https://doi.org/10.31649/1997-9266-2022-160-1-76-81

УДК 004.42

Є. С. Щербіна[1]
В. І. Месюра[1]

РОЗРОБКА ПРОТОКОЛУ ПЛАТІЖНИХ КАНАЛІВ НА БЛОКЧЕЙНІ STELLAR

[1]Вінницький національний технічний університет

Розглянуті питання щодо теми платіжних каналів та їх практичної імплементації у стеллар блокчейні. Описано загальну ідею платіжних каналів та технічні деталі, що притаманні їх імплементації саме у стеллар блокчейні.

Наведено технічні деталі устрою стеллар блокчейну, а саме описано стеллар аккаунти, транзакції та операції. Наведені типи стеллар операцій, що будуть використовуватися у статті. Детально описано яким властивостям повинна задовольняти транзакція, щоб вважатися коректною з точки зору стеллар блокчейну.

Описано протокол платіжних каналів на стеллар блокчейні, наведені відповідні діаграми. Описано основні дійові особи та елементи платіжних каналів. Пояснено роль відповідних аккаунтів, а саме хост аккаунту (host account), гостьового аккаунту (guest account) та спільного аккаунту (escrow account). Пояснено роль транзакцій, що використовуються у протоколі, а саме відкриваюча транзакція (funding transaction), службова транзакція (bump sequence transaction) та транзакція-зобов'язання (settlement transaction). Наведено схему, що показує у якому порядку та від імені яких аккаунтів публікуються транзакції.

Детально описано процес обміну транзакціями поза блокчейном (off-chain transaction exchange). Для ілюстрації залежності транзакцій одна від одної наведено схему позитивних та негативних випадків публікації транзакцій.

В останньому розділі розглядається механізм інвалідації застарілих транзакцій зобов'язань за допомогою часових обмежень на публікацію транзакцій. Наведена часова діаграма, що показує які транзакції можуть бути опубліковані в певний конкретний момент часу. Пояснено необхідність часової затримки між публікацією службової (bump sequence) транзакції та транзакції зобов'язання (settlement transaction). Пояснена необхідність використання властивостей порядкового номера (sequence number) аккаунту та транзакцій.

Ключові слова: криптовалюта, блокчейн, платіжні канали, позамережеві транзакції, стеллар блокчейн, масштабування блокчейну.

Вступ

Ідея платіжних каналів у блокчейні не є новою. У біткоїн блокчейні система платіжних каналів існує вже досить давно і навіть встигла еволюціонувати у мережу лайтнінг [1]. Мережа лайтнінг — це відносно нова технологія, що складається з платіжних каналів та механізму HTLC (Hash Time-Locked Contract) [2], [3]. Поєднання цих двох технологій дозволяє проводити платежі за допомогою посередників, так звані multihop платежі. Один з напрямків дослідницької роботи — це спробувати спроектувати ідеї, що існують на біткоїн блокчейні (платіжні канали, lightning network, тощо) на інші блокчейни. Оскільки специфікація блокчейнів і їхні можливості різні — це може бути досить нетривіальною задачею. В рамках цієї статті запропоновано механізм платіжних каналів для блокчейну Stellar.

Технічні деталі Stellar блокчейну

Стеллар аккаунти

Стеллар аккаунт — це механізм Стеллар блокчейну, що володіє грошима блокчейну — люменами. На початку кожний аккаунт асоційований з одним асиметричним ключем. Асиметричний ключ є парою ключів — приватний та публічний. Публічний ключ слугує унікальним ідентифікатором аккаунту. В подальшому додаткові асиметричні ключі можуть бути асоційовані з цим акаунтом, що надасть цим ключам частковий контроль над аккаунтом. Кожний асиметричний ключ

© Є. С. Щербіна, В. І. Месюра, 2022

має вагу, для того щоб авторизувати транзакцію необхідно, щоб сумарна вага усіх підписантів перевищила порогове значення, яке асоційовано з відповідним аккаунтом [4], [5].

Кожен аккаунт асоційований з певним числом, що має назву порядковий номер (sequence number). Це число збільшується з кожною транзакцією, виконаною від імені цього аккаунта.

Стеллар транзакції

Транзакція публікується від імені одного аккаунта. Цей аккаунт відповідальний за оплату усіх комісій, пов'язаних з цією транзакцією. Транзакція збільшує порядковий номер (sequence number) аккаунту, з яким вона асоційована.

Транзакція має два параметри мінімальний час (mintime) та максимальний час (maxtime), що встановлюють часові межі, коли ця транзакція може бути включена у блокчейн [6].

Стеллар операції

Кожна стеллар транзакція включає у себе одну чи більше операцій. Кожна операція має один асоційований з нею аккаунт, що може відрізнятися від аккаунту асоційованого з транзакцією.

Транзакція має бути авторизована аккаунтом, від імені якого вона публікується, та аккаунтами, які асоційовані з операціями транзакції.

В рамках статті автори використовують п'ять типів операцій:

– "Create Account" — створює аккаунт із зазначеним ідентифікатором;

– "Payment" — здійснити трансфер грошей з одного акаунту до іншого;

"Bump Sequence" — збільшити значення порядкового номера (sequence number) відповідного аккаунту;

– "Set Options" — додати або видалити підписанта (асиметричний ключ) з аккаунта чи змінити порогове значення, яке асоційовано з аккаунтом.

– "Account Merge" — видалити аккаунт.

Причини, що можуть призвести до помилки під час виконання транзакції:

– транзакція не підписана хоча б одним обов'язковим підписантом, іншими словами не досягнуте порогове значення, що асоційоване з відповідними аккаунтами;

– недостатньо коштів для виконання транзакції;

– порядковий номер аккаунта не збігається з порядковим номером транзакції, а саме не виконується рівність acc.seq_num = tx.seq_num + 1;

– час виконання транзакції знаходиться поза межами mintime та maxtime.

Якщо одна з операцій транзакції закінчується невдачею, то вся транзакція закінчується невдачею, і жодна з операцій не має ефекту на блокчейн [7].

Загальна ідея платіжних каналів безвідносно до блокчейну

Основна ідея полягає у тому, що дві сторони замикають певну суму коштів у спільному аккаунті. Під спільним аккаунтом мається на увазі наприклад 2-of-2 multisig, таким чином витрачати гроші з цього аккаунту можливо лише за допомогою взаємної згоди. Початкова транзакція, яка замикає гроші у вищезгаданому аккаунті зазвичай має назву відкриваюча транзакція (funding transaction).

Наступний крок — це обмін транзакціями-зобов'язаннями (settlement transactions). Ці транзакції розподіляють гроші зі спільного аккаунту на власні аккаунти, беручи до уваги попередні транзакції. Кожна зі сторін має свою копію транзакції-зобов'язання. Наприклад, якщо здійснено десять транзакцій, то кожна зі сторін має 10 транзакцій зобов'язань, проте лише остання відображає реальний стан речей. Отже, необхідно мати механізм інвалідації попередніх транзакцій-зобов'язань.

Розробка протоколу платіжних каналів на блокчейні Stellar

В рамках протоколу буде задіяно три акаунти:

– спільний аккаунт (escrow account);

– хост аккаунт (host sequence account);

– гостьовий аккаунт (guest sequence account).

Усі три акаунти створюються у момент відкриття каналу. Спільний аккаунт (escrow account) —

це спільний аккаунт, що відповідає за зберігання коштів, які можуть бути витрачені лише за згодою двох осіб. Хост аккаунт (host sequence account) та гостьовий аккаунт (guest sequence account) відповідають за публікацію відповідних службових (bump sequence) транзакцій. Публікація транзакцій-зобов'язань (settlement transaction) неможлива без публікації відповідної службової (bump sequence) транзакції.

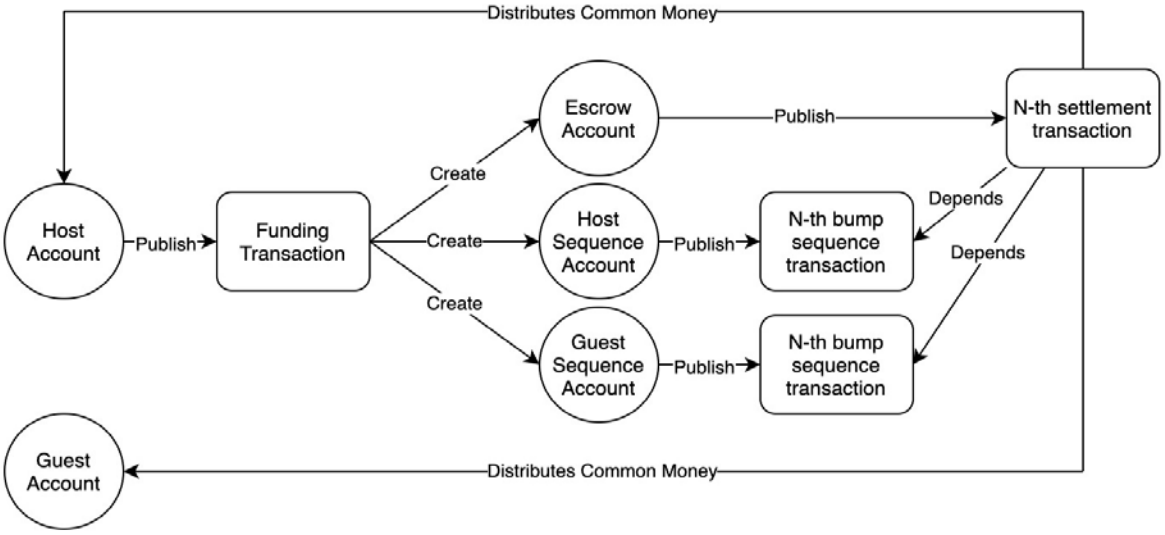

Рис. 1. Загальна схема платіжного каналу на стеллар блокчейні

Розглянемо основні дійові особи, елементи та процеси протоколу платіжних каналів. Перший крок хост аккаунт (host account) публікує відкриваючу транзакцію (funding transaction), відкриваюча транзакція своєю чергою створює три акаунти спільний аккаунт (escrow account), хост аккаунт (host sequence account) та гостьовий аккаунт (guest sequence account). Спільний аккаунт (escrow account) — ключовий аккаунт, оскільки він зберігає гроші протягом часу існування каналу.

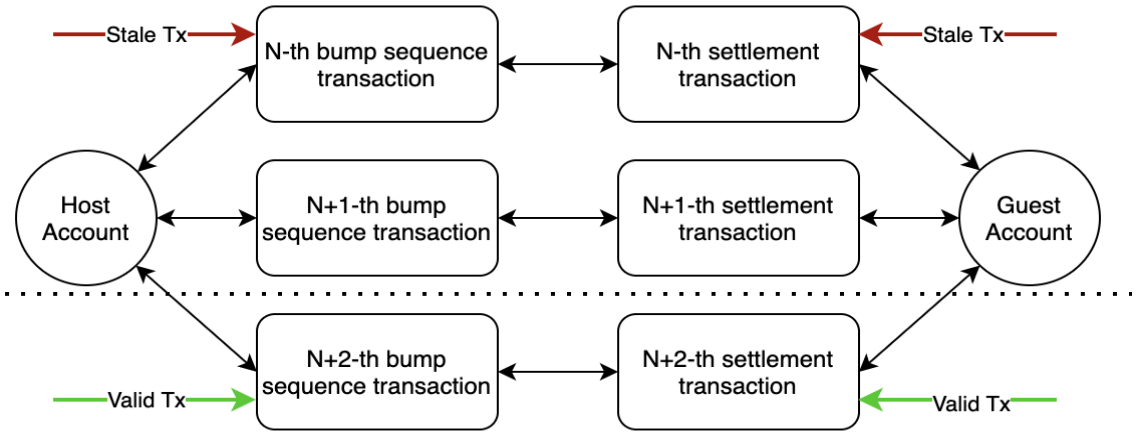

Рис. 2. Схема позамережевої транзакції у платіжному каналі

Надалі відбувається процес обміну відповідними версіями службових транзакцій (bump sequence transaction) та транзакцій-зобов'язань (settlement transaction). Нехай через деякий час прийнято рішення закрити канал, це відбувається за допомогою публікації N-th службовой (Bump Sequence) транзакції і потім N-th транзакції-зобов'язання.

N-th транзакція-зобов'язання розподіляє гроші зі спільного аккаунту до приватних акаунтів, а саме хост аккаунту та гостьового аккаунту. Варто зазначити, що N-th транзакція-зобов'язання не може бути опублікована без попередньої публікації відповідної N-th службової (bump sequence) транзакції. По суті службова (bump sequence) транзакція є допоміжною транзакцією, єдина мета якої зробити можливою публікацію транзакції-зобов'язання.

Розглянемо детальніше процес позамережевої (off-chain) транзакції. Позамережева (off-chain) транзакція складається з трьох основних етапів:

– позамережевий обмін службовими (bump sequence) транзакціями;

– позамережевий обмін транзакціями-зобов'язаннями;

– інвалідація попередніх службових (bump sequence) транзакцій та транзакцій-зобов'язань.

Варто зауважити, що кожна зі сторін має свою копію службової (bump sequence) транзакції та транзакції-зобов'язання, вони схожі між собою, проте незначні відмінності можуть мати місце. Інший важливий момент, що копія яку має Host Account підписана Guest Account і навпаки. Таким чином за необхідності Host Account може підписати транзакцію своїм асиметричним ключем і, маючи два підписи, опублікувати у блокчейні.

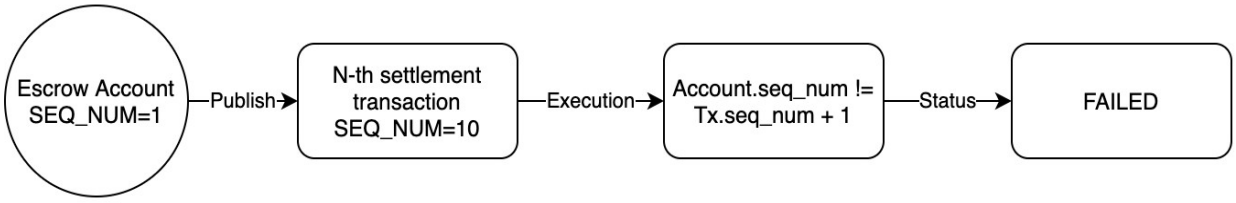

Рис. 3. Схема невдалої публікації транзакції зобов'язання

Розглянемо невдалий приклад публікації N-th Settlement транзакції. Початкове значення escrow_account.sequence_number дорівнює одиниці, а settlement_transaction.sequence_number дорівнює десяти. Під час виконання N-th settlement transaction буде виконана перевірка на умову tx.seq_num == account.seq_num + 1, в нашому випадку 10 == 1 + 1, зрозуміло, що перевірка завершиться з помилкою і буде здійснений відкат транзакції.

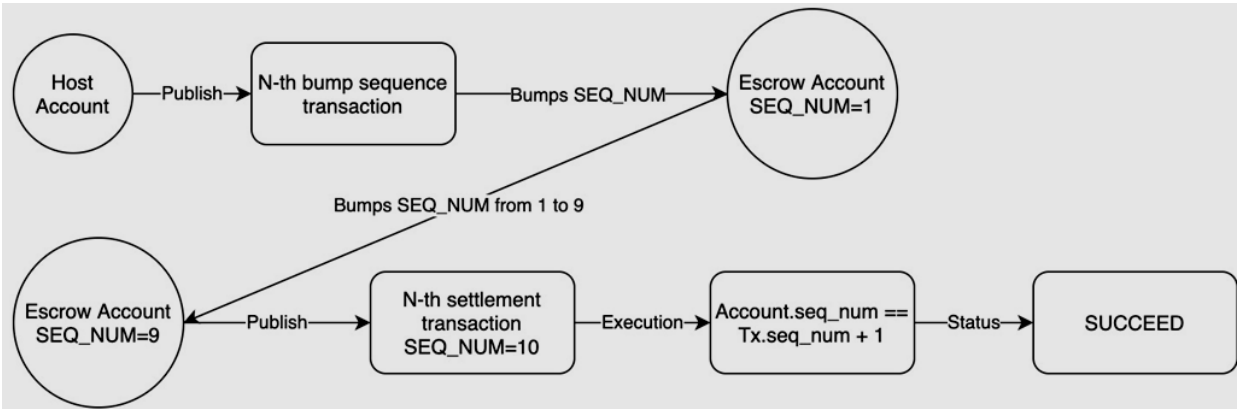

Рис. 4. Схема успішної публікації транзакції зобов'язання

Розглянемо успішний приклад публікації N-th Settlement транзакції. Початкове значення escrow_account.sequence_number дорівнює одиниці, а settlement_transaction.sequence_number дорівнює десяти. Host Account публікує N-th Bump Sequence транзакцію, ця транзакція збільшує порядковий номер спільного аккаунта (escrow account) до дев'яти. Після цього спільний аккаунт (escrow account) публікує N-th транзакцію зобов'язання (settlement transaction). Під час виконання N-th settlement transaction буде виконана перевірка на умову tx.seq_num == account.seq_num + 1, в нашому випадку 10 == 9 + 1, зрозуміло, що перевірка завершиться успішно і транзакція буде виконана успішно.

Розробка процедури інвалідації застарілих транзакцій зобов'язань

Одним з ключових моментів є інвалідація застарілих транзакцій. Необхідно запобігти сценарію, в якому одна із сторін, опублікує застарілу службову (bump_sequence) транзакцію і відповідну застарілу транзакцію зобов'язання. Для цього використовуються такі властивості Stellar блокчейну:

– можливість встановити часові обмеження в рамках яких транзакція вважається коректною;

– BumpSequence операція дозволяє збільшувати sequence number відповідного аккаунта, просто забороняє його зменшувати [8].

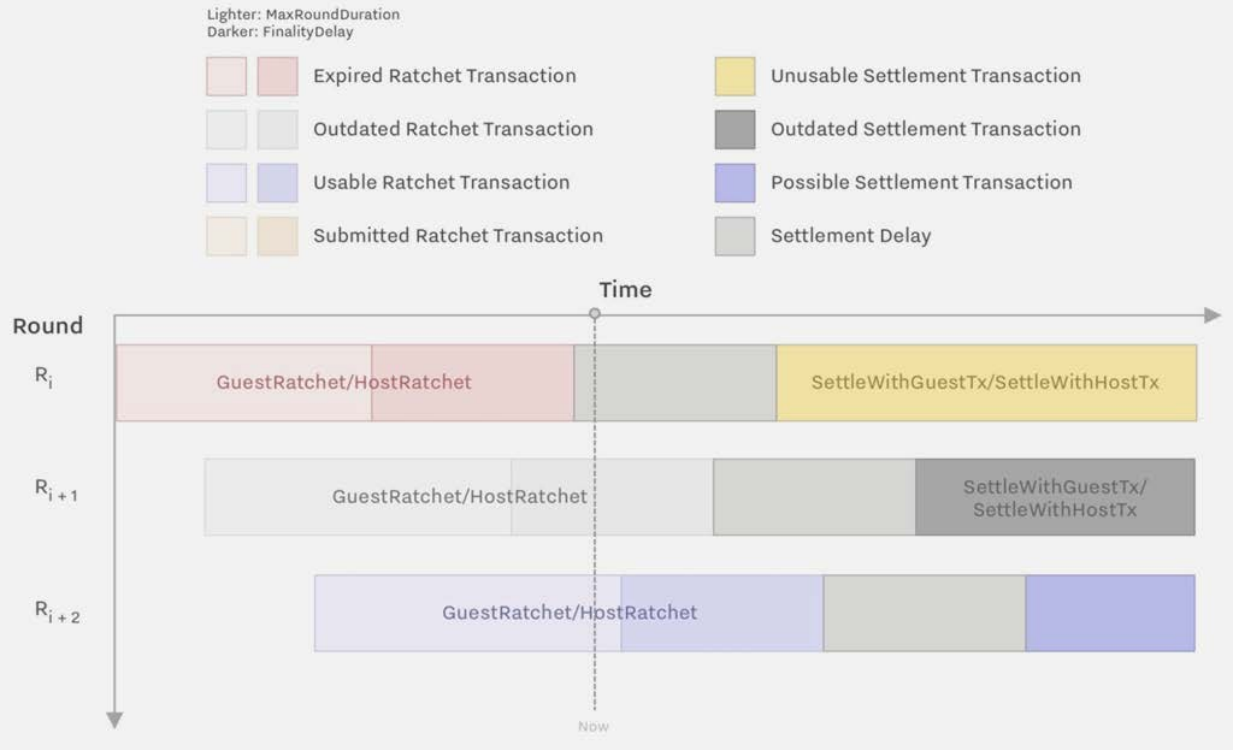

Рис. 5. Часова діаграма публікації транзакцій

Розглянемо механізм інваладації застарілих транзакцій детальніше. Зазначимо, що “ratchet transaction” та “bump sequence transaction” є синонімами. Перший важливий момент — це наявність часової затримки між “bump sequence”/”ratchet” транзакцією та відповідною транзакцією зобов’язанням. Таким чином неможливо швидко опублікувати дві транзакції, контрагент має певний час на те, щоби відреагувати на публікацію Bump Sequence транзакції. Другий важливий момент, полягає у тому, що у кожний конкретний момент часу частина Bump Sequence транзакцій є некоректними, оскільки вони не задовольняють часовим обмеженням (поточний час > максимальний час публікації транзакції), проте все ще можлива ситуація, коли в певний конкретний момент часу існує більше однієї коректної Bump Sequence транзакції. Цю ситуацію можна вирішити в такий спосіб: нехай сторона А публікує застарілу, проте все ще коректну (з погляду правил стеллар блокчейну) Bump Sequence транзакцію, користуючись часовою затримкою, сторона В може опублікувати останню Bump Sequence транзакцію і таким чином інвалідувати відповідну застарілу транзакцію зобов’язання.

Висновки

У роботі розглянуто ідею платіжних каналів, як з погляду загальної концепції так і з практичної імплементації на стеллар блокчейні. Проаналізовано стеллар блокчейн та його основні механізми, такі як аккаунти, транзакції, операції тощо.

Запропоновано протокол платіжних каналів на стеллар блокчейні, що базується на часових обмеженнях публікації транзакцій та використанні властивостей порядкового номера (sequence number) аккаунта і транзакцій. Наведено детальні схеми протоколу, а також розглянуто позитивні та негативні випадки публікації транзакцій.

Розглянуто механізм інвалідації застарілих транзакцій зобов’язань за допомогою часових обмежень на публікацію транзакцій, наведено відповідну часову діаграму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Harding, Almkglor. “Payment channels,” 2015. [Electronic resource]. Available: https://en.bitcoin.it/wiki/Payment_channels .

[2] Ladislav Mecir, “Lightning Network,” 2020. [Electronic resource]. Available: https://en.wikipedia.org/wiki/Lightning_Network .

[3] Joseph Poon, and Thaddeus Dryj, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016. [Electronic resource]. Available: https://lightning.network/lightning-network-paper.pdf .

[4] Carl Vitullo, and Jeesun Kim, “Accounts,” 2018. [Electronic resource]. Available: https://developers.stellar.org/docs/glossary/accounts/ .

[5] Carl Vitullo, and Jeesun Kim, “Multisigm” 2018. [Electronic resource]. Available: https://developers.stellar.org/docs/glossary/multisig/.
[6] Carl Vitullo, and Jeesun Kim,“Transactions,” 2018. [Electronic resource]. Available: https://developers.stellar.org/docs/glossary/transactions/ .
[7] Carl Vitullo, and Jeesun Kim, “Operations,” 2018. [Electronic resource]. Available: https://developers.stellar.org/docs/glossary/operations/ .
[8] Carl Vitullo, and Jeesun Kim, “List-of-operations,” 2018. [Electronic resource]. Available: https://developers.stellar.org/docs/start/list-of-operations/#bump-sequence .

Рекомендована кафедрою комп’ютерних наук ВНТУ

Стаття надійшла до редакції 24.01.2022

Щербіна Євгеній Сергійович — аспірант кафедри комп’ютерних наук, e-mail: evgeniy.shcherbina.es@gmail.com ;
Месюра Володимир Іванович — канд. техн. наук, доцент, професор кафедри комп’ютерних наук, e-mail: mesyura@vntu.edu.ua .
Вінницький національний технічний університет, Вінниця

E. S. Shcherbina[1]
V. I. Mesiura[1]

Payment Channels in Stellar Blockchain

[1]Vinnytsia National Technical University

The article is devoted to the topic of payment channels and their practical implementation in the Stellar blockchain. The general idea of payment channels and technical details that are inherent in their implementation in the Stellar blockchain are described.

The technical details of the Stellar blockchain are given, namely the Stellar accounts, transactions and operations are described. The types of stellar operations that will be used in the article are given. It describes in detail what properties a transaction must satisfy in order to be considered correct from the point of view of a Stellar blockchain.

The protocol of payment channels on a Stellar blockchain is described, the corresponding diagrams are given. The main actors and elements of payment channels are described. The role of the respective accounts is explained, namely the host account, the guest account and the escrow account. The role of the transactions used in the protocol is explained, namely the funding transaction, the bump sequence transaction and the settlement transaction. The scheme shows the order in which transactions are published.

The process of exchanging off-chain transactions is described in detail. To illustrate the dependence of transactions on each other, a diagram of positive and negative cases of publication of transactions is given.

The last section discusses the mechanism for invalidating obsolete commitment transactions through time limits on the publication of transactions. The timing chart shows which transactions can be published at a specific point in time. The need for a time delay between the publication of a bump sequence transaction and a settlement transaction is explained. The need to use the properties of the sequence number of the account and transactions is explained.

Keywords: cryptocurrency, blockchain, payment channels, off-chain transactions, Stellar blockchain, blockchain scaling.

Shcherbina Evgeniy S. — Post-Graduate Student of the Chair of Computer Science, e-mail: evgeniy.shcherbina.es@gmail.com ;
Mesiura Volodymyr I. — Cand. Sc. (Eng), Associate Professor, Professor of the Chair of Computer Science, e-mail: mesyura@vntu.edu.ua