذیرد. سازمان‌های معتبری به‌نام سازمان گواهینامه (CA)[16] وجود دارند که برای افراد گواهینامه صادر می کنند و در این گواهینامه‌ها، به‌صورت شکل شماره دو، هویت فرد را معرفی می‌کنند و یک جفت کلید عمومی و خصوصی را برای او صادر می‌نمایند.

شکل شماره دو

یک گواهینامه دیجیتالی

۱ـ هویت فرد (اسم و مشخصات)
۲ـ کلید عمومی فرد
۳ـ امضای دیجیتالی سازمان صادرکننده گواهینامه

بدیهی است که مجموعه تکنیک‌های فوق‌الذکر نقش مهمی را در تأمین امنیت سیستم‌های پولی الکترونیکی و مبادلات مربوطه به‌عهده دارند.

انواع سیستم‌های پول الکترونیکی

تاکنون سیستم‌های مختلف پول الکترونیکی طراحی و ارایه شده‌اند. هر یک از این سیستم‌ها دارای مزایا و معایب خاص خود می‌باشند، و در مورد هرکدام تلاش شده است که خصوصیات قبلی ذکر شده دربارهٔ پول الکترونیکی را به‌نحوی دارا باشند. برخی از مهمترین این سیستم‌ها عبارتند از:

۱) Millicent: هدف از ارایه این سیستم، انجام خرید و فروش برای کالا و یا خدمات با ارزش کم و پرداخت‌های جزیی بر روی اینترنت از یکصدم سنت تا پنج دلار می‌باشد. اگر چه مبلغ معامله دراین سیستم کوچک است، ولی به علت تعداد زیاد تراکنش‌ها، کل حجم پولی معاملات این سیستم قابل‌توجه است.

در این سیستم، نشانه‌های پول الکترونیکی به‌نام Scrip توسط ناشر منتشر می‌شود. این نشانه حامل پیام امضاشده‌ای است که ارزش و شمارهٔ خاص خود را دارد و همانند وجه نقد الکترونیکی است. این نشانه‌ها توسط بازرگان صادر و جمع‌آوری می‌شوند و فرآیندهای تأیید و شناسایی و رمزگذاری‌ها نیز به‌عهدهٔ او می‌باشد. در این سیستم، به‌دلیل آنکه هر بازرگان نشانه خود را منتشر می‌کند، لذا ممکن است که نگهداری آنها برای مشتریان به‌صرفه نباشد، لذا در سنجش از فرآیندهای تهیه این نشانه‌ها، دلال‌هایی تعبیه شده‌اند که نشانه‌های مختلف را تهیه و درموقع لزوم به مشتریان ارایه می‌کنند. از مزایای این سیستم، درجهٔ بالای گمنامی و سرعت معاملات به‌واسطه عدم تمرکز می‌باشد. درضمن، به‌دلیل پرداخت‌های کوچک، نیازی به رمزگذاری‌های پیچیده نیست.

۲) Digicash: دیوید چام[17] از پیشگامان سیستم‌های پول الکترونیکی، ارایه دهندهٔ این سیستم می‌باشد. در این سیستم، مشتری و تاجر در بانک Digicash ثبت نام کرده و برای ایشان یک حساب پول الکترونیکی باز می‌شود. ارتباط این اجزا توسط نرم‌افزار خاصی صورت می‌پذیرد. در این سیستم، مشتری می‌تواند یک عدد بزرگ (حدود ۱۰۰ رقم) را به‌عنوان پول تولید کند و برای امضا به بانک بفرستد. بعد از امضای آن عدد، می‌توان از آن به‌عنوان یک پول الکترونیکی استفاده کرد و آن را به تاجر تحویل داد. فرآیند امضای پول الکترونیکی توسط بانک هم به‌صورتی است که مشتری گمنام است و فقط در زمانی که بخواهد از پول سوء استفاده کنند و آنرا دوبار خرج نماید، مشخصاتش آشکار می‌شود.

تاجر هم پس از اینکه پول الکترونیکی را به بانک ارسال کرد و از عدم خرج مجدد آن مطمئن شد، آنرا قبول می‌کند و کالا را برای مشتری ارسال می‌دارد.

از مزایای این سیستم، گمنامی زیاد کاربر، امکان استفاده در معاملات و ارتباطات ناپیوسته، امکان استفاده روی کارت‌های هوشمند و سیستم‌های رمزگذاری قوی آن می‌باشد.

۳) Mondex: در هسته سیستم موندکس، کارت‌های هوشمند وجود دارند که قادر به پذیرش و ذخیره پول الکترونیکی می‌باشند. در این سیستم، نشانه‌های پول الکترونیکی که همانند وجه نقد می‌باشند، قابل استفاده روی کامپیوترهای شخصی و انتقال به‌وسیله کارت‌های هوشمند می‌باشند.

از خصوصیات بارز این سیستم، امکان انتقال دوطرفه پول بین بانک، مشتری و تاجر و همچنین، استفاده مستمر از آن می‌باشد. این سیستم، برای پرداخت از یک سنت تا چند صد دلار بهینه شده و هزینه‌های تراکنش آن کم است.

از دیگر مزایای این سیستم، امنیت زیاد به‌واسطه روش‌های قوی رمزگذاری، امکان استفادهٔ غیرپیوسته، کاربرد کارت‌های هوشمند به‌جای کیف پول، و امکان گسترش در جامعه می‌باشد.

تشریح انواع و ساختارهای هر یک از سیستم‌های پول الکترونیکی، نیاز به بحث‌های مفصل دارد که ان‌شاءا... در شماره‌های آتی به آن‌ها می‌پردازیم. ■

ادامه دارد

زیرنویس‌ها

1) Electronic Tokens
2) Physical Media
3) Security
4) Anonymity
5) Friendly Using
6) Portability
7) Reuseability
8) Infinite Duration
9) Off-line
10) On-line
11) Nonrepudiation
12) Double Spending
13) Lost Money
14) Symmetric Encryption
15) Asymmetric Encryption
16) Certificate Authority
17) Divid Chaum