

## ارائه یک طرح امضای وکالتی آستانه با قابلیت ابطال سریع جدید در چک الکترونیکی

گیلان‌دخت مفسر باقری<sup>۱</sup>، محمد بهشتی آت‌شگاه<sup>۲</sup>، رضا ابراهیمی آتانی<sup>۳\*</sup>

۱ - کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه گیلان ۲ - کارشناسی ارشد، دانشگاه صنعتی شریف

۳ - استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان

(دریافت: ۲۵/۱۰/۹۱۰۱، پذیرش: ۰۹/۰۴/۹۲)

### چکیده

مهم‌ترین فاکتور اعتبار بخشی به اسناد الکترونیکی به‌ویژه چک الکترونیکی که شامل بزرگ‌ترین ارقام تراکنشی در تجارت الکترونیکی می‌شود، بحث امضای روی آن جهت اعتبار بخشی به این سند الکترونیکی است. در میان انواع امضاهای دیجیتال، امضای وکالتی به‌عنوان نمونه‌ای از امضاهاست که در آن صاحب اصلی امضا قابلیت امضای خود را در اختیار فردی به نمایندگی خویش قرار می‌دهد تا فرد نماینده به وکالت از وی، قادر به تولید امضاء بر روی اسناد و مدارک باشد. یکی از چالش‌های پیش‌رو در این زمینه این است که صاحب اصلی امضاء قادر به جلوگیری از امضاهای ناخواسته باشد و هر لحظه امکان جلوگیری از تولید امضاء توسط نمایندگان سوءاستفاده‌گر را دارا باشد. در این مقاله، با افزودن قابلیت ابطال سریع به طرح امضای وکالتی آستانه چنین قابلیت‌هایی برای چک‌های الکترونیکی فراهم آورده شده است. طرح ارائه شده در مقابل جعل صاحب امضاء و همچنین جعل نماینده امن بوده و دیگر ملزومات امنیتی یعنی قابل تأیید بودن، غیرقابل انکار بودن، قابل شناسایی بودن و جلوگیری از سوء استفاده که برای یک طرح امضای وکالتی آستانه ضروری می‌باشند را برآورده می‌سازد.

**واژه‌های کلیدی:** امضاء دیجیتال، طرح امضاء وکالتی، امضای وکالتی آستانه، ابطال سریع وکالت، چک الکترونیکی.

### ۱. مقدمه

چک الکترونیکی یک ابزار نوین پرداخت است که متشکل از امنیت و سرعت بوده و دارای بازدهی تمام تراکنش‌های الکترونیکی همگون و توأم با زیرساخت‌های قانونی گسترش یافته می‌باشد. چک الکترونیکی قابلیت جایگزینی با چک‌های کاغذی را در فرآیندهای تجاری دارد. یکی از چالش‌های به‌کارگیری چک الکترونیکی قابلیت جایگزینی با چک‌های کاغذی را در فرآیندهای تجاری دارد. یکی از چالش‌های به‌کارگیری چک الکترونیکی، بحث تقویت امضاهای الکترونیکی به‌منظور به‌کار بردن الگوریتم‌های فعال پرداخت است. مفهوم چک الکترونیکی در طی پروسه‌ای پس از ابداع ecash توسط چوم<sup>۱</sup> در سال ۱۹۸۸ ارائه شد [۳-۱]. چک‌های الکترونیکی همچون چک‌های کاغذی دارای الزام قانونی برای پرداخت هستند و به‌جای امضاهای دست‌نویس، از امضاهای دیجیتالی در آنها استفاده می‌شود. چک الکترونیکی، یک سند دیجیتالی امضاء شده به‌صورت الکترونیکی است که می‌تواند سایر اسناد و اطلاعات صورت‌حساب، اعلامیه‌ها، پشت‌نویسی و واگذاری را با خود به‌همراه داشته باشد. در مورد چک کاغذی، با وجود الزام قانونی پرداخت از طرف صادرکننده، به‌دلیل مشکلاتی همچون موجود نبودن وجه کافی، قطعیت پرداخت

بانک‌ها که قلب تپنده جریان پولی و بدنه اقتصادی جامعه می‌باشند، همواره در چالش‌های فناوری‌های قدیم و تغییر به فناوری‌های جدید، درگیر هستند. وقتی سایر اجزاء یک جامعه با فناوری‌های جدید تغییر می‌کنند، اگر بانک‌ها نتوانند خود را به‌روزرسانی کنند، اقتصاد ضعیف و سیستم بانکی ناکارآمد جلوه خواهد کرد. از جمله تغییرات نهادی امور مالی و اقتصادی که به‌واسطه رشد خیره‌کننده اینترنت اتفاق افتاده و به‌طور فزاینده‌ای در حال گسترش است، رواج بانکداری الکترونیکی و در نتیجه پیدایش بانک‌های مجازی و یا اینترنتی است.

مهم‌ترین ویژگی این بانک‌ها حذف معضل موقعیت فیزیکی بین بانک و مشتری است. یکی از چالش‌های بزرگ بانکداری الکترونیکی که تا به امروز در اجرایی شدن آن بسیاری از کشورها به مشکلات فراوان برخورد کرده‌اند، تبدیل خدمات چک سنتی به چک الکترونیکی و پیاده‌سازی و اجرایی کردن قوانین پیرامون آن می‌باشد.

<sup>1</sup> chaum

\* ایمیل نویسنده پاسخگو: rebrahimi@guilan.ac.ir