به نام خداوند بخشنده‌ی مهربان

دانشگاه شیخ‌بهائی

دانشکده مهندسی

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر- نرم‌افزار

ارائه روش انکارناپذیر برای تجارت الکترونیک سیار

پژوهشگر

زهرا رجایی ریزی

استاد راهنما

دکتر احمد برآنی

مهر ۱۳۹۲

باسمه تعالی

جمهوری اسلامی ایران
وزارت علوم تحقیقات و فناوری

دانشگـــــــــاه شیـــــــــخ بهائی

دانشکده فنی مهندسی

گروه مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر خانم زهرا رجایی ریزی

تحت عنوان

ارائه روش انکارناپذیر برای تجارت الکترونیک سیار

در تاریخ **۹۲/۷/۱۰** توسط هیأت داوران زیر بررسی و با درجه ..... به تصویب نهائی رسید.

۱- استاد راهنمای پایان‌نامه	**دکتر احمد برآآنی دستجردی**	با مرتبه علمی	**دانشیار**	امضاء
۲- استاد داور داخل گروه	**دکتر مهدی باطنی**	با مرتبه علمی	**استادیار**	امضاء
۳- استاد داور خارج گروه	**دکتر حمید ملا**	با مرتبه علمی	**استادیار**	امضاء

دکتر سید محمدحسن فیض

مدیر تحصیلات تکمیلی

باسمه تعالی

اقرارنامه

اینجانب **زهرا رجایی ریزی** به شماره دانشجویی **۹۰۲۵۱۰٤** دانشجوی رشته **مهندسی کامپیوتر- نرم‌افزار** که پایان‌نامه خود تحت عنوان:

ارائه روش انکارناپذیر برای تجارت الکترونیک سیار

را نوشته و برای دفاع آماده کرده‌ام اعلام می‌نمایم که محتوا و نوشته‌های این پایان‌نامه متعلق به خودم بوده و هیچ قسمت از آن به طور مستقیم یا غیرمستقیم کپی و یا برگرفته از کار دیگران خارج از ضوابط متعارف نگارش پایان‌نامه نمی‌باشد. اینجانب نیز آگاهم که در صورتی که خلاف موضوع فوق‌الذکر در هر زمان و به هر طریق اثبات گردد از کلیه امتیازات مکتسبه از این پایان‌نامه محروم و ملزم به پذیرش عواقب و مجازات حقوقی ناشی از آن می‌باشم.

نام و نام‌خانوادگی امضا

تقدیم به

سه گوهر گرانبهای زندگیم

مادر دلسوزم، پدر فداکارم

و

همسر مهربانم

سپاس‌گزاری

تقدیر و تشکر شایسته از استاد فرهیخته جناب آقای دکتر براآنی که با نکته‌های دلاویز و گفته‌های بلند، صحیفه‌های سخن را علم پرور نمودند و همواره راهنما و راهگشای نگارنده در اتمام و اکمال پایان‌نامه بوده‌اند.

همچنین قدردانی می‌کنم از خانواده‌ی مهربانم که محیطی سرشار از امنیت و آرامش را برای نیل به این هدف فراهم آورده‌اند.

چکیده

تجارت سیار که یکی از فناوری‌های نوین در عرصه‌ی تجارت الکترونیک است، روز به روز محبوب‌تر می‌شود. این نوع تجارت راحتی و انعطاف‌پذیری را برای کاربران خود به ارمغان آورده است. با این حال، برخی از عوامل مانع پذیرش همه جانبه‌ی تجارت سیار می‌شود. امنیت همیشه بزرگ‌ترین چالش بوده است. انکارناپذیری که یکی از سرویس‌های امنیتی است، یک گواهی رمز شده برای تراکنش الکترونیک فراهم می‌آورد. تأمین این گواهی در تجارت سیار به دلیل محدودیت منابع در دستگاه سیار کمی مشکل است. کارهای مختلفی در سالیان اخیر در این زمینه انجام شده اما اغلب به محدودیت‌های موجود در این دستگاه‌ها توجه چندانی نشده است.

در این پایان‌نامه سعی شده تا با استفاده از روش‌های ساده، پروتکلی سبک وزن برای تأمین انکارناپذیری در تجارت سیار ارائه شود. رمزنگاری نامتقارن که معمولاً در پروتکل‌های امنیتی استفاده می‌شوند بسیار پیچیده و دارای بار محاسباتی زیادی هستند، در این پروتکل سعی شده است از روش‌های سبک وزن‌تر مثل روش تقسیم کلید برای نیل به هدف انکارناپذیری استفاده شود. همچنین از یک شخص نیمه معتمد نیز برای تولید گواهی استفاده شده است که نیازی به اعتماد کامل خریدار و فروشنده به شخص نیمه معتمد نیست. پس از طراحی پروتکل، آن را با استفاده از ابزار ارزیابی پروتکل AVISPA و محیط شبیه‌سازی و انیمیشن‌سازی SPAN شبیه‌سازی کرده و پروتکل پیشنهادی از لحاظ حملات ممکن بررسی و تحلیل شده و نشان داده شده است که این پروتکل مانع نفوذ حملات مهمی چون انکارناپذیری و جعل هویت است.

کلمات کلیدی: تجارت سیار (mobile commerce)، رمزنگاری (cryptography)، انکارناپذیری (non-repudiation)

فهرست مطالب

فهرست شکل‌ها

فهرست جداول

فصل اول

مقدمه

مقدمه

پیشرفت‌های سریع در دستگاه‌های ارتباطی سیار، فرصت‌های عظیمی را در زمینه‌های متنوع برنامه‌های کاربردی به وجود آورده است. یکی از این زمینه‌ها که هنوز در ابتدای راه است تجارت سیار[1] نام دارد. تجارت الکترونیک سیار یک تراکنش الکترونیکی یا تبادل اطلاعات است که مبلغی را برای استفاده از کالاها و سرویس‌هایی به حساب دیگری انتقال می‌دهد و این عمل با دسترسی سیار و بی‌سیم به شبکه‌ی کامپیوتری با استفاده از یک دستگاه الکترونیکی سیار انجام می‌پذیرد. دستگاه سیار یک ابزار ارتباطی بی‌سیم مثل تلفن‌های موبایل، PDAها، تبلت‌های بی‌سیم و کامپیوترهای سیار است [۱].

امروزه استفاده از دستگاه‌های سیار و اتصال به اینترنت و شبکه‌های گسترده‌ی دیگر در بین مردم بسیار رایج شده است. در واقع، در کشورهای پیشرفته، هر کس یک دستگاه موبایل شخصی دارد و معمولاً این دستگاه سیار همیشه در حالت روشن همراه اوست. اندازه‌ی این دستگاه‌ها روز به روز کوچک‌تر و از همه مهم‌تر قابلیت‌های ارتباطی، سرگرمی، محاسبه و ظرفیت آن‌ها در حال تغییر است. این پیشرفت‌ها، گسترش سرویس‌هایی که قبلاً به این شکل نبوده مثل تجارت سیار و کسب و کار سیار را ممکن می‌سازد.

تجارت الکترونیکی، راحتی و انعطاف‌پذیری سرویس‌های سیار را در هر زمان و هر مکان برای مشتریان خود فراهم آورده و نقش بسیار مهمی در پرداخت‌ها و بانکداری‌های امروزه داراست. بنابراین دستگاه‌های سیار به فرصتی باورنکردنی و روشی همگانی برای پرداخت و تراکنش‌های مالی روزانه تبدیل شده است.

با افزایش شیوع تجارت الکترونیکی، تجارت سیار و استفاده‌ی همگانی از دستگاه‌های موبایل، پیش‌بینی می‌شود که پرداخت سیار آینده‌ی بسیار روشنی در میان سرویس‌های دستگاه‌های موبایل خواهد داشت.

[1] Mobile Commerce (m-commerce)

اما متاسفانه برخی مسائل، مانع پذیرش همه جانبه‌ی پرداخت سیار می‌شوند. در میان این موانع، امنیت همیشه بزرگ‌ترین چالش بوده است. بر اساس تحقیقی که Unisys Security Index در سال ۲۰۰۸ انجام داده است، هفتاد و یک درصد از ۱۳۲۹۶ مشتری در ۱٤ کشور، به خاطر نگرانی‌های امنیتی، حاضر نیستند امور بانکی یا خرید آنلاین را از طریق دستگاه‌های موبایل خود انجام دهند. کمتر از ۱۰ درصد آن‌ها درحال حاضر، دستگاه‌های موبایل خود را برای انتقال پول، تراکنش‌های کارت اعتباری یا پس‌اندازهای خود به کار می‌گیرند [۲]. بنابر این استراتژی‌های امنیتی برای متقاعد کردن کاربران موبایل و سرویس‌دهندگان مالی در استفاده از تراکنش‌های پرداخت سیار ضروری است [۲].

با توجه به اینکه تجارت الکترونیک اکنون به تلفن‌های همراه و بازار تلفن‌های هوشمند به شکل تجارت موبایل راه گشوده است و جای تکنولوژی کارت‌های اعتباری را گرفته است، درنظر گرفتن مدلی با زیر ساختار امن در این پرداخت‌های سیار امری بسیار مهم است. طراحی مدلی امن برای حفاظت از تراکنش‌های پرداخت سیار نیازمند تعادلی بین امنیت و کارایی است. یک تراکنش مالی به حفاظت همه جانبه‌ای در رابطه با قابلیت اعتماد[۱]، تصدیق[۲]، جامعیت[۳] و انکارناپذیری[٤] نیاز دارد که طبیعتاً خواستار منابع محاسباتی قابل ملاحظه‌ای می‌باشد [۲].

متأسفانه دستگاه‌های سیار از یک طرف دارای محدودیت در قدرت پردازش و حافظه هستند و از طرف دیگر نگرانی‌های امنیتی و عدم اعتماد در آن‌ها بیشتر است. با وجود اینکه دستگاه‌های سیار مجهزی به بازار راه یافته‌اند، اما این دستگاه‌ها اغلب هزینه‌ی زیادی دارند و توسط اکثریت مردم مورد استفاده قرار نمی‌گیرند. در کشورهای در حال توسعه، تقاضای روبه رشد سیستم‌های پرداخت و بانکداری سیار، چالش جدیدی برای توسعه‌ی پروتکل‌های پرداخت مناسب و مطابق با نیازهای محاسباتی و ذخیره‌سازی ایجاد کرده است. بنابراین، طراحی مدلی امن، متناسب با محدودیت‌های دستگاه‌های موبایل و شبکه‌های بی سیم، چالشی مهم در موفقیت پرداخت سیار است [۲].

همانطور که گفته شد، امنیت در تجارت الکترونیک، با مسائل اساسی و مهمی همچون تصدیق هویت، تفویض، قابلیت اعتماد، جامعیت، دسترس‌پذیری و انکارناپذیری روبروست. در میان این مسائل، انکارناپذیری یکی از سرویس‌هایی است که برای مقابله با خطرات حمله‌ی داخلی استفاده می‌شود، این سرویس تقریباً هنوز به طور کامل مورد بررسی قرار نگرفته است. انکارناپذیری با قابلیت حل اختلافات در رابطه با وقوع یا عدم وقوع یک عمل یا رویداد، اهمیت خودش را در تراکنش‌های تجاری در تجارت الکترونیک یا سیار ثابت کرده است. انکارناپذیری در تجارت الکترونیک اخیراً توجه بسیاری را به خود جلب کرده است اما مسئله‌ی نظیر خود، یعنی انکار ناپذیری در تجارت سیار هنوز در ابتدای راه است [۳].

[1] Confidentiality
[2] Authentication
[3] Integrity
[4] Non-repudiation

انکارپذیری، رد یا انکار ناصحیح شرکت در یک ارتباط است. هدف سرویس انکارناپذیری این است که شواهدی در رابطه با رویداد انجام شده تولید، جمع آوری و نگه‌داری شود و در دسترس و مورد بررسی قرار گیرد تا بتوان اختلافاتی که در مورد وقوع یا عدم وقوع عمل یا رویدادی پیش می‌آید را حل کرد [۳].

در حال حاضر بیشتر پروتکل‌های انکارناپذیری از امضای دیجیتال برای تولید شواهد انکارناپذیری استفاده می‌کنند. امضای دیجیتال نسخه‌ی الکترونیکی همان امضای دستی سنتی است. ابداع امضای دیجیتال، روش تشخیص هویت افراد، امضای توافقات و انجام تجارت‌ها را تغییر داد. این امر باعث شد که تجارت برخط کالاها و سرویس‌ها در خانه‌ها و محیط‌های غیر رسمی بسیار مرسوم شود [۳].

امروزه امضای دیجیتال به عنوان یکی از مهم‌ترین فناوری‌های اینترنت شناخته می‌شود. با این حال امضاهای الکترونیک ارائه شده‌ی موجود، برای برنامه‌های سیار جدید مثل پرداخت سیار که دارای محدودیت‌هایی هستند بسیار هزینه‌بر هستند. با وجود اینکه تجارت سیار می‌تواند به عنوان تجارت الکترونیک سیار شناخته شود، ولی به علت نا امن بودن ذاتی شبکه‌های بی‌سیم و قابلیت‌های محدود دستگاه‌های سیار، نمی‌توانیم پروتکل‌های انکارناپذیری در تجارت الکترونیک را در این محیط جدید (تجارت سیار) به کار بگیریم. بنابراین نیاز به پروتکل‌های انکارناپذیری سبک وزن ولی به اندازه کافی امن داریم تا از تراکنش‌های محیط بی‌سیم محافظت کنند. پروتکل‌های انکارناپذیری در تجارت سیار باید بر پایه‌ی پروتکل‌های انکار ناپذیری موجود در تجارت الکترونیک باشند و طوری پیاده‌سازی شوند که متناسب با محدودیت‌های منابع در دستگاه‌های سیار و نیازمندی‌های خاص در انواع تراکنش‌های مختلف باشند [۳].

اکثر راه‌حل‌هایی که تاکنون ارائه شده است تحلیل کاملی از خصوصیات انکارناپذیری نداشته‌اند؛ به علاوه، برخی از آن‌ها، قابلیت‌های محدود دستگاه‌های دستی سیار را فراموش کرده‌اند و برخی دیگر فقط برای برخی موارد خاص مناسب هستند. بنابراین ما یک پروتکل سبک وزن برای انکارناپذیری[1] ارئه می‌کنیم که نه تنها انکارناپذیری و بیطرفی در تراکنش را پشتیبانی کند بلکه به جنبه‌های مختلف محدودیت‌های دستگاه‌های سیار نیز اهمیت داده و تولید شواهد به گونه‌ای باشد که بتواند بر محدودیت‌های قدرت محاسباتی این دستگاه‌ها غلبه کند [۳].

هدف این تحقیق آن است که با طراحی پروتکلی امن، انکارناپذیری در تجارت سیار پیاده‌سازی شود به طوریکه محدودیت‌ها و ظرفیت محاسباتی دستگاه‌های موبایل در این پروتکل لحاظ گردد و به این ترتیب اعتماد طرفین ارتباط نسبت به یکدیگر بالا رود.

راه‌حلی که در این پایان‌نامه ارائه می‌شود از یک شخص سوم نیمه معتمد[2] که در اینجا اپراتور شبکه‌ی سیار خواهد بود برای تولید گواهی بی‌طرف و قابل استناد بهره می‌برد. همچنین ایده‌ی اصلی این راه‌حل استفاده از روش

[1] Lightweight Non-Repudiation Protocol
[2] Semi-trusted Third Party

سبک وزن تقسیم کلید محرمانه توسط طرفین ارتباط برای نیل به این هدف است. در این راه‌حل تنها از توابع درهم‌ساز که بسیار سبک‌وزن است در سمت خریدار که دستگاه سیار است استفاده می‌شود، بنابراین میزان بار محاسباتی به میزان قابل توجهی نسبت به روش‌های مبتنی بر کلید متقارن و نامتقارن کاهش یافته است.

ادامه‌ی بخش‌های این پایان نامه به این صورت سازماندهی شده است: در فصل دوم، مروری روی ادبیات تجارت الکترونیک و تجارت سیار، انواع حملات و تهدیدها، رمزنگاری، انواع کلیدهای متقارن و نامتقارن و توابع درهم‌ساز خواهیم داشت و مختصری در مورد روش‌های کلیدی استفاده شده در راه‌حل پیشنهادی مثل روش توزیع کلید دیفی هلمن و روش تقسیم کلید محرمانه بحث خواهیم کرد.

فصل سوم به بررسی انواع روش‌ها و راه‌حل‌هایی که در سال‌های اخیر برای حل مشکل انکارناپذیری در تجارت سیار ارائه شده‌اند می‌پردازد و مزایا و معایب هر یک از روش‌ها را از دید محدودیت‌های محاسباتی و ذخیره‌سازی دستگاه‌های سیار معرفی می‌کند.

در فصل چهارم یک راه‌حل پیشنهادی با نام پروتکل سبک وزن انکارناپذیری با تمام جزئیات ارائه می‌شود. در این فصل همه‌ی مراحل پروتکل توسط روش نشانه‌گذاری معرفی شده نوشته شده و توضیح هر یک از مراحل به دقت شرح داده شده است. همچنین هر مرحله از لحاظ امنیتی و بروز حملات محتمل بررسی و به طور موشکافانه تحلیل شده است.

در فصل پنجم پروتکل پیشنهادی خود را به زبان سطح بالای HLPSL نوشته و آن را در یک ابزار اعتبارسنجی اتوماتیک پروتکل به نام AVISPA و با استفاده از محیط قدرتمند انیمیشن‌ساز پروتکل امنیتی[1] (SPAN) ارزیابی و شبیه‌سازی کردیم. پس از شبیه‌سازی پروتکل LNRP و اجرای آن با استفاده از پشتیبان‌های OFMC و CLASTE متوجه شدیم که پروتکل پیشنهادی همه‌ی اهداف مورد نظر را داراست و هیچ نوع حمله‌ای به آن وارد نیست. فصل ششم نیز فصل پایانی و متعلق به نتیجه‌گیری و کارهای آینده می‌باشد.

[1] Security Protocol Animator

فصل دوم

ادبیات موضوع

مقدمه

تجارت الکترونیکی را می‌توان انجام هرگونه امور تجاری بصورت آنلاین و از طریق اینترنت بیان کرد. این تکنیک در سال‌های اخیر رشد بسیاری داشته است و پیش‌بینی می‌شود بیش از این نیز رشد کند. تجارت الکترونیک به هرگونه معامله‌ای گفته می‌شود که در آن خرید و فروش کالا و یا خدمات از طریق اینترنت صورت پذیرد و به واردات و یا صادرات کالا و یا خدمات منتهی می‌شود. یکی از رایج‌ترین جنبه‌های تجارت الکترونیک تجارت سیار است که این روزها طرفداران بسیاری به خود جلب کرده است و خریدهای اینترنتی را در هر کجا و هر زمان بسیار راحت کرده است.

یکی از ارکان مهم در تجارت الکترونیک، تأمین امنیت است و این امنیت در تجارت سیار مهم‌تر و پیچیده‌تر است. در این فصل به بررسی مفاهیم کلیدی این پژوهش می‌پردازیم. در بخش اول این فصل به تاریخچه، تعریف و انواع تجارت الکترونیک می‌پردازیم، در بخش دوم مروری روی تجارت سیار خواهیم داشت. بخش سوم و چهارم به ترتیب به تهدیدات و حملات و امنیت تراکنش‌های اینترنتی اختصاص دارد. در بخش پنجم در مورد انواع ابزارهای رمزنگاری و در فصل ششم در مورد مسائل امنیتی تجارت سیار و در بخش هفتم در مورد روش دیفی هلمن بحث خواهیم کرد. بخش هشتم نیز در مورد روش تقسیم کلید مطالبی را ارائه می‌کند. در بخش نهم نتیجه‌گیری کوتاهی در رابطه با این فصل خواهیم داشت.

۲-۱ تجارت الکترونیک

در اواخر سال ۱۹۹۰ تجارت الکترونیک به عنوان روشی جدید برای کسب و کار پدیدار شد. در آن زمان سایت Azmon.com به سرعت در فروش کتاب پیشرفت کرد، eBay پس از آن در حراج اینترنتی گام نهاد و به یک سایت پردرآمد در این زمینه تبدیل شد. بعد از آن، سایت‌های بسیاری این پیشرفت جدید را تجربه کردند.

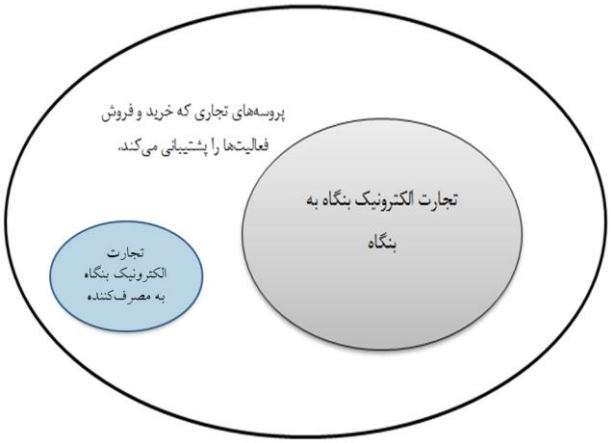
برای بسیاری از مردم، تجارت الکترونیک به معنای خرید از اینترنت است؛ اما تجارت الکترونیک شامل فعالیت‌های دیگری نظیر معامله‌ی تجاری یک شرکت با دیگر شرکت‌ها و همچنین پروسه‌های داخلی که شرکت‌ها برای پشتیبانی خرید، فروش، اجاره، برنامه‌ریزی و دیگر فعالیت‌ها استفاده می‌کنند می‌شود. برخی از کلمه‌ی کسب و کار الکترونیک به معنای گسترده‌تر استفاده می‌کنند. شرکت IBM کسب و کار الکترونیک را اینگونه تعریف می‌کند: «تغییر حالت پروسه‌های تجاری کلیدی با استفاده از فناوری اینترنت». بیشتر مردم کلمات تجارت الکترونیک و کسب و کار الکترونیک را به جای یکدیگر به کار می‌برند. فناوری اینترنت شامل اینترنت، شبکه‌ی جهانی وب و دیگر فناوری‌ها مانند انتقال بی‌سیم روی شبکه‌های تلفن همراه می‌شود [٤].

۲-۱-۱ انواع تجارت الکترونیک

دسته‌بندی انواع مختلف تجارت الکترونیک بر اساس موجودیت‌های شرکت‌کننده در تراکنش یا پروسه‌های تجاری در برخی مواقع مناسب است. پنج دسته‌ی کلی تجارت الکترونیک به این صورت است: بنگاه به مصرف‌کننده، بنگاه به بنگاه، پروسه‌های بنگاهی، مصرف‌کننده به مصرف‌کننده و بنگاه به دولت. ۳ دسته‌ی مهم که بیشتر استفاده می‌شوند عبارتند از [٤]:

- خرید مصرف‌کننده از اینترنت که معمولاً بنگاه به مصرف‌کننده[1] نامیده می‌شود.
- تراکنش‌هایی که بین بنگاه‌های مختلف بر روی وب انجام می‌گیرد و معمولاً بنگاه به بنگاه[2] نامیده می‌شود.
- تراکنش‌ها و پروسه‌های تجاری که شرکت‌ها، دولت و دیگر سازمان‌ها با استفاده از فناوری اینترنت، خرید و فروش‌ها را پشتیبانی می‌کنند.

[1] Business-to-Consumer (B2C)
[2] Business-to-Business (B2B)



شکل ۲-۱ اجزای تجارت الکترونیک [٤]

شکل ۲-۱ سه مؤلفه‌ی مهم تجارت الکترونیک را نشان می‌دهد. تجارت الکترونیک B2B از نظر حجم پول و تعداد تراکنش‌ها از تجارت الکترونیک B2C بزرگ‌تر است. با این وجود تعداد پروسه‌های تجاری بیشتر از تعداد کل تراکنش‌های B2C و B2B است.

بیضی بزرگ در شکل ۲-۱ که نشان دهنده‌ی پروسه‌های تجاری است که خرید و فروش فعالیت‌ها را پشتیبانی می‌کند، بزرگ‌ترین جزء تجارت الکترونیک است.

یک تراکنش، مبادله‌ی ارزش یا مقداری به حساب می‌آید مثلاً خرید، فروش یا تبدیل مواد خام به یک محصول تمام شده، یک تراکنش است. حسابرسان با ثبت تراکنش‌ها، به صاحبان تجارت کمک می‌کنند تا بهتر بتوانند میزان عملکرد خود را بسنجند. همه‌ی تراکنش‌ها حداقل یک فعالیت دارند و برخی تراکنش‌ها دارای چندین فعالیت هستند. البته همه‌ی فعالیت‌ها منجر به معیاری قابل اندازه‌گیری و در نتیجه قابل ثبت برای تراکنش‌ها نیستند [٤].

۲-۲ تجارت سیار

«تجارت سیار تراکنشی است که در آن حق مالکیت یا ارزش خاصی برای استفاده‌ی کالاها و خدمات به حساب دیگری منتقل می‌شود و البته این انتقال توسط دسترسی سیار به شبکه‌های کامپیوتری با کمک دستگاه‌های الکترونیکی انجام می‌شود [٥].»

امروزه دیدن مردم با دستگاه‌های سیاری که به اینترنت یا دیگر شبکه‌های ارتباطی متصل شده‌اند امری بسیار طبیعی است. همه‌ی ما احتمالاً ساعات زیادی در روز در فضای اینترنت به سر می‌بریم و حتی نمی‌توانیم دستگاه سیار یا لپ‌تاپی را بدون قابلیت اتصال به اینترنت تصور کنیم [۱].