Culminatin of Law Quarterly

14nd Year, No.2, Summer 2023

http://dx.doi.org/10.22034/thdad.2022.1972684.2295

The legal validity of data containing payment information based on cryptocurrency

Hossein Sadeghi[1], **Fatemeh Noori***[2], **Medi Naser**[3]

1. Assistant Professor of Law, Department of Business, Faculty of Entrepreneurship, University of Tehran, Tehran, Iran.

2. PhD in private law, Faculty of Law, University of Judicial Sciences and Administrative Services, Tehran, Iran.

3. PhD student in private law, Faculty of Law, University of Judicial Sciences and Administrative Services, Tehran, Iran.

Article Type:

Original Research

Pages: 37-63

Received: 2022 November 14

Revised: 2022 November 22

Accepted: 2022 December 21

Abstract

One of the uses that can be from cryptocurrency as a type of digital money is to use it as a means of payment. The most important legal issue in this regard is whether payment information based on cryptocurrency that is transferred and maintained in the form of electronic communication and data message, can be considered as a valid document? As long as the document of this information is not proven, the cryptocurrency payer cannot be considered clear from obligation in front of the recipient.

The present study is a fundamental type and research method is descriptive-analytic.

By dissection the legal ingredients of the document and its flow in e-documents and finally matching it with payment information based on cryptocurrency, it can be found that the information of this payment by the existence of a secure information system, the use of digital signature, asymmetric encryption algorithm and encrypted hash, In the stage of creation and at the time of registration of information, firstly is considered an electronic document and secondly is a valid document in the courts to prove payment.

Keywords: Cryptocurrency, Data, Electronic Document, legal validity

* Corresponding Author: fnouri67@yahoo.com

فصلنامه تعالی حقوق
سال چهاردهم، شماره ۲، تابستان ۱۴۰۲
http://dx.doi.org/10.22034/thdad.2022.1972684.2295

استنادپذیری حقوقی داده‌های متضمن اطلاعات پرداخت مبتنی بر رمزارز

حسین صادقی[۱]، فاطمه نوری*[۲]، مهدی ناصر[۳]

۱. استادیار حقوق گروه کسب و کار دانشکده کارآفرینی، دانشگاه تهران، تهران، ایران.

۲. دانش آموخته دکتری حقوق خصوصی، دانشکده حقوق، دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.

۳. دانشجوی دکتری حقوق خصوصی، دانشکده حقوق، دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.

نوع مقاله: علمی پژوهشی
صفحات: ۳۷-۶۳

تاریخ دریافت: ۱۴۰۱/۰۸/۲۳
تاریخ بازنگری: ۱۴۰۱/۰۹/۰۱
تاریخ پذیرش: ۱۴۰۱/۰۹/۳۰

چکیده

یکی از استفاده‌هایی که می‌توان از رمزارز به عنوان قسمی از پول دیجیتال داشت، استفاده از آن به عنوان وسیله پرداخت است. مهمترین مسأله حقوقی در این رابطه آن است که آیا اطلاعات پرداخت مبتنی بر رمزارز که در قالب ارتباط الکترونیک و داده پیام ایجاد، انتقال و حفظ می‌شود، می‌تواند به عنوان یک سند معتبر در نظرگرفته شود؟ مادامی که سندیت این اطلاعات اثبات نشود پرداخت‌کننده رمزارز نیز نمی‌تواند به استناد عمل خود در مقابل دریافت‌کننده بری‌الذمه تلقی شود.

پژوهش حاضر، از نوع بنیادی و روش تحقیق توصیفی- تحلیلی می باشد.

با بررسی ارکان حقوقی سند و جریان آن در اسناد الکترونیک و نهایتاً تطبیق آن با اطلاعات پرداخت مبتنی بر رمزارز می‌توان دریافت که اطلاعات این پرداخت به واسطه وجود سیستم اطلاعاتی مطمئن، بهره‌گیری از امضای دیجیتال، الگوریتم رمزنگاری نامتقارن و هش رمزگذاری شده هم در مرحله ایجاد و هم در زمان ثبت اطلاعات اولاً یک سند الکترونیک محسوب می‌شود؛ ثانیاً سندی معتبر و قابل ارائه در محاکم جهت اثبات پرداخت می‌باشد.

واژگان کلیدی: رمزارز، داده پیام، اسناد الکترونیک، استنادپذیری حقوقی

*. نویسنده مسئول: fnouri67@yahoo.com

درآمد

یکـــی از کارکردهای رمزارزها به عنوان یـــک ارز یا پول دیجیتال، کارکرد پولی آنهاست. با عنایت به این عملکرد، می‌توان از رمزارز در پرداخت مابه‌ازای قراردادی و یا ایفای تعهدات در فضای داخلی و بین‌المللی استفاده نمود. اما با توجه به اینکه رمزارزها ماهیت دیجتالی دارند، پرداخت توســط آنها هم در فضای الکترونیکی انجام می‌شود و اطلاعــات پرداخت هم در همین فضا بدون هرگونه نظــارت مرکزی حفظ و نگهداری می‌شود، جریان این کارکرد پولی مشروط است به اینکه بتوان به لحاظ حقوقی اطلاعات مربوط به انتقال وجوه توسط رمزارز را به‌عنوان دلیلی جهت اثبات پرداخت درنظرگرفت تا متعاقب آن، ارسال‌کننده وجه به استناد چنین پرداختی بری‌الذمه تلقی شود. بنابراین سوال اصلی تحقیق این است که آیا می‌توان اطلاعات پرداخت مبتنی بر رمزارز را دلیل از ســـنخ ســـند تلقی نمود و از آن برای اثبات پرداخت استمداد گرفت؟ در این صورت ارزش اثباتی آن تا چه اندازه است؟

همانطور کـــه می‌دانیم مطابق مبانی حقوقی و مـــاده ۱۲۵۸ قانون مدنی یکی از دلایلی که در اثبات ادعا مورد اســـتفاده قرار می‌گیرد ســـند است. از سوی دیگر در ارتباطات الکترونیک یک داده‌پیام با وجود شـــرایطی می‌تواند ســـند محســـوب شده و چنانچه شـــرایط ماده ۱۴ قانون تجارت الکترونیکی را دارا باشـــد ســـندی معتبر تلقی می‌گـــردد. در پژوهش حاضر برآنیم اطلاعات پرداخت مبتنی بر رمزارز را به عنوان یک داده‌پیام[1] که در بســـتر الکترونیک ایجاد، حفظ و نگهداری می‌شـــود بررسی نموده و با مبانی حقوقی مذکور تطبیق داده تا نهایتاً سندیت آن تبیین و اثبات گردد.

در راســـتای این بررسی چند نکته حائز اهمیت است اولاً در پرداخت رمزارزی، ســـندی مجزا صادر نمی‌شـــود یعنی پرداخت و اطلاعات پرداخـــت در هم تلاقی پیدا می‌کنند. مکانیزم پرداخت، خود بخشـــی از سند پرداخت است. ثانیاً یکی از ویژگی‌های سیســـتم‌های پرداخت الکترونیک امروزی، وجود یک نظـــارت مرکزی بر ارتباط میان پرداخت‌کننده و دریافت‌کننده اســـت. همین سیستم مرکزی پس از پرداخت، با صدور انواع اسناد پرداخت در اشکال مختلف و ثبت اطلاعات در سیستم‌های خود، کار را برای

---

۱. بند الف ماده ۲ قانون تجارت الکترونیکی: داده پیام (Data Message): هرنمادی از واقعه، اطلاعات یا مفهوم است که‌با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت،ذخیره یا پردازش می‌شود.

اثبات آســـان نموده اســـت. لکن در پرداخت رمزارزی مساله متفاوت است. در پرداخت توسط رمزارز، سیستمی با نظارت مرکزی وجود ندارد که اطلاعات را نگه دارد که با ارائه آن بتـــوان پرداخت را ثابت نمود بلکه اطلاعات پرداخت در دفتر کل الکترونیکی به نام بلاکچین که در دسترس همگان قرار دارد، بدون هرگونه نظارت مرکزی، ثبت می‌شود. ثالثاً فرایند پرداخت و ثبت آن در فضای باز اینترنت انجام شده که در دسترس همگان قرار دارد و قابلیت هرگونه تغییر و دستکاری در این سیستم وجود دارد.

برخـــی از ارزهای مجازی مانند بیت کویـــن عملکرد پولی را ارائه می‌دهند. برخی دیگر مانند اوراق بهاداری عمل می‌کنند که بازده آنها با عملکرد تجاری مرتبط اســـت. به عنوان مثال، یکی از مبادلات ارزهای مجازی، Binance، در سال ۲۰۱۷ یک ارز مجازی به نام BNB صادر کرد. علاوه بر هزینه‌های تخفیف شده برای معاملات در Binance، BNB با صرف ۲۰ درصد از ســـود ســـالانه Binance قول بازخرید توکن های BNB را می‌دهد. (ماکاتو یانوو همکاران، ۱۴۰۱، ۱۴۶)

موضوعات مذکور موجب می‌شـــود که احتساب اطلاعات پرداخت به عنوان یک سند محکمه پسند با ایراد مواجه شده و اهمیت بررسی حقوقی آن را هویدا نماید. پروسه پرداخت باید کلیه شـــرایط مطمئه را دارا باشد تا در نهایت سند پرداخت صحیح و قابل اســـتنادی از آن برداشـــت شود تا بتوان از آن در محاکم اســـتفاده نمود. با توجه به این موضـــوع ابتدا ضرورت دارد فرایند پرداختی را کـــه منتهی به ایجاد و ثبت این اطلاعات می‌شـــود مورد بازخوانی قرار دهیم و سپس ارکان سند الکترونیک را بررسی نموده و با اطلاعات پرداخت مبتنی بر رمزارز تطبیق داده تا مشـــخص شـــود آیا می توان از آن به عنوان ســـند معتبر حقوقی در جهت اثبات پرداخت استفاده نمود یا خیر؟ برای پاسخ به این پرســـش اصلی تحقیق، قانون داخلی یعنی قانون تجارت الکترونیکی و قانون نمونه بین‌المللی مصوب کمیسیون تجارت حقوق بین‌الملل سازمان ملل(آنسیترال) درخصوص تجارت الکترونیک (مصوب۱۹۹۶) که محبوب‌ترین مدل نیز دانســـته شـــده است (آلان داویدســـون, ۱۴۰۰, ص. ۱۳۲) و همچنین کنوانسیون استفاده از ارتباطات الکترونیک مصوب ۲۰۰۵ مورد بررسی قرار خواهد گرفت.

مقاله حاضر پژوهشـــی بدیع و نو می‌باشـــد و اگرچه مقالات متعددی در زمینه رمزارزها در ابعاد مختلف اقتصادی، فنی و حقوقی به رشته تحریر درآمده لکن مقاله با

یا کتابی که به بررسی موضوعات مندرج در این نوشته بپردازد در تحقیقات مؤلف یافت نشد.

۱. مروری بر سیستم پرداخت مبتنی بر رمزارز

فرایند پرداخت رمزارزی متشکل از سه مرحله است: ایجاد حساب، تایید تراکنش، نگهداری تراکنش. مرحله اول را کیف پول‌ها تأمین می‌کنند. مرحله دوم توسط گره‌های شبکه تأمین می‌شود و حفظ و نگهداری تراکنش هم وظیفه دفتر کلی به نام بلاکچین است. در راستای هدف تبیین سیستم پرداخت لازم است به طورجداگانه هرمرحله، بررسی گردد.

۱-۱. ایجاد حساب

هر شخصی برای اینکه بتواند از سیستم پرداخت مبتنی بر رمزارز جهت انجام تراکنش یا وصول مبالغ استفاده نماید لازم است ابتدا اقدام به ایجاد حساب نماید.

ایجاد حساب توسط کیف پول‌های الکترونیکی انجام می‌شود. کیف پول، یک برنامه است که بر روی نرم‌افزار یا سخت‌افزار مورد نظر شما نصب شده و عملیات وصول و ارسال رمزارز در آن انجام می‌شود.

با نصب یک کیف پول، کیف پول اقدام به ایجاد یک کلید خصوصی می‌نماید که از روی آن کلیدعمومی ایجاد شده و سپس آدرس کیف پول تولید می‌شود.[۱] این مسیر یک طرفه است و امکان ساخت کلیدخصوصی از روی کلیدعمومی و آدرس کیف پول وجود ندارد. بنابراین اگرچه آدرس کیف پول و کلید عمومی جهت انجام تراکنش در دسترس همگان قرار می‌گیرد اما کلیدخصوصی باید محرمانه نگاه داشته شده و در مکان ایمنی حفظ گردد.

از این پس، صاحب کیف پول می‌تواند با درج امضای دیجیتال خود از طریق کلیدهای عمومی و خصوصی -که در مبحث اعتبار امضاهای الکترونیکی، نحوه عملکرد آن تبیین گردیده است- اقدام به دریافت یا پرداخت مطمئن رمزارز نماید.

در هر ارسال وجه از دو جفت کلید استفاده می‌شود کلید عمومی و خصوصی

---

۱. کلیدعمومی و خصوصی یک رشته از اعداد یا حروف نامفهوم هستند که برای ایجاد امضای دیجیتالی و رمزنگاری داده‌ها تولید می‌شود. این دو کلید متناظر یکدیگر بوده و باهم مرتبطند.

فرستنده و کلید عمومی و خصوصی گیرنده. از کلید عمومی برای رمزگذاری و یا تأیید هویت و از کلید خصوصی برای امضای پیام و رمزگشـــایی اســـتفاده می‌شود (Satoshi Nakamoto, 2008, p. 2). به این شـــکل که فرســـتنده از کلید عمومی گیرنده برای رمزکردن اطلاعات تراکنش و از کلید خصوصی خود برای درج امضای دیجیتال و الصاق به پیام رمز شده و ارســـال برای فرستنده استفاده می‌نماید فرستنده با دریافت پیام از کلید خصوصی خود برای رمزگشـــایی پیام و از کلیدعمومی فرستنده برای تأیید هویت وی و احراز رضایت و اراده او به ارسال پیام استفاده می‌نماید (Xu, 2018, p. 52)

۱-۲. تأیید تراکنش

بعد از انجام تراکنش، و درج امضای دیجیتال توسط فرستنده، اطلاعات پرداخت شامل شـــماره حساب خروجی(فرستنده)، شماره حساب ورودی(گیرنده)، مبلغ و زمان تراکنش، برای شبکه و گره(نود)های[۱] موجود در شبکه ارسال می‌شود.

گره‌ها اطلاعات این تراکنش را دریافت نموده و دو موضوع را بررسی می‌نمایند:

۱) اصالت‌سنجی(انتســـاب)؛ این تکلیف توسط مقایسه و تطابق کلید عمومی و امضای دیجیتال انجام می‌شـــود. نودها بررسی می‌نمایند که آیا کلید عمومی فرستنده با امضای دیجیتالی او مطابقت دارد یا خیر؟ درصورتی که مطابقت احراز شـــود باتوجه به اینکه کلید عمومی و خصوصی متناظر یکدیگر هســـتند، ثابت می‌شود که پیام اصیل است و از صاحب واقعی حساب فرستاده شده است (عباسی, ۱۳۹۷, ص. ۱۴۸).

۲) مالکیت رمزارز؛ وظیفه دیگر نودها بررســـی موجودی حساب فرستنده است. فرســـتنده تنها زمانی می‌تواند مبلغی را ارسال نماید که موجودی داشته باشد و مالک رمزارزهایی باشـــد که قصد ارسال آن را دارد. بررســـی این موجودی توسط گره‌ها و با مقایســـه مجموع ورودی‌ها و خروجی‌های فرستنده انجام می‌شود (Quest, 2018, p. ۱۶۹) ؛ باتوجه به اینکه گره‌ها، لیست تمام تراکنش‌ها را دراختیار دارند امکان دستیابی

---

۱. گره‌ها (Nodes)، رایانه‌هایی هســـتند که بخشـــی از شبکه را تشـــکیل می‌دهند. برای تبدیل شدن به یک گره، کاربـــران باید نرم‌افـــزار مربوطه را بارگیری و نصب نموده که در طی آن تمام بـــلاک‌های بلاکچین(کلیه تراکنش‌های ثبت شـــده در دفتر کل الکترونیکی) از ابتدا در سیســـتم آنها بارگذاری می‌شود. نودها وظیفه نگهداری و به‌روزرسانی بلاکچین را برعهده دارند. نودها در سراسر جهان پراکنده‌اند و هرکسی می‌تواند با دریافت نرم‌افزار آن، نقش گره را ایفا نماید (Biddle, 2017, p. 166)

به این ورودی‌ها و خروجی‌ها برای آنها میسر است.

نودهـــا پس از بررســـی موضوعات مذکور باید در مورد یـــک تراکنش به توافق حداکثری- که به آن اجماع گویند-برسند. وقتی اجماع حاصل شد، تراکنش تایید شده و اطلاعـــات آن به دفتر کل(بلاکچین) اضافه می‌شـــود. در این مرحله تراکنش صحیحاً اتفاق افتاده و دیگر قابل برگشت نمی‌باشد (Quest, 2018, p. 177) و اطلاعات موجود در این دفتر کل، سند پرداخت محسوب می‌گردد.

مســـاله قابل بررسی آن است که از آنجایی که گره‌ها، در فضای اینترنت و بدون نظارت مرکزی هستند پس هم احتمال خرابی سیستم آنها وجود دارد که موجب توقف فعالیت شبکه می‌شود و هم احتمال خرابکاری و نفوذ و دستکاری اطلاعات توسط آنها؛ این مساله را معماری شبکه دفترکل یعنی بلاکچین با دو رویکرد حل نموده است:

۱) وجود سیستم توزیع‌شده و همتابه‌همتا؛ در این سیستم همه گره‌ها به یکدیگر متصل هســـتند بنابراین اگر برخی از سیستم‌ها دچار خرابی شوند سایرین وظایف آنها را انجام می‌دهند و شبکه از حرکت بازنمی‌ایستد و متوقف نمی‌شود. درحالی‌که در یک سیســـتم متمرکز گره‌ها فقط به سیستم مرکزی متصل‌اند و اگر سیستم مرکزی از کار افتد شبکه نیز متوقف می‌شود.

۲) ضرورت اجماع؛ مکانیزم تأیید تراکنش در این شبکه بر اساس نظر حداکثری یا اجماع اســـت. اکثریت گره‌های موجود در شبکه باید یک تراکنش را تأیید نمایند. در این حالت امکان خرابکاری به حداقل ممکن می‌رسد چراکه یک مهاجم برای نفوذ، باید اکثریت گره‌های شـــبکه را در دست داشته باشد که این تقریبا غیرممکن و محال است (عباسی, ۱۳۹۷, ص. ۲۵-۶۰).

۱-۳. نگهداری اطلاعات تراکنش

تراکنش‌های تایید شـــده در دفتر کلی به نام بلاکچین ذخیره می‌شود. اطلاعات این دفتر الکترونیکی به‌عنوان ســـند مثبت پرداخت مورد اســـتفاده قـــرار می‌گیرد. این دفترکل و نســـخه های آن بر روی یک شبکه غیرقابل اعتماد(اینترنت) قرار دارند و برای کلیه گره‌های غیر قابل اعتماد کپی می‌شـــوند و هیچ‌گونه نظارت مرکزی نیز بر روی آن وجود ندارد بنابراین طریقه عملکرد این سیستم باید به گونه‌ای مطمئن باشد که اشکالات

فوق را برطرف نموده تا بتوان به اسناد مبتنی بر آن اعتماد نمود.

بلاکچین نام خود را از نحوه ذخیره‌سازی داده تراکنش‌ها در بلاک‌هایی گرفته است که به یکدیگر متصل شده‌اند و یک زنجیره را شکل داده‌اند. زمان و تسلسل تراکنش‌ها در بلاک ثبت و تأیید می‌شود، سپس بلاک آماده اتصال به بلاکچین می‌شود. هر بلاک در بردارنده هش[1] بلاک، دسته‌ای از تراکنش‌های انجام گرفته، مهرزمانی و هش بلاک قبلی است. هش بلاک قبلی، بلاک‌ها را همچون زنجیره به یکدیگر متصل می‌کند و مانع از تغییر هر بلاک یا اضافه شدن بلاکی بین دو بلاک می‌شود (عباسی, ۱۳۹۷, ص. ۳۲) زیرا اگر مهاجم بخواهد اطلاعات یک بلاک را تغییر دهد این تغییر موجب تغییر در هش بلاک شده تغییر در هش یک بلاک، در کلیه بلاک‌ها اثرگذار بوده و ناهمگونی بلاک‌ها را آشکار می‌کند و بدین علت که تمام گره‌ها کپی تمام زنجیره را دارند از این تغییر مطلع شده و درنتیجه کل شبکه از آن اطلاع پیدا کرده و جلوی این حمله و تخریب گرفته می‌شود؛ لذا اگر مهاجم بخواهد تغییر غیرقابل کشفی داشته باشد لازم است تمام بلاک‌ها را از ابتدا تا آخرین بلاک ثبت شده تغییر دهد تا هش تمام بلاک‌ها متناسب با هم باشند که این کار عملاً محال است. به این ترتیب هرچقدر طول این زنجیره بیشتر شود اعتبار آن نیز بیشتر می‌شود. هر بلاک جدیدی که تشکیل می‌شود نه تنها بر اعتبار بلاک‌های پیش از خود بلکه بر اعتبار کل بلاکچین می‌افزاید. استفاده از مکانیزم هش رمزگذاری شده و اتصال هش هر بلاک به هش بلاک قبلی، باعث می‌شود که بلاکچین غیرقابل دخل و تصرف و تغییر باشد (عباسی, ۱۳۹۷, ص. ۱۷۳-۱۹۳)

---

۱. توابع درهم ساز یا هش (Hash Functions) توابع ریاضی هستند که بیشترین اهمیت را در اصول اولیه رمزنگاری دارند. تابع هش تابع یک طرفه‌ای است که داده‌های ورودی با طول دلخواه را تبدیل کرده و یک خروجی با طول ثابت تولید می‌نماید. خروجی را «مقدار هش(hash value) یا خلاصه پیام (message digest)» می‌نامند. خروجی تولید شده، یک عبارت غیرقابل درک است که مادامی که رمزگشایی نشده باشد، متن ورودی را نمایان نمی‌سازد. تابع هش سه ویژگی مهم دارد: ۱. یکطرفه است. بنابراین از خروجی نمی‌توان ورودی را درک و کشف کرد. ۲. اگر کوچکترین تغییری در اصل پیام رخ دهد، چکیده پیام هم تغییر می‌کند. ۳. منحصربه فرد است؛ یعنی امکان یافتن دو متن با چکیده یکسان غیرممکن است. یکی از گروه‌های مهم از توابع هش، توابع هش رمزنگاری شده هستند که نوعی اثرانگشت دیجیتالی برای هرداده تولید میکنند. توابع هش بلاکچین از این دسته هستند (کیانا, ۱۳۹۸, ص. ۵۲-۷۰).

۲. بررسی قابلیت انطباق ارکان سند الکترونیکی با اطلاعات پرداخت مبتنی بر رمزارز

اینک که با فرایند پرداخت و نحوه عملکرد دفتر نگهداری اطلاعات این پرداخت(بلاکچین) آشنا شدیم لازم است بررسی نماییم اطلاعاتی که در قالب داده‌پیام در این فرایند ایجاد و ثبت می‌شود آیا می‌تواند به عنوان یک سند الکترونیک درنظرگرفته شود و دراین‌صورت تا چه میزان سندیت و قدرت اثباتی دارد؟

در این راستا در درجه اول باید مشخص نمود به طور کلی چه چیزی می‌تواند به عنوان سند تلقی شود. سابقاً گفته شد سند عبارت است از «هرنوشته‌ای که در مقام دفاع یا دعوا قابل استناد باشد.» بنابر، این تعریف هر موضوعی نمی‌تواند سند محسوب شود و لازم است اولاً آن چیز نوشته باشد ثانیاً قابلیت استناد داشته باشد یعنی هر نوشته‌ای سند نیست؛ یک نوشته زمانی می‌تواند در اثبات دعوا مورد استفاده قرار گیرد و دلیل محسوب شود که قابلیت استناد را نیز دارا باشد. همانطوری که در فضای واقعی هر نوشته‌ای سند نیست و نیاز به دو رکن نوشته بودن و قابلیت استناد دارد، در فضای الکترونیکی و مجازی هم هر ارتباط الکترونیک و داده‌پیامی سند محسوب نمی‌شود و لازم است ارکان فوق در آن تأمین گردد. در این مبحث بررسی می‌نماییم که این دو وصف در اسناد الکترونیک چگونه تأمین می‌گردد و اینکه اطلاعات پرداخت رمزارزی که در دفتر کل بلاکچین ایجاد و ذخیره می‌گردد، اوصاف مذکور را داراست یا خیر؟ لذا تبیین دو رکن فوق الذکر را دو بند مجزا پی می‌گیریم.

۲-۱. ضرورت وجود نوشته

آنچه از ظاهر ماده ۱۲۸۴ برمی آید آن است که اولین شرط سندیت یک دلیل، نوشته بودن آن است. یک نوشته کاغذیِ واجد شرایط لازم، می‌تواند مصداق سند مثبِت ادعا باشد. در فضای واقعی بازشناسی نوشته از غیرنوشته امری بدیهی و مشخص است لکن در فضای الکترونیک چه طور؟

مطابق قوانین داخلی و بین المللی داده‌پیام و ارتباطات الکترونیک می‌توانند به عنوان نوشته درنظرگرفته شده و آثار حقوقی نوشته را داشته باشند. مطابق قانون نمونه تجارت الکترونیک آنستیرال مصوب ۱۹۹۶: «جایی که قانون، کتبی بودن اطلاعات را

لازم می‌داند این شرط از طریق داده پیام احراز می‌شود...»[1] همچنین در بند ۲ ماده ۹ کنوانسیون استفاده از ارتباطات الکترونیک مصوب ۲۰۰۵، آمده است: «جایی که قانون، مستلزم آن است که ارتباط یا قرارداد باید به صورت کتبی باشد، یا عواقبی برای فقدان نوشته بیان می‌کند، آن شرط با استفاده از ارتباط الکترونیک احراز می‌شود....»[2] ماده ۶ قانون تجارت الکترونیکی ایران نیز به تبعیت از دو مقرره بین‌المللی مذکور، به داده‌پیام (ارتباط الکترونیک) اعتبار بخشیده است: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده پیام در حکم نوشته است.»

با نگاه ظاهری به مفاهیم فوق باید گفت هر داده‌پیامی نوشته است و می‌تواند سندیت داشته باشد لذا در نوشته بودن و سندیت داشتن اطلاعات پرداخت رمزارزی شکی نیست. لکن این تفسیر صحیح نیست همانطور که هر ارتباطی در فضای واقعی، نوشته محسوب نمی‌شود هر ارتباط الکترونیک و داده‌پیامی نیز نوشته از سنخ سند تلقی نخواهد شد. به همین علت در قوانین مذکور نیز برای نوشته بودن یک داده‌پیام شرط و یا شروطی بیان شده است به عنوان مثال در قانون نمونه آمده: «... به شرطی که اطلاعات مندرج در آن قابل دسترسی باشد تا برای ارجاع بعدی قابل استفاده باشد.» در قانون ایران نیز اگرچه قانون‌گذار در ماده ۶ به هیچ شرطی از نوشته کتبی اشاره نکرده اما از مطالعه سایر مواد می‌توان به همان شرایطی رسید که در اسناد بین‌المللی نیز مورد تأکید قرارگرفته است.

با مطالعه اسناد حقوقی و قوانین به طور کلی در این خصوص می‌توان گفت جهت احراز نوشته بودن یک داده‌پیام از یکی از اصول اولیه در تجارت الکترونیک تحت عنوان اصل هم ارزی عملکردی[3] استفاده می‌شود؛ مطابق این اصل در اعتباربخشی اسناد الکترونیک، شکل و ظاهر آن با اسناد کاغذی قیاس نمی‌شود، بلکه عملکردهای آنها با هم مقایسه می‌شود؛ لذا اگر عملکردهای سند کاغذی در سند الکترونیک تأمین شود، همان اعتباری را خواهد داشت که سند کاغذی دارد (آلان داویدسون, ۱۴۰۰, ص. ۱۳۳).

1. UNCITRAL Model Law on Electronic Commerce 1996, Article 6(1)
2. United Nations Convention on the Use of Electronic Communications in International Contracts 2005, Article 9(2)
3. Functional Equivalency

در اســـناد بین‌المللی کارکردهای متفاوتی برای شرط کتبی بودن مورد توجه قرارگرفته اســـت.[۱] از این میان مهمترین و بنیادیترین عملکردهای نوشـــته کاغذی را می‌توان در چند دسته کلی تقسیم نمود که عبارت است از: ۱. ثبات و تغییرناپذیری نوشته ۲. دوام و بقای نوشته ۳. تشخیص اصل نوشته.

دراینجا لازم است سه عملکرد پیش گفته را به تفکیک مورد بررسی قرارداده و اطلاعات پرداخت مبتنی بر رمزارز را از حیث شـــمول یا عدم‌شمول این عملکردها مورد بررســـی قرارداده تا نهایتاً وجود شرط اول ســـندیت یعنی نوشته بودن در آن به اثبات رسد.

۲-۱-۱. ثبات و تغییر ناپذیری نوشته

یکی از کارکردهای مهم سند نوشته تغییرناپذیری آن است به طوری که دخل و تصرف در ســـند به راحتی قابل شناسایی بوده و موجب ازبین‌رفتن اعتبار و ارزش اثباتی آن می‌گردد. درحالی‌که ارتباطات الکترونیک و داده‌پیام‌ها ازآنجایی‌که در فضای دیجیتال ایجاد و نگهداری می‌شوند، می‌توانند مکرراً مورد دخل و تصرف و تغییرات واقع شوند بی آنکـــه از خود اثری برجای گذارند، لذا داده‌پیام‌ها و ارتباطاتی می‌توانند به عنوان نوشـــته درنظرگرفته شوند که با اتخاذ تدابیر امنیتی ثبات و تغییرناپذیری آنها تضمین شود.

از همیـــن رو دو اصل مهم امنیت اطلاعات در هر ارتباط الکترونیک یعنی حفظ محرمانگی و تمامیت ارتباط و پیام‌های ردوبدل شـــده در طی آن، همیشه مورد توجه بوده است؛ پیام‌هایی که میان اشخاص مختلف ردوبدل می‌شوند اولاً نباید توسط

---

۱. به عنوان مثال در پاراگراف ۴۸ راهنمای تصویب قانون نمونه آنســـیترال آمده اســـت: « در تدارک قانون نمونه، توجه ویژه‌ای به کارکردهایی که به طور سنتی توسط انواع مختلف «نوشته ها» در یک محیط کاغذی انجام می‌شد، صورت گرفت. به عنوان مثال در ذیل دلایلی احصا شده که نشان می‌دهد چرا قوانین کشورها تنظیم کتبی را الزام می‌نمایند: ۱. برای اینکه تضمین شـــود دلیل مادی‌ای برای وجود قصد طرفین برای ملزم کردن آنها به مفاد آن وجود دارد. ۲. تا به طرفین کمک کند از آثار ورودشان به قرارداد مطلع شوند. ۳. تا سندی که برای همه قابل خواندن باشد فراهم شود. ۴. ســـند در طی زمان غیرقابل تغییر باقی بماند و سابقه دائمی از معامله ایجاد شود. ۵. امکان تکثیر سند وجود داشته باشـــد. ۶. امکان تصدیق اطلاعات با امضا میســـر شود. ۷. امکان پذیرش سند توسط مراجع قضایی فراهم شود. ۸. قصد تنظیم کننده سند نهایی شده و سابقه‌ای از آن فراهم و نگهداری شود. ۹. امکان نگهداری آسان اطلاعات در قالب مادی میســـر شود. ۱۰. کنترل و بررسی‌های بعدی جهت اخذ مالیات و یا انجام حسابرسی یا سایر اهداف قانونی فراهم شود. ۱۱. سایر حقوق و تکالیف قانونی در مواردی که کتبی بودن جهت اعتبار لازم است، به وجود آید.»

اشخاص خارج از آن ارتباط، قابل رویت و کشف قرار گیرند که در این صورت محرمانگی داده پیام تأمین شده است و همچنین محتوای آن نباید مورد تغییر یا حذف قرار گیرند؛ یعنی هم خود پیام باید از رویت و خواندن مصون بماند هم تمامیت اطلاعات باید حفظ شده و مورد تعرض و تغییر قرار نگیرد.

این امنیت لازم است هم در مرحله تولید پیام برقرار شود یعنی وقتی پیام از سیستم «الف» به سمت سیستم «ب» حرکت می‌کند، کسی نباید بتواند آن را رویت نموده و دستخوش تغییر قرار دهد؛ هم در مرحله نگهداری؛ سیستمی که داده‌پیام در آن بایگانی و نگهداری می‌شود، باید بتواند در مقابل رویت و تغییر مقاومت نماید تا در مراجعات بعدی به داده پیام، به دلیل تضمین امنیت و عدم تغییرپذیری، اطلاعات و داده‌پیام‌ها قابل پذیرش و اعتماد باشند.

به همین دلیل است که در اعتباردهی اسناد الکترونیک ماده ۱۴ قانون تجارت الکترونیکی بیان می دارد: «کلیه داده‌پیام‌هائی که به طریق مطمئن ایجاد و نگهداری شده‌اند ازحیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه‌اشخاصی که قائم‌مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضائی و حقوقی است.»

بنابراین وجود ثبات و تغییرناپذیری در یک ارتباط الکترونیک نه تنها ضامن احراز شرط اول برابری عملکردی با نوشته کاغذی است بلکه مطابق ماده فوق تضمین‌کننده اعتبار آن ارتباط به عنوان یک سند قابل ارائه در محاکم نیز می‌باشد. فلذا اطلاعات پرداخت مبتنی بر رمزارز زمانی می‌تواند اثر حقوقی داشته و سندی معتبر تلقی گردد که هم در مرحله ایجاد اطلاعات توسط کیف پول‌ها و گره‌های سیستم و هم در مرحله نگهداری اطلاعات در بلاکچین، این امنیت و به تبع آن ثبات و تغییرناپذیری تأمین گردد.

تأمین این امنیت و عملکرد در اسناد الکترونیک بستگی مستقیم با سیستم اطلاعاتی دارد که داده‌پیام و ارتباط، در طی آن تولید شده و حفظ می‌شود. چراکه مطابق ماده ۱۴، هر داده‌پیامی نمی‌تواند حکم سند معتبر را داشته باشد، داده‌پیامی یک نوشته معتبر و درحکم سند است که به روش مطمئنی اولاً ایجاد ثانیاً نگهداری شده باشد و مطابق ماده ۱۱، اطمینان، از وجود یک سیستم اطلاعاتی مطمئن ناشی می شود.[1]

۱. ماده ۱۱: «سابقه الکترونیکی مطمئن عبارت است از داده‌پیامی که با رعایت شرایط یک سیستم اطلاعاتی مطمئن ذخیره شده و ....»

مطابق تعریف قانون، «سیستم اطلاعاتی سیستمی برای تولید، ارسال، ذخیره و پردازش داده‌پیام است.»[1] سیستم اطلاعاتی رمزارزی را می توان مجموعه‌ای از کیف‌پول‌ها، شبکه بلاکچین، گره‌ها، استخراج‌گران و دفترکل بلاکچین دانست که اطلاعات پرداخت به عنوان داده پیام در این بستر ایجاد و حفظ می شود.

در نگاه قانون هر سیستمی مطمئن نیست. سیستم اطلاعاتی مطمئن در قانون تعریف نشده صرفاً شرایطی برشمرده شده که در صورت جمع بودن این شرایط در یک سیستم اطلاعاتی، آن سیستم مطمئن خواهد بود؛ علت این امر آن است که نفوذ در سیستم‌ها به موازات تغییر و رشد فناوری، تغییر می‌نمایند لذا شیوه‌ها و ابزارهای حفاظت هم به همین مناسبت باید تغییر یابند. معرفی یک زیرساخت فنی ثابت به عنوان یک سیستم اطلاعاتی مطمئن مانع این متغیر و سیال بودن خواهد بود؛ لذا قانون‌گذار با ارائه معیار، بررسی و تطابق هر سیستمی را در هر زمانی و باهر نوع فناوری امکان‌پذیر نموده است.

شرایط سیستم اطلاعاتی مطمئن در بند «ح» ماده ۲ قانون تجارت الکترونیکی بدین شرح برشمرده شده است[2]:

۱. به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد.

منظور از سوءاستفاده، استفاده غیرمجاز و مراد از نفوذیابندگی به معنای دسترسی افراد رخنه‌گر از طریق شبکه یا محیط فیزیکی سیستم اطلاعاتی است درصورتی که سیستم در مقابل این خطرات محافظت نشود ممکن است اطلاعات فاش شود، تغییر یابد یا حذف شود (عبداللهی و شهبازی نیا, ۱۳۸۸, ص. ۱۲۵). بنابراین شرط مذکور، تضمین کننده محرمانگی و حفظ تمامیت داده‌پیام است.

در سیستم پرداخت مبتنی بر رمزارز این شرط محقق شده است. نحوه فعالیت گره‌های شبکه که به صورت همتابه‌همتا و با رای اکثریت است، نحوه انجام تراکنش و استفاده از امضای دیجیتالی در آن و نحوه ذخیره‌سازی تراکنش در بلاکچین که به

---

۱. بند «ز» ماده ۲ قانون تجارت الکترونیکی

قانون نمونه ۱۹۹۶ و کنوانسیون ۲۰۰۵ هم به ترتیب در مواد ۲ بند (f) و ۴ بند (f) تعریف مشابهی را ارائه داده‌اند.

۲. متناظر با این بحث، در بند ۲ ماده ۹ قانون نمونه آمده است: «اطلاعات در قالب داده پیام، باید از بار اثباتی لازم برخوردار باشند، در ارزیابی این بار اثباتی، باید به قابلیت اطمینان در نحوه تولید، ذخیره یا انتقال داده پیام، به قابلیت اطمینان در نحوه حفظ یکپارچگی اطلاعات، نحوه شناسایی اصل ساز و هر عامل مرتبط دیگر توجه نمود.»

صورت زنجیره به یکدیگر متصل بوده و قابل تغییر نمی‌باشـــند، همگی گویای غیرقابل نفوذ بودن این سیستم است.

۲. سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد.

قابلیت دسترسی یعنی سیستم خارج از دسترس نباشد و کارایی آن به گونه‌ای باشـــد که هنگام نیاز بتوان از اطلاعات اســـتفاده نمود. تصدی صحیح یعنی مدیریت و ســـازماندهی نیروی انســـانی به شیوه‌ای باشد که امنیت سیســـتم حفظ شود و وظایف اشـــخاص به‌گونه‌ای تفکیک شود که امکان سوءاستفاده آنان از اختیاراتشان کمتر شود (عبداللهی و شهبازی نیا, ۱۳۸۸, ص. ۱۲۷).

در مباحث پیشـــین گفته شد که معماری شـــبکه رمزارز و بلاکچین به‌گونه‌ای اســـت که تمامی اطلاعات در عین محفوظ ماندن، برای همگان دردســـترس هستند و اطلاعات تراکنش هر لحظه قابل رصد و پیگیری می‌باشد. این ویژگی، لطمه‌ای به امنیت سیســـتم نمی‌زند. همچنین به جهت عملکرد توزیع شـــده در این سیستم، تمام گره‌ها به یکدیگر متصل‌اند لذا خرابی در برخی گره‌ها، سیستم را از دسترس خارج نمی‌سازد.

۳. به نحوی معقول متناســـب بـــا اهمیت کاری که انجـــام می‌دهد پیکربندی وسازماندهی شده باشد.

معماری سیســـتم متناســـب با عملیاتی که در خلال آن انجام می‌شود باشد به طوری که از داخل و بیرون شـــبکه، نتوان موجبات توقف فعالیت سیستم یا خرابکاری در آن را فراهم نمود. باتوجه به پیکربندی و معماری سیســـتم رمزارزی این شـــرط نیز مهیا است.

البته قابل ذکر اســـت که اطمینان در سیســـتم رمزارزی صددرصدی نیست و می‌تـــوان از مصادیقی نیز نام برد که هکرها و مخرب‌ها توانســـته‌اند به سیســـتم نفوذ نمایند. بااین‌وجود در این باره می‌توان گفت واژه «معقولیت» به‌کاربرده شده در شماره یک، دو و ســـه از بند «ح» نشـــان می‌دهد که اطمینان متعارف کافی است و نیازی به اطمینان صددرصدی وجود ندارد؛ کما اینکه حتی در سیستم‌های پرداخت متمرکز نیز نفوذ مخرب‌ها، ویروس‌ها و هکرها دیده شده است و اساساً همین موضوع یکی از دلایل تلاش بی‌وقفه بشر برای به‌روزرسانی فناوری‌ها و رفع نقایص آن بوده است.

۴. موافق با رویه ایمن باشد.

رویه ایمن، رویه‌ای اســـت برای تطبیق صحت ثبت داده‌پیام، منشأ و مقصد آن بـــا تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا ویا ذخیره‌ســـازی داده‌پیام از یک زمان خاص. یک رویه ایمن ممکن است با استفاده ازالگوریتم‌ها یا کدها، کلمات یا ارقام شناسائی، رمزنگاری، روشهای تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود.[1]

امروزه بهترین روش ایمن و مطمئن جهت تأمین موارد مذکور که مهمترین آن حفظ محرمانگی و تمامیت داده اســـت، استفاده از امضای دیجیتال در تبادل اطلاعات می‌باشـــد، این امضا از علوم رمزنگاری در ســـاخت خود بهره برده که به جهت مکانیزم خاص خود به خوبی می‌تواند امنیت اطلاعات را فراهم آورد. استفاده از امضای دیجیتال هم موجب امنیت و اطمینان سیســـتم اطلاعاتی شـــده و هم داده‌پیام را از تغییر حفظ نموده و هرگونه تغییری در آن را قابل کشـــف می‌نماید. در سیستم پرداخت مبتنی بر رمزارز از این امضا برای انجام و تأیید تراکنش اســـتفاده می‌شـــود. مضافاً اینکه عملکرد بلاکچین نیز به جهت بهره‌گیری از علم رمزنگاری و استفاده از هش رمزگاری شده کلیه شرایط یک رویه ایمن را تأمین می‌نماید.

نتیجتاً درجهت مقایسه و تطبیق سیســـتم پرداخت مبتنی بر رمزارز با شرایط پیـــش گفته، دلایل زیر ثابت می‌نماید که عملکرد اول از نوشـــته یعنی تغییرناپذیری و ثبات در اطلاعات پرداخت مبتنی بر رمزارز تأمین شده است:

۱) استفاده از امضای دیجیتال در انتقال وجوه: یکی از مهمترین آثار استفاده از امضای دیجیتال، حفظ تمامیت داده‌پیام و کشف هرگونه تغییر در آن است. در پرداخت مبتنی بر رمزارز به جهت استفاده از علم رمزنگاری و امضای دیجیتال، این مهم، تأمین گردیده اســـت. لذا عملکرد اول سند نوشـــته یعنی ثبات و تغییر ناپذیری که می‌بایست در اسناد الکترونیک نیز تأمین شـــود، در اطلاعات پرداخت مبتنی بر رمزارز به واسطه امضای دیجیتال برقرار شده است.

۲) وجـــود اطمینان در مرحله ایجاد داده پیام: تبیین گردید که هر نوشـــته‌ای در حکم سند معتبر نیســـت و مطابق ماده ۱۴ قانون تجارت الکترونیکی باید به طریق مطمئن و در یک سیستم اطلاعاتی مطمئن ایجاد شود. معماری سیستم پرداخت و

---

۱. بند «ط» ماده ۲ قانون تجارت الکترونیکی

مجموع عملکرد میان گره‌ها و شبکه بلاکچین، به واسطه ویژگی‌هایی چون شبکه توزیع شـــده، ارتباط همتابه‌همتا، رمزنگاری داده‌ها، امضـــای دیجیتال و توابع هش رمزنگاری شده، سیستم پرداخت رمزارزی را به یک سیستم مطمئن تبدیل کرده است که تمامی شرایط سیستم اطلاعاتی مطمئن را تأمین نموده است.

۳) وجـــود اطمینان در مرحله حفظ و نگهداری داده‌پیام: همچنین مطابق ماده مذکور، بررسی شد که نه تنها ایجاد سند به طریق مطمئن شرط اعتباردهی به آن سند می‌باشـــد بلکه نگهداری مطمئن اطلاعات مندرج در ســـند نیز ضرورت دارد. اطلاعات پرداخـــت و تراکنش‌ها در پرداخـــت مبتنی بر رمزارز در بلاکچیـــن صورت می‌گیرد و مطالعه نمودیم که عملکرد بلاکچین و استفاده از توابع هش رمزنگاری در آن، بلاکچین را به یک سیستم مطمئن جهت نگهداری اطلاعات پرداخت تبدیل کرده است. بنابراین مقرره ماده ۱۴ که تأثیر بر ایجاد و نگهداری مطمئن داده‌پیام دارد نیز در این سیســـتم برقرار شده است.

۲-۱-۲. دوام و بقای نوشته

دومین عملکرد ســـند نوشـــته، قابلیت دوام و بقای مندرجات آن است. مراد از بقا آن اســـت که نوشته باید قابلیت نگهداری را داشته باشد سند مکتوب و کاغذی این قابلیت را دارد که برای سالیان متمادی همانطور که تنظیم شده باقی بماند تا در صورت لزوم از آن اســـتفاده شود و در محاکم به آن استناد شده و ابراز شود. ، این شرط تحت عبارت «قابلیت نگهداری جهت استفاده بعدی» مطابق قانون نمونه ۱۹۹۶ و کنوانسیون ۲۰۰۵ به عنوان عملکرد موردنظر قانونگذار در نوشـــته کاغذی، درنظرگرفته شـــده که چنانچه در ارتباط و پیام الکترونیک هم، احراز شـــود، ارزشـــی برابر با نوشته کاغذی و غیرالکترونیک خواهد داشت.

در ماده ۱۱ قانون تجارت الکترونیکی ایران نیز این موضوع با قدری تفاوت بیان شـــده: «سابقه الکترونیکی مطمئن عبارت اســـت از داده‌پیامی که با رعایت شرایط یک سیستم اطلاعاتی مطمئن ذخیره شده و به هنگام لزوم در دسترس و قابل درک است.» همچنین به عنوان یکی از شـــرایط تشـــخیص داده‌پیام اصل از کپی آن، در بند ۱ ماده ۸، ذکر شده است.

در این خصوص توجه شود که صرف حفظ و نگهداری داده‌پیام کافی نیست پیام می بایســت همانگونه که از ابتدا ایجاد شده، باقی بماند؛ یعنی تمامیت آن هم در حین نگهداری باید حفظ شــود. باعنایت به همین موضوع است که قانون گذار در ماده ۱۴، از عبارت «نگهداری به طریق مطمئن» اســتفاده نمود. همچنین مطابق بند ۱ ماده ۸ قانون نمونه ۱۹۹۶ حفظ تمامیت اطلاعات می‌بایست از تاریخی که پیام در شکل نهایی خود ایجاد شده، تضمین شود.

درخصوص اســناد پرداخت مبتنی بر رمزارز گفته شد که اطلاعات تراکنش در دفتــر کلی به نام بلاکچین ذخیره می‌گردد، مکانیــزم عملکرد این دفتر کل به‌گونه‌ای است که اولاً تمامی تراکنش‌ها به همراه اطلاعات مرتبط با آن از ابتدا تا به امروز در آن ذخیره شده است. ثانیاً این ذخیره‌سازی به جهت استفاده از علوم رمزنگاری و توابع هش رمزنگاری شده به طریق مطمئن و ایمن است لذا امکان تغییر در آن نیز راه ندارد. مضافاً اینکه در این سیستم اطلاعات پرداخت برای تمامی گره‌های فعال در شبکه ارسال می گردد به طوری که کوچکترین تغییر در اطلاعات قابل رویت برای تمام مردم در ســطح جهان می‌باشــد. بنابراین پس از انجام پرداخت در فضــای الکترونیکی اطلاعات ازبین نرفته و در بلاکچین ذخیره می‌شود که قابل بازیابی، درک و استفاده در مواقع لزوم می باشد. درنتیجه عملکرد دوم هم تأمین گردیده است.

۲-۱-۳. تشخیص اصل سند

عملکرد تشخیص اصل سند، بدین معناست که سند اصل از کپی آن، می‌بایست قابل تشخیص باشد، در سند مکتوب این امکان فراهم است؛ اما در اسناد دیجیتال ممکن اســت گفته شود به جهت خصیصه‌های ذاتی فضای الکترونیکی، امکان تشخیص اصل از کپی فراهم نیست چراکه اولاً نسخه اصل همان است که در ابتدا روی حافظه موقت رایانه تشکیل می‌گردد و از آن لحظه به بعد آنچه روی حافظه جانبی دیسکت سخت، سی دی و ســایر وسایل ذخیره، ارسال و یا چاپ و نمایش داده می‌شود، همگی مصادیقی از کپی محسوب می‌شوند و ثانیاً امکان تولید، ارسال و ذخیره مجدد و یا ارسال نسخه‌های متعدد از نسخه اولیه وجود دارد و عملاً نمی‌توان عاملی قطعی برای جلوگیری از تولید مکرر یا تمییز از اصل در اختیار کاربران گذاشت (صادقی نشاط, ۱۳۹۳, ص. ۸۴).

با این حال در اســـناد بین‌المللی[۱] و قانون ایران، با لحاظ شرایطی می توان اصل بودن سند را احراز نمود و داده‌پیام را به عنوان یک ارتباط اصل به محکمه ارائه نمود.

در ماده ۸ قانون تجارت الکترونیکی ایران آمده است: « هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارائه یا نگهداری شـــود، این امر با نگهداری و ارائه اطلاعات به صورت داده‌پیام نیز درصورت وجود شرایط زیرامکان‌پذیر می‌باشد:

الف- اطلاعات مورد نظر قابل دسترســـی بوده و امکان استفاده درصورت رجوع بعدی فراهم باشد.

ب- داده پیـــام به همان قالبی (فرمتی) که تولید، ارســـال و یا دریافت شـــده و یا به‌قالبی که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال و یا دریافت شده، نگهداری شود.

ج- اطلاعاتی که مشـــخص کننده مبداء، مقصد، زمان ارســـال و زمان دریافت داده‌پیام می‌باشند نیز درصورت وجود نگهداری شوند.

د- شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه درخصوص نگهداری داده‌پیام مرتبط با حوزه مسؤولیت خود مقرر نموده فراهم شده باشد.

در خصوص ماده مذکور چند نکته حائز اهمیت است:

۱) به اســـتناد ماده ۹۶ قانون آیین دادرسی مدنی، اصول اسناد و مدارک مثبت ادعا در جلسه اول رسیدگی می‌بایست ارائه شود؛ لذا ارائه اصل اسناد در جلسه اول یک الزام قانونی اســـت و مطابق ماده ۸ هرجا الزام قانونی به ارائه اصل اســـناد وجود داشته باشد، ارائه داده‌پیام با حصول شرایط فوق‌الذکر امکان پذیر است.

۲) بند «الف» ماده ۸ مبیّن یکی از عملکردهای نوشـــته بودن اســـت که سابقاً توضیح داده شد. لذا چنانچه این شرط مهیا شود هم شرط کتبی بودن احراز شده و هم داده‌پیام قابلیت اصل بودن را دارا است.

۳) بنـــد «ب» بر عدم تغییر محتـــوای داده‌پیام دلالـــت دارد و بازتابی از اصل تمامیت داده‌پیام است (حبیب زاده، ۱۳۹۶، ۲۰۱).

---

۱. مطابق بند ۱ ماده ۸ قانون نمونه ۱۹۹۶ ، «جایی که قانون مســـتلزم ارائه یا نگهداری اطلاعات در شـــکل اصلی خود می‌باشـــد این شـــرط از طریق داده پیام احراز می‌شود اگر الف: تضمین اطمینان‌بخشی در خصوص تمامیت اطلاعات از تاریخی که در ابتدا در شـــکل نهایی خود ایجاد شـــده وجود داشته باشـــد و ب: جای که ارائه اطلاعات لازم است، برای کسی که قرار است ارائه شود قابل نمایش باشد.» بند ۴ ماده ۹ کنواسیون ۲۰۰۵ نیز به همین موضوع پرداخته و مقرره مشابه ماده ۸ قانون نمونه را تدوین نموده است.

۴) منظور از اطلاعات در صدر ماده، متن پیام است و منظور از اطلاعات در بند «ج»، اطلاعات تکمیلی پیام است.

۵) باعنایت به بند «الف» و «ب»، گویی تضمین عملکرد سوم یعنی اصالت، در گرو دو عملکرد پیش‌گفته یعنی ثبات و دوام سند است.

۶) مطابق بند «د» هر ارگان رسمی می‌تواند شرط یا شروطی را بر موارد مذکور اضافه نماید.

در مقـــام تطبیق مفاد فوق با ســـند پرداخت مبتنی بر رمـــزارز باید گفت یک داده‌پیـــام حاوی پرداخت از طریق رمزارزهـــا و اطلاعات مربوط به آن درصورت حصول شرایط مذکور می‌تواند به عنوان یک سند (نوشته) اصل جهت اثبات ادعا مورد استفاده قرار گیرد؛ کافی است اطلاعات پرداخت در مکانی مطمئن ذخیره شود که قابل استفاده بعدی باشـــد، اطلاعات تکمیلی آن نیز ثبت گردد و تمامیت اطلاعات نیز حفظ شود تا در صورت عدم وجود شـــرط دیگری از ارگان‌های مالی کشـــور یا تأمین آن، بتوان سند پرداخت رمزارزی را به عنوان یک ســـند اصیل در محکمه ارائه داد و پرداخت را اثبات نمود؛ موضوعات مذکور در این رابطه برقرار است چراکه اولاً اطلاعات تراکنش در سایت بلاکچین با تمام جزئیات در معرض دید عموم قرار گرفته است و لذا به صرف مراجعه به این سایت می‌توان به این اطلاعات دست یافت. ثانیاً گفته شد معماری شبکه بلاکچین به‌گونه‌ای اســـت که اطلاعات بدون هرگونه تغییری و به همان شکلی که تولید شده در بلاکچین ذخیره می‌شـــود؛ بنابراین بند «ب» این ماده هم تأمین شده است. ثالثاً گفته شـــد که شماره حساب ورودی و خروجی، مهرزمانی(که حاوی اطلاعات زمانی تراکنش است) از جمله اطلاعاتی هســـتند که در بلاکچین ذخیره می‌شوند این اطلاعات شرط بند «ج» ماده مذکور را فراهم می‌آورد. رابعاً در مورد اصل ســـند پرداخت الکترونیکی، مطابق بند «د» ماده مذکور، شـــروط دیگری از ناحیه حاکمیت مطرح نشده که لازم به تطبیق آن با رمزارزها باشد.

۲-۲. قابلیت انتساب

با عنایت به ماده ۱۲۸۴ قانون مدنی ، شـــرط دوم برای آنکه نوشـــته‌ای، ســـند درنظرگرفته شود قابلیت استناد آن است و یک نوشته در صورتی قابل استناد است که

بر شـــخصی منتسب شـــود. یک ارتباط، زمانی می‌تواند اثرگذار باشد که بتوان آن را به شـــخصی منتسب نمود تا قابلیت ایجاد آثار بر منتسب الیه را داشته باشد. متداول‌ترین روش جهت انتســـاب نوشته به یک شخص، درج نشانه‌ای در نوشته تحت نام امضا است (شمس, ۱۳۸۸, ص. ۱۳۶-۱۳۷).

مطابق قانون نمونه آنسیترال مصوب ۲۰۰۱ راجع به امضای الکترونیک، «امضای الکترونیک به معنای داده در قالب الکترونیک اســـت که به یک داده‌پیام پیوســـت شده یـــا با آن ارتباط منطقـــی دارد به‌طوری‌که می‌تواند برای شناســـایی امضاکنندهٔ مرتبط بـــا آن داده‌پیام یا برای نشـــان دادن تأییـــد امضاکننده در مـــورد اطلاعات موجود در داده‌پیام استفاده شود.»[1] قانون تجارت الکترونیکی ایران نیز به تبع قانون نمونه، امضای الکترونیک را در قســـمت «ی» ماده ۲ اینگونه تعریـــف می‌کند:«هر نوع علامت منضم شـــده یا به نحو منطقی متصل شده به داده‌پیام اســـت که برای شناسائی امضاءکننده داده‌پیام مورد استفاده قرار می‌گیرد.»

می‌توان گفت مطابق اصل برابری عملکردی هر علامت و نشـــانه‌ای که کارکرد و هدف مدنظر در امضا را تأمین نماید، امضا نامیده می‌شـــود و شـــکل و فرم آن مناط اعتبار نیست. با عنایت به قوانین مذکور می‌توان گفت وجود امضا در ذیل یک نوشته، دو کارکرد اصلی دارد یکی اینکه هویت نویسنده را مشخص می‌نماید(احراز هویت) و دیگر اینکه اراده و رضایت وی را به ایجاد آن نوشـــته معلوم می‌دارد.[2] مجموع این دوکارکرد منتج به این می‌شود که نوشـــته، آثار حقوقی خود را بر نویسنده(امضاکننده) بار نماید اعم از اینکه امضا در قالب سنتی باشد یا مدرن و الکترونیکی.

امضاهای الکترونیک دارای اقسام مختلفی هستند که سطوح متفاوتی از امنیت را تأمین نموده و به تبع آن درجات مختلفی از اعتبار را دارا هستند.

قانـــون نمونه آنســـیترال ۲۰۰۱، در بند ۱ ماده ۶ بیان مـــی‌دارد:« در موردی که قانون امضای شـــخص را می‌طلبد آن شـــرط با داده‌پیام احراز می‌شـــود اگر امضای الکترونیک به کاررفته شـــده با درنظرگرفتن سایر شـــرایط از جمله توافق مرتبط، برای هدفی که داده‌پیام برای آن تولید یا ارسال شده، قابل اعتماد باشد.»

1. UNCITRAL Model Law on Electronic Signatures 2001, Article 2(a).

۲. به این موضوع در قسمت الف بند ۳ ماده ۹ کنوانسیون ۲۰۰۵ نیز اشاره شده است.

بنابرایـــن مطابق قانون نمونه هـــر امضای الکترونیـــک نمی‌تواند امضای معتبر درنظرگرفته شود و شرط اعتباردهی، قابلیت اعتماد است.

در بند ۳ ماده مذکور، جهت احراز قابلیت اعتماد چهار پیش شرط لازم دانسته شده است: الف. مرتبط بودن امضا(دادۀ حاوی امضا) به امضاکننده ب. کنترل امضاکننده بر امضای(دادۀ حاوی امضا) خود در زمان امضاکردن. ج. قابلیت شناســـایی هر تغییری در امضا پس از درج آن (حفظ تمامیت امضا) د. قابلیت شناسایی هر تغییری در محتوا، در مواردی که هدف از امضا، حفظ تمامیت اطلاعاتی است که امضا بدان مرتبط است.

در قانـــون تجـــارت الکترونیکی ایران نیـــز اگرچه قانونگـــذار در ماده ۷ به یک اعتباردهی کلی به امضا بســـنده کرده اســـت.[۱] اما مطابق ســـایر مواد، امضای ســـاده و مطمئن را از یکدیگر تفکیک نموده و شـــرایط امضای مطمئن را در ماده ۱۰ بیان کرده است؛ به طوری که ماده ۱۰ برماده ۷ حاکم بوده و چنانچه امضایی شرایط اطمینان ساز مصرح در ماده را نداشته باشد امضای معتبری نیست (فیضی چکاب, ۱۳۸۹, ص. ۱۸۶) همچنین در ماده ۱۴ در تبیین شـــرایط یک سند معتبر، به ایجاد سند به طور مطمئن اشـــاره شـــده و یکی از مراحل ایجاد سند، درج امضا در ذیل آن است و لذا اطمینان در امضا از مقدمات ایجاد سند مطمئن و به تبع آن اعتبار سند است؛ پس تا امضا مطمئن نباشد، سند هم معتبر و قابل استناد نیست.

ماده ۱۰ در بیان شرایط مذکور بیان می‌دارد:« امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف- نسبت به امضاءکننده منحصربه‌فرد باشد.

ب- هویت امضاءکننده داده‌پیام را معلوم نماید.

ج- به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد.

د- به نحوی به یک داده‌پیام متصل شـــود که هر تغییری در آن داده‌پیام قابل تشخیص و کشف باشد.»

یکی از معتبرترین و ایمن ترین امضاها در دنیای مدرن امروزی که مبتنی بر علوم رمزنگاری بوده و کلیه شروط فوق الذکر را تأمین می‌نماید، امضاهای دیجیتالی هستند.

---

۱. مـــاده ۷ قانون تجارت الکترونیکـــی ایران بیان می‌دارد:« هرگاه قانون وجود امضـــا را لازم بداند امضای الکترونیکی مکفی است.»

امضـــای دیجیتالی به معنای رمزنگاری خلاصه پیام(هش) اســـت (حبیب زاده, ۱۳۹۶, ص. ۳۰۵). در ایـــن تکنولوژی از الگوریتم رمزنگاری نامتقارن[1] و تابع درهم‌ســـاز(هش) به طور همزمان اســـتفاده می‌شود. یعنی فرستنده داده پیام از یک سو، متن اصلی پیام را رمزگذاری کرده و برای گیرنده ارســـال می‌نماید و از ســـوی دیگر از طریق تابع هش پیام را خلاصه نموده و خلاصه آن را رمز نموده و برای گیرنده ارسال می‌نماید. گیرنده با بازگشـــایی اصل پیام و مقایسه آن با خلاصه پیام هم از تمامیت پیام اطمینان حاصل می‌کند و هم از انتساب آن به فرستنده.

امضای دیجیتال علاوه بر اینکه شرط دوم از سند بودن یک داده‌پیام را اثبات می نماید و موجب انتساب یک ارتباط الکترونیک به خالق آن می‌گردد تضمین‌کننده حفظ محرمانگی و تمامیت اطلاعات آن ارتباط نیز می‌باشـــد بنابراین سیستم اطلاعاتی که در فرایند خود از این مکانیزم استفاده نماید تبدیل به یک سیستم مطمئن خواهد شد.

در روش استفاده از امضای دیجیتالی، نتایج زیر حاصل می‌شود:

۱) محرمانگی پیام حفظ می‌شـــود؛ زیرا اصل پیام توسط کلیدعمومی گیرنده، رمزگذاری شده است لذا صرفاً توسط گیرنده که کلید خصوصی متناظر را در دست دارد قابل رمزگشایی، خواندن و درک می‌باشد، نه سایر اشخاص.

۲) تمامیت داده حفظ شـــده و هر تغییری در داده‌پیام قابل کشـــف است؛ زیرا تطابق و مقایسه خلاصه پیام و هش ارسالی از طرف فرستنده و خلاصه‌ای که گیرنده از متن اصلی می‌گیرد، مشخص می‌نماید که در آن تغییری رخ داده است یا خیر. چنانچه هر دو هش یکســـان باشند معلوم می‌شـــود تمامیت داده حفظ شده و در مسیر انتقال، دستخوش تغییر واقع نشده اســـت. چراکه مکانیزم تابع هش به‌گونه‌ای است که تغییر حتی یک حرف یا نشانه در اصل پیام، موجب تغییر در هش و خلاصه پیام می شود.

۳) انتســـاب داده‌پیام به فرستنده قابل احراز است (اصالت سنجی)؛ زیرا خلاصه پیام توسط کلیدعمومی‌ای رمزگشایی می‌شود که تنها یک کلید خصوصی متناظر با

---

۱. الگوریتم نامتقارن یکی از روش‌های رمزنگاری اســـت که در امضای دیجیتالی از آن اســـتفاده می‌شود. در این روش، دو کلید متناظر وجود دارد که از یکی برای رمزگذاری و از دیگری برای رمزگشـــایی اســـتفاده می‌شود. به این دو کلید، کلید عمومی و خصوصی گفته می‌شـــود. کلید عمومی در دسترس همگان قرار می‌گیرد؛ اما کلید خصوصی باید از دید عموم پنهان مانده و توسط صاحب آن به طریقه ایمن حفظ شود (گروه مولفین نبض دانش، ۱۳۹۸، ۱۰۵-۱۰۴).

آن وجود دارد که متعلق به یک هویت اســـت بنابراین قطعا این پیام توسط دارنده این کلید عمومی ساخته شده زیرا تنها او می‌تواند توسط کلید خصوصی متناظر خود، پیام را رمز نماید.

باعنایـــت به مطالعـــات فوق‌الذکر درمی‌یابیـــم که اولاً امضـــای دیجیتال از ایمن‌ترین امضاهای الکترونیک به شـــمار رفته و کلیه شـــروط امضای قابل اعتماد و مطمئن را داراست. ثانیاً درج آن در داده‌پیام و ارتباطات الکترونیک دربردارنده اعلام رضایت ممضی از یک سو و انتساب محتوای امضا شده به وی از سوی دیگر می‌باشد (Biddle, 2017, p. 2).

ازآنجایی‌که ارسال وجوه و انجام فرایند پرداخت از طریق رمزارزها برپایه امضای دیجیتـــال و مبتنی بر الگوریتم نامتقارن توســـط دو کلیدعمومی و خصوصی اســـت و این الگوریتم هم در ایجاد تراکنش(توســـط فرســـتنده) و هم در تأیید تراکنش(توسط گـــره ها) مورد اســـتفاده قرار می‌گیرد، می‌توان گفت علاوه بر اینکه رضایت فرســـتنده به ارســـال وجوه احراز می‌شود، انتساب داده‌پیام به سازنده آن(یعنی همان فرستنده یا ارســـال‌کننده وجه) نیز به نحو مطمئن اثبات می‌گردد و لذا رکن دوم از ایجاد یک سند معتبر یعنی قابلیت انتساب نیز در پرداخت رمزارزی برقرار شده است.

برآمد

سند به عنوان یکی از مهمترین دلایل در اثبات ادعا به شمار می‌رود. یک دلیل زمانی سند محسوب می‌شود که اولاً نوشته باشد. ثانیاً آن نوشته به شخصی منتسب شود تا قابلیت استناد پیدا کند. در فضای الکترونیک که کلیه ارتباطات، الکترونیکی بوده و در قالب داده‌پیام است تنها داده‌پیامی را می‌توان نوشته دانست که کارکردهایی برابر با نوشته کاغذی داشته باشد یعنی باثبات بوده و تغییرات در آن قابل کشف باشد، باقی و قابل دسترس باشد و همچنین قابلیت ارائه اصل آن نوشته نیز وجود داشته باشد. چنین داده‌پیامی اگر ممضی به نشانه‌ای جهت انتساب به پدیدآورنده آن نیز باشد اعتباری همچون سند کاغذی خواهد داشت.

بااین‌حال همانطور که در فضای غیرالکترونیک، اسناد کاغذی دارای اعتبار و ارزش یکسانی نیستند در فضای الکترونیک هم همینطور است و ارزش اثباتی اسناد الکترونیک وابسته به اطمینان در طریق ایجاد داده‌پیام و حفظ آن است. مطابق ماده ۱۴ قانون تجارت الکترونیکی تنها این داده‌پیام‌ها هستند که به عنوان سند معتبر و محکمه‌پسند قابل ارائه می‌باشند.

در مقام تطبیق با مبانی مذکور، اطلاعات پرداخت به شیوه رمزارزی زمانی می‌تواند به عنوان سند معتبر درنظرگرفته شود که از یک سو مفهوم حقوقی سند در آن محقق شود و از سوی دیگر اطلاعات این پرداخت در مسیر ایجاد و انتقال توسط کیف پول‌ها و گره‌های شبکه ایمن بوده و در زمان ثبت و نگهداری در بلاکچین نیز از اطمینان لازم برخوردار باشند.

با تحلیل و بررسی صورت گرفته در این پژوهش دریافتیم که هر دو موضوع فوق‌الذکر در اطلاعات پرداخت مبتنی بر رمزارز تأمین شده است زیرا اولاً وجود کارکردهای نوشته در اطلاعات پرداخت محرز است چراکه ۱. به واسطه وجود سیستم اطلاعاتی مطمئن، امضای دیجیتال، الگوریتم نامتقارن و هش رمزگذاری شده در مسیر انتقال داده‌ها و همچنین ثبت آنها در بلاکچین عملکرد اول نوشته یعنی ثبات و تغییرناپذیری تأمین شده است. ۲. پس از انجام پرداخت در فضای الکترونیک اطلاعات ازبین‌نرفته و در بلاکچین ذخیره می‌شود که قابل بازیابی، درک و استفاده در مواقع لزوم می‌باشد فلذا عملکرد دوم نیز اثبات می‌شود. ۳. اطلاعات ذخیره شده در بلاکچین،

شـــرایط مقرر در ماده ۸ قانون تجارت الکترونیکی را نیز تأمین می‌نماید لذا ارائه اصل اطلاعات در محاکم نیز امکان‌پذیر است.

ثانیاً این نوشـــته قابلیت اســـنتاد را نیز دارد آن هم با مدرن‌ترین فناوری یعنی امضای دیجیتال. امضای دیجیتال با بهره‌گیری از کلید عمومی و خصوصی مطمئن‌ترین و ایمن‌ترین امضا در دنیای مدرن امروزی محســـوب می‌شـــود. این امضا علاوه بر احراز هویت و انتســـاب داده به سازنده آن، حفظ تمامیت آن را نیز تأمین می نماید. بنابراین اســـتفاده از امضای دیجیتال در فرایند پرداخت مبتنی بر رمزارز شرط انتساب را نیز در بالاترین درجه خود تأمین نموده است.

ثالثاً به واســـطه عملکرد گره‌ها و بلاکچین، وجـــود الگوریتم های رمزنگاری و امضـــای دیجیتال اطمینان مصرح در ماده ۱۴ هم در زمان ایجاد، هم در زمان انتقال و هم در زمان نگهداری و ثبت اطلاعات تأمین شده است.

با عنایت به مطالب مذکور می‌توان نتیجه گرفت با توجه به جریان ارکان ایجاد ســـند الکترونیک یعنی احراز علمکردهای نوشـــته از یک سو و قابلیت انتساب از سوی دیگر در پرداخت مبتنی بر رمزارز، اطلاعات این پرداخت، در حکم سند بوده و همچنین سیستم پرداخت مبتنی بر آن، یک سیستم مطمئن بوده که هم در مرحله ایجاد و هم در مرحلـــه نگهداری با یک رویه ایمن اطلاعات را به وجـــود آورده و حفظ می‌نماید و لذا مطابق ماده ۱۴ قانون تجارت الکترونیکی ایران و اســـناد بین‌المللی می‌توان ســـند پرداخت ناشـــی از آن را یک ســـند مطمئن و معتبر تلقی نموده و از آن در محاکم در راستای اثبات پرداخت استفاده نمود.

منابع

الف) فارسی

آلان داویدسون، ***رسانه های اجتماعی و حقوق تجارت الکترونیک***، مترجمان: حسین صادقی، فاطمه نوری و مهدی ناصر، شرکت چاپ و نشر بازرگانی، تهران، ۱۴۰۰.

حبیب زاده، طاهر، ***حقوق فناوری اطلاعات: ادله الکترونیکی***، اسناد الکترونیکی و امضای الکترونیکی(مطالعه تطبیقی)، ج۴، چاپ اول، میزان، تهران، زمستان ۱۳۹۶.

شمس، عبدالله، ***آیین دادرسی مدنی***، ج ۳، چاپ پانزدهم، انتشارات دراک، تهران، ۱۳۸۸.

صادقی نشاط، امیر، ***اعتبارسنجی اسناد الکترونیک***، فصلنامه پژوهش حقوق خصوصی، سال سوم، شماره هشتم، پاییز ۱۳۹۳

عباسی، جواد، بلاکچین: ***آشنایی با مفاهیم بنیادی***، چاپ اول، موسسه کتاب مهربان نشر، تهران، ۱۳۹۷.

عبداللهی، محبوبه؛ شهبازی نیا، مرتضی، ***سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی***، نشریه پژوهشهای حقوقی، شماره ۱۶، پاییز و زمستان۱۳۸۸، صص ۱۲۳ الی ۱۳۱.

ماکاتو یانو، کریس دای، کنیچی ماسودا و یوشیو کیشیموتو، ***بلاکچین و رمز ارزها***، مترجمان: حسین صادقی، حامد رسولخانی، مهدی ناصر و خانم زهرا خاتونی، انتشارات حقوق یار، تهران، ۱۴۰۰

فیضی چکاب، غلامنبی، ***اعتبار حقوقی دلیل و امضای الکترونیکی***(مرور اجمالی برخی منابع ملی و بین المللی)،ویژه نامه هفته پژوهش، سال دوازدهم، شماره ۳۰، پاییز ۱۳۸۹، صص ۱۷۵ الی ۲۰۴.

کیانا، کیانوش، ***آشنایی با زنجیره بلوکی(بلاکچین)***، چاپ اول، انتشارات ناقوس، تهران، ۱۳۹۸.

گروه مؤلفین نبض دانش، ***شناخت مفاهیم، شیوه سرمایه گذاری و کسب درآمد از ارزهای دیجیتال***، چاپ اول، انتشارات نبض دانش، تهران ، ۱۳۹۸.

ب) انگلیسی

Books and Articles

Biddle, B. (2017) Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace, Arizona State University (ASU) - College of Law, Available at: https://ssrn.com/abstract=3022170.

Quest, M. (2018), Cryptocurrency Master Bundle: 101 Cryptocurrency. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf.

Xu, M. Tian, Y. Li, J. (2018) Blockchain an Illustrated Guidebook to Understanding Blockchain, Translated by Jie Liv, Skyhorse Publishing, USA.

Regulations and Guides

UNCITRAL Model Law on Electronic Commerce 1996

The Guide to Enactment of UNCITRAL Model Law of Electronic Commerce 1996

UNCITRAL Model Law on Electronic Signatures 2001

United Nations Convention on the Use of Electronic Communications in International Contracts 2005