УДК 336.743

Гарабурда Д.О.
Бойко О.Р.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ BLOCKCHAIN НА ПРИКЛАДІ BITCOIN

Вінницький національний технічний університет

Анотація
Розглянуто особливості застосування технології Blockchain на прикладі Bitcoin, що дозволяє підвищити захищеність електронних даних від зовнішнього впливу третіх осіб.
Ключові слова: гаманець, адреса, блок, транзакція, хеш.

Abstract
Features of the application of technology Blockchain in Bitcoin, which can increase the security of electronic data from external influence of third parties.
Keywords: wallet, address, block, transaction, hash.

Вступ

Сьогодні питання захисту інформації від несанкціонованого доступу з боку третіх осіб стоїть дуже жорстко. Мережа інтернет розвивається дуже стрімко і кількість випадків шахрайства зростає у геометричній прогресії, що вимагає нових та ефективних рішень у сфері захисту електронної інформації. На допомогу приходить технологія Blockchain, яка знайшла широке застосування у криптовалюті Bitcoin і на протязі багатьох років показує свою ефективність.

Метою роботи є визначення особливостей застосування технології Blockchain на прикладі Bitcoin та огляд можливості застосування даної технології для інших сфер застосування електронної інформації.

Результати роботи

Технологія Blockchain дозволяє досягти високого показника надійності та безпеки електронної інформації за рахунок використання хешування деревовидної структури знизу – вверх. Такий підхід дозволяє захищати дані від несанкціонованого доступу так як зміна хоча б одного параметру цієї структури викликає невідповідність хешу структури вище, так як вони зав'язані один на одному.

Усе вище сказане підтверджується застосування даної технології та адаптація її до криптовалюти Bitcoin. Найвищою структурною одиницею у криптовалюті Bitcoin є блок. Блок являє собою певний реєстр виконаних операцій в мережі. Послідовність блоків формує собою історію здійснених операцій за весь період та дозволяє відслідкувати рух коштів від самого початку. Блок зберігає транзакції, які, в свою чергу, зберігають адреси гаманців звідки списуються монетки та адреси гаманців куди ці монетки будуть зараховуватися. Тому можна сформувати чітку ієрархічну структуру зверху – вниз: блок – транзакція – адреса [1]. Тепер найголовніше питання, як забезпечується безпека даних від впливу третіх осіб в мережі. Для забезпечення цілісності даних використовується ланцюжок хешів знизу – вверх. На хеш транзакції впливає послідовність адрес, монет та розмір транзакції в байтах тощо. На даному етапі у випадку зміни хоча б одного параметру транзакції з боку третьої сторони викличе зміну загального хешу транзакції. Так як транзакції вкладаються у вищий структурний елемент, що називається блоком, їх хеші впливають на загальний хеш блоку. Окрім цього на загальний хеш блоку впливає хеш попереднього блоку, показник складності, який розраховується майнерами для вирішення задачі (хеш блоку повинен мати, наприклад, на початку 15 нулів), розмір блоку у

байтах тощо. Таким чином мережа контролює правильність блоків розраховуючи хеши структури знизу - вверх та співставляючи їх з хешами присутніми в структурі. У разі виявлення зміни мережа відкидає такий блок і не вважає його правильним.

Таким чином технологія Blockchain показує високі показники захищеності електронної інформації у криптовалюті Bitcoin уже на протязі багатьох років за рахунок використання деревовидної структури хешів.

Висновки

Встановлено, що технологія Blockchain являється ефективним засобом забезпечення цілісності електронної інформації, що підтверджується успішністю використання у криптовалюті Bitcoin на протязі багатьох років. Уряди багатьох країн вважають дану технологію захисту інформації перспективною та вкладають кошти у її розвиток та адаптування до різноманітних сфер технологічнх процесів. Це показує що дана технологія має перспективи у розвитку та застосуванні в майбутньому. Наступним кроком дослідження є адаптація технології Blockchain для нових сфер технологічних процесів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Анопулус А. Овладение Биткойном / А. Анопулус – М. : O'Really Media, Inc., 2014 – 298 с.

Гарабурда Дмитро Олегович – аспірант, факультет комп'ютерних систем та автоматики, Вінницький національний технічний університет, Вінниця, e-mail: seelseel93@gmail.com.

Бойко Олексій Романович – канд. техн. наук, доцент кафедри автоматики електроніки та комп'ютерних систем управління, Вінницький національний технічний університет.

Науковий керівник: ***Бісікало Олег Володимирович*** – д-р техн. наук, професор, декан факультету комп'ютерних систем та автоматики, Вінницький національний технічний університет, м. Вінниця.

Haraburda Dmytro O. – Department of Computer Systems and Automatic, Vinnytsia National Technical University, Vinnytsia, e-mail: seelseel93@gmail.com.

Boyko Oleksiy R. – Cand. Sc. (Eng.), Assistant Professor of Computer Systems and Automatic, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Bisikalo Oleh V.*** — Dr. Sc. (Eng.), Professor, Dean of the Computer Systems and Automatic, Vinnytsia National Technical University, Vinnytsia.