УДК 004.023

Щербіна Є.С.
Месюра В.І.

ПРОГРАМНА РЕАЛІЗАЦІЯ ЯДРА КРИПТОВАЛЮТИ

Вінницький національний технічний університет

Анотація
Розглянуто актуальність задачі розпізнавання образів. Розглянуто існуючі методи розв'язання поставленої задачі, та запропоновано використання методу Віоли-Джонс для її вирішення.
Ключові слова: *розпізнавання образів, метод Віоли-Джонса, метод Хаара.*

Abstract
The relevance of the problem of pattern recognition was considered. The existing methods for solving this problem was considered and suggested the use of Viola-Jones method to solve it.
Keywords: *pattern recognition, Viola-Jones method, Haar method.*

Вступ

На сьогоднішній день у світі дуже розповсюджений спосіб оплати з використанням електронних гаманців та готівки, переведеної у криптовалюту. Існує декілька сотень різних видів криптовалют, проте найпопулярнішою є біткоін - електронна валюта, концепт якої був озвучений 2008 року Сатосі Накамото.

Огляд існуючих криптовалют

У сучасному світі найбільш розповсюдженими є такі криптовалюти: біткоін(bitcoin), лайткоін(litecoin), праймкоін(primecoin) та неймкоін(namecoin). Кожна з них має свої недоліки, наприклад: біткоін має доволі низьку швидкість обробки транзакцій - на кожну витрачається приблизно десять хвилин. Лайткоін, хоч і має більшу швидкість обробки транцакцій, проте це очевидно створює форки блокчейну. Щодо прайм коін, то дана валюта має доволі цікаву особливість - розрахунки, що ведуться майнерами, допомагають у аналізі теорії чисел, а не є даремними, як в усіх інших валютах. Неймкоін має всі ті ж самі недоліки, що й біткоін, проте з огляду на те, що він був створенний пізніше, він не користується особливою популярністю.

Огляд недоліків Bitcoin

Так як біткоін є найпершою криптоволютою, він встиг акумулювати велику кількість недоліків, таких як:

1. Штучне обмеження мови програмування транзакцій;
2. Пластичність транзакцій (Transaction Malleability);
3. Довгий час підтвердження транзакцій;
4. Централізація через невдало обраний алгоритм майнінгу;
5. Складна процедура внесення змін до реалізації криптовалюти.

З огляду на те, що впроваджувати вирішення перелічених вище проблем по технічним і політичним причинам є складною задачею, доцільною вважається розробка власного виду криптовалюти.

Висновки

На сьогоднішній день зацікавлення біткоін тільки зростає, як і зростає кількість компаній, чия робота базується на операціях з цією валютою. У великих містах навіть проводиться чимало спеціальних навчальних курсів, де вивчають нюансам роботи з даною віртуальною валютою. Тому, з огляду на вище розглянуті проблеми, доцільною є розробка власної інтерпритації криптовалюти, яка не буде містити у собі проблеми, як наприклад проблема зі штучним обмеженням на мову програмування транзакцій (смарт-контрактів).

Для подальших досліджень потрібно провести відповідні модифікації класичного алгоритму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
3. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
4. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
5. A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
6. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
7. W. Feller, "An introduction to probability theory and its applications," 1957.

Щербіна Євгеній Сергійович — *студент групи 1КН-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sototonamitol@gmail.com*

Науковий керівник – ***Месюра Володимир Іванович****— канд. техн. наук, доцент, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.*

Evgeniy S. Scherbina *— student of Information Technologies and Computer Engineering Department, 2CS-13b, Vinnytsia National Technical University, Vinnytsia, e-mail: sototonamitol@gmail.com*

Supervisor - ***Volodymyr I. Mesyura*** *— Cand. Sc (Eng.), Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.*