Технічні науки

УДК 004.3

Довжик Дмитро Вікторович
студент
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Довжик Дмитрий Викторович
студент
Национального технического университета Украины
"Киевский политехнический институт имени Игоря Сикорского"
Dovzhyk Dmytro
Student of the
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Потапова Катерина Романівна
кандидат технічних наук, доцент кафедри системного
програмування і спеціалізованих комп'ютерних систем
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Потапова Екатерина Романовна
кандидат технических наук, доцент кафедры системного
программирования и специализированных компьютерных систем
Национальный технический университет Украины
"Киевский политехнический институт имени Игоря Сикорского"
Potapova Kateryna
PhD, Associate Professor
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

СИСТЕМА ОНЛАЙН-ГОЛОСУВАННЯ НА БАЗІ ТЕХНОЛОГІЇ BLOCKCHAIN З ВИКОРИСТАННЯМ НАЦІОНАЛЬНИХ СТАНДАРТІВ ШИФРУВАННЯ

СИСТЕМА ОНЛАЙН-ГОЛОСОВАНИЯ НА БАЗЕ ТЕХНОЛОГИИ BLOCKCHAIN С ИСПОЛЬЗОВАНИЕМ НАЦИОНАЛЬНЫХ СТАНДАРТОВ ШИФРОВАНИЯ

ONLINE-VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY USING NATIONAL ENCRYPTION FACILITIES

Анотація. *Розглянута можливість розробки системи онлайн-голосування на базі технології Blockchain. Проблема подібних існуючих систем у тому, що збереження даних і підрахунок голосів здійснюється на одному сервері, тому вони є вразливими до хакерських атак. Використання технології Bockchain дозволяє зробити систему голосування децентралізованою та більш захищеною від зовнішнього втручання. Електронно-цифровий підпис, що використовується для шифрування даних блоку Blockchain, ґрунтується на використанні алгоритму шифрування даних та функції гешування. Тому в роботі розглянуті алгоритм симетричного блокового перетворення Калина та функція гешування Купина, яка визначені у національних стандартах захисту інформації. Разом вони можуть бути використані для розробки системи онлайн-голосування у межах нашої країни.*

Ключові слова: *онлайн-голосування, блокчейн, захист інформації, функція гешування, шифрування, електронний цифровий підпис.*

Аннотация. *Рассмотрена возможность разработки системы онлайн-голосования на базе технологии Blockchain. Проблема подобных существующих систем в том, что хранение данных и подсчет голосов осуществляется на одном сервере, поэтому они уязвимы к хакерским*

атакам. Использование технологии Bockchain позволяет сделать систему голосования децентрализованной и более защищенной от внешнего вмешательства. Электронно-цифровая подпись, которая используется для шифрования данных блока Blockchain, основывается на использовании алгоритма шифрования данных и функции хеширования. Поэтому в работе рассмотрены алгоритм симметричного блочного преобразования Калина и функция хеширования Купина, которые определены в национальных стандартах защиты информации. Вместе они могут быть использованы для разработки системы онлайн-голосования в пределах нашей страны.

Ключевые слова: *онлайн-голосование, блокчейн, защита информации, функция хеширования, шифрование, электронная цифровая подпись.*

Summary. *The possibility of developing an online voting system based on Blockchain technology is considered. The problem with such existing systems is that the data is stored and the votes are counted on a single server, so they are vulnerable to hacker attacks. The use of Bockchain technology allows to make the voting system decentralized and more protected from external interference. The electronic digital signature used to encrypt Blockchain data is based on the use of a data encryption algorithm and hashing function. Therefore, the Kalyna algorithm of symmetric block transformation and the Kupyna hashing function are considered in the work, which are defined in the national standards of information protection. Together, they can be used to develop an online-voting system within our country.*

Key words: *online-voting, blockchain, information protection, hashing function, encryption, electronic digital signature.*

Постановка проблеми. Голосування на виборах до різних органів державної влади є одним з методів волевиявлення суспільства. Альтернативою традиційному голосуванню є електронне, так зване онлайн-голосування. На сьогодні багато країн розглядають можливість впровадження систем онлайн-голосування з метою удосконалення різних аспектів виборчого процесу.

Чому саме блокчейн розглядається як рішення для чесного голосування? Тому що, блокчейн вирішує основну проблему традиційного голосування – централізацію. Основна ідея технології блокчейн полягає у децентралізації зберігання даних, кожен з учасників ланцюга має свою копію даних, усі зміни вносяться поступово та розповсюджуються між усіма учасниками ланцюга, інформація в ній відкрита для всіх і кожного. Таким чином, дуже складно підробити результат голосування, для цього знадобиться зламати усіх користувачів без винятку та змінити їх копії даних, що в дійсності досить складно. В наш час майже кожен громадянин України має доступ до інтернету, тому електронна система голосування могла б сильно оптимізувати витрати на виборчий процес та пришвидшити його, і разом з тим зробити голосування більш прозорим. Маючи таку систему можна було б проводити будь-які голосування у кілька натискань на смартфоні або комп'ютері, починаючи від голосувань в об'єднаних громадах та закінчуючи голосуванням за голову держави.

В найпростішому значенні блокчейн представляє собою серію незмінних записів даних з мітками часу, якими управляє кластер комп'ютерів, які не належать якому одному суб'єкту. Кожен з цих блоків даних зашифрований та пов'язаний один з одним за допомогою криптографічних принципів. Етап шифрування блоків вимагає використання криптографічних алгоритмів, які можуть вирішити такі проблеми як безпека, висока доступність та швидкість виконання транзакцій. Ці криптографічні алгоритми повинні відповідати стандартам

криптографічного захисту інформації в Україні, для можливості використання у державних структурах.

Аналіз існуючих рішень. Концепція електронного голосування стає дедалі популярнішою у Європі. Естонія запровадила електронне голосування ще в 2005 році, і переважна більшість населення зараз голосує електронним способом. Ця система базується на національному посвідченні особи, яке видається всім громадянам Естонії. Посвідчення містять зашифровані дані, які можна використовувати для ідентифікації власника. Це дозволяє власнику здійснювати низку онлайн заходів, підписання цифрових документів, доступ до їхньої інформації у державній базі даних та онлайн-голосування. Щоб мати змогу голосувати, виборець повинен ввести свою картку у спеціальний зчитувач карток, а потім отримати доступ до голосування на веб-сайті. Потім ввести свій PIN-код і система перевірить, чи має право виборець голосувати. Після підтвердження виборець може подати / змінити свій голос впродовж чотирьох днів до дня закінчення виборів.

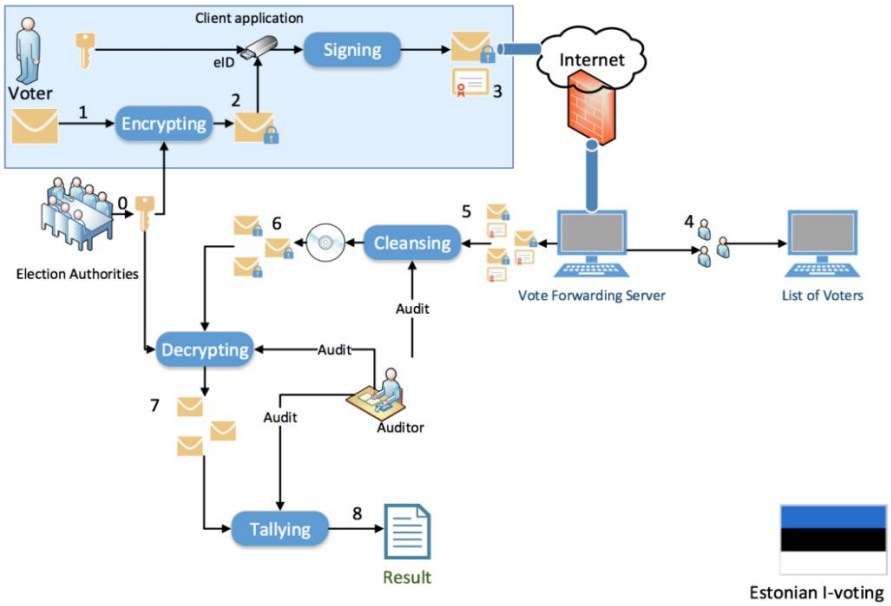

Рис. 1. Естонська система електронного голосування

Коли виборець віддає свій голос, він проходить через загальнодоступний сервер перенаправлення, зашифровується і зберігається до кінця виборів. Після виборів усі голоси зберігаються на DVD-дисках, видаляються із сервера, а потім передаються на сервер для підрахунку голосів, який відключений від усіх мереж. Цей сервер розшифровує і підраховує голоси, а потім виводить результати. Кожен етап цього процесу є зареєстрованим та перевіреним.

Під час місцевих виборів 2013 року дослідники спостерігали і вивчали процес голосування і виявили ряд потенційних ризиків для системи безпеки. Одним з таких ризиків є можливість встановлення зловмисного програмного забезпечення на машині на стороні клієнта, яке відстежує користувача, який голосує, а потім, без відома користувача, може змінити його голос на іншого кандидата. Інший можливий ризик є у тому, що зловмисник може безпосередньо заразити DVD-диск, який використовується для налаштування серверів та передачі голосу [1].

Постановка задачі. Задача полягає у розробці системи онлайн-голосування з використанням технології Blockchain для забезпечення надійності та захищеності процесу голосування та його результатів. Будь-яке програмне забезпечення, яке займається шифруванням інформації (особливо користувацької) повинно відповідати державним стандартам. Тому є необхідність розглянути функцію гешування Купина, яка визначена у національному стандарті криптографічного захисту інформації ДСТУ 7564:2014, та алгоритм симетричного блокового перетворення Калина, визначений у стандарті ДСТУ 7624:2014. Разом вони можуть використовуватись для гешування блоку у блокчейн технологіях, з метою розробки державних блокчейн систем придатних для захисту інформації у межах нашої країни.

Виклад основного матеріалу дослідження. Блокчейн (chain of block) – це розподілена база даних, у якій пристрої зберігання даних не

підключені до загального сервера. Ця база даних зберігає постійно зростаючий список упорядкованих записів, званих блоками. База захищена від підробки та переробки. Кожен блок містить мітку часу та посилання на попередній блок геш дерева. Для запису нового блоку, необхідно послідовне зчитування інформації про старі блоки.

Функціонування блокчейну відбувається в режимі P2P (комп'ютерна мережа, де всі учасники рівноправні). Всі операції проводяться між суб'єктами безпосередньо. А здійснюються вони за рахунок того, що всі учасники підключені до однієї мережі — блокчейн.

Запис нового блоку в мережу блокчейн включає в себе 5 етапів:

1) Запит на здійснення транзакції в мережу. Користувач, який хоче надіслати дані іншому користувачеві, формує транзакцію та відправляє його до мережі. Система створює унікальний ключ для доступу до надісланих даних. Відправник передає цей ключ одержувачу.

2) Обробка транзакції і складання з неї нового блоку. Дані транзакції обробляються системою і утворюють блок, що містить зашифровану інформацію від інших користувачів.

3) Поширення нового блоку серед усіх учасників. Система знаходиться у всіх користувачів одночасно, і постійно перевіряє, чи відповідає копія інформації, раніше внесеної в базу.

4) Внесення нового блоку до всіх екземплярів блокчейну. Якщо під час перевірки блок буде визнаний відповідним, він буде внесений в усі копії та доповнить вже існуючий ланцюг. Система забезпечить унікальний цифровий підпис, за допомогою якого новий блок можна буде відстежити.

5) Завершення операції. Після створення нового блоку, одержувач зможе скористатись переданим відправником унікальним ключем, для отримання відправленої інформації.

У найпростішій формі база даних представляє з себе ланцюжок блоків, який може бути представлений у вигляді файлу формату JSON.

Структура блоку:

- кожен блок складається з адреси, дати і часу створення, геша і списку транзакцій (рис. 2);
- адреса – публічний ключ, що генерується алгоритмом шифрування, на основі вигаданого користувачем приватного ключа;
- дата і час – час створення транзакції (блоку);
- геш – обчислюється за допомогою функції гешування від адреси попереднього блоку і суми гешів всіх транзакцій поточного блоку;
- інформація – повідомлення, сума грошей (криптовалюта), документи, історія хвороб, програмний код (смарт контракти) і т. д.

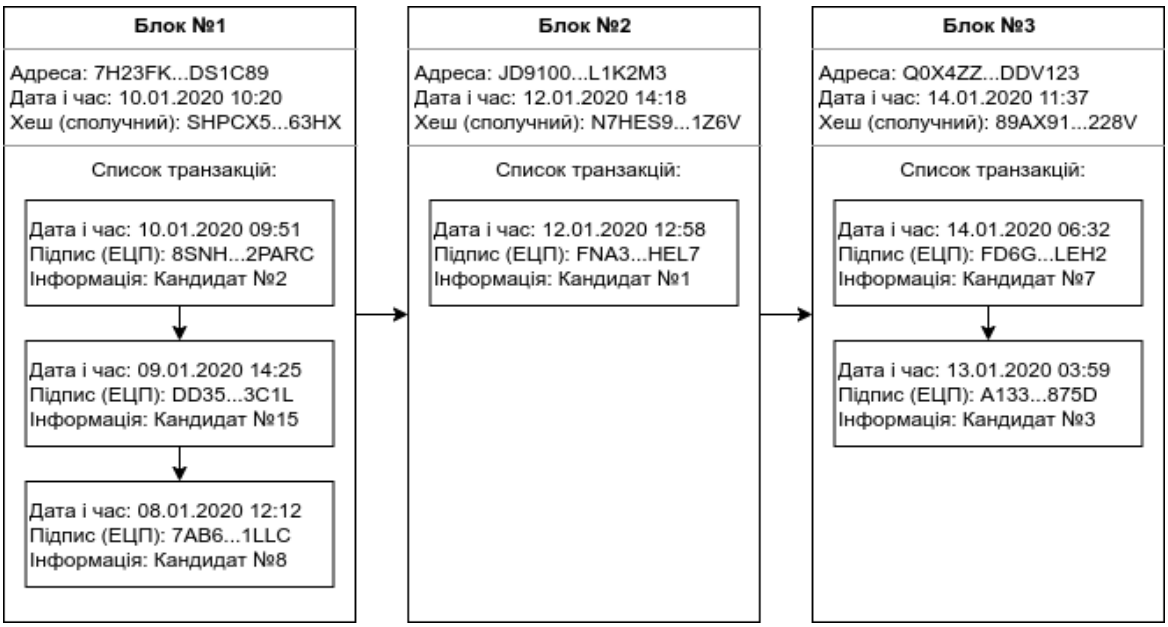

Рис. 2. Приклад системи блокчейн з трьох блоків

Електронний цифровий підпис. З метою запобігання фальсифікації інформації всередині транзакції, кожна транзакція всередині блоку підписується електронним цифровим підписом (ЕЦП).

Електронно-цифровий підпис — це послідовність байтів, утворена перетворенням інформації з використанням криптографічного алгоритму для перевірки особи автора електронного документа [1].

ЕЦП ґрунтується на використанні блочного шифрування та геш-функції.

Алгоритм створення підпису інформації (документа). Для створення підпису необхідні:

- алгоритм шифрування (блочний симетричний шифр Калина);
- геш-функція (криптографічна геш-функція Купина);
- інформація, яка повинна бути передана.

Стандарт ДСТУ 7624:2014 [2] визначає сучасний блоковий шифр Калина та його режими роботи для приховування семантичного вмісту та запобігання несанкціонованій модифікацій повідомлень. Шифр є гнучким і підтримує розмір блоку та довжину ключа до 512 бітів. Це єдиний у світі стандарт шифрування блоків, який підтримує такий рівень безпеки. Для порівняння широко поширений AES забезпечує максимальну довжину ключа 256 біт. У той же час, Калина має більш високу продуктивність, ніж AES, у програмній реалізації на більшості сучасних 64-розряднихплатформах для настільних і серверних систем з однаковою довжиною ключа.

ДСТУ 7624:2014 визначає десять режимів роботи блокового шифру. Для порівняння, міжнародний стандарт ISO/IEC10116 має лише шість режимів (вони також є в національному стандарті України). Порівняно з аналогами в країнах регіону і всієї Європи в цілому, додаткові режими надають більше можливостей українським розробникам засобів криптографічного захисту інформації.

Шифр Калина — це високостійкий та швидкий симетричний шифр, орієнтований на сучасні продуктивні апаратні платформи.

Стандарт ДСТУ 7564:2014 визначає функцію гешування Купина, яка забезпечує високостійке і гнучке криптографічне перетворення [3]. Її

можна використовати і як незалежний стандарт для забезпечення цілісності, так і як додаткове перетворення в складі цифрового підпису.

Геш-функція Купина має ключову особливість, яка відрізняє її від інших існуючих алгоритмів генерації гешу. Купина може бути використана в технології блокчейну, які враховують динамічність геш-функції, причому динамічною є не тільки сама функція, але і довжина виходу геш-функції.

При використанні динамічного розміру блоку динамічність виходу геш-функції не впливає на кількість транзакцій, що містяться в блоці, але покращує криптографічні властивості блокчейну, такі як криптостійкість.

Функція Купина — це ітеративна геш-функція, заснована на архітектурі Меркле-Дамгора [4]. Вона використовує функцію стиснення Девіса-Мейєра, яка базуєтьсяна конструкції блокового шифру Івена-Мансура [5]. Геш-функція Купина побудована на функції стиснення, що складається з двох фіксованих перестановок, структура яких запозичена у блокового шифру Калина, та за структурою є підстановлювально-перестановочною мережею. Результатом геш-функції є послідовність бітів від 8 до 512 біт. Варіант функції, який повертає *n* біт, позначається як Купина-*n* [6]. Основними режимами роботи функції гешування, рекомендованими до застосування, є Купина-256, Купина-384 і Купина-512.

Проектування системи. Для того, щоб стримувати різні кібератаки, такі як, наприклад, атака відмови в обслуговуванні (distributed denial-of-service attack (DdoS)), головною задачею якої є вичерпання ресурсів комп'ютерної системи шляхом надсилання декількох підроблених запитів є протокол підтвердження роботи. Система голосування оперує блокчейн мережею. Кожен голос створює новий блок у ланцюгу мережі. Користувачі відправляють запити на систему, а вона, в свою чергу, створює новий блок, шифрує та записує дані. Для недопускання конфліктів запису, а також для верифікації блоків використовується алгоритм досягнення консенсусу — Proof-of-work.

Завдання досягнення консенсусу базується на голосуванні. Консенсус - поняття прийняття рішення, яке б задовольняло більшість опитаних.

Існує два обґрунтованих випадки невірного функціонування розподіленої системи:

1) відмова вузла. Проблема у тому, що вузол який відмовив стає недоступним для інших частин системи, і якщо, наприклад, він має унікальні дані то система в такому випадку втрачає цілісність. Розповсюджені приклади таких випадків: відмова сервера або якогось з його компонентів, відмова системи зберігання даних, збій у операційній системі, втрата підключення до мережі, тощо;

2) візантійська помилка. Цей випадок цікавий тим, що вузол продовжує працювати, але працює некоректно. Такий вид помилок найважче ідентифікувати та виправляти. Наприклад, пошкодження пакетів і т.д.

Proof-of-work (PoW) — алгоритм досягнення консенсусу в блокчейні, який являє собою набір певних математичних правил і функцій, що дозволяють досягти угоди між усіма учасниками і забезпечити працездатність мережі.

Щоб брати участь в перевірці транзакції, учасникам необхідно публічно довести проведену роботу. Це правило запобігає атаці на систему в тому випадку, якщо зловмисник створює несправжніх виборців [7]. Чим більше зроблено роботи, тим більше можливостей зробити наступний блок і отримати підтвердження. Схема роботи алгоритму зображений на рис. 3.

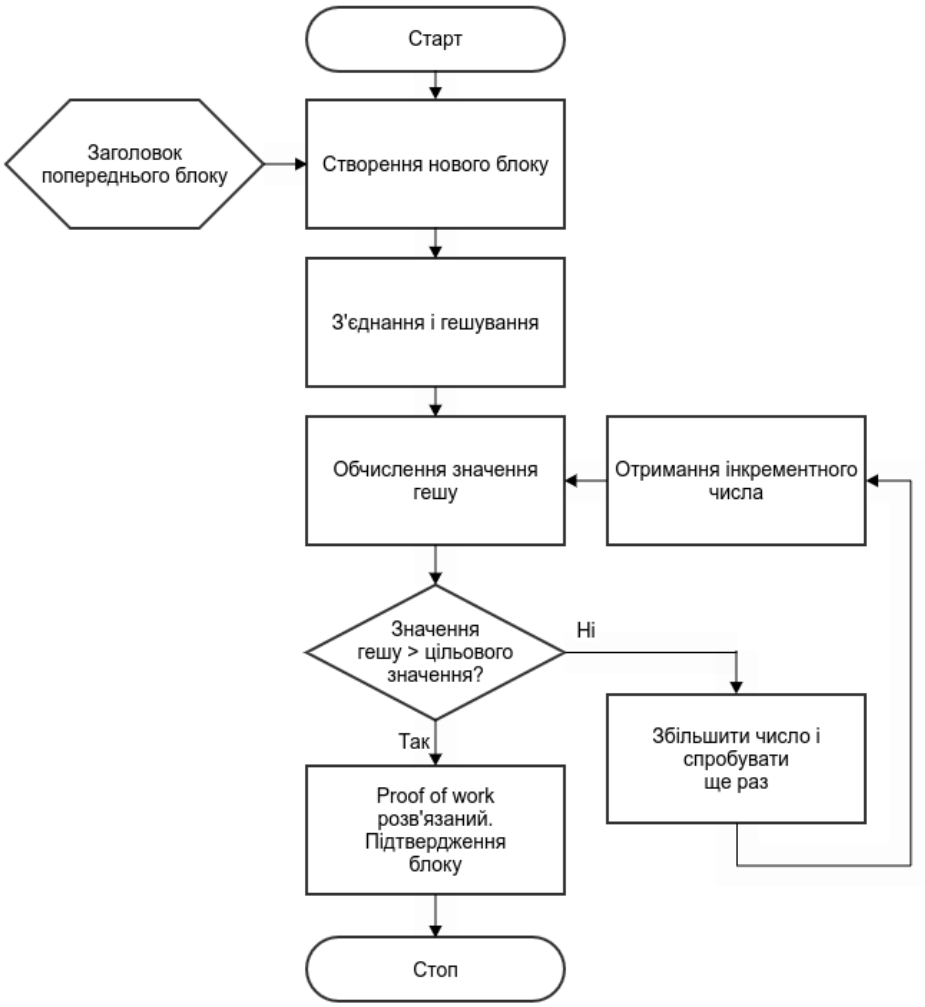

Рис. 3. Схема роботи алгоритму консенсусу Proof-of-work

PoW вважають найлегшим і в той же час найстабільнішим алгоритмом в контексті повної децентралізації та анонімності.

Опис функціоналу системи. Додаток повинен надавати користувачеві можливість виконувати наступні дії:

1) зареєструватися у системі;
2) переглядати усіх кандидатів;
3) віддавати голос користувача за бажаного кандидата;
4) сповіщати користувача про успішно відданий голос. Можливі наступні варіанти:
    a. сповіщення в системі логування;
    b. повідомлення на електронну пошту.

5) Переглядати статистику роботи системи.

На рис. 4 зображена діаграма прецедентів високого рівня. На ній зображені можливі дії користувача, абстраговані від деталей.

Рис. 4. Діаграма прецедентів додатку

Основні вимоги до системи:

1) можливість легко та просто зареєструватися та проголосувати;
2) зрозумілий процес голосування з дотриманням усіх вимог;
3) охоплення широкого кола потенційних користувачів - система повинна бути легкою у використанні.

Концептуальна діаграма класів структури даних. На основі сутностей, виділених із прецедентів, можна побудувати концептуальну діаграму класів моделі застосунку [8]. Для розробки алгоритму розподілу запитів в системі по реплікаціям використано мову програмування C++. Для моделювання роботи блокчейн використано об'єктно орієнтований підхід та патерни. Це дає змогу змоделювати роботу блокчейн мережі. Для моделювання роботи алгоритму досягнення консенсусу використано мову програмування C++. Для створення геш значення використано бібліотеку std::hash. Інтерфейс для системи розроблено за допомогою фреймворку Qt. На рис. 5 зображена діаграма класів моделі даних користувача.

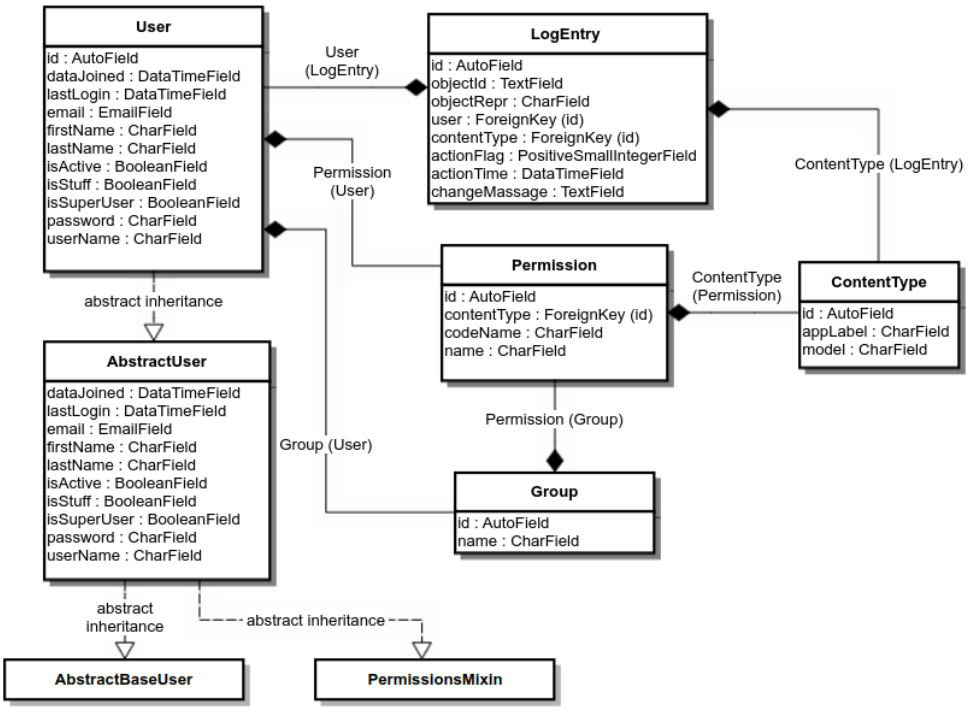

Рис. 5. Діаграма класів моделі даних користувача

Висновки. Розглянуто використання технології Blockchain у електронному голосуванні та актуальність концепції даного програмного забезпечення. Зроблено загальний опис предметної області задачі, сформовано функціонал, який повинна забезпечувати система. Було розглянуто прецеденти використання системи та алгоритм консенсусу Proof-of-Work для досягнення угоди між учасниками голосування. Також розглянуто питання впровадження блочного симетричного шифру Калина та геш-функції Купина, що описані у національних стандартах криптографічного захисту інформації, для шифрування блоку блокчейну.

Література

1. Dovzhyk D., Potapova K., Online-voting system based on blockchain technology // Priority directions of science and technology development. Abstract of the 2-nd International scientific and practical conference. SPC "Sci-conf.com.ua". Kyiv, Ukraine. 2020. PP. 248-249.

2. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. Введ. 01–07–2015. К.: Мінекономрозвитку України, 2015.
3. Держспецзв'язку впроваджує нові стандарти криптографічного захисту інформації. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=120158&cat_id=119123.
4. Merkle R.C. Secrecy, authentication, and public key systems // Department of Electrical Engineering, Stanford University, 1979. PP. 13-15.
5. Black J., Rogaway P., Shrimpton T. Black-box analysis of the block-cipher-based hash-function constructions from pgv // Advances in Cryptology. August 18-22. 2002. Proceedings. Vol. 2442. Lecture Notes in Computer Science. PP. 320-335.
6. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації // Функція ґешування. Введ. 01–04–2015. К.: Мінекономрозвитку України, 2015.
7. Voting using blockchain and smart contracts. URL: https://medium.com/swlh/voting-using-blockchain-and-smart-contracts
8. Blockchain Architecture. URL: https://mlsdev.com/blog/156-how-to-build-blockchain-architecture