DOI: 10.46340/eppd.2021.8.5.18

Vladyslav Shkolnyi

ORCID ID: <https://orcid.org/0000-0002-9044-7003>

Taras Shevchenko National University of Kyiv, Ukraine

FORMS AND TYPES OF FORMATION OF VIRTUAL ASSETS (CRYPTOCURRENCIES)

Владислав Школьний

Київський національний університет імені Тараса Шевченка, Україна

ФОРМИ ТА ВИДИ ФОРМУВАННЯ ВІРТУАЛЬНИХ АКТИВІВ (КРИПТОВАЛЮТИ)

The article considers the principles of the emergence of virtual assets (cryptocurrencies) and the impact on these events of economic, socio-political relations through technological features. The paper considers the influence of the Austrian School of Economics and its achievements on the emergence and development of modern virtual assets, namely they considered the impact on the choice of available currencies: 1) as the purchase of goods and services, 2) as a reserve for future needs; 3) as deferred payments; 4) as a unit of account. According to Hayek's theoretical framework, market forces will determine the relative values of different competing currencies. As a result, exchange rates between competing currencies will float freely. The ideas of scientists such as Hayek and Mises and the ideas of the Austrian school of economics formed the basis of such a political trend as cryptoanarchism. Cryptoanarchism can be described as the realization of cyberspace and the manifestation of anarchism, a philosophy whose main goal is to respect human freedoms in cyberspace, regardless of status.

The author dwells on the characteristics of the DigiCash system, the Hashcash project, as well as the concept of Proof-of-Work in the context of their impact on the formation and development of modern cryptocurrencies. In addition, a comparative analysis is made of the functioning of the decentralized digital money system with traditional digital money systems. In particular, it is emphasized that a decentralized approach eliminates the possibility that a certain organization will be able to block transactions. The article also raises the issue of preconditions and circumstances for the emergence of the bitcoin concept, aimed at ensuring that anyone can independently manage their funds without the intervention of third parties.

Keywords: bitcoin, cryptocurrency, virtual asset, blockchain, electronic money.

Постановка проблеми. У даний час питання емісії криптовалют та блокчейну сьогодні є надзвичайно гострим, оскільки в цих правовідносинах приватний інтерес суперечить публічному і навпаки. Тому під тиском глобалізації світ зараз переходить до гібридизації публічного до приватного регулювання, а віртуальні активи (криптовалюта) з блокчейном – це лише інструмент, за допомогою якого є намагання регулювати суспільні відносини на приватному рівні, не полишаючи спроб відокремитися від публічних інституцій з їх контролем.

Аналіз останніх досліджень і публікацій. Питання, пов'язані з формуванням ідеї такого феномену, як криптовалюти, розглядалися у роботах вітчизняних і зарубіжних дослідників, зокрема Д. Погрібний, Тімоті К. Мей, Ф. Хаєк, Л. Мізес, Дж. Д. Девідсон, В. Різ-Могт та інших дослідників.

Мета. Метою дослідження є формування ідеї віртуальних активів (криптовалют) та визначення видів віртуальних активів (криптовалют).

Викладення основного матеріалу.

До створення першої криптовалюти були спроби створити проекти, які могли б врахувати ідеї як австрійської школи економіки, так і криптоанархістів. На думку О. Баранова, особливо це стосувалося розвитку ідеї Інтернету речей (IoT)¹ та її реалізації, оскільки її реалізація вимагала

¹ Баранов, О. (2016). "Інтернет речей" як правовий термін. *Юридична Україна*, 5-6, 96-103.
<http://nbuv.gov.ua/UJRN/urykr_2016_5-6_16> (2021, серпень, 31).

міри вартості, яка була б незалежною від дії третьої сторони щодо операції між сторонами, і особливо втручання держави. Ця форма може забезпечити незалежне та обов'язкове виконання зобов'язань між сторонами, яке не базуватиметься на законі та примусі, а передбачатиметься програмним кодом.

Ідею незалежних контрактів на основі програмного забезпечення (цифрових протоколів) запропонував Нік Сабо¹, який мав забезпечити, перевірити, сприяти виконанню зобов'язань між сторонами без втручання третіх сторін, вони отримали назву інтелектуальними контрактами (smart contracts), але для реалізації цієї ідеї не було належної валюти, яка виступала: мірою вартості, засобом обміну поза банківською системою, якій можуть довіряти обидві сторони зобов'язання.

Прикладом продажу валют в Інтернеті можна назвати перші платіжні механізми, які можна назвати електронними грошима або електронними ідентифікаторами, оскільки вони не створювали незалежної вартості, а були лише електронним виразом державних фіатних грошей, прив'язаних до банківської системи і функціонували виключно в ній. Цей цифровий вираз валюти, що має характеристики децентралізації та залежить від волі третіх сторін, які працюють та підтримують їх, основною метою яких, як правило, був попит на торгівлю в кіберпросторі. Прикладом такої реалізації можна назвати VisaCash² або Mondex³, функцією яких було заощадження грошей на програмному забезпеченні, де гроші обчислювались на рахунку та продавались через чіп, вбудований у пластикову картку та прив'язаний до банківського рахунку, на якому зберігався електронний аналог фіатних грошей. У наш час ця система набула широкого поширення, а електронні гроші разом із Інтернет-банкінгом увійшли в масовий обіг. Слід зазначити, що таке рішення має недоліки, обумовлені вимогою довіри до третьої особи, та призводить до централізації відносин з електронними грошима.

Альтернативою електронним грошам мав стати проєкт DigiCash, який пропонував «електронні монети», які користувачі Інтернету могли придбати, «завантаживши» вартість зі свого банківського рахунку в електронний гаманець, що зберігається на їх персональному комп'ютері⁴. Творцем DigiCash вважається американський криптограф і вчений Девід Чаум. В цілому це була спроба Чаум протестувати різні пропозиції щодо створення платіжної системи, що не відслідковується⁵.

Система DigiCash мала дві функції, які відокремлювали її від попередніх систем, пропонуючи користувачам засоби захисту власної фінансової інформації від кіберзлочинців, та пропонували більшу анонімність користувачам, стурбованим конфіденційністю даних. Рішення було запропоноване у формі сліпих підписів, що представляють пару відкритих та приватних ключів, які разом дають можливість отримувати та передавати кошти між користувачами, таким чином для передачі коштів іншій особі потрібно було лише знання відкритого ключа, приватний залишався основним власником засобів, що давало йому право на розпорядження своїми активами, пізніше цю ідею перейняли криптовалюти⁶.

Вчений також захистив від проблеми подвійної трати своїх цифрових монет, тим самим забезпечивши неможливість подвійного платежу тими ж коштами, але проблема централізації контролю третьою стороною не була вирішена, що означало можливість фальсифікації грошового балансу своїх користувачів. На жаль, DigiCash збанкрутував і не зміг зайняти своє місце, але була можливість попрацювати над помилками та розробити шляхи вирішення проблем у майбутньому⁷.

¹ Szabo, N. (1994), Trusted Third Parties Are Security Holes. *Phonetic Sciences, Amsterdam* <<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/ttps.html>> (2021, серпень, 31).

² Adams, L. S. (1997). Task Force on Stored-Value Cards, A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money, *Bus Law*, 653.

³ An official website of the United States Government (2000). *Network, u.s. dept of the treasury, a survey of electronic cash, electronic banking, and internet gaming* <http://www.fincen.gov/news_room/tp/files/e-cash.pdf> (2021, серпень, 31).

⁴ Strassel, K. A. (1995). DigiCash Trial Puts Electronic Currency on Internet Network – Dutch Concern, Others Search for More Secure Methods of Cyberspace Commerce. *The Wall Street Journal*, April, 17, B6D.

⁵ Chaum, D. (1998). Blind signatures for untraceable payments. *BME Department of Networked Systems and Services (HIT)* <<http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>> (2021, серпень, 31).

⁶ Там само.

⁷ Там само.

Необхідно згадати про проєкт Hashcash. Система Hashcash була запропонована у травні 1997 року британським фахівцем в галузі криптографії та шифропанку Адамом Беком. З назви проєкту випливає, що він побудований на основі хешування. Хешування – це процес перетворення будь-якого масиву даних у вихідний бітовий рядок заданої довжини, що складається з шістнадцяткового числа. Це при додаванні до речення хоча б одного додаткового символу повністю змінює бітовий термін на виході. Більше того, хеш цих двох словесних конструкцій не можна передбачити, після першого хешування неможливо обчислити на основі існуючої послідовності хешів другого. Єдиний спосіб – це хешування двох речень цих конструкцій. Проєкт формалізував метадані електронної пошти (відправник, одержувач, час) як протокол. Відправник повинен був додати до метаданих довільне число. Вихідні метадані будуть хешовані та перетворені у довільну послідовність символів.

На думку фахівця Адама Бека, особливістю є те, що не кожен хеш вважається дійсним. Натомість двійкова версія хешу повинна починатися з певної кількості нулів, наприклад, 20 нулів. Відправник може генерувати хеш, починаючи з 20 нулів, включаючи довільне слово, але відправник не може заздалегідь знати, яким він буде наприкінці процесу. Щоб сформувати дійсний хеш, відправник повинен використовувати єдину доступну йому опцію: повний метод підбору. Йому доводиться пробувати різні числові показники, поки він не знайде правильної комбінації. Все це вимагає певних комп'ютерних розрахунків, які називаються Proof-of-Work¹.

Вперше концепція Proof-of-Work була описана в 1993 році в роботі авторів Синтії Дворк і Мони Наор «Pricing via Processing, or, Combatting Junk Mail, Advances in Cryptology»². Proof-of-Work став фактично першою концепцією, заснованою на віртуальній нестачі та відсутності централізації: ця модель прив'язувала цифрові дані до реальних, обмежених обчислювальних потужностей. Такий дефіцит був гарною передумовою для створення валюти. Незважаючи на свою назву, Hashcash не міг стати повноцінними грошима. Важливо, щоб отриманий доказ виконаної роботи не мав значення для одержувача. На відміну від грошей, їх неможливо витратити знову деінде. Більше того, щорічне прискорення обчислювальної потужності призведе до того, що докази виконаної роботи будуть виконуватися швидше, але з меншими витратами, що спровокує гіперінфляцію Hashcash. Однак концепція Proof-of-Work стала основою для подальших досліджень у галузі цифрових грошей.

Це відображено в протоколах біткойнів та ефіру. Сама концепція в них була мінливою. На відміну від Hashcash та пропозицій на його основі, дефіцит сам по собі не використовується як гроші. Натомість Hashcash пропонує конкуренцію. Майнер, який першим обчислює правильний хеш блоку в мережі біткойн або ефір, вирішує, як додати транзакції в такий блок. Теоретично будь-який учасник змагається на рівних умовах, як і в лотереї: навіть дрібні майнери можуть статистично виграти і закрити блок, отримавши криптовалюту. Після отримання нового блоку та підтвердження транзакцій скасувати його буде неможливо. Зловмисникові потрібно буде виконати такий самий обсяг роботи, який потрібен для вилучення блоку, на додаток до кожного додаткового блоку, що за звичайних обставин стає експоненціально складним завданням. Реальні ресурси, які потрібно витратити на атаку, зазвичай набагато перевищують потенційний прибуток, що надає користувачам біткойнів упевненості в завершенні кожної транзакції. Таким чином, така прийнята концепція одночасно вирішує дві проблеми. Вирішує проблему подвійних витрат шляхом децентралізації, і нові монети з'являються без участі централізованого емітента. Proof-of-Work сам по собі не може бути грошима, але децентралізована система цифрових грошей не могла не з'явитися без цієї технології.

Традиційні цифрові грошові системи використовують централізований реєстр для відстеження існуючих балансів. Подібний алгоритм використовують центральні банки, комерційні банки, VISA та інші провайдери платіжних послуг для контролю бази даних, в якій перелічені права власності. Оскільки це вже є проблемою для криптоанархістів, це не виключає державного контролю за фінансовими потоками шляхом регулювання, і учасникам системи майже завжди доводиться розкривати особисту інформацію.

¹ Back, A. (2002). A Denial of Service Counter-Measure. *Hashcash* <<http://www.hashcash.org/papers/hashcash.pdf>> (2021, серпень, 31).

² Dwork, C., Naor, M. (2001). Pricing via Processing or Combatting Junk Mail, *Annual International Cryptology Conference* <https://link.springer.com/chapter/10.1007/3-540-48071-4_10> (2021, серпень, 31).

Механізм вирішення цієї проблеми був запропонований комп'ютерним інженером, який відомий своїми знаннями в області криптографії та криптовалюти Вей Даєм, у проєкті b-money: всі учасники повинні зберігати копії реєстру транзакцій замість єдиної централізованої організації¹. Як тільки була здійснена наступна операція, учасники повинні були оновити свої реєстри. Більше того, замість справжніх імен Вей Дай запропонував використовувати відкриті ключі. Цей децентралізований підхід виключає можливість того, що одна організація зможе блокувати транзакції. У той же час користувачі отримали достатній рівень анонімності. Ці ідеї лягли в основу блокчейну – системи, за якою ордер працює ліву частку криптовалют, прикладами яких є біткойн, ефіріум, біткойн-кеш.

Їм також була запропонована інша версія, де не кожен учасник мережі мав копію реєстру. Натомість були введені нові поняття: звичайні користувачі та сервери. Однак лише сервери, що є вузлами мережі, зберігали копії реєстру. Щоб перевірити успішність транзакції, користувачам потрібно буде посылатися на випадкову послідовність серверів. У разі конфлікту продавець просто відмовляється передати товар контрагенту. У той же час, що «кожен сервер зобов'язаний внести стандартний депозит на спеціальний рахунок, який би використовувався для штрафу або винагороди у разі підтвердження недобросовісності». Сервери також повинні були періодично публікувати та криптографічно перевіряти баланси учасників.

Якщо це здається звичним, то і в цьому немає нічого дивного: друга версія b-money дещо нагадує те, що ми сьогодні знаємо як концепцію Proof-of-Stake. Цей консенсус став альтернативою Proof-of-Work, де підтвердження вимагало не підтвердження виконаної роботи, а внесення застави на страхування, що зазвичай втілюється в сучасних криптовалютах.

Під впливом фінансової кризи 2008 року, коли недовіра до банківської системи та уряду була на піку, людина, яка назвала себе Сатоші Накомото², представила свою статтю, закріпивши ідею децентралізованої валюти, ставши її «білою книгою» під назвою біткойн, яка була втіленням оцифрованого золота. Біткойн зміг засвоїти всі ідеї та філософію, яка цьому передувала. За словами вченого, біткойн був створений для того, щоб будь-яка людина могла самостійно управляти своїми коштами без втручання третіх осіб. Після того, як проєкт був підтриманий спільнотами по всьому світу, Сатоші Накомото перестав приймати будь-яку участь у проєкті³.

Висновок. Підсумовуючи викладене, можливо прослідкувати, що ідея віртуальних активів завжди цікавила світову спільноту. Очевидно, що криптовалюта – це порівняно новий інструмент фінансового ринку, але його вартість не залежить від кількості вкладеної праці, як це традиційно характерно для звичайних товарів і послуг. Оцінка структури криптовалюти показала, що біткоіни як і раніше є найпоширенішим її видом.

Сьогодні операції з криптовалютами, зокрема з біткойнами як найпоширенішою його різновидом, привертають увагу багатьох жителів планети, причому не тільки професіоналів, а й звичайних громадян. Одні хочуть заробити і активно цим займаються, інші намагаються зрозуміти, що це таке і в чому його секрет.

References:

1. Baranov, O. (2016). "Internet rechey" yak pravovyy termin ["Internet of Things" as a legal term]. *Yurydychna Ukrayina* [Legal Ukraine], 5-6, 96-103. <http://nbuv.gov.ua/UJRN/urykr_2016_5-6_16> (2021, August, 31). [in Ukrainian].
2. Szabo, N. (1994), Trusted Third Parties Are Security Holes. *Phonetic Sciences, Amsterdam* <<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/ttps.html>> (2021, August, 31). [in English].
3. Adams, L. S. (1997). Task Force on Stored-Value Cards, A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money, *Bus Law*, 653. [in English].
4. An official website of the United States Government (2000). *Network, u.s. dept of the treasury, a survey of electronic cash, electronic banking, and internet gaming* <http://www.fincen.gov/news_room/rp/files/e-cash.pdf> (2021, August, 31). [in English].

¹ Dai, W. (1998) B-Money. *Weidai* <<http://www.weidai.com/bmoney.txt>> (2021, серпень, 31).

² Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". *Nakamotoinstitute* <<http://nakamotoinstitute.org/bitcoin/>> (2021, серпень, 31).

³ Там само

5. Strassel, K. A. (1995). DigiCash Trial Puts Electronic Currency on Internet Network – Dutch Concern, Others Search for More Secure Methods of Cyberspace Commerce. *The Wall Street Journal*, April, 17. [in English].
6. Chaum, D. (1998). Blind signatures for untraceable payments. *BME Department of Networked Systems and Services (HIT)* <<http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>> (2021, August, 31). [in English].
7. Back, A. (2002). A Denial of Service Counter-Measure. *Hashcash* <<http://www.hashcash.org/papers/hashcash.pdf>> (2021, August, 31). [in English].
8. Dwork, C., Naor, M. (2001). Pricing via Processing or Combatting Junk Mail, *Annual International Cryptology Conference* <https://link.springer.com/chapter/10.1007/3-540-48071-4_10> (2021, August, 31). [in English].
9. Dai, W. (1998) B-Money. *Weidai* <<http://www.weidai.com/bmoney.txt>> (2021, August, 31). [in English].
10. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". *Nakamotoinstitute* <<http://nakamotoinstitute.org/bitcoin/>> (2021, August, 31). [in English].