DOI: https://doi.org/10.36059/978-966-397-599-3-69

АРХІТЕКТУРА ЦВЦБ ЯК ІНСТРУМЕНТ ТРАНСФОРМАЦІЇ ФІНАНСОВОГО МОНІТОРИНГУ В УКРАЇНІ

Пантюхов Адріан Олександрович
аспірант кафедри міжнародних фінансів,
Київський національний університет імені Тараса Шевченка

Станом на липень 2025 року 137 країн, що презентують 98% ВВП світу, досліджують цифрові валюти центральних банків (ЦВЦБ). Згідно з опитуваннями BIS (Papers No. 159, 2024), 85 з 93 опитаних центральних банків ведуть роботу над роздрібними чи/та над оптовими проєктами [1]. При цьому ЦВЦБ не була запущена у розвинутих економіках: три активні системи (Sand Dollar на Багамах, JAM-DEX на Ямайці та eNaira в Нігерії) працюють в відносно малих юрисдикціях і широко розповсюджені. Так, МВФ оцінює, що у 2023-му 98,5 % гаманців eNaira не були використані – протягом першого року після запуску [2]. Це піднімає питання, що ключовий бар'єр впровадження – не технологія, а відсутність довіри споживачів [13], зумовлена незрозумілим балансом між зручністю, зрозумілістю фінансового моніторингу та конфіденційністю користувачів. Для України – економіки з високою часткою тіньової економіки, де НБУ планує тестування е-гривні [9], це безпосередньої практичне питання. Відсутність широких пілотних тестів раніше посилює виклик, адже попередні пілоти охоплювали маленькі суми, та стосувались не споживачів, а зацікавлених осіб – працівників НБУ. Додає значущості шлях до євроінтеграції, регіону де парламентарі підтримують запуск європейського CBDC, необхідність моніторингу коштів на повоєнне відновлення та високого рівня проникнення безготівкових транзакцій.

1. Дворівнева модель: зобов'язання та дистрибуція. Консенсус більшості центральних банків демонструє, що базовий напрям досліджень – це гібридна архітектура ЦВЦБ [1]. Регулятор випускає цифрову валюту як пряме зобов'язання. Таким чином звільнюючи людей від ризику неплатоспроможності банків. Водночас дистрибуцію та KYC клієнтів здійснюють комерційні посередники – переважно банки. Це дозволяє зняти потребу у розбудові широкої інфраструктури паралельної традиційній фінансовій. Ця модель реалізована в Китаї: e-CNY (225 млн гаманців, 16,7 трлн юанів оброблених транзакцій), цифровий євро (проведені перші фази підготовки, першочергова підтримка від законодавців, можливий запуск з 2029 р.) [3], в Індії, цифрова рупія (8 млн гаманців, зростання оборотів на 334 % за рік) [2]. Цифрова гривня попри затягування процесу відбору технологічного партнера, планується за схожою схемою на базі розподіленого реєстра (DLT) зі збереженням

даних споживачів у посередників, без концентрації додаткових даних у емітента – Національного банку. Це повторює рекомендації EDPB 02/2025 щодо обробки персональних даних у блокчейн-системах.

2. Анонімність для невеликих транзакцій, як новий стандарт. У лютому 2025 р. Міжнародна група з протидії відмиванню брудних грошей (FATF) замінила у рекомендаціях слово «співмірність» (commensurate) на «пропорційність» (proportionate). Таким чином погодивши спрощення перевірки для низькоризикових транзакцій. Це підтверджує світовий тренд до «вибіркової приватності». В Китаї ЦВЦБ діє за декілька рівневою системою: e-CNY дозволяє відкрти гаманець за номером телефону, тобто з мінімальним, або відсутнім KYC з лімітом 2 тисячі юанів. В ЄС ЄЦБ розглядає паралельний підхід: офлайн-платежі без збору даних для посередників та онлайн-платежі до 3 тисяч євро з псевдонімізованою обробкою. Доціально для е-гривні буде адаптувати декілька рівневу модель із прив'язкою до лімітів Закону № 361-IX (належна перевірка здійснюється при операції з віртуальними активами на суму понад 30 тисяч грривень) [14] та з офлайн-функціоналом в умовах обмеженого інтернет-покриття та електрозабезпечення.

3. Захист приватності за допомогою криптографії. Проєкт BIS Tourbillon (2023) дослідив впровадження анонімності споживача, на фундаменті сліпих підписів Девіда Чаума, одного з батьків криптографії [4]. Так, емітент ЦВЦЬ може підтвердити справжність платіжного засобу, не маючи в наявності даних, які дали б змогу пов'язати її з конкретним користувачем. Водночас швейцарський національний банк допоміг протестувати протокол eCash 2.0, який дає можливість добровільного одностороннього скасування анонімності споживачем для проходження первинної перевірки, або для запобігання руху незаконних фінансових потоків. Технологія доказів з нульовим розголошенням (ZKPs), яка протестована в блокчейн-мережах для збереження конфіденційності, дозволяє проходити фінансовий моніторинг: відповідність AML-критеріям, не розкриваючи суми чи споживача. Однак Банк Кореї (2024) зазначив про суттєве зниження операційної ефективності. Офлайн-платежі також можливо захистити: IDEMIA влітку 2024 р. протестувала першу офлайн-транзакцію ЦВЦБ, яка зазначена, як квантово-стійка. Банк Канади підтверджує: оптимальним є гібридний підхід [5].

4. Зміна парадигми від постфактумного до превентивного моніторингу. ЦВЦБ дають можливість фінансовому моніторингу перейти від ex-post моделі контролю (пошук невідповідностей встановленим правилам після здійснення транзакції) до ex-ante моделі (дизайн, який унеможливлює проведення незаконних фінансових транзакцій). Проєкт BIS Mandala (8 банків) запроваджує виконання регуляторних вимог прямо у інфраструктуру ЦВЦБ: перевірка на

дотримання санкцій, KYC клієнта та керування потоками капіталу у відповідних юрисдикціях імплементується до платежу. Щобільше криптографічний доказ проходження комплаєнсу пов'язаний з кожною транзакцією ЦВЦБ без розкриття особи чи компанії. Стандарт обміну електроними фінансовими повідомленнями ISO 20022 (близько 40% транскордонного трафіку SWIFT) надає підготовлені дані для скринінгу транзакцій. AI-моделі, як RegTech можуть покращити точність при виявлені операцій для глибокої перевірки на 40% при зниженні знаходження хибних результатів на 70%. Для е-гривні можливість імпленетувати програмованість, як для запобігання незаконним фінансовим потокам, так і для обмеження характеристик платежу – є базовим сценарієм. Це дозволить адмініструвати цільові соціальні виплати з обмеженням напрямів використання, та контроль, або запрограмоване розподілення коштів відновлення.

5. Конфлікт принципа мінімізації даних GDPR та дотримання вимог AML. Протиріччя між принципом на мінімізацію даних, збереження адекватного і релевантного обсягу згідно GDPR та вимогами на збереження інформації про транзакції – 5-10 років за AML-правилами може бути вирішено архітектурою системи. Рамкові рекомендації EDPB 02/2025 передбачають зберігання даним поза блокчейн мережами, при розміщенні у розподіленому реєстрі лише хешів операцій (за використання сліпих підписів, та криптографії це дозволить розірвати зв'язок між користувачем та його даними). ЄЦБ забороняє фінансовим посередникам використовувати у комерційних цілях платіжні дані без погодження споживача. Новий Регламент ЄС з AML (2024/1624, чинний з липня 2027) буде поширюватись на «всі форми грошей центрального банку, випущених для роздрібного використання» та запровадить обов'язкову ідентифікацію клієнтів для транзакцій від 3 тисяч євро. НБУ заявив, що не буде зберігати персональні дані споживачів. Це збігається з парадигмою захисту конфіденційності, проте для дотримання необхідно імплементувати у Закон № 361-IX.

Можна сформувати чотири ключових принципи для формування архітектури е-гривні. По-перше, запровадження дворівневої моделі доступу емітент-дистриб'ютор, із зберіганням конфідейних даних поза мережею. Вибір технологічного провайдера який забезпечить реальний рівень приватності через імплементацію сліпих підписів, ZKP, – є запорукою розвитку довіри до ЦВЦБ. По-друге, декілька рівнева анонімність із максимальним «готівковим» рівнем приватності для маленьких платежів, що забезпечить фінансову інклюзію та відповідність AML-принципам згідно останнім змінам FATF – щодо принципу пропорційності. По-третє, формування системи попередження ex-ante, а не постфактумного відслідковування – суттєво знизить витрати на фінансовий моніторинг. По-четверте, використання унікальних

конкуретних переваг України – високий рівень цифровізації (22,5 млн користувачів застосунку Дія) створить сприятливе середовище для випробовувань з мінімальними інфраструктурними вкладеннями. Успіх е-гривні має базуватись не лише на технічній інноваційності, а й на прозорісті контролю, незалежного нагляду та закріпленням у законодавстві права та гарантій на приватність.

Список використаних джерел:

1. BIS. Advancing in tandem – results of the 2024 BIS survey on central bank digital currencies and crypto. BIS Papers No. 159. August 2025.
2. IMF. Central Bank Digital Currency: Progress and Further Considerations. Policy Paper No. 2024/052. 2024.
3. ECB. Preparation phase of a digital euro – Closing report. October 2025.
4. BIS Innovation Hub. Project Tourbillon: exploring privacy, security and scalability for CBDCs. November 2023.
5. Bank of Canada. Privacy-Enhancing Technologies for CBDC Solutions. Staff Discussion Paper 2025-1. January 2025.
6. BIS. Privacy-enhancing technologies for digital payments. Working Paper No. 1242. 2025.
7. FATF. Updates to Standards to promote financial inclusion. February 2025.
8. EDPB. Guidelines 02/2025 on processing of personal data through blockchain technologies. April 2025.
9. National Bank of Ukraine. E-hryvnia: official project page. URL: https://bank.gov.ua/en/payments/e-hryvnia
10. BIS Innovation Hub. Project Mandala: embedding policy compliance in cross-border transactions. Phase 2. November 2025.
11. BIS Innovation Hub. Project Leap phase 2: quantum-proofing payment systems. 2025.
12. NIST. Post-Quantum Cryptography Standards: FIPS 203, 204, 205. August 2024.
13. IMF. Central Bank Digital Currency Data Use and Privacy Protection. FinTech Notes 2024/004. 2024.
14. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом...» № 361-IX від 06.12.2019.