УДК 004.023

Щербіна Є.С.
Месюра В.І.

АНАЛІЗ МОВ НАПИСАННЯ СМАРТ КОНТРАКТІВ ІСНУЮЧИХ КРИПТОВАЛЮТ

Вінницький національний технічний університет

Анотація
Розглянуто існуючи мови написання смарт- контрактів. Розглянуто їх переваги та надоліки. Проведено аналіз існуючих вразливостей. Проведено аналіз середовище виконання(runtime) смарт-контрактів.
Ключові слова: криптоалюти, біткоін, ефириум, смарт-контракт.

Abstract
Considered existing smart-contract languages. Considered their benefits and drawbacks. Analyzed existing vulnerabilities. Analyzed runtime of smart-contracts.
Keywords: crypto-currency, bitcoin, ethereum, smart- contract.

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 підходів до написання смарт- контрактів

У сучасному світі існує декілька підходів до написання смарт-контрактів. Коротко розглянемо їх.
1) Bitcoin (Bitcoin-Scrypt) обмежена стекова мова програмування. Відсутні цикли I/O операції, дані зберігаються у двох стеках(основний/допоміжний). Bitcoin-Scrypt є низькорівневою мовою програмування. Ведуться розробки, щодо написання транслятора із деякої JavaScript-like, c- like мови програмування у Bitcoin-Scrypt.
2) Ethereum (Solidity, Serpent, …). Ethereum має дуже розвинуту систему написання смарт- контрактів. Ethereum має свою віртуальну машину EVM(Ethereum Virrtual Machine), має декілька спеціалізованих високорівневих мов програмування(Solidity, Serpent, тощо) які компілються у байт-код для EVM. На відміну від Bitcoin-Scrypt Solidity надає програмісту можливість працювати з регістровою пам'яттю та інші потужні можливості, але має і деяки обмеження, що були введені в цілях безпеки.
3) Останній варант - надання майже повної свободи у написанні смарт-контрактів. Програмісту надається можливість писати смарт-контракти на Rust, Java, тощо. За для безпеки увесь код смарт-контрактів має бути проаналізований програмістами перед розгортанням.

Огляд існуючих вразливостей у середовищах написання смарт-контрактів

1) Аналіз mutability-problem у біткойн.
2) Аналіз опкодів, у реалізації яких були знайдені вразливості.
3) Аналіз атак на смарт-контракти, наприклад DAO.

Висновки

На сьогоднішній день можна виділити три основні підходи для написання смарт-контрактів, вони є результатом компромісу між функціональними можливостями і безпекою. В ході роботи ми проаналізуемо ці мови програмування та їх середовище виконання(runtime).

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-17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sototonamitol@gmail.com*

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, 1CS-17m, Vinnytsia National Technical University, Vinnytsia, e-mail: sototonamitol@gmail.com*

Volodymyr I. Mesyura *— Ph.D., Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.*