УДК 004.032.26
DOI: 10.31673/2412-9070.2020.064243

А. В. ДЗИМА, студент;
І. С. ЩЕРБИНА, канд. техн. наук, доцент;
А. М. ШТІММЕРМАН, ст. викладач;
С. В. ПРОКОПОВ, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

МЕТОДИ ШИФРУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ БЛОКЧЕЙН-ТЕХНОЛОГІЇ

Проаналізовано методи блокчейн-технологій для шифрування текстової інформації як сучасний інструмент для захисту текстових даних користувачів у мережі. У час стрімкого розвитку мережі Інтернет все частіше постає питання безпечного передавання текстової інформації між користувачами. Пересилання текстової інформації через мережу Інтернет — поширена ситуація, а захист таких даних відіграє дуже важливу роль у функціонуванні великої кількості компаній. Нині існує низка варіантів передавання текстової інформації, які потребують належного рівня захисту в процесі передавання. Методи передавання та шифрування залежать від загальних потреб відправника та отримувача.

Ключові слова: шифрування; блокчейн; смарт-контракти; месенджер; криптографія.

Вступ

Постановка проблеми полягає у визначенні найбільш ефективних методів захисту текстової інформації в мережі, адже нині завдяки криптографії та блокчейн стає можливим створення технологій, що дадуть змогу дійсно безпечно передавати текстову інформацію між користувачами в мережі Інтернет із використанням децентралізованих онлайн-сервісів на базі технології блокчейн, що працюють на основі смарт-контрактів та реалізовані як єдина децентралізована віртуальна машина. Тому за основу взято методи шифрування текстової інформації за допомогою блокчейн-технологій.

Аналіз останніх досліджень і публікацій. Дана тематика дуже предметно описується в працях таких вчених, як Р. Рівест, А. Шамір та Л. Адлеман (Массачусетський технологічний інститут) [1], а також таких науковців, як М. Бахтіарі, М. Маароф [2], О. Вербіцький [3], Д. Тепскотт, А. Тепскотт [4].

Мета статті полягає в обґрунтуванні важливості безпечного передавання текстової інформації між користувачами в мережі Інтернет та використання сучасних методів шифрування інформації на основі блокчейн-технологій.

Основна частина

Завдяки криптографії та блокчейн сьогодні стає досяжним створення технологій, що дадуть змогу дійсно безпечно передавати текстову інформацію між користувачами в мережі Інтернет. Реалізувати це уможливлюють методи шифрування текстової інформації на базі блокчейн-технологій. Розглянемо докладніше, що охоплюють дані методи.

Шифрування — це спосіб приховування початкового сенсу повідомлення або іншого документа, що забезпечує спотворення його первинного вмісту. Перетворення звичайного, зрозумілого вмісту в код називається ***кодуванням***. При цьому йдеться про взаємну однозначну відповідність між символами тексту і коду — у цьому і полягає засаднича відмінність кодування від шифрування. Зазвичай кодування і шифрування помилково приймають за одне і те саме, забуваючи про те, що для відновлення закодованого повідомлення досить знати правило заміни, тоді як для розшифрування вже зашифрованого повідомлення крім знання правил шифрування потрібен ключ до шифру. Під ключем у даному разі розуміємо конкретний секретний стан параметрів алгоритмів шифрування і дешифрування.

Симетричне шифрування — це метод криптографії, в якому один ключ відповідає за шифрування і дешифрування даних. Сторони, що беруть участь, мають цей ключ, пароль або кодову фразу, і вони можуть використовувати його для дешифрування або шифрування будь-яких повідомлень. Згідно з проектом захисту відкритих веб-додатків деякі з найбільш поширених алгоритмів, що застосовуються для симетричної криптографії, містять у собі стандарт шифрування даних (DES), який використовує 56-бітові ключі.

DES-симетричний алгоритм шифрування, в якому один ключ використовується як для шифрування, так і для розшифрування даних. Алгоритм DES широко застосовувався у процесі зберігання і передавання даних між різними обчислювальними системами, у поштових системах, в електронних системах креслень і під час електронного обміну комерційною інформацією.

Стандарт DES реалізовувався як програмно, так і апаратно. Підприємствами різних країн було налагоджено масовий випуск цифрових пристроїв, що використовують DES для шифрування даних. Усі пристрої проходили обов'язкову сертифікацію щодо відповідності стандарту. Алгоритм DES, який найбільш детально показує схему шифрування, використовувану в блокчейн, зображено на рисунку.

Схема симетричного шифрування за алгоритмом DES

Підставляння відбувається у восьми блоках підставлення. Під час виконання цієї операції 48 бітів даних діляться на вісім 6-бітових підблоків, кожний з яких за своєю таблицею замінюється чотирма бітами.

Асиметрична криптографія, також відома як криптографія з відкритим ключем, використовує загальнодоступні та закриті ключі для шифрування та дешифрування даних. Ключі — це просто великі числа, з'єднані разом, але не ідентичні (асиметричні). Один ключ із пари може бути відомий усім, він називається відкритим ключем. Другий ключ із пари зберігається в секреті, він називається закритим ключем. Будь-який із ключів може використовуватися для шифрування повідомлення, а для дешифрування застосовується протилежний ключ тому, який було використано для шифрування повідомлення. Надійність шифрування безпосередньо залежить від розміру ключа, а подвоєння довжини ключа забезпечує експоненціальне збільшення міцності, хоча і знижує продуктивність. З примноженням обчислювальної потужності зростає виявлення ефективніших алгоритмів факторингу, а отже, і здатність збільшувати розмір ключа. У разі асиметричного шифрування для забезпечення конфіденційності, цілісності, автентичності і відмовостійкості користувачі і системи мають бути впевнені, що відкритий ключ є справжнім і належить заявленій особі або суб'єктові, а також що його не було підроблено або замінено зловмисниками.

Алгоритм шифрування RSA — криптографічний алгоритм із відкритим ключем, що ґрунтується на обчислювальній складності задачі факторизації великих цілих чисел. RSA є першим алгоритмом шифрування з відкритим ключем [1]. Назва системи походить від перших літер прізвищ її авторів — Рональд Рівест, Аді Шамір і Леонард Адлеман — трьох вчених із Массачусетського технологічного інституту. Після вивчення опублікованої 1976 року статті Вітфілда Діффі та Мартіна Хеллмана «Нові напрямки в криптографії», яка заклала основи криптографії з відкритим ключем, Рівест, Шамір і Адлеман розпочали пошуки математичної функції, яка дала б змогу реалізувати модель системи, описаної в статті. Після опрацювання більш як 40 можливих варіантів вченим вдалося відшукати алгоритм, що грунтується на тому, наскільки легко діставати великі прості числа і наскільки складно розкладати на множники твір двох великих простих чисел. Для шифрування використовується проста операція піднесення до степеня за модулем N. Для розшифрування потрібно обчислити функцію Ейлера від числа N, тобто знати розкладання числа N на прості множники (у цьому полягає завдання факторизації). У криптографічній системі RSA відкритий і закритий ключі складаються з пари цілих чисел. Саме тому блокчейн-методи шифрування якнайкраще відповідають поставленому завданню.

Висновки

Дослідження проблеми безпечного передавання даних між користувачами в мережі Інтернет показало, що завдяки сучасним технологіям блокчейн та криптографії уможливлюється функціонування платформ, які забезпечують конфіденційність, безпеку та цілісність у процесі обміну даними між користувачами в мережі Інтернет, а завдяки гнучкості, універсальності та доступності може бути реалізовано в багатьох сферах життя.

Список використаної літератури

1. ***Rivest R., Shamir A., Adleman L.*** *A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM. NYC: ACM, 1978.*

2. ***Bakhtiari M., Maarof M. A.*** *Serious Security Weakness in RSA Cryptosystem // IJCSI. 2012.*

3. ***Вербіцький О. В.*** *Вступ до криптології. Львів: ВНТЛ, 1998. 248 с.*

4. ***Тепскотт Д., Тепскотт А.*** *Блокчейн-революція. Київ: Літопис, 2019. 492 с.*

А. В. Дзыма, И. С. Щербина, А. Н. Штиммерман, С. В. Прокопов

МЕТОДЫ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Проанализированы методы блокчейн-технологий для шифрования текстовой информации как современный инструмент для защиты текстовых данных пользователей в сети. Во время стремительного развития сети Интернет все чаще возникает вопрос безопасной передачи текстовой информации между пользователями. Пересылка текстовой информации через сеть Интернет — распространенная ситуация, а защита таких данных играет очень важную роль в функционировании большого количества компаний. В настоящее время существует ряд вариантов передачи текстовой информации, которые требуют надлежащего уровня защиты в процессе передачи. Методы передачи и шифрования зависят от общих потребностей отправителя и получателя.

Ключевые слова: шифрование; блокчейн; смарт-контракты; мессенджер; криптография.

A. V. Dzyma, I. S. Shcherbyna, A. M. Shtimmerman, S. V. Prokopov

METHODS FOR ENCRYPTING TEXT INFORMATION USING BLOCKCHAIN TECHNOLOGIES

The article analyzes the methods of blockchain technologies for encrypting text information as a modern tool for protecting the text data of users on the network. During the rapid development of the Internet, the question of the secure transfer of text information between users is increasingly raised. Sending text information over the Internet is a common situation, and the protection of such data plays a very important role in the functioning of a large number of companies. Currently, there are a number of options for the transmission of text information, which require an appropriate level of protection during transmission. Transmission and encryption methods depend on the general needs of the sender and receiver.

Thanks to cryptography and blockchain, it is now possible to create technologies that will allow you to truly securely transmit textual information between users on the Internet. Methods of encrypting text information based on blockchain technologies make it possible to implement this. You need to consider what these methods consist of Encryption is a way to hide the original meaning of a message or other document that distorts its original content. Converting plain, clear content into code is called encoding. This implies that there is a mutual unambiguous correspondence between the symbols of the text and the code — this is the fundamental difference between encoding and encryption. Encryption and encryption are often mistaken for the same thing, forgetting that to recover an encrypted message, it is enough to know the replacement rule, while to decrypt an already encrypted message in addition to knowing the rules of encryption, you need a cipher key. The key in this case means a specific secret state of the parameters of encryption and decryption algorithms.

Keywords: encryption; blockchain; smart contracts; messenger; cryptography.

УДК 621.395.348.4:004.4 **DOI:** 10.31673/2412-9070.2020.064448

V. M. DANYLCHENKO, Senior Lecturer;
V. R. MYKOLAICHUK, Senior Lecturer;
O. M. TKALENKO, PnD in technics, Associate Professor;
A. S. DIDKIVSKYI, student,
State University of Telecommunications, Kyiv

INITIAL SETUP OF PBX SERVER BASED ON ASTERISK

The development of information technology is very dynamic, in particular, actively developing computer networks, which are increasingly used for telephone conversations. Recently, there has been increased interest in IP-telephony technologies, in other words PBX, the use of which can significantly reduce the cost of telephone communication within the company. PBX (Private Branch exchange) is a system of devices that provides automatic connection and support of telephone communication between subscribers of this PBX, who use special end devices — telephones. A virtual PBX is a powerful telephone system that uses an Internet connection as opposed to standard telephone services. A standard PBX is used to transfer calls from the Internet to a public telephone switching network. Virtual PBX can be considered as a more economical version, because no equipment is involved, everything is virtual and hosted by the service provider. Currently, the open communication platform Asterisk occupies almost 85% of the open source PBX market. The Asterisk automatic telephone exchange supports both IP-telephony protocols and traditional communication lines. All basic and advanced PBX functions are supported: voice menu, call recording, call statistics, voicemail, queuing and operator distribution. Video communication is directly supported. The latest versions of Asterisk support call encryption. Asterisk has simple and well-documented interfaces for integration with other systems, making it easy to embed communications in business processes and business applications. There are a large number of various graphical tools for administering Asterisk, both paid and free, among which the most popular is the free WEB interface FreePBX.

Keywords: Server; IP-address; IP-telephony; Asterisk; FreePBX web-management; PBX; VoIP protocol.

Introduction

Today, the development of informative technologies is very active, in particular, computer networks are actively developing, they are increasingly used by users for telephone conversations. Recently, there has been an increased interest in IP-telephony technologies, in other words, automatic telephone exchange, the use of which can significantly reduce the cost of telephone communication within the company. For this reason, many companies began to switch to use PBX (private branch exchange) — the system of devices that provides automatic connection and maintenance of telephone communication between the subscribers of this PBX, using special terminal devices for this — telephone sets.

Research analysis

Asterisk, in conjunction with the required equipment, has absolutely all the capabilities of a traditional PBX, supports a large number of VoIP protocols and provides voice mail, conference, interactive voice menu, call queuing and other functions.