Богомаз Олексій
КІТ-м120Б

Лабораторна робота №5

Мета: Ознайомитись з технологією MerkleTree

Завдання:

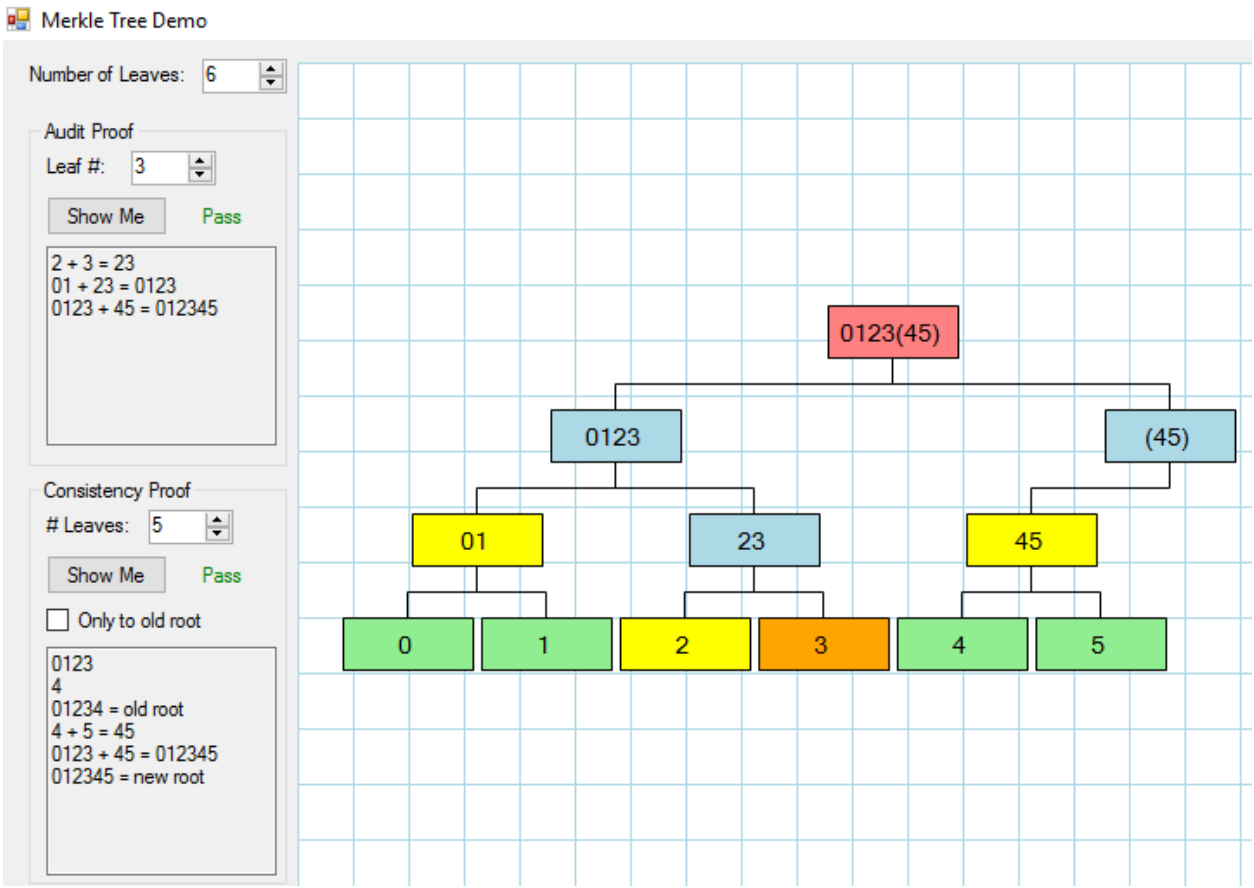
Створити екосистему (та продемонструвати її роботу), що складається з наступних компонентів:

- сервер. Має інформацію о файлах мережі у наступному вигляді:
  - merkle root
  - Перелік клієнтів, що мають хоча б частину контенту файлу та перелік блоків, які вони мають
- клієнт, що має хоча б частину контенту файлу. Дії, що можна проводити над клієнтом:
  - запитати частину файла. На вхід подається merkle root цього файлу, індекс блоку. На вихід дається контент файлу або помилка, якщо такого блоку немає
  - виконати верифікацію блока. На вхід подається merkle root, block hash. На вихід подається обрізане під-дерево (гілку до запитаного геша) стосовно алгоритму. Якщо block hash відсутній або невалідний - повертаєтсья стосовна помилка.
- клієнт, що завантажує файл. Послідовність дій, що виконується:
  - отримує будь-яким чином merkle root бажаного для завантажування файлу
  - виконує завантаження блоку:
  - питає у сервера перелік клієнтів, що має певну частину цього файлу.
  - завантажує блок
  - виконує верифікацію блоку:
  - виконує гешування блоку

- обирає будь-який інший сервер, що має цей блок та питає його частину merkle дерева. Якщо інший сервером нема, питаємо у того, з якого завантажували
- самостійно проводить верифікацію гілки дерева
- якщо усе добре - зберігає блок, оновлює внутрішню базу даних, посилає запит на сервер для додання зпису, що даний клієт має блок з тиким індексом для певного файлу (merkle root)

Хід роботи

Демо-версія дозволяє досліджувати створення дерев Merkle та проводити перевірку аудиту та узгодженості. Графічна поверхня реалізована як вбудована служба FlowSharp.

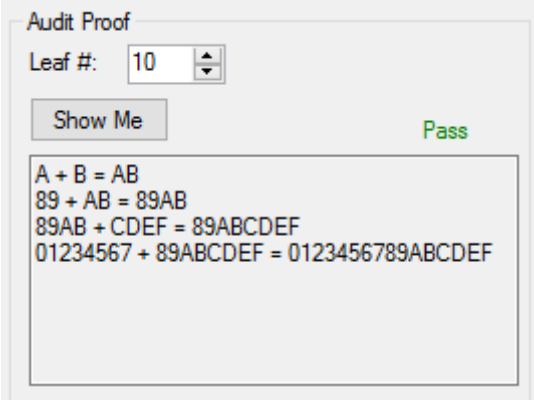


Демо-версія взаємодіє зі службою FlowSharp за допомогою веб-розетки на порту 1100 з метою створення фігур та з'єднувачів на полотні.

Зміна кількості листків

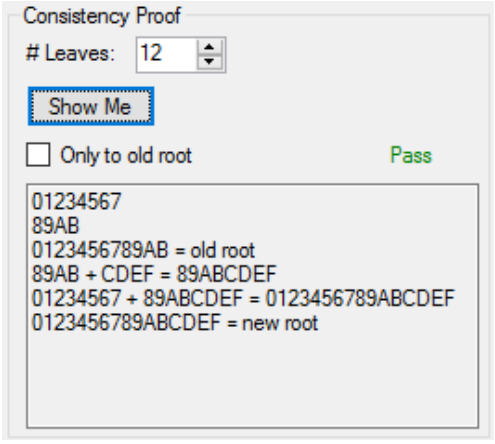
Можна вибрати до 16 листків. Хеш-лист, що імітує лист, для зручності надання представлений як 0-F

Тестування доказу аудиту

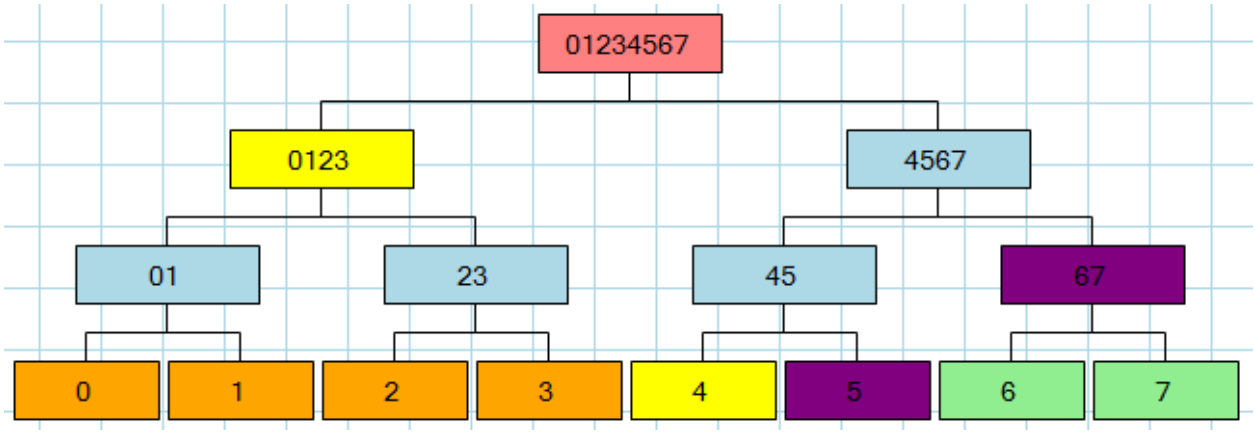


Ми можемо перевірити доказ аудиту, вибравши аркуш, який ви хочете перевірити (вибір номера аркуша - 0-15, де 10-15 представлені у вигляді АФ на графіку.) Коли ми натискаємо Показати, відображається доказ і запущена процедура перевірки. Графік також показує вам вузли, що беруть участь у проведенні перевірки аудиту (див. Численні знімки екрана вище).

Перевірка доказу узгодженості



Ми можемо перевірити стійкість консистенції, вибравши кількість листків, для яких ви хочете перевірити консистенцію. Вузли, що беруть участь у обчисленні старого кореня, позначені жовтим кольором, вузли для закінчення перевірки за допомогою перевірки перевірки - фіолетовим:



Висновок: в результаті роботи була створена програма для дослідження створення та аудиту дерева.