УДК 336.741.243:004.738.5
DOI 10.33111/vz_kneu.21.20.01.01.005.011

Бойко В.П.
аспірант кафедри міжнародних фінансів
ДВНЗ «КНЕУ імені Вадима Гетьмана»
проспект Перемоги, 54/1, Київ, Україна
e-mail: viktorboiko@kneu.edu.ua
ORCID: 0000-0002-2810-7788

ЕВОЛЮЦІЯ ДЕЦЕНТРАЛІЗОВАНИХ ПЛАТІЖНИХ СИСТЕМ ЯК ІННОВАЦІЙНОГО ВИДУ ГРОШЕЙ

Boiko Viktor
PhD student in International Finance
KNEU named after Vadym Hetman
Peremohy avenue, 54/1, Kyiv, Ukraine
e-mail: viktorboiko@kneu.edu.ua
ORCID: 0000-0002-2810-7788

EVOLUTION OF DECENTRALIZED PAYMENT SYSTEMS AS AN INNOVATIVE MONEY

Анотація. Стаття присвячена дослідженню передумов появи децентралізованих платіжних систем. Історичні події та наукові досягнення було поділено на періоди за технологічними прийомами шифрування, що застосовувались в різні часи. Перший період (приблизно з 3-го тисячоліття до нашої ери) — це період моноалфавітних шифрів, основний принцип яких полягав у заміні алфавіту вихідного тексту іншим алфавітом через заміну букв іншими буквами або символами. Другий період (приблизно з IX століття нашої ери) пов'язаний з появою різних варіантів поліалфавітних шифрів. Третій період (перша половина XX століття) характеризується впровадженням електромеханічних пристроїв. При цьому тривало використання поліалфавітних шифрів. Наступним є період переходу до математичної криптографії (з середини 1970-х до кінця 1990-х років XX століття) завдяки поширенню способу криптографії з відкритим ключем.
У статті досліджено історію руху Шифропанків та ідеологію, яка була проголошена у маніфестах Тімоті Мея та Еріка Хьюза. У цих маніфестах визнається, що приватність — це сила вибіркового розкриття особистості світу і діяльність руху Цифропанків спрямована на побудову анонімних систем для захисту конфіденційності, анонімних систем пересилання пошти, цифрових підписів і електронних грошей.
Також проаналізовано роботу сучасних децентралізованих платіжних систем і визначено, що системи на основі алгоритму Proof-of-work засновані на обчислювальній потужності обладнання. Більшість нових блокчейн проектів йдуть дешевшим шляхом і використовують алгоритм Proof-of-stake. Функціональні криптоактиви — це лише операційне середовище, що дозволяє передачу певної вартості між користувачами без будь-яких посередників та без необхідності довіряти один одному або надавати персональні дані. Гібридні (змішані) криптоактиви — це змішані концепції, які можуть мати або гібридну систему консенсусу в мережі, або можуть поєднувати два чи навіть кілька функціональних криптоактива. А от цифрова валюта центральних банків поки що не має практичної реалізації, але її запровадження активно просувається.

Ключові слова: біткоін, блокчейн, децентралізована платіжна система, криптовалюта,криптографія, рух Шифропанків

Annotation. The article is devoted to the research of prerequisites for the emergence of decentralized payment systems. Historical events and scientific developments have been

© Бойко В., 2020

divided into periods by technological encryption techniques used at different times. The first period (from about the 3rd millennium BC) is the period of mono-alphabetic ciphers, the basic principle of which is to replace the alphabet of the original text with another alphabet by replacing letters with other letters or symbols. The second period (approximately from the 9th century AD) is associated with the emergence of different variants of polyalphabetic ciphers. The third period (the first half of the XX century.) is characterized by the introduction of electromechanical devices. At the same time, the use of poly-alphabetic ciphers continued. The next is the period of transition to mathematical cryptography (from the mid-1970s to the end of the 1990s) due to the spread of open-key cryptography.
This article has analyzed the history of the Cypherpunk's movement and ideology, which was proclaimed by Timothy May and Eric Hughes. In their manifestos acknowledge that privacy is the power to selectively reveal oneself to the world and the activities of the Cypherpunk's movement are aimed at building anonymous privacy protection systems, anonymous mail forwarding systems, digital signatures and electronic money.
Also has been analyzed the modern decentralized payment systems and it is determined that the systems on the Proof-of-work algorithm are based on the computing power of the equipment. Most new blockchain projects go the cheaper way and use the Proof-of-stake algorithm. Functional crypto-assets are just an operating environment that allows the transfer of value between users without any intermediaries and without the need to trust one another or provide personal information. Hybrid (mixed) crypto-assets are mixed concepts and can either have a hybrid network consensus system or can combine two or even several functional crypto-assets. Currently the digital currency of the central banks has not been practically implemented, but its introduction is actively advancing.

Keywords: Bitcoin, blockchain, decentralized payment system, cryptocurrency, cryptography, the Cypherpunk'smovement.

JEL code: L17; N70; O33

Постановка проблеми. Історично ставлення людей до грошей змінювалось і в різні часи у різних частинах світу «загальним еквівалентом обміну» виступали різні цінності — мушлі Каурі або шовк з часом витіснили золото і срібло, які у підсумку еволюціонували в національні валюти. Така еволюція грошей пов'язана зі зміною суспільних відносин, розширенням міжнародної торгівлі та становленням інституту держави. Актуальність дослідження полягає у тому, що поява децентралізованих платіжних систем також має еволюційний характер — в їх основі лежить публічна поява криптографії як науки, яка має свої історичні особливості у поширенні ідей і напрацювань різних дослідників. Тому дослідження появи таких інноваційних способів розрахунків дозволяє окреслити напрями їх поширення в якості грошей.

Аналіз останніх досліджень і публікацій. У статті проаналізовано результати досліджень, що вплинули на появу і поширення децентралізованих платіжних систем. Книга Д. Кана «Зломщики кодів» дозволила виокремити періоди розвитку криптографії на основі еволюції способів шифрування. Напрацювання Д. Чаума, А. Бека, Н. Сабо, В. Дая та інших дослідників лягли в основу технології блокчейн і криптовалют. Приділено увагу і сучасним дослідженням цифрових валют центральних банків від фахівців Банку міжнародних розрахунків і Національного банку України.

Виділення не вирішених раніше частин загальної проблеми. Прихильники криптовалют вважають їх різновидом грошей і не звертають увагу на аргументацію скептиків, які зазначають про відсутність внутрішньої вартості та вважають крип-

товалюти грошовим сурогатом. Унікальні властивості криптовалют, що не можуть запропонувати традиційні платіжні системи, полягають у можливості здійснення псевдонімних і безвідмовних операцій, а це означає, що на перший план виходить поведінка споживачів і мережевий ефект стає визначальним для поширення таких технологій. Тому дослідження того як ідеї застосування різних способів шифрування і забезпечення конфіденційності в мережі Інтернет перетворюються на ідеї створення децентралізованих платіжних систем дозволить краще зрозуміти, чи є у криптовалюти шанси стати валютою майбутнього.

Методика дослідження передбачає описання основних історичних етапів розвитку криптографії та її ролі в суспільному житті. Особливої уваги заслуговує період останніх 30-40 років. Аналіз досліджень і напрацювань різних науковців дозволить класифікувати сучасні напрямки поширення криптовалют і пояснити перспективи їх сприйняття у суспільстві в якості грошей.

Мета статті — на основі аналізу історії криптографії та напрацювань різних дослідників визначити сучасні концепції розвитку децентралізованих платіжних систем.

Виклад основного матеріалу дослідження. Історія криптографії налічує близько 4 тисяч років і до недавніх часів була досить закритою темою для досліджень. У дослідженні історії розвитку різних способів шифрування визначною є книга Девіда Кана 1967 року «Зломщики кодів» [1]. Вона є ретельно задокументованою історією криптографії і описує історію шифрів і людей, які ламали ці шифри з часів стародавніх єгиптян і до закінчення Другої світової війни. Для виокремлення періодів розвитку та ускладнення способів шифрування можна використати технологічні прийоми, що застосовувались в різні часи. Перший період, починаючи приблизно з 3-го тисячоліття до н. е., характеризується панування моноалфавітних шифрів, основний принцип яких полягав у заміні алфавіту вихідного тексту іншим алфавітом через заміну букв іншими буквами або символами. Такі шифри можна зустріти на стародавніх єгипетських похованнях, які мали не стільки мету засекречування повідомлень, скільки звернення уваги на здобутки похованих людей.

Другий етап розвитку шифрів можна пов’язати з появою поліалфавітних шифрів, які почали використовуватись приблизно з IX ст. на Близькому Сході, а згодом поширились у Європі. Слід відзначити, що в Європі досить повільно розвивались криптографія і тайнопис до початку епохи Відродження. Це було пов’язано з переконаністю багатьох людей у тому, що криптографія була різновидом чорної магії. В епоху Відродження алхіміки використовували різні способи шифрування для засекречування важливих частин формул і текстів. Згодом і Католицька Церква почала широко використовувати тайнопис і шифри. Ключі шифрування Габріеля Лавінде, секретаря антипапи Климентія VII, датовані 1379 роком і є найдавнішими серед відомих сьогодні. Вони поєднували в собі елементи коду і шифру — крім шифроалфавіту заміни, кожен такий ключ включав невеликий список з понад десятка широко поширених слів або імен, яким поставлено у відповідність дволітерні кодові еквіваленти. Це найдавніший з відомих зразок номенклатора — гібридної системи шифрування, яка в наступні 450 років поширилася по всій Європі.

Наступний період (перша половина XX ст.) характеризується впровадженням електромеханічних пристроїв у роботу шифрувальників. При цьому трива-

ло використання поліалфавітних шифрів. Під час Другої світової війни стало широко відомим сімейство шифрувальних машин «Енігма», яка налічує величезну кількість моделей і варіацій дизайну. Ранні моделі були комерційними і вироблялись починаючи з 1920-х років. Різні німецькі військові служби стали використовувати ці машини, вносячи велику кількість власних змін для підвищення безпеки. Інші країни також користувалися її кресленнями для створення своїх власних шифрувальних машин. У цей період криптографія стала прерогативою військових.

З середини 1970-х до кінця 1990-х років XX ст. — період переходу до математичної криптографії. До 1970-х років криптографія залишалася «класичною» криптографією з секретним ключем. Принципи криптографії з відкритим ключем описали Вітфілд Діффі та Мартін Хеллман у 1976 році. Застосування цього методу вирішило недоліки традиційного шифрування, що полягали у необхідності розподілу ключів. При традиційному шифруванні необхідно щоб усі учасники обміну даними або мали загальний ключ, який має бути якимось безпечним чином їм доставлено, або використовували послуги певного довіреного центру розподілення ключів. Схема криптографії з відкритим ключем передбачає, що кожен користувач системи має два ключі — відкритий ключ і приватний ключ. Відкритий ключ може бути поширений без шкоди для безпеки, а приватний ключ тримається на безпечному носії інформації. При зашифровуванні повідомлення використовується відкритий ключ одержувача, який може розшифрувати його, використавши власний приватний ключ.

Найвідомішою стала опублікована у 1977 році система RSA (абревіатура від прізвищ Рональда Райвеста, Аді Шаміра і Леонардо Адлемана з Массачусетського технологічного інституту) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел. Згодом цей алгоритм було запатентовано в США, що суттєво обмежувало його публічне використання. Публічним впровадженням цього алгоритму для персональних комп'ютерів зацікавився Філіп Цимерман, який у 1991 році створив програмне забезпечення для шифрування електронної пошти PGP (Pretty Good Privacy), що включало запатентовані алгоритми RSA і стало найбільш широко використовуваним в світі. В RSA Data Security були незадоволені поширенням PGP і вважали, що було скоєно крадіжку інтелектуальної власності. Але захист Цимермана в суді наполягав на тому, що він не продавав PGP, а поширив його як своєрідний дослідницький проект.

Створення анонімних цифрових грошей — ідея, вперше запропонована і реалізована Девідом Чаумом, ученим із каліфорнійського університету в Берклі. Ще у 1981 році була опублікована робота «Невідстежувана електронна пошта, зворотні адреси та цифрові псевдоніми», яка поклала початок дослідженням в області зашифрованих комунікацій в Інтернеті [2], а в 1982 році розроблено концепцію «сліпих підписів», яка стала основою для подальших розробок у напрямку створення цифрових грошей [3]. У 1990 році в Амстердамі була заснована компанія DigiCash, основним продуктом якої стала цифрова грошова система — eCash з грошовою одиницею CyberBucks. Ключовим проблемним моментом було те, що компанія мала централізований контроль над грошовою системою і не було технології, щоб запропонувати повністю незалежну валюту [4].

У ці часи різні дослідники робили перші кроки і з часом їх ставало все більше. Йдеться про зародження руху Шифропанків у Кремнієвій долині (штат Каліфорнія, США). Спілкування в середовищі Шифропанків здебільшого відбувалось через поштову розсилку «The List» — електронне місце публікації списку, який зазвичай генерував більше 50 повідомлень на день і які розсилав на електронні поштові скриньки із списку. Методика роботи Шифропанків була звичною для хакерів.

Опублікована у 1993 році в журналі Wired стаття Стівена Леві «Криптоповстанці» [5] розповідає про появу руху Шифропанків і завдяки цій статті виник термін криптоанархізм — філософія, яка закликає до використання сильної криптографії для захисту приватності і особистої свободи. Перша офіційна зустріч представників руху Шифропанків відбулася на початку осені 1992 року за запрошенням двох програмних інженерів, які розвивали інтерес до криптографії. Одним з них був Тімоті Мей, колишній співробітник компанії Intel і автор широко розповсюдженого «Маніфесту криптоанархістів». Інший — Ерік Хьюз, який згодом став модератором фізичних зустрічей Шифропанків.

Маніфест криптоанархістів Тімоті Мея було опубліковано у 1992 році після установчої зустрічі Шифропанків, але його було проголошено ще у 1988 році на конференції «Crypto ’88». У маніфесті наголошується на важливості розвитку технологій, що дозволяють анонімно спілкуватися і взаємодіяти один з одним у мережі. Автор визнає, що поширення криптографії матиме і негативні прояви у появі можливостей незаконної торгівлі зброєю та наркотиками, але констатує, що зупинити поширення криптоанархії неможливо [6].

У маніфесті Шифропанків Еріка Хьюза, що датований березнем 1993 року, проголошується, що приватність — це сила вибіркового розкриття особистості світу і діяльність руху Шифропанків спрямована на побудову анонімних систем для захисту конфіденційності, анонімних систем пересилання пошти, цифрових підписів і електронних грошей. У маніфесті обґрунтовано необхідність створення анонімних систем взаємодії між людьми у «відкритому суспільстві». «Для того щоб приватність була широко поширеною, вона повинна бути частиною соціального договору. Люди повинні прийти і разом розгорнути ці системи для загального блага» [7].

У березні 1997 року Адам Бек в електронному листі поштової розсилки для Шифропанків описав концепцію схеми відправки електронних повідомлень на базі часткової колізії хеш-функції, яку він назвав Hashcash. «Ідея використання часткових хешей полягає в тому, що вони можуть бути довільно дорогими для обчислення, і тим не менш, можуть бути перевірені миттєво» [8]. Hashcash був не першим таким рішенням. Ще у 1992 році була опублікована стаття «Ціноутворення через обробку або боротьба з небажаною поштою» дослідників із компанії IBM Синтії Уорк і Моні Наор [9]. Була запропонована система, в якій кожному відправнику доведеться додавати в лист певні дані, а точніше — вирішення математичної задачі, унікальної для кожного окремого випадку. Синтія Уорк і Моні Наор запропонували три потенційно придатні головоломки, засновані на криптографії з відкритим ключем і електронному підписі. Додавання рішення задачі не повинно було бути складним, а середньостатистичний комп’ютер повинен був здійснювати необхідні обчислення в ідеалі всього за кілька секунд. Одержувач, у свою чергу, легко міг перевірити правильність

рішення. Метою було зробити розсилку небажаних електронних листів збитковою справою. Сьогодні така концепція називається Proof-Of-Work (тобто доказ проведеної роботи з певних обчислень) і є основою роботи багатьох криптовалют. Ідея Hashcash Адама Бека була дуже схожою на пропозицію дослідників із компанії IBM і переслідувала ту ж мету, але мала додаткові області застосування і була побудована на основі хешування, що являє собою процес перетворення будь-якого масиву даних у вихідну бітову строку встановленої довжини, а пропозиція Синтії Уорк і Моні Наор мала за основу криптографічні головоломки.

Стаття Адама Бека із концепцією Hashcash [10] була опублікована лише в серпні 2002 року і, як і пропозиція Синтії Уорк і Моні Наор, ніколи не були реалізовані у великих масштабах. Пропонувались різні варіанти для використання технології, але жоден з них не був успішним. Для більшості з них відсутність мережевого ефекту стало визначальним фактором. Проте вони дійсно створили щось нове — з огляду на те, що тоді основною перевагою цифрових продуктів була легкість, з якою вони копіювалися, Proof-Of-Work став, по суті, першою концепцією, що була заснована на віртуальному дефіциті і відсутності централізації: ця модель прив'язала цифрові дані до реальних, обмежених обчислювальних потужностей. Така дефіцитність закладала основу для створення цифрових грошей, але невирішеною проблемою залишалось те, що отриманий доказ виконаної роботи не має цінності для одержувача — на відміну від грошей, його не можна витратити повторно. Крім того, розвиток технологій і зростання обчислювальних потужностей призвели б до того, що докази роботи проводилися б швидше, але при менших витратах, що провокувало б гіперінфляцію Hashcash. Концепція Proof-Of-Work же не могла сама по собі виступати грошима, але децентралізована система цифрових грошей могла б не з'явитися без цієї технології [11]. Варто зауважити, якщо ми розглядаємо сучасні криптовалюти із концепцією Proof-Of-Work у якості грошей, то у певному сенсі це є повноцінні гроші, оскільки функціонування таких децентралізованих мереж (обробка трансакцій і їх безпека) спирається на роботу спеціального обладнання і досить значну витрату електроенергії. Тобто їх вартість виражається, щонайменше, у амортизації обладнання та вартості електроенергії.

Ще одна пропозиція створення анонімної електронної готівки на основі криптографії, яка обговорювалась серед Шифропанків була описана у 1996 році Лорі Лоу, Сьюзан Сабетт і Джеррі Солінасом, дослідниками відділу криптології Управління досліджень і технологій інформаційного забезпечення Агентства національної безпеки США [12]. Вони визначили, що поняття електронної готівки має включати властивості анонімності та непростежуваності платежів. Було описано механізм роботи протоколу на основі аутентифікації користувачів за допомогою цифрового підпису та запропоновані конкретні варіанти реалізації системи електронних грошових операцій. У дослідженні було визначено необхідні властивості безпеки анонімних цифрових грошей: конфіденційність, ідентифікація користувача, цілісність повідомлення та неможливість відмови (скасування) операції.

Вей Дай, дослідник з Вашингтонського університету, який захоплювався ідеями криптоанархізму, також зробив суттєвий вклад у розробку концепцій децентралізованих платіжних систем. Ідея електронних грошей, яка отримала назву «B-money» [13], була запропонована в листопаді 1998 року і мала дещо

альтернативне рішення, а точніше —два рішення. Механізм першого передбачав, що всі учасники повинні зберігати і оновлювати копії реєстру трансакцій замість єдиної централізованої організації. Але залишилась не вирішеною проблема повторного витрачання. Тому Вей Дай відразу ж запропонував другу версію, згідно якої копія реєстру зберігалася не у кожного учасника мережі та вводилися нові поняття — регулярні користувачі і сервери. Тільки сервери, які є вузлами мережі, зберігали копії реєстру. Щоб перевірити, чи успішно була здійснена трансакція, користувачі повинні були б звернутися до випадкової послідовності серверів. Вей Дай не уточнив, чи будь-хто може запустити сервер, проте додав, що кожен сервер зобов'язаний внести стандартний депозит у спеціальний акаунт, який би використовувався для штрафів у разі доведення несумлінної поведінки. Сервери також зобов'язані були періодично публікувати і криптографічно завіряти бази даних із залишками на рахунках учасників. Це поклало початок концепції Proof-Of-Stake (тобто підтвердження наявним резервом), яка є також досить поширеною у роботі сучасних криптовалют. Також він впровадив ранню концепцію смарт-контрактів. Цей тип контрактів поєднував Proof-Of-Stake і арбітражну систему, в рамках якої сторони договору і арбітр повинні були внести депозити на спеціальний акаунт [14]. Функціонування децентралізованої мережі на основі концепції Proof-Of-Stake не передбачає роботи обладнання та витрат електроенергії. Тому виникають питання щодо повноцінності таких грошей — розробники таких систем виступають емітентом криптовалюти, цінність якої формується лише ринковими механізмами попиту і пропозиції. Для розробників така криптовалюта є нематеріальним активом — уречевленою формою їх інтелектуальної роботи, а для користувачів її цінність проявляється у функціональних можливостях, які вони отримують. Варто відзначити, що механізм роботи таких децентралізованих мереж, крім традиційних математичних прийомів криптографічного шифрування, заснований ще й на певних моделях досягнення консенсусу (наприклад, відома модель вирішення задачі візантійських генералів).

Вагомий вклад у розвиток децентралізованих платежів вніс ще один відомий дослідник Нік Сабо, який також був учасником руху Шифропанків і автором проекту «Bit Gold», а також розробив концепцію смартконтрактів ще у 1990-х роках [15]. Він деякий час працював у компанії DigiCash Девіда Чаума і зіткнувся на практиці з недоліками цієї платіжної системи. Оскільки платіжна система компанії була централізованою, то це дозволяло дуже легко і швидко сфальсифікувати грошові баланси клієнтів. Отже, стало очевидним, що наявність довіреної особи є серйозною потенційною уразливістю цифрових платіжних систем.

Вперше концепція створення Bit Gold була запропонована в 1998 році, але публічно пояснена лише в 2005 році. Ідея частково спиралася на попередні дослідження і мала в основі алгоритм Proof-Of-Work, запропонований Адамом Беком. Для встановлення права власності у Bit Gold існував цифровий реєстр, в якому правильні хеші присуджувалися відкритим криптографічним ключам тих, хто їх створив. Підтримувати працездатність реєстру в мережі Bit Gold повинен був так званий «property club», який представляв собою сервери, що відстежують перехід права власності на хеші від одних відкритих ключів іншим.

Невирішеною проблемою була інфляція, зумовлена розвитком комп'ютерної техніки і важливо було забезпечити грошам властивість рідкості. Вирішенням

було додавання часової мітки в процесі виконання алгоритму, але ще одним питанням, що постало перед дослідником — взаємозамінність грошових одиниць, створених у різний час. Нік Сабо вирішив і цю проблему запропонувавши свого роду «надбудову» над основним протоколом Bit Gold, де «банки» комбінували б хеші різних періодів в однакові за цінністю «пакети». І лише у 2008 році він описав свої ідеї в авторитетному блозі Unenumerated і виявив бажання зайнятися першою реальною імплементацією [16].

Ідеї Hashcash, Bit Gold і B-money лягли в основу створення найпопулярнішої сьогодні децентралізованої платіжної системи Bitcoin дослідника або групи дослідників під псевдонімом Сатоши Накамото, яка з'явилась в кінці 2008 року [17]. Функція хешування, застосована в Hashcash у поєднанні з алгоритмом періодичного перерахунку складності обчислень дозволяють забезпечити обробку трансакцій і механізм стабільної емісії нових одиниць віртуальних грошей, а також їх надійну перевірку. Із концепції B-money було взято ідею децентралізованого зберігання реєстру трансакцій і періодичної синхронізації між серверами (оновлення бази даних), а ідея відносно випадкового розподілу емісії, застосована в Bit Gold, дозволила створити конкурентне середовище серед серверів на основі обчислювальної потужності обладнання. Все це стало основою революційної технологій блокчейн, яка дозволяє збирати трансакції у блоки, підписувати їх із використанням хешфункції та поширювати серед серверів.

Запущена в часи світової фінансової кризи 2008 року мережа Bitcoin разом зі звичайними даними має додатковий запис до початкового блоку (генезис блоку номер 0) «The Times 03/Jan/2009 Chancellor on brink of second bailout for banks». Це посилання до відповідної статті британської газети The Times, в якій говориться, що уряд збирається «купити» чергові мільярди «токсичних боргів» банків. Банкіри самі собі свідомо створили мільярди «токсичних активів», заробили на них мільярди і тепер «продають» їх уряду.

Луї Руане звертає увагу на пряму залежність діяльності центральних банків і зростання нерівності у доходах [18]. Головною проблемою він називає грошово-кредитну політику центральних банків, що направлена на збільшення грошової маси та інфляцію як механізм отримання конкурентних переваг у міжнародній торгівлі. При цьому важливим є ефект перерозподілу новостворених грошей в економіці (ефект Кантільона). Процес інфляції споживчих цін запускається появою диспропорцій між грошовою масою та пропозицією товарів і послуг на ринку, але проявляється не одразу і перші, хто отримує новостворені гроші, мають можливість витратити їх без суттєвого впливу інфляції. І якщо найбідніші в суспільстві будуть першими одержувачами новостворених грошей, то інфляція цілком може стати причиною зменшення нерівності.

Отже, специфічна цифрова валюта Bitcoin позиціонується як альтернатива грошам центральних банків, існує лише в мережі Інтернет, не має емісійного центру і повністю позбавлена цензури трансакцій. Обмеження загальної пропозиції у 21 мільйон одиниць та механізм скорочення емісії робить її стійкішою та прогнозованішою щодо інфляції. Однак Донг Хе стверджує, що у мережі Bitcoin не вистачає важливих функцій, які повинні забезпечувати стабільні грошові системи [19]:

– захист від ризику структурної дефляції;

– можливість гнучко реагувати на тимчасове підвищення попиту на гроші і таким чином згладжувати діловий цикл;

– здатність функціонувати як кредитор останньої інстанції.

Негативні прояви структурної дефляції більше стосуються самої мережі Bitcoin і її вплив на глобальну фінансову систему поки що не значний. Закладені алгоритмом механізми обробки операцій та емісії передбачають зменшення впливу емісії з часом на співвідношення попиту і пропозиції. Сьогодні Bitcoin розглядається більше як спекулятивний актив. Довгострокові інвестиції хоч і виглядають привабливою ідеєю, але ціна повністю залежить від попиту. Головний аргумент прихильників криптовалют буде полягати у неможливості втручатись у процес емісії і грошова маса буде передбачуваною у часі. Це, на жаль, важко сказати про національні валюти. Реагування на підвищення попиту на гроші є функцією не самих грошей, а грошової системи окремої країни (або регіону). Еластичність грошової маси мають забезпечувати посередники через механізм часткового резервування, приймаючи на себе всі ризики. За таких умов наявність кредитора останньої інстанції може призводити до зловживань і махінацій.

Якщо розглядати криптовалюти в якості грошей, їх можна розподілити за такими напрямами:

– криптовалюти на основі алгоритму Proof-Of-Work;

– криптовалюти на основі алгоритму Proof-Of-Stake;

– функціональні криптоактиви;

– гібридні (змішані) криптоактиви;

– цифрова валюта центральних банків.

Алгоритм Proof-of-work заснований на необхідності виконання на стороні клієнта деякої досить тривалої роботи (знаходження рішення задачі), результат якої легко і швидко перевіряється на стороні сервера. Ймовірність створення чергового блоку вище у володаря потужнішого устаткування. Постійна робота обладнання вимагає великих витрат електроенергії. При використанні алгоритму Proof-of-stake ймовірність формування учасником чергового блоку в блокчейні пропорційна частці такого учасника одиниць даної криптовалюти від її загальної кількості і не залежить від потужності обладнання. Існує ще багато менш популярних алгоритмів (proof of concept, proof of authority, proof of activity і інші), переважно схожі на алгоритм Proof-of-stake. Отже, різниця полягає у тому, що емісія може мати або не мати собівартості у вигляді амортизації обладнання та витрат на електроенергію. Більшість нових блокчейн проектів йдуть дешевшим шляхом, що робить таку криптовалюту певною мірою неповноцінними грошима.

Функціональні криптоактиви в якості грошей важко сприймати. Це, як правило, емітовані (просто створені) активи на різних блокчейнах (наприклад, Ethereum, EOS, TRON, NEO, Stellar). Створення криптоактивів — це створення смарт контракту, який визначає базові принципи обігу таких активів. Такі криптоактиви можуть знайти застосування у різних видах діяльності — виступати цифровими жетонами для платежів за товари або послуги або, наприклад, бути еквівалентом акцій команди розробників. Сам по собі такий актив — це лише операційна оболонка, що дозволяє його передачу між користувачами без участі посередників і необхідності довіряти один одному або надавати персональні дані.

Гібридні (змішані) криптоактиви засновані на змішаних концепціях і можуть мати або гібридну систему консенсусу в мережі, або можуть поєднувати два чи навіть кілька функціональних криптоактива. Прикладом перших можна назвати мережу Dash, в якій послідовно застосовуються 11 різних функцій хешування та є так звані «мастер ноди», що використовуються для підвищення анонімності операцій. Прикладом поєднання є проект MakerDAO, який має два функціональні криптоактиви: токен DAI на базі блокчейну Ethereum, який має механізм саморегуляції, що вирівнює його вартість у відношенні 1:1 із американським доларом; та токен Maker, який використовується для погашення комісій за використання смарт-контрактів, а також для голосування з питань функціонування проекту, управління ризиками та бізнес-логіку платформи.

Цифрова валюта центральних банків поки що залишається в режимі тестування. Фахівці Банку міжнародних розрахунків дослідили ініціативи центральних банків різних країн у впровадженні цифрової валюти і результати пілотних проектів неоднозначні. Такі проекти вимагають ґрунтовного дослідження впливу на економіку, але все ж таки деякі країни активно просуваються до впровадження [20]. Результати досліджень Національного банку України електронної гривні у цілому позитивні, але мають бути вирішені фундаментальні питання щодо моделі функціонування цифрової гривні (централізована або децентралізована) та технології, що має використовуватися (публічні або приватні блокчейни, власні доопрацювання), а також рівня анонімності користувачів при здійсненні операцій з електронною гривнею [21].

Висновки і перспективи подальших наукових досліджень. Отже, історично способи шифрування та гроші ніяк не були пов’язані. Лише протягом кількох останніх десятиліть пошуки механізмів забезпечення конфіденційності в мережі Інтернет створили передумови для появи концепції децентралізованих електронних грошей, вільних від впливу центральних банків. Головною рушійною силою зростаючої популярності децентралізованих платіжних систем можна назвати накопичення напрацювань різних дослідників, що створило умови для їх впровадження, а мережевий ефект від інновацій був підтриманий ще й зростанням недовіри до банківської системи у часи світової фінансової кризи 2008–2009 рр.

Децентралізовані платіжні системи мають ряд переваг у порівнянні із банками — швидкі та безвідмовні трансакції не вимагають ідентифікації особи, а також порівняно низька вартість операцій без обмежень національними кордонами. Але важливими питаннями, що мають бути вирішені, залишаються стабільність курсу таких грошей і правове регулювання різних країн у сфері грошового обігу. Поява конкурента для валют центральних банків може обмежити можливості ефективного здійснення грошово-кредитної політики, яку, на жаль, у наші часи важко назвати ефективною. Проте криптовалюти не є повноцінною альтернативою національним валютам, а виступають скоріш як компліментарні платіжні системи, що вирішують певні функціональні задачі.

Проведене дослідження етапів розвитку інновацій на основі прийомів шифрування дозволяє побудувати схематично весь процес еволюції (рис. 1).

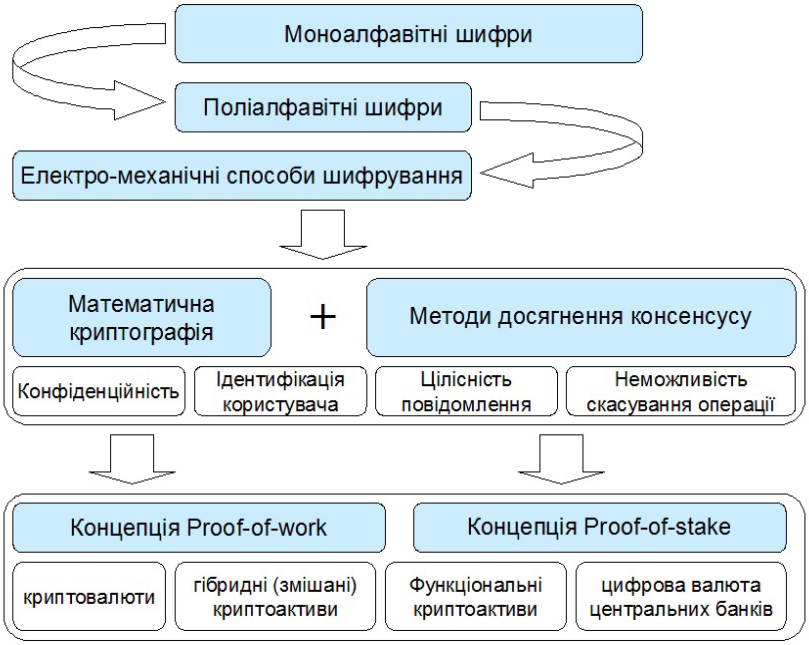

Рис. 1. Основні етапи еволюції децентралізованих платіжних систем

Джерело: побудовано автором.

Дослідження сучасних напрямів розвитку децентралізованих платіжних систем як інноваційного виду грошей дозволяє виокремити: криптовалюти на основі алгоритмів Proof-Of-Work та Proof-Of-Stake, функціональні криптоактиви, гібридні (змішані) криптоактиви та цифрову валюту центральних банків. На жаль, цифрова валюта центральних банків у жодній країні світу публічно поки що не працює. Такі проекти доцільно запускати в країнах із слабо розвиненою банківською системою.

Грошовим сурогатом можна назвати лише деякі криптовалюти і це вимагає детальнішого дослідження. Тому перспективи подальших наукових розробок полягають у проведенні тестування популярних криптовалют на предмет відповідності основним функціям грошей і розподілі їх за основними видами (повноцінні/неповноцінні, функціональні, цифровий еквівалент різних активів). Особливу увагу необхідно приділити питанням ліквідності, рівня децентралізації та наявності у різних блокчейн проектів достатньої кількості (або потенційної кількості) користувачів.

Література

1. Kahn D. The Codebreakers [Електронний ресурс] / David Kahn. — 1973. — Режим доступу: https://archive.org/details/1973TheCodebreakersTheStoryOfSecretWrittingDavidKahn.

2. Chaum D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Електронний ресурс] / David Chaum. — 1981. — Режим доступу: https://chaum.com/publications/chaum-mix.pdf.

3. Chaum D. Blind signatures for untraceable payments [Електронний ресурс] / David Chaum. — 1982. — Режим доступу: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.

4. Wirdum A. The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream [Електронний ресурс] / Aaron van Wirdum — Режим доступу: https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream.

5. LevyS. Crypto Rebels [Електронний ресурс] / WIRED, 1993 — Режим доступу: https://www.wired.com/1993/02/crypto-rebels/

6. May T. The Crypto Anarchist Manifesto [Електронний ресурс] / Timothy C. May. — 1992. — Режим доступу: https://activism.net/cypherpunk/crypto-anarchy.html.

7. Hughes E. A Cypherpunk's Manifesto [Електронний ресурс] / Eric Hughes. — 1993. — Режим доступу: https://www.activism.net/cypherpunk/manifesto.html.

8. Back A. Hash cash postage implementation [Електронний ресурс] / Adam Back. — 1997. — Режим доступу: http://www.hashcash.org/papers/announce.txt

9. Dwork C. Pricing via Processing or Combatting Junk Mail [Електронний ресурс] / C. Dwork, M. Naor. — 1992. — Режим доступу: https://link.springer.com/chapter/10.1007/3-540-48071-4_10.

10. Back A. Hashcash — A Denial of Service Counter-Measure [Електронний ресурс] / Adam Back. — 2002. — Режим доступу: http://www.hashcash.org/papers/hashcash.pdf.

11. Wirdum A. The Genesis Files: Hashcash or How Adam Back Designed Bitcoin's Motor Block [Електронний ресурс] / Aaron van Wirdum — Режим доступу: https://bitcoinmagazine.com/articles/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block.

12. Law L. How to make a mint: the cryptography of anonymous electronic cash [Електронний ресурс] / L. Law, S. Sabett, J. Solinas. — 1996. — Режим доступу: https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm.

13. Dai W. B-money [Електронний ресурс] / Wei Dai. — 1998. — Режим доступу: http://www.weidai.com/bmoney.txt.

14. Wirdum A. The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It [Електронний ресурс] / Aaron van Wirdum — Режим доступу: https://bitcoinmagazine.com/articles/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it.

15. Wirdum A. The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin [Електронний ресурс] / Aaron van Wirdum — Режим доступу: https://bitcoinmagazine.com/articles/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin.

16. Szabo N. Bit gold markets [Електронний ресурс] / Nick Szabo // Unenumerated. — 2008. — Режим доступу: https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html.

17. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Satoshi Nakamoto. — 2008. — Режим доступу: https://bitcoin.org/bitcoin.pdf.

18. Rouanet L. How Central Banking Increased Inequality [Електронний ресурс] / Louis Rouanet // Mises Institute. — 2017. — Режим доступу: https://mises.org/library/how-central-banking-increased-inequality.

19. He D. Monetary Policy in the Digital Age [Електронний ресурс] / Dong He // The International Monetary Fund. — 2018. — Режим доступу: https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.htm.

20. BIS Quarterly Review [Електронний ресурс] // Bank for International Settlements. — 2020. — Режим доступу: https://www.bis.org/publ/qtrpdf/r_qt2003.htm.

21. Аналітична записка за результатами пілотного проекту «Е-гривня» [Електронний ресурс] // Національний банк України. — 2019. — Режим доступу: https://bank.gov.ua/admin_uploads/article/Analitichna_zapiska_E-grivnya.pdf?v=4.

References

1. Kahn D. (1973), «The Codebreakers», [Electronic resource], Access mode: https://archive.org/details/1973 The Codebreakers The Story Of Secret Writting David Kahn [In English].
2. Chaum D. (1981), «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», [Electronic resource], Access mode: https://chaum.com/publications/chaum-mix.pdf [In English].
3. Chaum D. (1982), «Blind signatures for untraceable payments», [Electronic resource], Access mode: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum. BlindSigForPayment.1982.PDF [In English].
4. Wirdum A. (2018), «The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream», [Electronic resource], Access mode: https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream [In English].
5. LevyS. (1993), «Crypto Rebels», [Electronic resource], Access mode: https://www.wired.com/1993/02/crypto-rebels [In English].
6. May T. (1992), «The Crypto Anarchist Manifesto», [Electronic resource], Access mode: https://activism.net/cypherpunk/crypto-anarchy.html [In English].
7. Hughes E. (1993), «A Cypherpunk's Manifesto», [Electronic resource], Access mode: https://www.activism.net/cypherpunk/manifesto.html [In English].
8. Back A. (1997), «Hash cash postage implementation», [Electronic resource], Access mode: http://www.hashcash.org/papers/announce.txt [In English].
9. Dwork C., Naor M. (1992), «Pricing via Processing or Combatting Junk Mail», [Electronic resource], Access mode: https://link.springer.com/chapter/10.1007/3-540-48071-4_10 [In English].
10. Back A. (2002), «Hashcash — A Denial of Service Counter-Measure», [Electronic resource], Access mode: http://www.hashcash.org/papers/hashcash.pdf [In English].
11. Wirdum A. (2018), «The Genesis Files: Hashcash or How Adam Back Designed Bitcoin's Motor Block», [Electronic resource], Access mode: https://bitcoinmagazine.com/articles/genesis-files-hashcash-or-how-adam-back-designed-bitcoins-motor-block [In English].
12. Law L., Sabett S., Solinas J. (1996), «How to make a mint: the cryptography of anonymous electronic cash», [Electronic resource], Access mode: https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm [In English].
13. Dai W. (1998), «B-money», [Electronic resource], Access mode: http://www.weidai.com/bmoney.txt [In English].
14. Wirdum A. (2018), «The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It», [Electronic resource], Access mode: https://bitcoinmagazine.com/articles/genesis-files-if-bitcoin-had-first-draft-wei-dais-b-money-was-it [In English].
15. Wirdum A. (2018), «The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin», [Electronic resource], Access mode: https://bitcoinmagazine.com/articles/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin [In English].
16. Szabo N. (2008), «Bit gold markets», [Electronic resource], Access mode: https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html [In English].
17. Nakamoto S. (2008), «Bitcoin: A Peer-to-Peer Electronic Cash System», [Electronic resource], Access mode: https://bitcoin.org/bitcoin.pdf [In English].
18. Rouanet L. (2017), «How Central Banking Increased Inequality», [Electronic resource], Access mode: https://mises.org/library/how-central-banking-increased-inequality [In English].
19. He D. (2018), «Monetary Policy in the Digital Age», [Electronic resource], Access mode: https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.htm [In English].

20. Bank for international settlements (2020), «BIS Quarterly Review», [Electronic resource], Access mode: https://www.bis.org/publ/qtrpdf/r_qt2003.htm [In English].
21. National bank of Ukraine (2019), «Analitychna zapiska za rezultatamy pilotnogo proektu 'E-hgivnya'», [Electronic resource], Access mode: https://bank.gov.ua/admin_uploads/article/Analitichna_zapiska_E-grivnya.pdf?v=4 [In Ukrainian].

Стаття надійшла 03.02.2020

УДК: 33;364-6;364-2.
DOI 10.33111/vz_kneu.21.20.01.02.012.018

Верховод І.С.
к.е.н., доцент
Мелітопольській державний педагогічний університет
м. Мелітополь, 72300, вул. Гетьманська, 20
e-mail: rina_verkhovod@mdpu.org.ua
https://orcid.org/0000-0002-9176-2574
Верба Д.В.
к.е.н., доцент
ДВНЗ «КНЕУ імені Вадима Гетьмана»
проспект Перемоги, 54/1, Київ, Україна
e-mail: denys.verba@kneu.ua
https://orcid.org/0000-0002-8712-4027

ТЕОРЕТИЧНІ ОСНОВИ ІДЕНТИФІКАЦІЇ СОЦІАЛЬНОЇ СФЕРИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ ТА РОЗРОБКИ ПОЛІТИКИ ЇЇ РОЗВИТКУ

Irina Verkhovod
Ph.D., Associate Professor Department of Economy,
Bohdan Khmelnitsky State Pedagogical University of Melitopol,
Melitopol, Ukraine
e-mail: rina_verkhovod@mdpu.org.ua
https://orcid.org/0000-0002-9176-2574
Verba Denys
Ph.D., Associate Professor department of Economic Theory,
KNEU named after Vadym Hetman
Peremohy avenue, 54/1, Kyiv, Ukraine
e-mail: denys.verba@kneu.ua
https://orcid.org/0000-0002-8712-4027

THEORETICAL FUNDAMENTALS OF THE SOCIAL SPHERE IDENTIFICATION AND DESIGNING OF ITS DEVELOPMENT POLICY

Анотація. Стаття присвячена формулюванню концептуальних підходів до організації ресурсного забезпечення соціальної сфери і містить спробу теоретичного узгодження та гармонізації поширених у вітчизняній науковій літературі підходів до диференціації масштабів ресурсного забезпечення соціальних галузей із принципами сучасних досліджень внеску соціальної сфери у примноження суспільного добробуту. Зокрема, досліджуються обмеження, що накладаються принципами управління ресурсним забезпеченням соціальної сфери на можливості розвитку національної економіки та характер розподілу вигід і тягот її функціонування між економічними суб'єктами.

© Верховод І., Верба Д., 2020