

Г. О. Черноволик
С. В. Бевз
С. М. Бурбело
В. В. Войтко
І. С. Мельник

РОЗРОБКА ЕКОСИСТЕМИ ДЛЯ ЕМІСІЇ ТА ПЕРЕКАЗУ КРИПТОВАЛЮТИ

Вінницький національний технічний університет

Анотація

Розглянуто особливості розробки криптовалюти. Набір програмних додатків призначений для емісії криптовалюти, обробки запитів та подання UI для зручного доступу користувачів до можливостей системи.

Ключові слова: Криптовалюта, хешування, блокчейн, транзакція.

Abstract

Features of cryptocurrency development are considered. A set of software applications designed for cryptocurrency issuance, request processing and presentation of the user interface for easy user access to system capabilities.

Keywords: Cryptocurrency, hashing, blockchain, transaction.

Вступ

На сьогоднішній день цифровізація зачіпає навіть найвіддаленіші куточки світу. І час, коли світ повністю перейде на цифрову валюту, вже не так далеко. Зараз існує чимало варіантів реалізації централізованих та децентралізованих криптовалют. Але це тільки початок, тому реалізація екосистеми для функціонування криптовалюти є актуальним питанням.

Метою роботи є розробка власної централізованої криптовалюти з використанням передових технологій.

Об'єктом дослідження є фактори, що впливають на зацікавленість користувача у переході до використання цифрової валюти.

Предметом дослідження є механізми функціонування криптовалюти.

Головною задачею роботи є розробка екосистеми криптовалюти, спрямованої на валютну емісію і збереження та керування ресурсами користувачів.

Розробка програмних додатків для емісії та переказу криптовалюти

Екосистема додатків складається з:

- веб-клієнта для управління гаманцями користувачів, включаючи перегляд історії транзакцій, баланс, створення нових транзакцій;
- консольного клієнта для емісії криптовалюти, а саме для обчислення хешів нових транзакцій і відправлення результатів на сервер для перевірки та зберігання;
- веб-дodatка на стороні сервера для обробки даних із клієнтських програм і забезпечення збереження даних через зв'язок з базою даних MS SQL Server.

У процесі розробки програмних додатків для емісії та переказу криптовалюти були використані такі технології: C#, ASP .NET MVC, ASP .NET Core, Web API, REST, Dapper, SQL, SignalR, HTML5, JS, jQuery, AJAX, CSS, Bootstrap, Serilog, IOC, TDD, GIT, MSTest, NSubstitute.

Загальну модель функціонування екосистеми наведено на рис. 1.

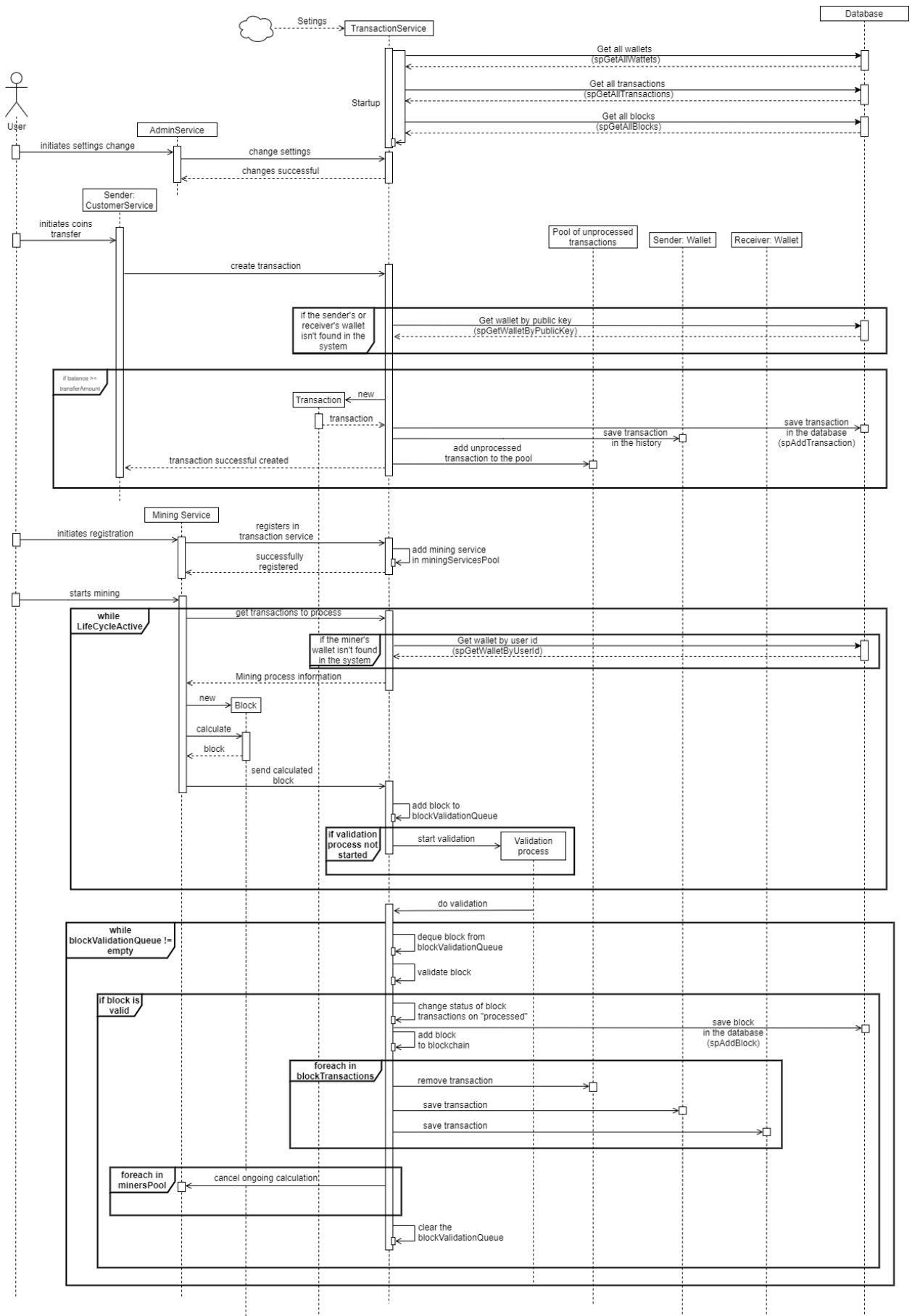


Рис.1. Загальна модель функціонування екосистеми додатків для емісії та переказу криптовалюти

Для формування та збереження криптовалюти використовуються дві важливі структури: транзакція і блок. Транзакція виступає ключовою одиницею всієї системи, оскільки криптовалюта у системі не зберігається у відкритому вигляді, як просте поле у програмному коді, а існує у вигляді взаємозв'язку кількох структур, найпростішою з яких є сама транзакція. Транзакції для затвердження системою спочатку потрапляють у тимчасове сховище очікування. З цього сховища час від часу відбирається певна кількість транзакцій, яка бере участь у емісії криптовалюти. Під час емісії формується блок з відібраних транзакцій. Транзакції з цього блоку підлягають хешуванню та подальшому збереженню у базі даних у захищеному вигляді. Ці блоки формують ланцюг, у якому кожен блок створюється, використовуючи дані із попереднього ланцюга. Це забезпечує цілісність системи та захист від зміни даних.

У моделі (рис. 1) продемонстровано загальний життєвий цикл транзакції, а саме: емісію (реєстрацію певної кількості одиниць у системі), потрапляння до електронного гаманця користувача, використання криптовалюти у переказі на інший гаманець – процеси, які проходить транзакція від створення до її затвердження системою.

Висновок

Розроблений прототип криптовалютної системи дозволить зробити ще один крок до залучення цифрових технологій у повсякденне життя. Адже основа криптовалютної системи – це абсолютна безпека, створена особливостями збереження, формування даних та простотою використання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cryptocurrency development. [Електронний ресурс]. Режим доступу до ресурсу: <https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343>.
2. Blockchain basics. [Електронний ресурс]. Режим доступу до ресурсу: <https://www.investopedia.com/terms/b/blockchain.asp>.
3. SHA-256 hashing [Електронний ресурс]. Режим доступу до ресурсу: <https://infosecwriteups.com/breaking-down-sha-256-algorithm-2ce61d86f7a3>.
4. Block calculation example [Електронний ресурс]. Режим доступу до ресурсу: <https://dlt-repo.net/how-to-calculate-a-bitcoin-block-hash-manually/>.

Черноволик Галина Олександрівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: lina2433@gmail.com.

Бевз Світлана Володимирівна – кандидат технічних наук, доцент кафедри електричних станцій і систем, Вінницький національний технічний університет, м. Вінниця, e-mail: svbevz@i.ua.

Бурбело Сергій Михайлович – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: smburbelo@gmail.com.

Войтко Вікторія Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: dekanfki@i.ua.

Мельник Ілля Сергійович – студент групи ІПІ-19мс2, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: iLegend1706@gmail.com

Galyna Chernovolyk – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lina2433@gmail.com.

Svitlana Bevz – Ph.D., Associate Professor, Department of Power Plants and Systems, Vinnitsa National Technical University, Vinnitsa, e-mail: svbevz@i.ua.

Sergii Burbelo – Ph.D., Associate Professor of Software Engineering, Vinnitsa National Technical University, Vinnitsa, e-mail: smburbelo@gmail.com.

Viktoriia Voitko – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dekanfki@i.ua.

Melnyk Ilya – student of ІПІ-19ms2, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: iLegend1706@gmail.com.