روش های گمنامی طرح پول دیجیتالی برند در شبکه TCP/IP

صفورا جانوسپاه
دانشجوی کارشناسی ارشد کامپیوتر- نرم افزار
دانشگاه آزاد اسلامی واحد تهران جنوب
Jano.azad@gmail.com

دکتر محسن عشوریان
عضوهیات علمی و استادیار
دانشگاه آزاد اسلامی واحد شهر مجلسی
mohsena@yahoo.com

چکیده

ساختار سیستم پول دیجیتالی مدل برند بر دو مفهوم امضاء دیجیتالی و مسئله ارائه بنا شده است . سیستم برند یک سیستم کاملا غیر بلادرنگ با قابلیت ردیابی است و بعنوان سیستمی کارا می باشد . این سیستم بر امنیت و سهولت و مهمتر از همه گمنامی تاکید دارد. در این مقاله روش های مختلف ایجاد گمنامی در سیستم پول دیجیتالی در شبکه TCP/IP مورد بحث و بررسی قرار میگیرد .

کلمات کلیدی : *پول دیجیتالی، گمنامی، شبکه TCP/IP، غیربلادرنگ، شبکه خصوصی، شیءگرا، کنترل کننده .*

۱- مقدمه

تجارت الکترونیک پدیده ای نو بر فعالیتهای تجاری و اقتصادی با استفاده از روشهای الکترونیکی است و به دو صورت مستقیم و غیر مستقیم وجود دارد. سه عنصر اولیه در تجارت الکترونیک محاسبه، ارتباط و ذخیره سازی است و بهره وری سیستم با استفاده از این سه عنصر بالا میرود. یکی از مهمترین مراحل در چرخه تجارت

الکترونیک، پرداخت پول میباشد. اصولاً پرداخت یکی از اجزاء اصلی تجارت بوده و هیچ معامله ای بدون پرداخت کامل نیست. بدون یک مکانیزم مناسب برای پرداخت الکترونیکی، کاربرد تجارت الکترونیک نامفهوم است. پول دیجیتالی پیشنهاد شده توسط تعداد زیادی از دانشمندان ، ترکیب سه مشخصه فوق به صورت تئوری را ممکن میسازد و محیطی امن، ساده و گمنام را در شبکه اینترنت ایجاد میکند .

۲- کلاس بندی مدلهای پول دیجیتالی:

دو ویژگی غیر بلادرنگ و بلادرنگ بودن و گمنامی و قابلیت ردیابی، می تواند با هر کدام از مدلهای پول دیجیتالی ترکیب شود و مجموعه ای از چهار ترکیب، قابل ردیابی و بلادرنگ ، قابل ردیابی وغیربلادرنگ، گمنام وبلادرنگ، گمنامی و غیر بلادرنگ بوجود آورد .

۱-۲- مدل گمنام و بلادرنـــگ

در مدل گمنام و بلادرنگ ، حضور بانک در قرارداد پرداخت برای کنترل پرداخت پول الزامی است. بانک کنترل میکند که آیا قبلا پول پرداخت شده است ؟ در این حالت پروتکل های پرداخت و واریز به حساب با هم ترکیب میشوند و از دو باره خرج شدن روز پول دیجیتالی جلوگیری میکنند . با این وجود مشخص نیست چه کسی از رمز پول دو بار استفاده میکند ، مشتری یا فروشنده ؟

سیستمی با بانک اطلاعاتی بزرگی در پروتکل پرداخت ، برای کنترل خرج شدن مجدد پول پیشنهاد شد .[7] البته سیستم پیشنهادی کارایی وقابلیت اجرایی را بشدت محدود می کرد .

بالاخره پس از تحقیقات فراوان ، گروه دیگری از دانشمندان سیستم جدیدی با بانک اطلاعاتی کوچکتری پیشنهاد کردند که با سیستم پرداخت الکترونیکی سازگار بود . ولی هنوز بانک در پروتکل پرداخت حضور داشت .[8] در این سیستم محاسبات زیاد ی انجام میشد و در نتیجه بانک را به اشتباه می انداخت .

بعدا همین گروه ، از مفهوم حساب گمنام استفاده کردند و برای سادگی کار روشهایی خاصی را برای ایجاد گمنامی در سیستم بکار بردند. حساب گمنام ، نوعی حساب است که در آن هویت دارنده حساب مشخص نیست و مشتری قبل از انجام معامله پول را به حساب گمنامی واریز میکند وسپس از این حساب برای خرید محصولات و خدمات استفاده میکند .

مزیت اصلی این مدل ، جلوگیری از دو بار خرج شدن رمز پول دیجیتالی است .

۲-۲- مدل گمنام وغیر بلادرنگ

در سیستم پول دیجیتالی غیر بلادرنگ ، حجم کار ارتباطی ومحاسباتی بانک در قرارداد پرداخت کاهش می یابد و نیازی به مداخله بانک در پرداخت های پول دیجیتالی به صورت غیر بلادرنگ نیست . در این صورت پول دیجیتالی در معرض خطر دوبار خرج شدن قرار میگیرد ولی فروشنده ، تا زمانی که قرار داد پرداخت تکمیل نشده نمی تواند بانک را مجبور کند مقدار رمز پول دیجیتال را ثبت کند . بعنوان راه حلی، پول دیجیتالی غیر بلادرنگ هویت خرج کننده را برای بار دوم ، پس از دریافت اطلاعات فاش می کند.

برای سیستمی با قابلیت ردیابی، می توان با داشتن اطلاعاتی صحیح از هویت مشتری دو بارخرج کننده پول دیجیتالی را فاش کرد. در اینصورت حالت گمنامی سیستم پیچیده تر می شود.در حالت گمنام، هویت بطور ماهرانه ای در پول دیجیتالی کد می شود و مشتری با توجه به هویت کد شده اطلاعات کمی در طول پروتکل پرداخت منتشر میکند که این اطلاعات برای تشخیص هویت مشتری کافی نیست، با این وجود میتوان هویت مشتری را تشخیص داد .

پول دیجیتالی گمنام غیربلادرنگ از این نظریه برای کشف هویت دو بار خرج کننده ، استفاده میکند. با وجود عنصری خود بازبین در داخل رمز پول دیجیتال ، کسی که پول دیجیتالی را دریافت می کند میتواند بدون دخالت بانک مقدار پول را ببیند. جالب است به این نکته توجه شود که رمز پول دیجیتالی واقعی و رمز پول دیجیتالی

واریزشده به حساب با هم متفاوتند و رمز پول دیجیتال در صورتی تسویه میشود که واقعی باشد و هنوز تسویه نشده باشد .

مشکل پول دیجیتالی گمنام و غیر بلادرنگ تشخیص هویت کسی است که رمز پول دیجیتالی را دو بارخرج میکند. و بین بانک و مشتری محیط نا امن جهت پیاده سازی سیستم پول دیجیتالی بوجود می آید .

برند سیستم پیشنهادی اش بر مبنای دو نظزیه امضاء دیجیتال و مسئله ارائه اولین سفارش کارمیکند. این سیستم تقریبا جزء کار آمد ترین سیستم های غیر بلادرنگ با قابلیت رد یابی است . [2]

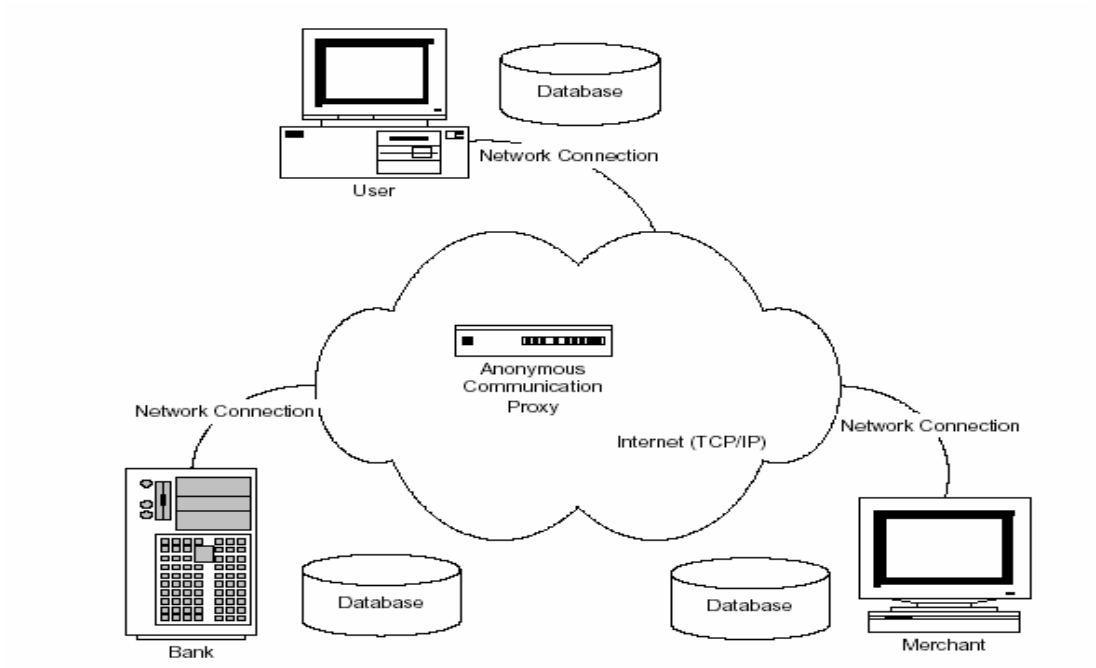
ازنظر فنی، طرح گمنام غیر بلادرنگ قوی تر از طرح گمنام بلادرنگ است، زیرا طرح گمنام غیر بلادرنگ براحتی می تواند طرح گمنام بلادرنگ را تغییر بدهد. به همین دلیل طرح گمنام غیر بلادرنگ اهمیت بیشتری دارد .

طرح غیر بلادرنگ برای معاملات کوچک و غیر بلادرنگ برای معاملات بزرگ استفاده میشود و این نقطه تعادلی بین امنیت وکارایی ایجاد میکند.

۳- مدل پول دیجیتالی برند

طرح پول دیجیتالی برند، نوعی پول دیجیتالی گمنام غیربلادرنگ است که بر اساس تئوری اعداد کار می کند که بعنوان "مسئله ارائه"شناخته شده است.[1] مسئله ارائه معادل محاسبات مشکل لگاریتم گسسته تا در سیستم RSA می باشد. ولین مسئله ارائه بر اساس طرح پول دیجیتال توسط برند پیشنهاد شده است . طرح برند ، یک سری اثبات ریاضی برای امنیت سیستم ارائه می دهد.

پول دیجیتالی، سیستم پرداختی برای انجام معاملات غیربلادرنگ بصورت امن است و هویت پرداخت کننده را فاش نمی کند. مدل اصلی پول دیجیتالی شامل سه بخش : بانک ، مشتری و فروشنده و چهار پروتکل : تنظیم حساب، برداشت ازحساب ، پرداخت و واریز به حساب می باشد. پول دیجیتالی عبارت از چرخه ای از نشانه های رمز دار بین سه جزء است که از طریق پروتکل های مذکور با هم ارتباط دارند(شکل -۱).



شکل –۱) سیستم پول دیجیتالی

طرح برند نوعی پول دیجیتالی غیر بلادرنگ و غیر قابل ردیابی است، پرداخت با این دو ویژگی و ترکیب در یک طرح کار ساده ای نیست. طرح برند، روش مناسبی برای شبیه سازی دو جنبه مهم امنیت و گمنامی بکار میبرد. طرح برند با استفاده ازامضاء دیجیتالی و ارائه ساخته می شود.[6] بانک روی رمز پول دیجیتال را امضاء میکند، با امضای بانک برروی پول دیجیتال ، مشتری برای استفاده از پول محدود می شود، با این محدودیت مشتری فقط می تواند خروجی را تغییر دهد واطلاعات هویت مشتری دست نخورده باقی میماند. در نتیجه مشتری نمی تواند ساختار داخلی رمز را خراب کند و مالک به ردیابی کسی که در طول پردازش رمز پول را دوبار خرج میکند، کمک میکند. این محدودیت از اینکه بانک بتواند رمز پول های برداشته شده و واریز شده از/به حساب را با هم تطبیق دهد، جلوگیری میکند و در نتیجه مشتری گمنام باقی میماند.

مشتری برای استفاده از رمز پول در پروتکل پرداخت نیاز به اثبات مالکیت خودش روی رمز دارد و مالکیت او بواسطه اطلاعات نمایش داده شده بر روی رمز، اثبات می شود . در فرضیات لگاریتم گسسته ودفی-هلمن[14]، هیچ کس به غیر از مالک رمز قانونی نمی تواند مالکیت را ثابت کند. علاوه بر این ، مشتری در مدت زمان اثبات

مالکیت ، اطلاعاتی ارائه میدهد، که تنها قسمتی از اطلاعات ، هویت مشتری را فاش نمی کند ولی با دو قسمت اینکار انجام می شود . در این روش بانک میتواند کسی که از رمز پول دوباراستفاده میکند را ردیابی کند، یا به عبارتی طرح ، پس از دریافت اطلاعات وسیله ای برای نمایش هویت دوبارخرج کننده فراهم می کند.

۴- ارسال پیام در شبکه اینترنت بصورت گمنام

یکتا بودن آدرس IP عامل موثری برای پیدا کردن شخص و موقعیت جغرافیایی آن است . کاربران Dialup، در شبکه واقعی نیستند، با این که شناخت کاربر در هر موقعیت جغرافیایی که با اینترنت در ارتباط باشد کار مشکلی است ولی ISP به طرف مقابل کمک میکند تا برخی اطلاعات قابل تغییر کاربر را بدزد و به حریم شخصی کاربران تجاوز کند. این کار برای کاربران روی خط بیشتر اتفاق می افتد . بنابراین اتصال ISP ها در حالت گمنامی بلادرنگ خیلی ضعیف است .

زمانیکه هویت کاربردر اثر مراجعات سلسله مراتبی در وب ردیابی می شود، دشمن راحتتر میتواند به صورت دو مرحله ای حمله کند. در اولین مرحله دشمن، آدرس IP وب سایت فعال را در بانک اطلاعاتی خود ذخیره میکند، در مرحله بعدی ، دشمن برای شخص دام می گذاردو مشخصات فردی و آدرس IP شخص را بدست می آورد، این نوع حمله بسیار خطر ناک است.

برای جلوگیری از این حمله های خطرناک چوم Mix-net را معرفی کرد ، و تکنولوژی ارتباط گمنام را بنا کرد. [9,10] در این سیستم، فرستنده و گیرنده با یک زنجیر به نام Mix به یکدیگر متصل میشوند. هر Mix در زنجیر، اطلاعات شناخته شده ای را در پیغام ورودی سانسور میکند و سپس خروجی آن را به Mix بعدی میفرستد، در این روش ساختار مسیریابی و رمز نگاری با استفاده از کلید عمومی میباشد. سیستم های ارتباطی گمنام دیگری مثل مسیریابی لایه لایه[3]، شبکه مستقل [12, 4] وپناهگاه مجاز [13, 5,11] هم وجود دارد که زیر بنای همه اینها Mix-net است .

در این مقاله ، از نظریه چوم ، برای توسعه مدل ارتباطی شبکه خصوصی سیستم پول دیجیتالی استفاده می شود. مدل توسعه یافته، محیط ارتباطی گمنامی است که بعنوان زیر شبکه ضروری Mix-net کامل یا سیستم لایه لایه رفتار میکند .

۵- گسترش گمنامی در شبکه TCP/IP

سیستم پول دیجیتالی ، پروتکلTCP/IP را درکلاس شبکه قرار می دهد و آنرا بعنوان یک جعبه سیاه ارتباطی بکار میبرد . با وجود اینکه مسئله گمنامی ، ذاتا در TCP/IP وجود دارد ولی کلاس شبکه تغییری در ساختار موجود TCP/IP ایجاد نمیکند . تنها راه برای حل مسئله گمنامی نهفته در TCP/IP ، توسعه پروتکل اصلی با همان ساختار موجود و بدون هیچ گونه تغییر ی، می باشد.

کلاس شبکه در سیستم پول دیجیتالی، از روش TCP اصلی برای ایجاد ارتباط استفاده می کند و این باعث میشود گمنامی درستی بوجود نیاید . چرا که دو طرف رابطه ، از آدرس IP یکدیگر اطلاع دارند . با وجودی که ممکن است آگاهی از آدرس IP ، هویت درست ارتباط را نشان ندهد ولی سطح گمنامی پول دیجیتالی را کاهش میدهد .

راه حل پیشنهادی برای ایجاد گمنامی در TCP/IP توسعه کلاس شبکه می باشد . راه حل پیشنهادی ، با معماری شیئ گرای استفاده شده در ساختار پول دیجیتالی سازگار است وبرای اینکار از شبکه خصوصی و کنترل کنندها استفاده میشود.

۶- شبکه خصوصی

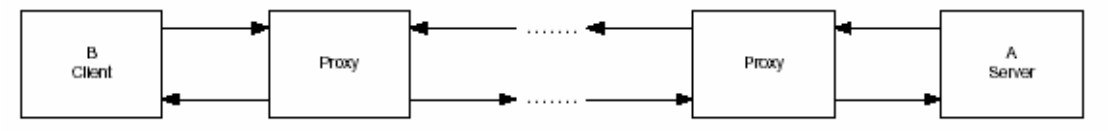
شبکه خصوصی کلاس گسترش یافته ای از شبکه برای ایجاد ارتباط گمنام در سیستم پول دیجیتالی است . در شبکه خصوصی به جای ارتباط مستقیم کاربر با Server ، به کنترل کننده گمنام (ACP) وصل می شود و بسته اطلاعاتی را به ACP و ACP بسته را به Server میفرستد . با این روش ، کاربر گمنام می ماند ، مگر اینکه ACP با بانک یا فروشنده توطئه کرده باشند . ولی در حالت عادی ، Server فقط ACP را بعنوان فرستنده پیام

می شناسد . برای گمنامی بیشتر ACP ها (حداقل ۲ ACP متفاوت ومستقل) به شکل زنجیر کانال ارتباطی گمنام مورد نیاز می باشد و بسته قبل از اینکه به مقصد نهایی برسد از میان ACP ها عبور میکند . در این روش زیر مجموعه ای از مسیر یابی های لایه لایه وجود دارد [3].روشی که در شبکه خصوصی استفاده میشود ، بیشترین گمنامی را در سیستم پول دیجیتالی ایجاد میکند ، ولی نمیتواند حمله های فعالی که اطلاعات شبکه را استراق سمع و ترافیک شبکه را مانیتور میکند راخنثی کند . برای بالا بردن درجه گمنامی بر ضد حمله های فعال، استفاده از رمز نگاری کلید عمومی برای شبکه خصوصی الزامی است .

۷- کنترل کننده های متعدد

روش پیشنهادی با کنترل کننده های متعدد در شبکه خصوصی ، به این صورت که کنترل کننده شبکه خصوصی مستقیما به Server وصل نمی شود ، به کنترل کننده شبکه خصوصی دیگری وصل میشودهمانطور که در شکل-۲ مشاهده میشود . تعداد کنترل کننده شبکه خصوصی به درخواست سطح گمنامی ارتباط ، بستگی دارد.هر چه تعداد کنترل کننده های شبکه خصوصی بیشتر باشد سطح گمنامی شبکه بالاتر میرود .

در این ارتباط سریال ، مهاجم باید کنترل کننده های شبکه خصوصی را با هویت Client تطبیق دهد .ولی با وجود سطح گمنامی بالایی که ایجاد می شود ، هزینه ها افزایش میی ابد، سرباربرقراری ارتباط زیاد میشود و زمان زیادی برای عبور بسته های اطلاعاتی بصورت گمنام در شبکه تلف می شود .



شکل - ۲) مدل شبکه خصوصی با کنترل کننده های متعدد

۸- نتیجه گیری

در این مقاله ابتدا طرح پول دیجیتالی برند که پول دیجیتالی از نوع غیر بلادرنگ و گمنام است، معرفی شد و سپس برای ایجاد گمنامی بیشتر در این سیستم در شبکه TCP/IP اینترنت راه های مختلفی که توسط دانشمندان متعددی پیشنهاد شده بود مورد بررسی قرار گرفت . استفاده از بانک اطلاعاتی بزرگ که البته سیستم پیشنهادی کارایی وقابلیت اجرایی را بشدت محدود می کرد . و بانک اطلاعاتی کوچک ، در این سیستم با وجود سازگاری باسیستم های پرداخت الکترونیکی ، محاسبات زیادی انجام میشد و در نتیجه بانک را به اشتباه می انداخت . سپس استفاده از حسابهای گمنام پیشنهاد شد و مزیت اصلی این مدل ، جلوگیری از دو بار خرج شدن رمز پول دیجیتالی بود.

روش Mix-net ، در این روش ساختار مسیریابی و رمز نگاری با استفاده از کلید عمومی مطرح شد که روش نسبتا مناسبی میباشد ، و به دنبال آن مدل لایه لایه ای وچندین روش دیگر مطرح شد و در نهایت توسعه شبکه خصوصی و استفاده از کنترل کننده های متعدد که از روش Mix-net برگرفته شده است گمنامی کاربر را تا حد زیادی افزایش میدهد ولی هزینه ها و سربارارتباطی شبکه را زیاد میکند و زمان زیادی برای عبور بسته های اطلاعاتی از شبکه تلف میکند .

منابع

[1] Brands, S. (1993). “An Efficient Offline Electronic Cash System Based On The Representation Problem.” CWI Technical Report CS-R9323.
[2] Brands, S. (1993b). “Untraceable Offline Cash in Wallets with Observers.” Advances in Cryptology, Crypto ’93, LNCS 773. Springer Verlag. 302-318.149
[3] Syverson, P. F., Goldschlag, D. M., Reed, M. G. (1997). “Anonymous onnections and Onion Routing.” IEEE Symposium on Security and Privacy
[4] Goldberg, I. and Shostack, A. (1999). “Freedom Network 1.0 Architecture and Protocols.” Zero Knowledge Systems.
[5] Rennhard, M., Rafaeli, S., Mathy, L., Plattner, B., Hutchison, D. (2001). “An Architecture for an Anonymity Network.” IEEE 10th Intl. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. 165-170.
[6] Schnorr, C. P. (1990). “Efficient Identification and Signatures for Smart Cards.” Advances in Cryptology, Crypto’89. Springer-Verlag. 239-252.

[7] Chaum, D. (1985). “Security Without Identification: Transaction Systems to Make Big Brother Obsolete.” Communications of the ACM. 28. 1030-1044.
[8] Camenisch, J., Piveteau, J., Stadler, M. (1994). “An Efficient Electronic Payment System Protecting Privacy.” Third European Symposium on Research in Computer Security (ESORICS 94). 207-215.
[9] Chaum, D. (1982). “Blind Signatures for Untraceable Payments.” Advances in Cryptology, Crypto ’82. 199-203.
[10] Chaum, D. (1982b). “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.” Communications of the ACM. 4(2).
[11] Freedman, M. J. (2000). “Design and Analysis of an Anonymous Communications Channel for the Free Haven Project.” Massachusetts Institute of Technology:Bachelor Thesis.
[12] Boucher, P., Shostack, A., Goldberg, I. (2000). “Freedom System 2.0 Architecture.”Zero Knowledge Systems.
[13] Dingledine, R. R. (2000). “The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven.” Massachusetts Institute of Technology: Master Thesis.
[14] Diffie, W. and Hellman, M. (1976). “New Directions in Cryptography.” IEEE Transactions in Information Theory. 22. 644-654.