Інформаційні технології

УДК 004.852

**Сидоренко Захар Андрійович**

бакалавр комп'ютерних наук

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

**Сидоренко Захар Андреевич**

бакалавр компьютерных наук

Национального технического университета Украины

«Киевский политехнический институт имени Игоря Сикорского»

**Sydorenko Zakhar**

bachelor of computer science of

The National Technical University of Ukraine

«Kyiv Polytechnic Institute»

# АНАЛІЗ ТА РЕАЛІЗАЦІЯ SMART CONTRACT

# АНАЛИЗ И РЕАЛИЗАЦИЯ SMART CONTRACT

# ANALYSIS AND IMPLEMENTATION OF SMART CONTRACT

**Анотація:** Проведено аналіз основних плюсів та мінусів смарт-контрактів, а також наведене приклад реалізації.

**Ключові слова:** smart contract, Blockchain, блок, ланцюжок блоків.

**Аннотация**: Проведен анализ основных плюсов и минусов смарт-контрактов, а также приведены примеры реализации.

**Ключевые слова**: smart contract, Blockchain, блок, цепочка блоков.

**Annotation:** The analysis of the main advantages and disadvantages of smart contracts has been carried out, as well as an example of implementation.

**Keywords:** smart contract, blockchain, block, chain of blocks.

Сьогодні існує окремий тип юристів, який займається складанням і супроводом контрактів. Такі контракти написані юридичною мовою, містять велику кількість сторінок і не завжди до кінця зрозумілі звичайним людям.

Традиційні контракти не тільки важкі в складанні, але і вимагають залучення третіх осіб для забезпечення їх дотримання. У випадку розбіжностей, сторони змушені звертатися до судів, що забирає ще більше часу і грошей [1].

З наближенням цифрової ери, прогрес торкнувся і цієї важливої частини суспільних взаємовідносин. У 1994 році юрист і криптограф Нік Сабо описав концепцію розумних контрактів (smart contracts), визначивши такий контракт як "електронний протокол передачі інформації, що забезпечує виконання сторонами умов контракту".

На думку автора концепції, смарт-контракти дозволили б забезпечувати автоматичне виконання умов угод (виробництво виплат, конфіденційність і навіть примусове виконання зобов'язань сторін) з мінімальними витратами на їх супровід і без необхідності залучення третіх осіб для забезпечення довіри.

Хоча технологія, здатна підтримувати смарт-контракти, з тих пір помітно розвинулася, запропоноване Сабо визначення і зараз точно виражає суть поняття [2].

У широкій інтерпретації, першим і найпростішим смарт-контрактом можна назвати протокол для здійснення транзакцій в мережі біткоін, адже її можна визначити наступним чином: «Блокчейн - це розподілений реєстр,

що дозволяє користувачам передавати інформацію та цінність без допомоги банків і посередників»

Виникнення технології блокчейн відкрило перспективу для створення систем, що дозволяють укладати і автоматично виконувати операції для досягнення заздалегідь заданих умов, минаючи централізованих посередників.

На відміну від юридичної мови паперових договорів, код не має подвійного тлумачення та інших лінгвістичних аспектів. Оскільки смарт-контракти є програмами і створюються на основі комп'ютерної логіки, сторони угоди можуть бути впевнені, що умови, прописані в коді контракту, будуть дотримані неухильно і не можуть бути змінені заднім числом [3].

Варто відзначити, що в останній рік жорсткість дотримання цієї властивості була піддана серйозному випробуванню, що в підсумку призвело до ідеологічного розколу в суспільстві найпопулярнішою на сьогодні системи для розумних контрактів Ethereum і подальшого хардфорку (певна зміна програмного коду, яка змінює структуру блоку, тобто зміна протоколу).

Проте відмова від послуг централізованих посередників і автономне виконання смарт-контрактів дозволяють істотно економити на забезпеченні чесності їх дотримання. Так як будь-який окремо взятий посередник може виявитися зацікавленим в тому чи іншому результаті угоди, оскільки вартість угоди може бути дуже великою.

Тому важливою особливістю розумних контрактів на блокчейні є децентралізоване виконання. Умови, необхідні для дотримання розумних контрактів, поширюються по всій розподіленій мережі блокчейн за допомогою тих самих механізмів, які передають інформацію про звичайні транзакції. Коли комп'ютери в мережі отримують інформацію про контракт, кожен з них приходить до незалежного рішенням щодо

виконання умов контракту, після чого звіряється з іншими вузлами мережі. Таким чином, жодна сторона не може самостійно вплинути на рішення, оскільки виконання угоди знаходиться в руках всієї системи цілком.

Щоб краще зрозуміти принцип роботи смарт-контрактів, можна порівняти їх з телефонними і торговими автоматами. Зазвичай для здійснення торгових операцій виробник, і кінцевий покупець стикаються з великою кількістю посередників, але в разі смарт-контрактів, опущена в автомат монета дозволить відразу отримати товар або послугу.

Найпростішим прикладом смарт-контракту є мультипідпис (multisig, escrow). За допомогою такого контракту контрагенти, які один одному не довіряють, можуть заморозити деяку суму монет на блокчейн таким чином, що в разі необхідності витратити цю суму будуть потрібні підписи більше половини учасників. Подальше ускладнення таких контрактів дозволяє вибудовувати моделі для голосувань про розподіл коштів у рамках децентралізованих фондів [4].

На практиці це означає, що інвестор, приймаючи участь в ICO і відправляючи криптовалюту на гаманець проекту, може бути впевнений в тому, що в разі провалу краудсейл-кампанії, його кошти будуть автоматично повернені. А в разі успішного збору заявленої суми, кошти будуть перераховані розробникам тільки тоді, коли достатня кількість учасників активують свої ключі, тим самим особисто підтверджуючи сумлінність проекту.

Смарт-контракти потенційно можна використовувати і для будь-яких фінансових дій в реальному світі - страхування, реєстрація і передача власності, кредитування, краудфандінг і так далі.

Нижче наведений код (Рис. 1), написаний для звичайного розумного контракту на блокчейн-платформі Ethereum. Контракти можуть бути написані в будь-якому блокчейні, але Ethereum найбільш популярний, оскільки надає необмежені можливості для написання розумних контрактів і роботи з ними.

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Рис. 1 Код для розумного контракту [5]

В майбутньому смарт-контракти, швидше за все, стануть невід'ємною частиною нашого життя. Крім якісних змін у фінансовому секторі і побутовій сфері, розумні контракти можуть змінити і саму ділову інфраструктуру, яка допомагає функціонувати суспільству. Цілі дисципліни юриспруденції стануть непотрібними або зміняться до невпізнанності. Замість багатосторінкових паперових контрактів, де

потрібно вивіряти кожне слово, люди будуть користуватися смарт-контрактами, створеними за шаблоном або створювати унікальні контракти з допомогою універсальної цифрового мови. У той же час, повсякденна побутова економічна діяльність людей стане більш структурованою і безпечною без видимого ускладнення для споживача.

**Література:**

1. Antonopoulos Andreas Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Antonopoulos Andreas – K. : NGITS, 2014. – C. 150 – 290
2. Tapscott Don, Tapscott Alex Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Tapscott Don, Tapscott Alex – K. : Information Systems, 2016 – C. 100 – 150.
3. Vigna Paul, Casey Michael The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / Vigna Paul, Casey Michael – K. : Economic, 2015 – C. 200 – 210.
4. Skinner Chris Value Web / Skinner Chris – K. : Information technologies, 2016 – C. 150 – 175.
5. Blockchain Wallet API: Bitcoin Wallet API – Blockchain – Режим доступа: https://www.ethereum.org/token/. - Дата доступу : 30.06.2017.