УДК 004.023

АНАЛІЗ МОВ НАПИСАННЯ СМАРТ КОНТРАКТІВ ІСНУЮЧИХ КРИПТОВАЛЮТ

Щербіна Євгеній, Месюра Володимир

Вінницький національний технічний університет

Анотація

Розглянуто існуючі мови написання смарт-контрактів. Розглянуто їх переваги та надоліки. Проведено аналіз існуючих вразливостей. Проведено аналіз середовища виконання (runtime) смарт-контрактів.

Abstract

Considered existing smart-contract languages. Considered their benefits and drawbacks. Analyzed existing vulnerabilities. Analyzed runtime of smart-contracts.

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.

Bitcoin

Bitcoin — електронна валюта, концепт якої був озвучений 2008 року Сатосі Накамото, і представлений ним 2009 року, базується на самоопублікованому документі Сатосі Накамото. Повна капіталізація ринку біткоїнів на 5 грудня 2017 року, коли курс сягав 12 000 $, становить 200 млрд USD. Середня ціна одного біткоїна на 30 листопада 2017 року — понад 10 000 $.

У грудні 2017 року Bitcoin став шостою за капіталізацією валютою світу, обійшовши рубль, фунт і південнокорейську вону. 7 грудня курс досяг свого чергового максимуму в 17,7 тис. дол.. Наступний ріст до 20 тис. доларів відбувся 17 грудня, потім курс впав до 16 тис. У 2018 році курс продовжив падати. Періодично підіймаючись і падаючи на 10-20%, станом на 5 квітня 2018 року 1 Bitcoin коштує 6800 дол [1].

Ethereum

Ethereum — платформа для створення практично будь-яких децентралізованих онлайн-сервісів на базі блокчейна (Đapps), що працюють на базі смарт-контрактів. Реалізована як єдина децентралізована віртуальна машина. Ідея була втілена 30 липня 2015 року. Оскільки Ethereum сильно спрощує і здешевлює впровадження блокчейна, його впроваджують як великі гравці, такі як Microsoft, IBM, Acronis, Сбербанк, банківський консорціум R3, так і нові стартапи [2].

Огляд існуючих підходів до написання смарт-контрактів

У сучасному світі існує декілька підходів до написання смарт-контрактів. Коротко розглянемо кожен із них:

- Bitcoin (Bitcoin-Scrypt) обмежена стекова мова програмування. В ній відсутні цикли I/O операції, дані зберігаються у двох стеках (основний/допоміжний). Bitcoin-Scrypt є низькорівневою мовою програмування. Ведуться розробки, щодо написання транслятора з деякої JavaScript-like, c-like мови програмування у Bitcoin-Scrypt [3].

- Ethereum (Solidity, Serpent, …). Ethereum має дуже розвинуту систему написання смарт-контрактів. Він має свою віртуальну машину EVM (Ethereum Virrtual Machine),

декілька спеціалізовних високорівневих мов програмування (Solidity, Serpent, тощо) які компілюються у байт-код для EVM. На відміну від Bitcoin-Scrypt Solidity надає програмісту можливість працювати з регістровю пам'яттю та інші потужні можливості, але має і деякі обмеження, що були введені в цілях безпеки.

- Останній варіант - 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 проаналізовний програмістами перед розгортанням [4].

Огляд існуючих вразливостей у середовищах написання смарт-контракті

- Аналіз mutability-problem у біткойн.
- Аналіз опкодів, у реалізації яких були знайдені вразливості
- Аналіз атак на смарт-контракти, наприклад DAO [5].

Анализ вихідного коду середовищ виконання смарт-контрактів

- Проаналізувати код BitcoinScrypt у reference implementation Bitcoind: https://github.com/bitcoin/bitcoin.
- Проаналізувати package txscrypt в імплементаії Bitcoin протоколу на мові програмування GoLang https://github.com/btcsuite/btcd [6].
- Проаналізувати код Go-Ethereum (https://github.com/ethereum/go-ethereum) - імплемнтації Ethereum протоколу на мові програмування GoLang.
- Проанлізувати специфікацію EVM (Ethereum Virtual Machine) та інших високоріввневих мов програмування (Solidity, Serpent, тощо), що компілюються у байт-код для EVM.
- Спробувати застосувати класичні атаки (атаки, що застосовуються для продуктів, що написані на мовах програмування C/C++/Java/C#) на смарт-контракти, що реалізовані на мовах програмуання Solidity, Serpent, BitcoinScrypt тощо [7].

Висновки

На сьогоднішний 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 використаних джерел:

1. Види криптовалют і їх популярність [Електронний ресурс]. — Режим доступу: https://pingblockchain.com/vidi-kriptovaljut-i-ih-populjarnist/
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. 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
4. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133.
5. W. Feller, "An introduction to probability theory and its applications," 1957
6. A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
7. 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