УКРАЇНА

(19) UA (11) 129680 (13) C2

(51) МПК (2025.01)
G06F 21/00
G06F 21/32 (2013.01)

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2021 06144**

(22) Дата подання заявки: **16.09.2019**

(24) Дата, з якої є чинними права інтелектуальної власності: **03.07.2025**

(31) Номер попередньої заявки відповідно до Паризької конвенції: **16/374,517, 19191716.0**

(32) Дата подання попередньої заявки відповідно до Паризької конвенції: **03.04.2019, 14.08.2019**

(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку: **US, EP**

(41) Публікація відомостей про заявку: **16.02.2022, Бюл.№ 7**

(46) Публікація відомостей про державну реєстрацію: **02.07.2025, Бюл.№ 27**

(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору PCT **PCT/US2019/051358, 16.09.2019**

(72) Винахідник(и):
Коен Джоел (US),
Родін Бартломей Роберт (US)

(73) Володілець (володільці):
КІЧЕЙНЕКС АҐ,
Dorfstrasse 38, 6340 Baar, Switzerland (CH)

(74) Представник:
Бочаров Максим Анатолійович, реєстр. №367

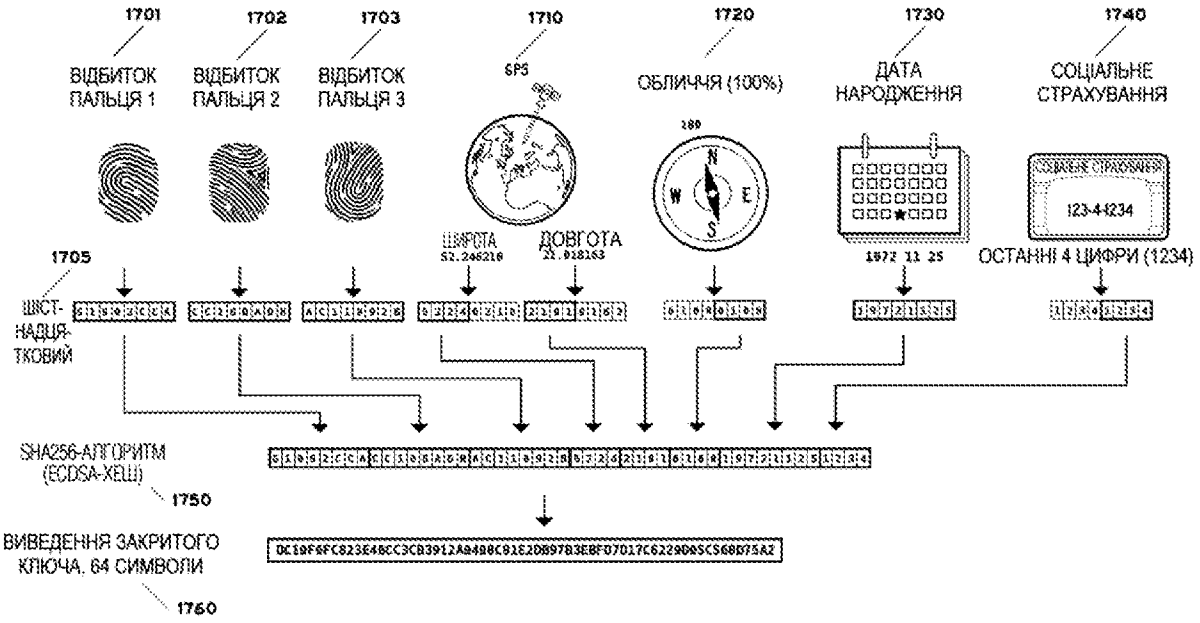
(56) Перелік документів, взятих до уваги експертизою:
US 20180268414 A1, 20.09.2018
US 2017/0085562 A1, 23.03.2017

UA 129680 C2

(54) ГЕНЕРУВАННЯ БІОМЕТРИЧНОГО ЦИФРОВОГО ПІДПИСУ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИ

(57) Реферат:

Розкриті системи, способи і пристрій для генерування біометричного цифрового підпису для верифікації особи. У деяких варіантах здійснення спосіб верифікації особи користувача містить зчитування щонайменше одним датчиком біометричної інформації від користувача. Спосіб додатково включає генерування сенсорним пристроєм біометричних даних із біометричної інформації. Крім того, спосіб включає хешування за допомогою користувацького пристрою з використанням алгоритму нечіткого хешування або алгоритму хешування (такого як алгоритм не-нечіткого хешування) щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача. Крім того, спосіб включає порівняння вузлом верифікації біометричного цифрового підпису з попереднім біометричним цифровим підписом для користувача. Крім того, спосіб включає верифікацію вузлом верифікації користувача, коли вузол верифікації визначає, що біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису користувача.


1701
ВІДБИТОК ПАЛЬЦЯ 1
1702
ВІДБИТОК ПАЛЬЦЯ 2
1703
ВІДБИТОК ПАЛЬЦЯ 3
1710
GPS
ШИРОТА
52.246216
ДОВГОТА
21.018163
1720
ОБЛИЧЧЯ (100%)
189
N
W
E
S
1730
ДАТА НАРОДЖЕННЯ
1972 11 25
1740
СОЦІАЛЬНЕ СТРАХУВАННЯ
123-4-4234
ОСТАННІ 4 ЦИФРИ (1234)
1705
ШІСТНАДЦЯТКОВИЙ
SHA256-АЛГОРИТМ (ECDSA-ХЕШ)
1750
ВИВЕДЕННЯ ЗАКРИТОГО КЛЮЧА, 64 СИМВОЛИ
1760
DC19F6FC823E48CC3CB3912A8498C81E2D897B3EBF07017C62290085C5680D75A2
1700

Фіг. 17

Перехресне посилання на споріднені заявки

Ця заявка запитує пріоритет і перевагу Європейської патентної заявки № 19191716.0, поданої 14 серпня 2019 р., і є частковим продовженням, а також запитує пріоритет і перевагу заявки на патент США № 16/374 517, поданої 3 квітня 2019 р., повне розкриття якої прямо включене в цей документ за допомогою посилання.

Галузь техніки, до якої належить винахід

Це розкриття стосується верифікації особи. Зокрема, це розкриття стосується генерування біометричного цифрового підпису для верифікації особи і верифікації розрахунків для розподілених реєстрів.

Рівень техніки

Опублікована заявка на патент США № US20160050213A1 стосується системи і способу надання профілю ідентифікації. У першому аспекті винахід забезпечує спосіб надання профілю інформації, яка стосується ідентифікації об'єкта, який включає етапи надання щонайменше одного елемента ідентифікаційної інформації органу ідентифікації, при цьому орган ідентифікації збирає біометричну інформацію від об'єкта і використовує ідентифікаційну інформацію і біометричну інформацію для формування профілю інформації, що стосується ідентифікації об'єкта. У другому аспекті винахід передбачає систему для надання профілю інформації, яка стосується ідентифікації об'єкта, що містить базу даних, призначену для надання щонайменше одного елемента ідентифікаційної інформації органу ідентифікації, при цьому орган ідентифікації збирає біометричну інформацію від об'єкта, що використовує пристрій збирання біометричної інформації, і процесор використовує ідентифікаційну інформацію і біометричну інформацію для формування профілю інформації, яка стосується ідентифікації об'єкта. Біометрична інформація може включати в себе щонайменше одне з наступного: відбиток пальця, сканування сітківки, сканування долоні і сканування обличчя.

Опублікована заявка на патент США № US20170279801 A1 стосується систем і способів забезпечення багатофакторної верифікації особи на основі ланцюжка блоків (блокчейна). Адреси для верифікації можуть бути встановлені в ланцюжку блоків шляхом: зв'язування ідентифікаторів з особами, які раніше підтвердили особисту ідентичність, призначення адрес верифікації в ланцюжку блоків окремим особам і запису ідентифікаторів і біометричних даних, пов'язаних з людьми, за відповідними адресами верифікації. Багатофакторна верифікація особи на основі ланцюжка блоків з використанням адрес верифікації може виконуватися шляхом: отримання одного або більше ідентифікаторів у зв'язку з одним або більше запитами на верифікацію особи однієї або більше осіб, витягання біометричних даних, пов'язаних з однією або більше особами, з відповідних адрес верифікації і верифікації особи однієї або більше людей після отримання співпадаючих біометричних даних і закритих ключів. Біометричні ідентифікатори звичайно включають в себе фізіологічні характеристики, але можуть також включати в себе поведінкові характеристики і/або інші характеристики. Фізіологічні характеристики можуть бути пов'язані з формою тіла людини (наприклад, один або більше відбитків пальців, вени на долоні, розпізнавання обличчя, ДНК, відбиток долоні, геометрія руки, розпізнавання райдужної оболонки ока, сітківка, аромат або запах і/або інші фізіологічні характеристики). Поведінкові характеристики можуть бути пов'язані з шаблоном поведінки людини (наприклад, одне або більше з ритму набору тексту, ходи, голосу і/або інших поведінкових характеристик). Біометричні дані можуть включати в себе одне або більше зображення або інше візуальне представлення фізіологічної характеристики, запис поведінкової характеристики, шаблон фізіологічної характеристики і/або поведінкової характеристики і/або інші біометричні дані.

Опублікована заявка на патент США № US20180309581 A1 розкриває спосіб і систему для децентралізованого біометричного підписання цифрового контракту. Створюється цифрова ідентифікація, яка включає в себе закритий ключ. Закритий (секретний) ключ був зашифрований на мобільному пристрої з використанням захоплених біометричних даних. Генерується цифровий хеш цифрового контракту. Користувач, який використовує біометричні дані, аутентифікується. Авторизується використання біометричних даних. У відповідь на використання авторизованих біометричних даних зашифрований закритий ключ розшифровується. Цифровий хеш підписується розшифрованим закритим ключем. Підписаний цифровий хеш зберігається в ланцюжку блоків.

Опублікована патентна заявка США № US20190036692 A1 описує метод генерування ключа відновлення, що реалізовується процесором, з мнемонічної пропозиції і коду персонального ідентифікаційного номера (PIN), щоб користувачі могли керувати своїми власними обліковими даними з використанням смарт-контракту в ланцюжку блоків. Спосіб включає в себе етапи генерування з використанням першого криптографічного процесора на першому пристрої,

пов'язаному з користувачем, першого набору облікових даних; генерування мнемонічної пропозиції з псевдовипадкових даних; застосування алгоритму отримання ключа для генерування ключа відновлення і умовної реєстрації ідентифікатора ключа відновлення для першого відкритого (загальнодоступного) ключа першого пристрою у смарт-контракті в ланцюжку блоків. Перший набір облікових даних включає в себе першу пару відкритого і закритого ключів, сумісну з ланцюжком блоків, пов'язану з користувачем. Перша пара відкритого і закритого ключів, сумісна з ланцюжком блоків, включає в себе перший відкритий ключ і перший закритий ключ. Перший закритий ключ обмежений першим криптографічним процесором на першому пристрої.

Розподілені реєстри, такі як ланцюжок блоків, забезпечують унікальну систему запису транзакцій. Як правило, розподілені реєстри зберігають журнал транзакцій, який може бути відтворений у розподіленій мережі. Криптографія і цифрові підписи часто використовуються для визначення дійсних сторін і транзакцій, так що всі сторони узгоджують стан реєстру в режимі реального часу без необхідності покладатися на довірену третю сторону. Однак в деяких випадках користувач може втратити свій цифровий підпис для розподіленого реєстру. Отримання іншого діючого цифрового підпису може виявитися обтяжливим і тривалим процесом.

У контексті вищевикладеного існує потреба в поліпшеній системі і способі генерування дійсного цифрового підпису для користувача.

Суть винаходу

Це розкриття стосується способу, системи і пристрою для генерування біометричного цифрового підпису для верифікації особи. У одному або більше варіантах здійснення спосіб верифікації особи користувача включає зчитування щонайменше одним датчиком біометричної інформації від користувача. Спосіб додатково включає генерування сенсорним пристроєм біометричних даних із біометричної інформації. Крім того, спосіб включає передавання сенсорним пристроєм біометричних даних користувацькому пристрою. Крім того, спосіб включає хешування користувацьким пристроєм щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача. Крім того, спосіб включає передавання користувацьким пристроєм біометричного цифрового підпису у вузол верифікації. Крім того, спосіб включає порівняння вузлом верифікації біометричного цифрового підпису з попереднім біометричним цифровим підписом користувача. Крім того, спосіб включає верифікацію вузлом верифікації користувача, коли вузол верифікації визначає, що біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису користувача.

У одному або більше варіантах здійснення спосіб додатково включає, коли користувач верифікований, генерування і передавання вузлом верифікації на користувацький пристрій сигналу підтвердження верифікації, який вказує, що користувач верифікований. Щонайменше, в одному варіанті здійснення спосіб додатково включає скасування верифікації вузлом верифікації користувача, коли вузол верифікації визначає, що біометричний цифровий підпис не ідентичний попередньому біометричному цифровому підпису користувача. У деяких варіантах здійснення спосіб додатково включає, коли користувач не верифікований, генерування і передавання вузлом верифікації на користувацький пристрій сигналу скасування верифікації, який вказує, що користувач не верифікований. У одному або більше варіантах здійснення вузол верифікації визначає, що біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису для користувача, коли вузол верифікації визначає, що біометричний цифровий підпис на сто (100) відсотків співпадає з (наприклад, ідентичний) попереднім біометричним цифровим підписом користувача.

Щонайменше, в одному варіанті здійснення, коли користувач верифікований, спосіб додатково включає надання користувачеві можливості передавати призначення блока даних від користувача бенефіціару; надання користувачеві можливості передавати право власності на майно від користувача до бенефіціара; надання користувачеві можливості отримувати медичні записи для користувача; надання користувачеві можливості голосувати від імені користувача; надання користувачеві можливості отримувати проїзні документи для користувача; і/або надання користувачеві можливості здійснювати банківські операції від імені користувача.

У одному або більше варіантах здійснення біометрична інформація містить щонайменше три відбитки пальця, щонайменше фрагмент послідовності дезоксирибонуклеїнової кислоти (ДНК), щонайменше фрагмент щонайменше однієї ознаки обличчя, ізотопну інформацію по запаху, щонайменше фрагмент ознаки ока, звукову інформацію від голосу, тривимірне (3D) сканування поверхні щонайменше фрагмента користувача і/або двовимірне (2D) сканування поверхні щонайменше фрагмента користувача.

Щонайменше, в одному варіанті здійснення користувацький пристрій використовує алгоритм хешування або алгоритм нечіткого хешування для хешування щонайменше фрагмента біометричних даних. У одному або більше варіантах здійснення користувацький пристрій використовує алгоритм цифрового підпису з еліптичною кривою (ECDSA) для хешування щонайменше фрагмента біометричних даних. У деяких варіантах здійснення користувацький пристрій використовує алгоритм SHA-256, алгоритм Меркла-Дамгарда, алгоритм MD5, алгоритм SHA-1, алгоритм SHA-2, алгоритм дайджеста-160 повідомлення оцінки примітивів цілісності RACE (RIPEMD-160), алгоритм Whirlpool або алгоритм BLAKE2 для хешування щонайменше фрагмента біометричних даних.

У одному або більше варіантах здійснення біометричний цифровий підпис генерується шляхом додаткового хешування користувацьким пристроєм додаткової ідентифікуючої інформації. У деяких варіантах здійснення додаткова ідентифікуюча інформація містить інформацію про місцерозташування, інформацію про температуру, інформацію про вологість, інформацію про дату, інформацію про час, інформацію про висоту, інформацію про відстань і/або особисту інформацію.

Щонайменше, в одному варіанті здійснення біометричний цифровий підпис є закритим ідентифікаційним ключем для користувача. У одному або більше варіантах здійснення користувацький пристрій являє собою смартфон, планшет, персональний комп'ютер, портативний комп'ютер, інтелектуальний годинник, інтелектуальне телебачення (телевізор), автомобіль або обчислювальний пристрій. У деяких варіантах здійснення користувацький пристрій містить щонайменше один датчик, сенсорний пристрій і/або вузол верифікації.

У одному або більше варіантах здійснення спосіб верифікації особи щонайменше одного користувача включає зчитування щонайменше одним датчиком біометричної інформації від користувача. Спосіб додатково включає генерування сенсорним пристроєм біометричних даних з біометричної інформації. Крім того, спосіб включає передавання сенсорним пристроєм біометричних даних користувацькому пристрою. Крім того, спосіб включає хешування користувацьким пристроєм щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача. Крім того, спосіб включає збереження користувацьким пристроєм щонайменше фрагмента біометричного цифрового підпису користувача в розміщувальному біометричному цифровому підписі, що зберігається кожною щонайменше з n (наприклад, шести (6)) людей, щоб генерувати розміщувальний біометричний цифровий підпис для кожної з n осіб, так що комбінація розміщувальних біометричних цифрових підписів щонайменше для числа m (наприклад, чотирьох (4)) з n людей містить всі дані біометричного цифрового підпису для користувача, де число m більше половини числа n. Крім того, спосіб включає генерування користувацьким пристроєм відновленого біометричного цифрового підпису для користувача з використанням розміщувальних біометричних цифрових підписів щонайменше для числа m з n людей. Крім того, спосіб включає передавання користувацьким пристроєм відновленого біометричного цифрового підпису у вузол верифікації. Крім того, спосіб включає порівняння вузлом верифікації відновленого біометричного цифрового підпису з попереднім біометричним цифровим підписом користувача. Крім того, спосіб включає верифікацію вузлом верифікації користувача, коли вузол верифікації визначає, що відновлений біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису користувача.

Щонайменше, в одному варіанті здійснення система для верифікації особи користувача містить щонайменше один датчик для зчитування біометричної інформації від користувача. Система додатково містить сенсорний пристрій для генерування біометричних даних із біометричної інформації і для передавання біометричних даних на користувацький пристрій. Крім того, система містить користувацький пристрій для хешування щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача і для передавання біометричного цифрового підпису у вузол верифікації. Крім того, система містить вузол верифікації для порівняння біометричного цифрового підпису з попереднім біометричним цифровим підписом користувача і для верифікації користувача, коли вузол верифікації визначає, що біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису для користувача.

У одному або більше варіантах здійснення, коли користувач верифікований, вузол верифікації додатково генерує і передає на користувацький пристрій сигнал підтвердження верифікації, який вказує, що користувач верифікований. Щонайменше, в одному варіанті здійснення вузол верифікації не верифікує користувача, коли вузол верифікації визначає, що біометричний цифровий підпис не ідентичний попередньому біометричному цифровому підпису для користувача. У деяких варіантах здійснення, коли користувач не верифікований, вузол

верифікації додатково генерує і передає на користувацький пристрій сигнал скасування верифікації, який вказує, що користувач не верифікований. У одному або більше варіантах здійснення користувацький пристрій містить щонайменше один датчик і сенсорний пристрій.

Щонайменше, в одному варіанті здійснення користувацький пристрій повинен використовувати алгоритм хешування або алгоритм нечіткого хешування для хешування щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача. У одному або більше варіантах здійснення користувацький пристрій повинен використовувати алгоритм цифрового підпису з еліптичною кривою (ECDSA) для хешування щонайменше фрагмента біометричних даних. У деяких варіантах здійснення користувацький пристрій використовує алгоритм SHA-256, алгоритм Меркла-Дамгарда, алгоритм MD5, алгоритм SHA-1, алгоритм SHA-2, алгоритм дайджеста-160 повідомлення оцінки примітивів цілісності RACE (RIPEMD-160), алгоритм Whirlpool або алгоритм BLAKE2 для хешування щонайменше фрагмента біометричних даних.

Ознаки, функції і переваги можуть бути досягнуті незалежно в різних варіантах здійснення цього розкриття або можуть бути об'єднані ще в інших варіантах здійснення.

Короткий опис креслень

Ці й інші особливості, аспекти і переваги цього розкриття стануть більш зрозумілими з урахуванням наступного опису, прикладеної формули винаходу і супровідних креслень, на яких:

Фіг. 1A - схема, яка показує розкриту систему генерування біометричного цифрового підпису для верифікації особи користувача згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 1B - це блок-схема послідовності операцій, яка показує розкритий спосіб генерування біометричного цифрового підпису для верифікації особи користувача згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 2 - схема, яка ілюструє процес хешування біометричних даних, отриманих із відбитків пальців користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 3 - схема, яка ілюструє процес хешування біометричних даних, отриманих із крові користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 4 - схема, яка ілюструє процес хешування біометричних даних, отриманих при скануванні обличчя користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 5 - схема, яка ілюструє процес хешування біометричних даних, отриманих із запаху користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 6 - схема, яка ілюструє процес хешування біометричних даних, отриманих внаслідок сканування очей користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 7 - схема, яка ілюструє процес хешування біометричних даних, отриманих із голосу користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 8 - схема, яка ілюструє процес використання біометричних цифрових підписів для передавання власності між ініціатором (наприклад, користувачем) і бенефіціаром, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 9 - схема, яка ілюструє процес верифікації користувача шляхом перевірки достовірності біометричного цифрового підпису для користувача, щоб виконати транзакцію, яка потребується користувачем, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 10 - схема, яка ілюструє процес хешування даних місцерозташування для користувача разом із біометричними даними, отриманими від користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 11 - схема, яка ілюструє процес верифікації користувача шляхом перевірки достовірності підпису супутника (наприклад, супутника глобальної системи позиціонування (GPS)), що містить дані про місцерозташування, для користувача, показаного на фіг. 11, для виконання транзакції, яка потребується користувачем, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 12 - схема, яка ілюструє процес збереження фрагмента біометричного цифрового підпису для користувача в розміщувальних біометричних цифрових підписах, які зберігаються у інших людей, для генерування розміщувальних біометричних цифрових підписів для кожної з

інших людей, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 13 - схема, яка ілюструє процес використання розміщувальних біометричних цифрових підписів від людей, зображених на фіг. 12, для генерування відновленого біометричного цифрового підпису для користувача згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 14 - схема, яка ілюструє процес верифікації користувача шляхом перевірки достовірності відновленого біометричного цифрового підпису для користувача, показаного на фіг. 13, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 15 - схема, яка ілюструє різні типи транзакцій, які можуть відбуватися після верифікації користувача шляхом перевірки достовірності біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 16 - схема, яка ілюструє різні типи додаткової ідентифікуючої інформації, яка може бути хешована разом з біометричними даними, отриманими від користувача, для генерування біометричного цифрового підпису для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Фіг. 17 - схема, яка ілюструє процес генерування біометричного цифрового підпису для користувача шляхом хешування біометричних даних від користувача разом з додатковою ідентифікуючою інформацією і особистою інформацією для користувача, згідно щонайменше з одним варіантом здійснення цього розкриття.

Здійснення винаходу

Розкриті тут способи і пристрій забезпечують оперативну систему генерування біометричного цифрового підпису для верифікації особи. У одному або більше варіантах здійснення система забезпечує генерування біометричного цифрового підпису, верифікацію особи і верифікацію розрахунків для розподілених реєстрів. Зокрема, система за цим розкриттям генерує біометричний цифровий підпис для користувача шляхом хешування за допомогою алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування (наприклад, алгоритму не-нечіткого хешування)) біометричних даних від користувача, де біометричний цифровий підпис може використовуватися для верифікації особи користувача, яка може використовуватися для верифікації розрахунків у розподілених реєстрах. Потрібно зазначити, що криптографічна хеш-функція має певні властивості, які роблять її придатною для використання в криптографії. Алгоритм хешування (наприклад, алгоритм не-нечіткого хешування) перетворює дані довільного розміру в бітовий рядок фіксованого розміру (наприклад, хеш-код). І навпаки: алгоритм нечіткого хешування перетворює дані довільного розміру в бітовий рядок нефіксованого розміру (наприклад, хеш-код).

Система цього розкриття вирішує проблему генерування цифрового підпису, коли джерело (наприклад, користувач) може створювати і захищати свій цифровий підпис, що походить із його власних біометричних даних. У одному або більше варіантах здійснення система, згідно з цим розкриттям, застосовує використання алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування (такого як алгоритм не-нечіткого хешування)) для генерування цифрового підпису з біометричних даних. При використанні алгоритму нечіткого хешування (на противагу алгоритму хешування (наприклад, алгоритму не-нечіткого хешування)) отримані біометричні дані з джерела не обов'язково повинні мати точність у сто (100) відсотків, оскільки нечіткий хеш створює цифровий підпис, що не вимагає 100-відсоткової точності біометричних даних.

Генерування цифрового підпису з нечітким хешем підвищує конфіденційність і безпеку, коли потрібно декілька транзакцій з біометричного джерела в публічному реєстрі, дозволяючи генерувати нові цифрові підписи і порівнювати їх з вихідним цифровим підписом, який зберігається в розподілених реєстрах.

У наші дні втрата закритих ключів - дуже поширена проблема. Закриті ключі зламуються з комп'ютерів і смартфонів. Стандартний спосіб згенерувати закритий ключ - використати випадковий генератор для генерування закритого ключа або використати фразу SEED (мнемоніка). SEED містить основну адресу з відповідним закритим ключем, і всі дочірні адреси будуть згенеровані з цього SEED. Якщо людина втратить телефон або комп'ютер, він/вона може згенерувати адреси з допомогою SEED, використовуючи інший інтелектуальний пристрій або комп'ютер. На жаль, якщо хакер або зловмисник отримає доступ до SEED, цей користувач також може повторно згенерувати закриті ключі.

Система і спосіб, згідно з цим розкриттям, створюють рівень безпеки шляхом генерування закритих ключів "у польоті" (без зусиль), наприклад, шляхом доступу до геометричних даних і даних геолокації користувача. Це дозволяє згенерувати ключ, який не зберігається на жодних пристроях, але генерується, серед іншого, тілом користувача і геологічними переміщеннями. Рішення не тільки захищає користувача від крадіжки, а також може використовуватися для

аутентифікації для різних служб, яким необхідно призначити обліковий запис або службу конкретній людині.

Рішення з геолокацією створює безпечне середовище, а це означає, що хтось, не присутній в геолокації, наприклад, людина в Північній Кореї, не зможе згенерувати закритий ключ користувача, що проживає, наприклад, в США, де він повинен знаходитися у себе вдома, щоб згенерувати свій закритий ключ і підписати транзакцію (яка підписана його закритим ключем). Зловмисник повинен знаходитися в цьому місці, щоб імітувати генерування закритого ключа, включаючи володіння зразком біометричних даних власника, наприклад, трьома відбитками пальців або скануванням обличчя.

У нижченаведеному описі викладені численні деталі, щоб надати більш повний опис системи. Однак фахівцеві в цій галузі техніки буде очевидно, що розкрита система може застосовуватися на практиці без цих конкретних деталей. У інших випадках добре відомі особливості не були описані детально, щоб зайвий раз не ускладнювати розуміння системи.

Варіанти здійснення цього розкриття можуть бути описані тут в термінах функціональних і/або логічних компонентів і різних етапів обробки. Потрібно розуміти, що такі компоненти можуть бути реалізовані за допомогою будь-якої кількості компонентів апаратного, програмного забезпечення і/або мікропрограмного забезпечення, сконфігурованих для виконання вказаних функцій. Наприклад, варіант здійснення цього розкриття може використовувати різні компоненти інтегральної схеми (наприклад, елементи пам'яті, елементи обробки цифрових сигналів, логічні елементи, довідкові таблиці і т. п.), які можуть виконувати різні функції відповідно до керування одного або більше процесорами, мікропроцесорами або іншими пристроями керування. Крім того, фахівці в цій галузі техніки зрозуміють, що варіанти здійснення цього розкриття можуть бути реалізовані на практиці в поєднанні з іншими компонентами, і що описані тут системи є просто зразковими варіантами здійснення цього розкриття.

Скорочено традиційні технології і компоненти, що стосуються верифікації особи, й інші функціональні аспекти системи (і окремі робочі компоненти систем) не можуть бути описані тут детально. Крім того, з'єднувальні лінії, показані на різних кресленнях, що містяться в цьому документі, призначені, щоб представляти зразкові функціональні зв'язки і/або фізичні з'єднання між різними елементами. Потрібно зазначити, що багато альтернативних або додаткових функціональних взаємозв'язків або фізичних з'єднань можуть бути присутніми в одному або більше варіантах здійснення цього розкриття.

Фіг. 1А - схема, яка показує розкриту систему 100 генерування біометричного цифрового підпису для верифікації особи користувача 105 згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні датчики 110a-110n показані підключеними з можливістю передавання даних (через провід і/або по бездротовому зв'язку) до сенсорного пристрою 120. Сенсорний пристрій 120 містить процесор(и) 123, інтерфейс 122 зв'язку і пам'ять 121. Потрібно зазначити, що в інших варіантах здійснення сенсорний пристрій 120 може містити більшу або меншу кількість компонентів, ніж показано на фіг. 1А. В одному або більше варіантах здійснення датчики 110a-110n можуть містити різні типи датчиків, включаючи, крім іншого, пристрої сканування зображень, пристрої виявлення хімічних речовин, датчики температури, датчики вологості, датчики висоти, датчики напряму і/або приймачі сигналів системи глобального позиціонування (GPS). Крім того, в деяких варіантах здійснення може бути більша або менша кількість датчиків 110a-110n, ніж показано на фіг. 1А.

Крім того, на фіг. 1А показано, що користувацький пристрій 130 містить процесор(и) 133, інтерфейс 132 зв'язку і пам'ять 131. Аналогічно сенсорному пристрою 120, в інших варіантах здійснення користувацький пристрій 130 може містити більшу або меншу кількість компонентів, ніж показано на фіг. 1А. Сенсорний пристрій 120 зв'язаний з можливістю передавання даних (через провід (наприклад, універсальну послідовну шину (USB)) і/або бездротовим способом) з користувацьким пристроєм 130. У одному або більше варіантах здійснення користувацький пристрій 130 являє собою обчислювальний пристрій, асоційований з користувачем 105. Різні типи обчислювальних пристроїв можуть використовуватися для користувацького пристрою 130 розкритої системи 100, зокрема, крім іншого, смартфон, планшет, персональний комп'ютер, портативний комп'ютер, інтелектуальний годинник, інтелектуальне телебачення (телевізор), автомобіль або обчислювальний пристрій (наприклад, будь-який обчислювальний пристрій, на якому може працювати операційна система, наприклад Android, OSX, Windows, Unix або майбутні операційні системи).

Користувацький пристрій 130 підключений з можливістю передавання даних (через провід і/або бездротовим способом), наприклад, через Інтернет 145 (і/або іншу загальнодоступну і/або приватну мережу(і) і/або інтрамережу(і)) до вузла (наприклад, вузла верифікації) 140. Вузол 140

складається з процесора(ів) 143 і бази 144 даних. У інших варіантах здійснення вузол 140 може містити більшу або меншу кількість компонентів, ніж показано на фіг. 1А. В одному або більше варіантах здійснення вузол 140 являє собою обчислювальний пристрій, такий як сервер. Потрібно зазначити, що в одному або більше варіантах здійснення для вузла 140 можуть використовуватися різні типи обчислювальних пристроїв. У деяких варіантах здійснення користувацький пристрій 130 може містити щонайменше одне з датчиків 110a-110n, сенсорного пристрою 120 і/або вузла (наприклад, вузла верифікації) 140.

Під час роботи розкритої системи 100 щонайменше один датчик 110a-110n зчитує біометричну інформацію від користувача 105. Різні типи біометричної інформації можуть бути отримані від користувача 105, зокрема, крім іншого, інформація про відбитки пальців, інформація зі зразка крові (наприклад, послідовність дезоксирибонуклеїнової кислоти (ДНК)), інформація про риси обличчя, інформація про ізотопи із запаху, інформація про характеристики ока, звукова інформація з голосу, тривимірне (3D) сканування поверхні щонайменше фрагмента користувача 105 і/або двовимірне (2D) сканування поверхні щонайменше фрагмента користувача 105.

Після того, як щонайменше один датчик 110a-110n зчитав біометричну інформацію від користувача 105, щонайменше один датчик 110a-110n передає (дротовим і/або бездротовим способом) біометричну інформацію на сенсорний пристрій 120. Після того, як сенсорний пристрій 120 приймає біометричну інформацію користувача 105, щонайменше один процесор 123 перетворює біометричну інформацію (наприклад, у форматі аналогових даних) в біометричні дані (наприклад, у форматі цифрових даних, такому як двійкове число і/або шістнадцяткове число). У одному або більше варіантах здійснення сенсорний пристрій 120 може зберігати біометричні дані в пам'яті 121. Після того, як сенсорний пристрій 120 перетворив біометричну інформацію в біометричні дані, інтерфейс 122 зв'язку (наприклад, який може містити передавач і/або приймач) сенсорного пристрою 120 передає (дротовим і/або бездротовим способом) (наприклад, через USB) біометричні дані користувача 105 на користувацький пристрій 130.

Після того, як інтерфейс 133 зв'язку (наприклад, який може містити передавач і/або приймач) користувацького пристрою 130 приймає біометричні дані для користувача 105, щонайменше один процесор 133 користувацького пристрою 130 використовує алгоритм нечіткого хешування (або альтернативно алгоритм хешування) для хешування щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача 105. У одному або більше варіантах здійснення користувацький пристрій 130 використовує алгоритм цифрового підпису з еліптичною кривою (ECDSA) для хешування щонайменше фрагмента біометричних даних для генерування біометричного цифрового підпису для користувача 105. Потрібно зазначити, що різноманітні алгоритми різних типів (наприклад, алгоритми хешування і алгоритми нечіткого хешування) можуть використовуватися користувацьким пристроєм 130 розкритої системи 100 для хешування, зокрема, крім іншого, алгоритм SHA-256, алгоритм Меркла-Дамгарда, алгоритм MD5, алгоритм SHA-1, алгоритм SHA-2, алгоритм дайджеста-160 повідомлення оцінки примітивів цілісності RACE (RIPEMD-160), алгоритм Whirlpool і алгоритм BLAKE2.

Крім того, потрібно зазначити, що в одному або більше варіантах здійснення, крім біометричних даних від користувача щонайменше фрагмент додаткової ідентифікуючої інформації для користувача 105 може бути хешований (разом зі щонайменше фрагментом біометричних даних), щонайменше одним процесором 133, що використовує алгоритм нечіткого хешування або алгоритм хешування для генерування біометричного цифрового підпису для користувача 105. Можуть використовуватися різноманітні різні типи додаткової ідентифікуючої інформації для користувача 105, включаючи, крім іншого, інформацію про місцерозташування, інформацію про температуру, інформацію про вологість, інформацію про дату, інформацію про час, інформацію про висоту, інформацію про відстань і/або особисту інформацію (наприклад, дату народження і/або щонайменше фрагмент номера соціального страхування).

У одному або більше варіантах здійснення біометричний цифровий підпис користувача 105 може використовуватися як закритий ідентифікаційний ключ користувача 105. Користувач 105 може використовувати цей закритий ідентифікаційний ключ, щоб мати можливість провести транзакції, отримувати доступ до даних і/або брати участь в діях. Щонайменше, в одному варіанті здійснення користувацький пристрій 130 зберігає біометричний цифровий підпис в пам'яті 131.

У одному або більше варіантах здійснення, коли користувач 105 бажає провести транзакцію (наприклад, здійснити банківську транзакцію, передати призначення блока даних ланцюжка блоків від користувача 105 бенефіціару і/або дозволити користувачеві 105 передати право

власності від користувача 105 до бенефіціара), отримати доступ до даних (наприклад, отримати медичні записи для користувача 105 і/або отримати проїзні документи для користувача) і/або брати участь в діяльності (наприклад, голосувати від імені користувача 105), користувач 105 може бути верифікований шляхом підтвердження його біометричного цифрового підпису. Для верифікації користувача 105 з використанням цього процесу інтерфейс 132 зв'язку користувацького пристрою 130 спочатку передає (дротовим і/або бездротовим способом), наприклад, через Інтернет 145 (і/або іншу загальнодоступну і/або приватну мережу(і)) і/або інтрамережу(і)), біометричний цифровий підпис користувача 105 вузлу (наприклад, вузлу верифікації) 140. Щонайменше, один процесор 143 вузла 140 верифікації порівнює біометричний цифровий підпис користувача 105 з попереднім біометричним цифровим підписом користувача 105. Попередній біометричний цифровий підпис користувача 105 являє собою біометричний цифровий підпис, який був раніше згенерований і підтверджений для користувача 105 в минулому.

У одному або більше варіантах здійснення база 144 даних містить щонайменше одну базу даних. У одному або більше варіантах здійснення щонайменше одна з баз даних бази 144 даних вузла 140 містить попередній біометричний цифровий підпис для користувача 105. Щонайменше, в одному варіанті здійснення щонайменше одна з баз даних бази 144 даних містить біометричні цифрові підписи для множини різних користувачів (включаючи користувача 105). Щонайменше, в одному варіанті здійснення щонайменше одна з баз даних бази 144 даних являє собою розподілений реєстр (наприклад, який містить ланцюжок блоків).

Після того, як щонайменше один процесор 143 порівняв біометричний цифровий підпис для користувача 105 з попереднім біометричним цифровим підписом для користувача 105, якщо щонайменше один процесор 143 визначить, що біометричний цифровий підпис для користувача 105 ідентичний попередньому біометричному цифровому підпису користувача 105, щонайменше один процесор 143 потім підтверджує біометричний цифровий підпис, який верифікує користувача 105. У одному або більше варіантах здійснення щонайменше один процесор 143 визначає, що біометричний цифровий підпис для користувача 105 ідентичний попередньому біометричному цифровому підпису для користувача 105, коли щонайменше один процесор 143 визначає, що біометричний цифровий підпис для користувача 105 на сто (100) відсотків співпадає (наприклад, ідентичний) попередньому біометричному цифровому підпису користувача 105.

Після того, як щонайменше один процесор 143 визначає, що біометричний цифровий підпис користувача 105 ідентичний попередньому біометричному цифровому підпису користувача 105, щонайменше один процесор 143 генерує сигнал 141 підтвердження верифікації, який вказує, що біометричний цифровий підпис був підтверджений. Потім вузол 140 передає (дротовим і/або бездротовим способом), наприклад, через Інтернет 145, сигнал 141 підтвердження верифікації на інтерфейс 132 зв'язку користувацького пристрою 130, щоб повідомити користувача 105 про те, що біометричний цифровий підпис був підтверджений і, таким чином, користувач 105 був верифікований. Після того, як користувач 105 був верифікований, користувач 105 може провести транзакцію (наприклад, передати призначення блока в ланцюжку блоків), отримати доступ до даних і/або брати участь у діяльності.

Однак, якщо щонайменше один процесор 143 визначає, що біометричний цифровий підпис користувача 105 не ідентичний попередньому біометричному цифровому підпису користувача 105, щонайменше один процесор 143 генерує сигнал 142 скасування верифікації, який вказує, що біометричний цифровий підпис не був підтверджений. Потім вузол 140 передає (дротовим і/або бездротовим способом), наприклад, через Інтернет 145, сигнал 142 скасування верифікації на інтерфейс 132 зв'язку користувацького пристрою 130, щоб повідомити користувача 105 про те, що біометричний цифровий підпис не був підтверджений і, таким чином, користувач 105 не був верифікований. Оскільки користувач 105 не був верифікований, користувач 105 не може провести транзакцію, отримувати доступ до даних і/або брати участь у діяльності. Як вже згадувалося вище, потрібно зазначити, що в деяких варіантах здійснення користувацький пристрій 130 містить вузол 140.

Фіг. 1B - це блок-схема послідовності операцій, яка показує розкритий спосіб 150 генерування біометричного цифрового підпису для верифікації особи користувача згідно щонайменше з одним варіантом здійснення цього розкриття. На початку 155 способу 150 щонайменше один датчик зчитує біометричну інформацію від користувача 160. Потім сенсорний пристрій генерує біометричні дані з біометричної інформації 165. Потім сенсорний пристрій передає біометричні дані на користувацький пристрій 170. Потім користувацький пристрій 170 хешує щонайменше фрагмент біометричних даних, щоб згенерувати біометричний цифровий підпис для користувача 175. Потім користувацький пристрій передає біометричний цифровий

підпис на вузол 180 верифікації. Потім вузол верифікації порівнює біометричний цифровий підпис із попереднім біометричним цифровим підписом користувача 185. Потім вузол верифікації верифікує користувача, коли вузол верифікації визначає, що біометричний цифровий підпис ідентичний попередньому біометричному цифровому підпису для користувача 190. Потім спосіб 150 завершується 195.

Фіг. 2 - схема, яка ілюструє процес 200 хешування біометричних даних 240, отриманих із відбитків 220 пальців користувача 105, для генерування біометричного цифрового підпису 250 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні зразок 210 відбитка пальця, що містить зображення відбитків 220 пальців (наприклад щонайменше трьох відбитків пальців) (наприклад, біометричну інформацію), спочатку виходить (наприклад, зчитується і/або відображається) з пальців користувача 105. Зображення відбитків 220 пальців (наприклад, біометрична інформація, наприклад, у форматі аналогових даних) перетворюються в біометричні дані (наприклад, цифрові дані, такі як двійкове число 230 і/або шістнадцяткове число 240). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 230 або шістнадцяткове число 240) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 250 для користувача 105.

Фіг. 3 - схема, яка ілюструє процес 300 хешування біометричних даних 340, отриманих із крові 311 користувача 105, для генерування біометричного цифрового підпису 350 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні зразок 310 крові спочатку виходить шляхом витягання крові 311 із пальця користувача 105. Щонайменше, один хімічний детекторний пристрій (наприклад, датчик) визначає щонайменше фрагмент послідовності 320 ДНК (наприклад, біометричну інформацію, наприклад, що містить нуклеотиди) крові 311. Послідовність 320 ДНК (наприклад, біометрична інформація, наприклад, що містить нуклеотиди) перетворюється в біометричні дані (наприклад, цифрові дані, такі як двійкове число 330 і/або шістнадцяткове число 340). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 330 або шістнадцяткове число 340) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 350 для користувача 105.

Фіг. 4 - схема, яка ілюструє процес 400 хешування біометричних даних 340, отриманих зі сканування 410 обличчя користувача 105, для генерування біометричного цифрового підпису 350 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні сканування 413 обличчя (наприклад, зображення, створене з тривимірного об'єкта на основі біометричних даних 410) (наприклад, біометрична інформація) спочатку виходить (наприклад, зчитується і/або відображається) шляхом сканування за допомогою сканера 412 зображень щонайменше фрагмента обличчя 411 користувача 105. Сканування 413 обличчя (наприклад, біометрична інформація) перетворюється в біометричні дані (наприклад, цифрові дані, такі як двійкове число 420 і/або шістнадцяткове число 430). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 420 або шістнадцяткове число 430) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 440 для користувача 105.

Фіг. 5 - схема, яка ілюструє процес 500 хешування біометричних даних 530, отриманих із запаху 511 користувача 105, для генерування біометричного цифрового підпису 540 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні зразок 511 аромату (наприклад, запаху, феромону) спочатку зчитується від користувача 105. Щонайменше, один хімічний детекторний пристрій (наприклад, датчик) визначає хімічний склад (наприклад, біометричну інформацію, наприклад, що містить ізотопні дані 510) 512 зразка 511 аромату. Хімічний склад (наприклад, біометрична інформація, наприклад, що містить ізотопні дані 510) 512 перетворюється в біометричні дані (наприклад, цифрові дані, такі як двійкове число 520 і/або шістнадцяткове число 530). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 520 або шістнадцяткове число 530) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 540 для користувача 105.

Фіг. 6 - схема, яка ілюструє процес 600 хешування біометричних даних 630, отриманих зі сканування 610 ока (наприклад, сканування райдужної оболонки ока і/або сканування сітківки) користувача 105 для генерування біометричного цифрового підпису 640 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні око 611 користувача 105 сканується за допомогою сканера (наприклад, тепловізора, датчика) для отримання сканування 610 райдужної оболонки (наприклад, біометричної інформації), щонайменше фрагмента райдужної оболонки 612 користувача 105. Сканування 610 райдужної

оболонки ока (наприклад, біометрична інформація) перетворюється в біометричні дані (наприклад, цифрові дані, такі як двійкове число 620 і/або шістнадцяткове число 630). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 620 або шістнадцяткове число 630) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 640 для користувача 105.

Фіг. 7 - схема, яка ілюструє процес 700 хешування біометричних даних 730, отриманих з голосу 711 користувача 105, для генерування біометричного цифрового підпису 740 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні зразок 710 голосу виходить шляхом зчитування голосу 711 від користувача 105. Щонайменше, один пристрій приймача звуку (наприклад, датчик, мікрофон) зчитує (наприклад, записує) голос 711 (наприклад, біометричну інформацію, наприклад, що містить звукову інформацію 712) від користувача 105. Біометрична інформація (наприклад, що містить звукову інформацію 712) голосу 711 перетворюється в біометричні дані (наприклад, цифрові дані, такі як двійкове число 720 і/або шістнадцяткове число 730). Щонайменше, фрагмент біометричних даних (наприклад, двійкове число 720 або шістнадцяткове число 730) хешується з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 740 для користувача 105.

Фіг. 8 - схема, яка ілюструє процес 800 використання біометричних цифрових підписів 831, 833 для передавання власності 832 між ініціатором (наприклад, користувачем) і бенефіціаром, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні користувач (наприклад, ініціатор) 105 бажає передати блок 832 даних, який призначений користувачеві (наприклад, ініціатору) 105, в розподіленому реєстрі 842 ланцюжка блоків бенефіціару. Біометричний цифровий підпис 831 спочатку генерується 810 для користувача 105 (наприклад, ініціатора). Для генерування біометричного цифрового підпису 831 біометрична інформація (наприклад, тривимірне (3D) сканування тіла) 811 виходить від користувача (наприклад, ініціатора) 105. Електронний пристрій (наприклад, користувацький пристрій) 130, асоційований з користувачем (наприклад, ініціатором) 105, хешує, використовуючи алгоритм нечіткого хешування (або альтернативно алгоритм хешування), біометричні дані з біометричної інформації 811 для генерування біометричного цифрового підпису 831 для користувача (наприклад, ініціатора) 105. Крім того, біометричний цифровий підпис 833 для бенефіціара генерується і надається електронним пристроєм (наприклад, користувацьким пристроєм) 841, асоційованим з одержувачем.

Після того, як біометричний цифровий підпис 831 підтверджений і користувач (наприклад, ініціатор) 105 верифікований (див. фіг. 9 для цього процесу), блок 832 даних передається в ланцюжок блоків 842 від користувача (наприклад, ініціатора) 105 бенефіціару, і транзакція в розподіленому реєстрі підтверджується 840. Для передавання блока 832 даних біометричний цифровий підпис 831 для користувача (наприклад, ініціатора) 105 більше не буде призначатися блоку 832 даних, і замість цього біометричний цифровий підпис 833 для бенефіціара буде призначений цьому блоку 832 даних.

Фіг. 9 - це схема, яка ілюструє процес 900 верифікації користувача (наприклад, ініціатора) 105 шляхом перевірки достовірності біометричного цифрового підпису 920 для користувача 105, щоб виконати транзакцію, яка потребується користувачем 105, згідно щонайменше з одним варіантом здійснення цього розкриття. Під час процесу 930 верифікації згенерований біометричний цифровий підпис 920 для користувача (наприклад, ініціатора) 105 порівнюється 932 з попереднім біометричним цифровим підписом 931 для користувача (наприклад, ініціатора) 105. Якщо згенерований біометричний цифровий підпис 920 для користувача (наприклад, ініціатора) 105 ідентичний попередньому біометричному цифровому підпису 931 для користувача (наприклад, ініціатора) 105, згенерований біометричний цифровий підпис 920 підтверджується 934, і розподілений реєстр оновлюється 950 шляхом передавання блока 951 даних ланцюжка 953 блоків від користувача (наприклад, ініціатора) 105 бенефіціару. Для передавання блока 951 даних біометричний цифровий підпис 920 для користувача (наприклад, ініціатора) 105 більше не буде призначатися блоку 951 даних, і замість цього біометричний цифровий підпис 940 для бенефіціара буде призначений цьому блоку 951 даних.

Однак, якщо виявляється, що згенерований біометричний цифровий підпис 920 для користувача (наприклад, ініціатора) 105 не ідентичний попередньому біометричному цифровому підпису 931 для користувача (наприклад, ініціатора) 105, згенерований біометричний цифровий підпис 920 буде скасований 933, і користувач 105 не зможе провести транзакцію.

Фіг. 10 - це схема, яка ілюструє процес 1000 хешування даних 1051 місцерозташування

(наприклад, широти, довготи) для користувача 105 разом з біометричними даними 1052, отриманими від користувача 105, для генерування біометричного цифрового підпису 1050 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні користувацький пристрій 130 користувача 105 отримує інформацію про місцерозташування (наприклад, широту і довготу) для користувача 105, наприклад, через виявлення 1020 сигналу системи глобального позиціонування (GPS), приймаючи сигнал 1023 GPS, що виходить від GPS-супутника 1021 на Землю 1022. Інформація про місцерозташування (наприклад, широта і довгота) перетворюється в двійкове число 1030 (наприклад, дані GPS кодуються в двійкові дані 1030) і/або шістнадцяткове число 1040 (наприклад, дані GPS мають шістнадцятковий формат 1040). Потрібно зазначити, що в інших варіантах здійснення користувацький пристрій 130 може отримувати інформацію про місцерозташування (наприклад, широту і довготу) для користувача 105, використовуючи різні системи позиціонування, відмінні від GPS, зокрема, крім іншого, глобальну навігаційну супутникову систему (ГЛОНАСС), Galileo, Compass (BeiDou) або супутникову систему Quazi-Zenith (QZSS).

Дані GPS (наприклад, які містять двійкове число 1030 і/або шістнадцяткове число 1040) хешуються з використанням алгоритму хешування або, альтернативно, алгоритму нечіткого хешування для генерування підпису 1051 GPS для користувача 105. Крім того, біометричні дані користувача 105 хешуються з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 1052 для користувача 105. Підпис 1051 GPS і біометричний цифровий підпис 1052 разом утворюють повний біометричний цифровий підпис (наприклад, безпечний біометричний цифровий підпис GPS) 1050 для користувача 105.

Фіг. 11 являє собою схему, яка ілюструє процес 1100 верифікації користувача 105 шляхом перевірки достовірності підпису супутника (наприклад, супутника GPS), яка містить дані про місцерозташування (наприклад, широту і довготу), для користувача 105 на фіг. 11, щоб виконувати транзакцію, що потребується користувачем 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні користувач 105 бажає передати призначення блока даних (наприклад, даних 1110 із захищеним доступом, таких як блок даних у ланцюжку блоків 1112) бенефіціару. Щоб завершити цю транзакцію, користувач 105 повинен бути верифікований. Для цього варіанта здійснення користувач 105 верифікується шляхом перевірки достовірності біометричного цифрового підпису користувача 105 і перевірки достовірності місцерозташування користувача 105. У варіанті здійснення, показаному на цьому кресленні, біометричний цифровий підпис користувача 105 вже підтверджений.

Щоб підтвердити місцерозташування користувача 105, користувацький пристрій 1111 користувача 105 отримує інформацію про місцерозташування (наприклад, широту і довготу) для користувача 105, наприклад, через систему глобального позиціонування (GPS), приймаючи сигнал GPS 1123, що випромінюється від супутника GPS 1121 на Землю 1122 (наприклад, визначаючи місцерозташування за сигналом 1120 GPS). Інформація про місцерозташування (наприклад, широта і довгота) перетворюється в двійкове число (наприклад, дані GPS кодуються в двійкові дані) і/або шістнадцяткове число (наприклад, дані GPS є шістнадцятковими). Дані GPS (наприклад, що містять двійкове число і/або шістнадцяткове число) хешуються з використанням алгоритму хешування (або, альтернативно, алгоритму нечіткого хешування) для генерування підпису 1131 GPS для користувача 105.

Під час процесу 1130 верифікації згенерований підпис 1131 GPS для користувача (наприклад, ініціатора) 105 порівнюється 1132 з попереднім підписом 1051 GPS (див. фіг. 10) для користувача (наприклад, ініціатора) 105. Якщо згенерований підпис 1131 GPS для користувача (наприклад, ініціатора) 105 виявляється ідентичним попередньому підпису 1051 GPS для користувача (наприклад, ініціатора) 105, згенерований підпис 1131 GPS підтверджується 1134, і транзакція ініціюється (наприклад, підтвердження 1140 ланцюжка блоків) оновленням розподіленого реєстру шляхом передавання блока даних ланцюжка блоків 1142 від користувача (наприклад, ініціатора) 105 бенефіціару.

Однак, якщо виявляється, що згенерований підпис 1131 GPS для користувача (наприклад, ініціатора) 105 не ідентичний попередньому підпису 1051 GPS для користувача (наприклад, ініціатора) 105, згенерований підпис 1131 GPS скасовується 1133, і користувач 105 не зможе провести транзакцію.

Фіг. 12 являє собою схему, яка ілюструє процес 1200 збереження фрагмента біометричного цифрового підпису 1230 для користувача ("Ви") 105 для розміщувальних біометричних цифрових підписів 1251-1256, якими володіють інші люди 1241-1246, для генерування розміщувальних біометричних цифрових підписів 1251-1256 для кожної з інших людей 1241-1246, згідно щонайменше з одним варіантом здійснення цього розкриття. Для цього варіанта

здійснення люди 1241-1246, які пов'язані і/або асоційовані з користувачем 105, кожна може мати розміщувальний біометричний цифровий підпис 1251-1256, який містить фрагмент біометричного цифрового підпису 1230 для користувача 105, так що користувач 105 може використовувати свої розміщувальні біометричні цифрові підписи 1251-1256 для відновлення повного біометричного цифрового підпису 1230 для користувача 105.

На цьому кресленні призначені для користувача дані (наприклад, вихідні дані 1220, такі як дані 1221 GPS, біометричні дані 1222 і/або персональні дані 1223) спочатку виходять 1210 від користувача 105. Призначені для користувача дані (наприклад, вихідні дані 1220) хешуються з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 1230 для користувача 105.

Фрагмент біометричного цифрового підпису 1230 користувача 105 зберігається для кожного розміщувального біометричного цифрового підпису 1251-1256 для кожної людини 1241-1246 (наприклад, n людей, наприклад, шість (6)) для генерування розміщувального біометричного цифрового підпису 1251-1256 для кожної з людей 1241-1246, так що комбінація розміщувальних біометричних цифрових підписів 1251-1256 щонайменше для частини людей (наприклад, m кількість людей, наприклад, чотири (4)) 1241-1244 містить увесь біометричний цифровий підпис 1230 для користувача 105, де число m є числом, яке перевищує половину числа n.

Наприклад, в одному варіанті здійснення біометричний цифровий підпис 1230 користувача 105 містить 64 символи, і кожен з розміщувальних біометричних цифрових підписів 1251-1256 для людей 1241-1246 містить фрагмент загальної кількості символів (наприклад, 32 символи). Таким чином, наприклад, кожен із розміщувальних біометричних цифрових підписів 1251-1256 для людей 1241-1246 містить всього 32 символи. Потрібно зазначити, що в інших варіантах здійснення розміщувальний біометричний цифровий підпис 1251-1256 для людей 1241-1246 може кожен містити більш або менш в загальній складності 32 символи і/або кожен може містити різну кількість символів один для одного (наприклад, половина розміщувальних біометричних цифрових підписів 1251-1253 може містити всього 30 символів, а інша половина розміщувальних біометричних цифрових підписів 1254-1256 може містити в загальній складності 34 символи).

Фіг. 13 - схема, яка ілюструє процес 1300 використання розміщувальних біометричних цифрових підписів 1251-1256 від людей 1241-1246 за фіг. 12 для генерування відновленого біометричного цифрового підпису 1320 для користувача 105, згідно щонайменше з одним варіантом здійснення це розкриття. На цьому кресленні розміщувальні біометричні цифрові підписи 1252, 1253, 1255, 1256 від числа m (наприклад, чотирьох (4)) числа n (наприклад, шість (6)) людей 1242, 1243, 1245, 1246 використовуються для відновлення біометричного цифрового підпису 1320 для користувача 105. Потім відновлений біометричний цифровий підпис 1320 для користувача 105 може бути підтверджений 1330 для користувача 105, який повинен бути верифікований 1340.

Фіг. 14 - схема, яка ілюструє процес 1400 верифікації користувача 105 шляхом перевірки достовірності відновленого біометричного цифрового підпису 1320 для користувача 105, показаного на фіг. 13, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні дані 1221 GPS, біометричні дані 1222 і/або особисті дані 1223 від користувача 105 хешуються з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 1230 для користувача 105. Розміщувальні біометричні цифрові підписи 1252, 1253, 1255, 1256 від числа m (наприклад, чотирьох (4)) числа n (наприклад, шість (6)) людей 1242, 1243, 1245, 1246 використовуються для відновлення біометричного цифрового підпису 1320 для користувача 105. Відновлений біометричний цифровий підпис 1320 порівнюється 1420 з біометричним цифровим підписом 1230 для користувача 105. Якщо виявляється, що відновлений біометричний цифровий підпис 1320 для користувача 105 ідентичний біометричному цифровому підпису 1230 для користувача 105, відновлений біометричний цифровий підпис 1320 підтверджується 1430.

Варіант здійснення, в якому шість (6) людей ("друзів") використовуються для зберігання частин закритого ключа користувача, унікальний тим, що тільки чотири (4) з 6 "друзів" можуть використовуватися для того, щоб: а) відновити закритий ключ, якщо сталася втрата; або б) підписати транзакцію без присутності користувача (у випадку смерті людини). Це рішення для резервного копіювання, при якому жодна з 6 людей не знає, ким є інші, або яка частина закритого ключа у них є.

Фіг. 15 - схема, яка ілюструє різні типи транзакцій, які можуть відбуватися після верифікації користувача 105 шляхом перевірки достовірності біометричного цифрового підпису для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. Як показано на цьому кресленні, різні типи транзакцій, які можуть відбуватися, включають в себе,

крім іншого, передавання призначення блоків даних у ланцюжку блоків з використанням біометричних цифрових підписів 1510, ідентифікацію призначення блоків даних в ланцюжку блоків із використанням біометричних цифрових підписів 1520, ідентифікацію користувача 105 для голосування під час процесу голосування 1530, ідентифікацію користувача 105 для отримання медичних записів 1540, ідентифікацію користувача 105 для отримання проїзної документації 1550 і ідентифікацію володіння банківськими рахунками для проведення банківських транзакцій з використанням біометричних цифрових підписів 1560.

Фіг. 16 - схема, яка ілюструє різні типи додаткової ідентифікуючої інформації, яка може бути хешована разом з біометричними даними, отриманими від користувача 105, для генерування біометричного цифрового підпису для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. Як показано на цьому кресленні, різні типи додаткової ідентифікуючої інформації, які можуть бути використані, включають в себе, крім іншого, температуру 1610 навколишнього середовища, вологість 1620 навколишнього середовища, календарний діапазон 1630 дат, часовий діапазон 1640 і діапазон 1650 висот і діапазон 1660 сторін світу.

Фіг. 17 - схема, яка ілюструє процес 1700 генерування біометричного цифрового підпису 1760 для користувача 105 шляхом хешування біометричних даних 1701, 1701, 1703 від користувача 105 разом із додатковою ідентифікаційною інформацією 1710, 1720 і особистою інформацією 1730, 1740 для користувача 105, згідно щонайменше з одним варіантом здійснення цього розкриття. На цьому кресленні біометрична інформація у вигляді відбитків пальців 1701, 1701, 1703 отримана від користувача 105. Біометричні дані (у вигляді шістнадцяткових чисел 1705) генеруються з біометричної інформації відбитків пальців 1701, 1701, 1703.

Крім того, виходить додаткова ідентифікуюча інформація для користувача 105. Додаткова ідентифікуюча інформація містить інформацію 1710 місцерозташування GPS (наприклад, широту і довготу) та інформацію 1720 кардинального напрямку. Цифрові числа (наприклад, шістнадцяткові числа 1705) генеруються з додаткової ідентифікуючої інформації.

Крім того, особиста інформація отримана від користувача 105. Особиста інформація містить дату 1730 народження користувача 105 і останні чотири цифри номера соціального страхування користувача 105. Цифрові числа (наприклад, шістнадцяткові числа 1705) генеруються з особистої інформації.

Цифрові числа 1750 (наприклад, всі шістнадцяткові числа 1705) для біометричної інформації (наприклад, відбитки пальців 1701, 1703, 1703), додаткова ідентифікаційна інформація (наприклад, інформація 1710 місцерозташування GPS і інформація 1720 кардинального напрямку), і особиста інформація (наприклад, дата 1730 народження і останні чотири цифри номера соціального страхування 1740) хешуються з використанням алгоритму нечіткого хешування (або, альтернативно, алгоритму хешування) для генерування біометричного цифрового підпису 1760 для користувача 105.

Хоча були показані і описані конкретні варіанти здійснення, потрібно розуміти, що наведене вище обговорення не призначене для обмеження обсягу цих варіантів здійснення. Хоча варіанти здійснення і варіанти багатьох аспектів винаходу були розкриті й описані в цьому документі, таке розкриття надається тільки з метою пояснення і ілюстрації. Таким чином, різні зміни і модифікації можуть бути зроблені без виходу за межі формули винаходу.

Якщо способи, описані вище, вказують на певні події, що відбуваються в певному порядку, фахівці в цій галузі техніки, що користуються перевагою цього розкриття, зрозуміють, що порядок може бути змінений і що такі модифікації відповідають варіаціям цього розкриття. Крім того, частини способів можуть виконуватися одночасно в паралельному процесі, коли це можливо, а також виконуватися послідовно. Крім того, може бути виконано більше або менше кроків способів.

Відповідно, варіанти здійснення призначені для ілюстрації альтернатив, модифікацій і еквівалентів, які можуть потрапити під обсяг формули винаходу.

Хоча тут були розкриті певні ілюстративні варіанти здійснення і способи, з вищевикладеного розкриття для фахівців у цій галузі техніки може бути очевидно, що зміни і модифікації таких варіантів здійснення і способів можуть бути виконані без відхилення від істинного духу і обсягу цього розкриття. Існує багато інших прикладів, кожний з яких відрізняється від інших тільки деталями. Відповідно, передбачається, що це розкриття буде обмежене тільки ступенем, необхідною прикладеною формулою винаходу, а також правилами і принципами застосовного законодавства.

ФОРМУЛА ВИНАХОДУ

1. Спосіб верифікації особи користувача, який включає етапи, на яких:
приймають за допомогою користувацького пристрою біометричні дані, асоційовані з біометричною інформацією користувача;
хешують щонайменше фрагмент біометричних даних і щонайменше фрагмент додаткової ідентифікуючої інформації, щоб згенерувати біометричний цифровий підпис користувача;
зберігають щонайменше фрагмент біометричного цифрового підпису з розміщеним біометричним цифровим підписом користувальницьких пристроїв, що відповідає кожному із щонайменше числа n людей, так що комбінація розміщених біометричних цифрових підписів для щонайменше числа m із числа n людей містить всі з біометричних цифрових підписів користувача;
отримують розміщені біометричні цифрові підписи від інших користувацьких пристроїв, які відповідають іншим користувачам, асоційованим з користувачем, причому кожен із цих розміщених біометричних цифрових підписів містить фрагмент попереднього біометричного цифрового підпису користувача;
відновлюють попередній біометричний цифровий підпис зі згаданих фрагментів розміщених біометричних цифрових підписів;
порівнюють біометричний цифровий підпис із попереднім біометричним цифровим підписом користувача; і
верифікують користувача, коли зроблено визначення того, що біометричний цифровий підпис збігається з попереднім біометричним цифровим підписом користувача.

2. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу передати блок даних блокчейна від користувача іншому користувачу.

3. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу передати право власності на майно від користувача іншому користувачу.

4. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу отримувати медичні записи користувача.

5. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу голосувати від імені користувача.

6. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу отримувати проїзні документи для користувача.

7. Спосіб за п. 1, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу здійснювати банківські операції від імені користувача.

8. Спосіб за п. 1, який **відрізняється** тим, що користувацький пристрій використовує алгоритм хешування або алгоритм нечіткого хешування для хешування щонайменше фрагмента біометричних даних.

9. Спосіб за п. 1, який **відрізняється** тим, що згадана додаткова ідентифікуюча інформація містить щонайменше інформацію про місцезнаходження, інформацію про температуру, інформацію про вологість, інформацію про дату, інформацію про час, інформацію про висоту, інформацію про дальність або особисту інформацію.

10. Спосіб за п. 1, який **відрізняється** тим, що біометричний цифровий підпис є секретним ключем ідентифікації для користувача.

11. Спосіб за п. 1, який **відрізняється** тим, що користувацький пристрій являє собою смартфон, планшет, персональний комп'ютер, портативний комп'ютер, інтелектуальний годинник, інтелектуальне телебачення (телевізор), автомобіль або обчислювальний пристрій.

12. Спосіб за п. 1, який **відрізняється** тим, що число m є числом, що перевищує половину числа n.

13. Спосіб верифікації особи щонайменше одного користувача, причому спосіб включає етапи, на яких:
приймають біометричні дані, асоційовані з біометричною інформацією користувача;
хешують щонайменше фрагмент біометричних даних і щонайменше фрагмент ідентифікуючої інформації користувача, щоб згенерувати біометричний цифровий підпис користувача, при цьому ідентифікуюча інформація містить одну або більше з: інформації про місцезнаходження, інформації про температуру, інформації про вологість, інформації про дату, інформації про час, інформації про висоту, інформації про дальність і особистої інформації;

зберігають щонайменше фрагмент біометричного цифрового підпису користувача у розміщеному біометричному цифровому підписі користувацьких пристроїв, які відповідають кожному зі щонайменше числа n людей, так що комбінація розміщених біометричних цифрових підписів для щонайменше числа m із числа n людей містить біометричні цифрові підписи користувача;

порівнюють біометричний цифровий підпис із попереднім біометричним цифровим підписом користувача; і

визначають на основі згаданого порівняння, що біометричний цифровий підпис збігається з попереднім біометричним цифровим підписом; і

приймають сигнал підтвердження верифікації, який вказує, що користувач верифікований на основі згаданого визначення.

14. Спосіб за п. 13, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу здійснювати доступ до блока даних блокчейна.

15. Спосіб за п. 13, який **відрізняється** тим, що, коли користувач верифікований, спосіб додатково включає етап, на якому дозволяють користувачу передати блок даних блокчейна від користувача іншому користувачу.

16. Система верифікації особи користувача, яка містить:

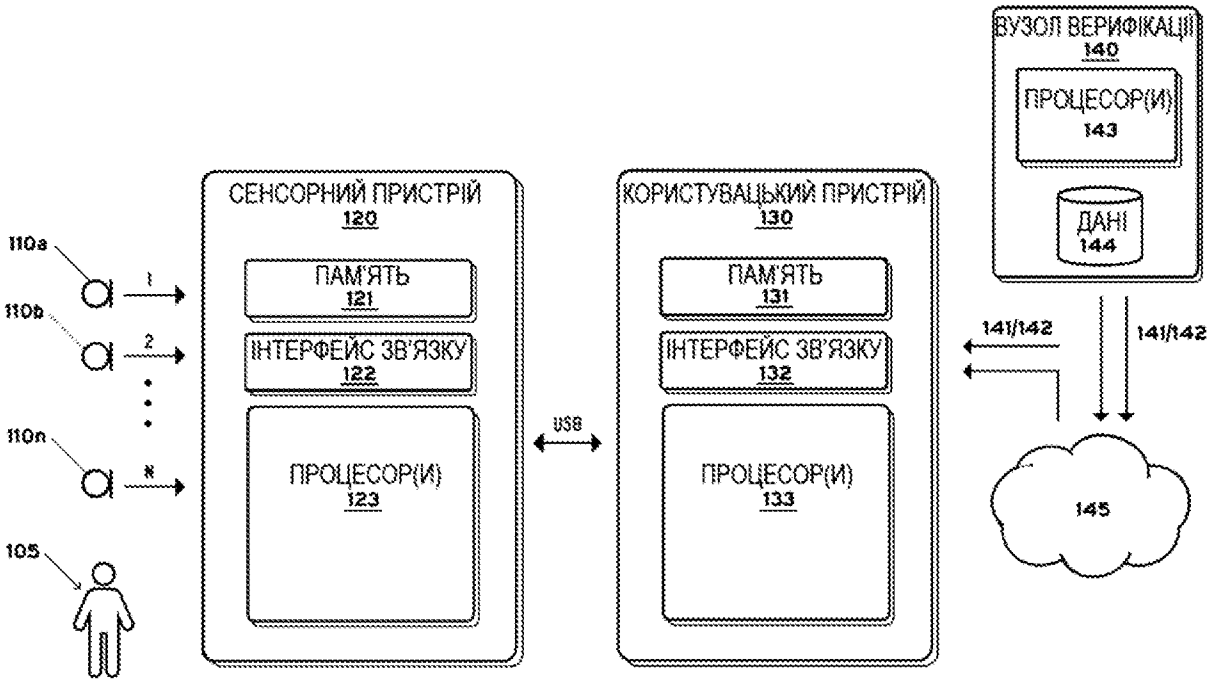
базу даних, яка зберігає щонайменше фрагмент хешованого біометричного цифрового підпису користувача і розміщений біометричний цифровий підпис користувальницьких пристроїв, які відповідають кожному зі щонайменше числа n людей, так що комбінація розміщених біометричних цифрових підписів для щонайменше числа m із числа n людей містить біометричні цифрові підписи користувача; і

щонайменше один апаратний процесор, виконаний з можливістю виконання інструкцій, які наказують системі виконувати операції, які включають: отримання розміщених біометричних цифрових підписів від інших користувацьких пристроїв, які відповідають іншим користувачам, асоційованим із користувачем, причому кожен із цих розміщених біометричних цифрових підписів містить фрагмент попереднього біометричного цифрового підпису користувача; відновлення попереднього біометричного цифрового підпису зі згаданих фрагментів розміщених біометричних цифрових підписів; порівняння біометричного цифрового підпису з попереднім біометричним цифровим підписом користувача і верифікацію користувача, коли біометричний цифровий підпис збігається з попереднім біометричним цифровим підписом користувача.

17. Система п. 16, яка **відрізняється** тим, що число m є числом, що перевищує половину числа n.

18. Система п. 16, яка **відрізняється** тим, що, коли користувач верифікований, операції додатково включають дозвіл користувачу здійснювати доступ до блока даних блокчейна.

19. Система п. 16, яка **відрізняється** тим, що, коли користувач верифікований, операції додатково включають дозвіл користувачу передати блок даних блокчейна від користувача іншому користувачу.



100

Фіг. 1A

155 ПОЧАТОК

160 ЗЧИТУВАННЯ ЩОНАЙМЕНШЕ ОДНИМ ДАТЧИКОМ БІОМЕТРИЧНОЇ ІНФОРМАЦІЇ ВІД КОРИСТУВАЧА

165 ГЕНЕРУВАННЯ СЕНСОРНИМ ПРИСТРОЄМ БІОМЕТРИЧНИХ ДАНИХ ІЗ БІОМЕТРИЧНОЇ ІНФОРМАЦІЇ

170 ПЕРЕДАВАННЯ СЕНСОРНИМ ПРИСТРОЄМ БІОМЕТРИЧНИХ ДАНИХ КОРИСТУВАЦЬКОМУ ПРИСТРОЮ

175 ХЕШУВАННЯ КОРИСТУВАЦЬКИМ ПРИСТРОЄМ ЩОНАЙМЕНШЕ ЧАСТИНИ БІОМЕТРИЧНИХ ДАНИХ ДЛЯ СТВОРЕННЯ БІОМЕТРИЧНОГО ЦИФРОВОГО ПІДПИСУ ДЛЯ КОРИСТУВАЧА

180 ПЕРЕДАВАННЯ КОРИСТУВАЦЬКИМ ПРИСТРОЄМ БІОМЕТРИЧНОГО ЦИФРОВОГО ПІДПИСУ У ВУЗОЛ ВЕРИФІКАЦІЇ

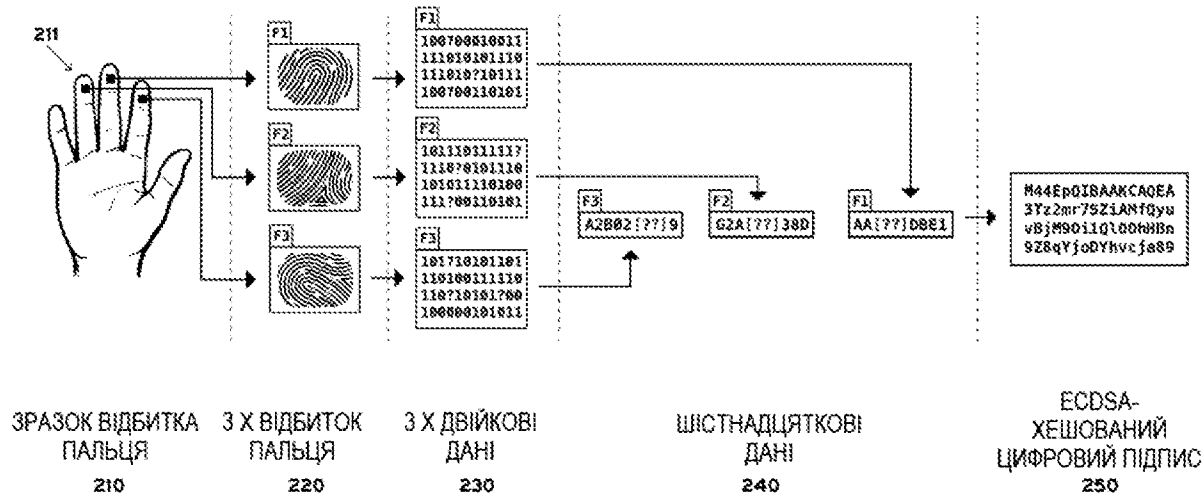
185 ПОРІВНЯННЯ ВУЗЛОМ ВЕРИФІКАЦІЇ БІОМЕТРИЧНОГО ЦИФРОВОГО ПІДПИСУ ІЗ ПОПЕРЕДНІМ БІОМЕТРИЧНИМ ЦИФРОВИМ ПІДПИСОМ ДЛЯ КОРИСТУВАЧА

190 ВЕРИФІКАЦІЯ ВУЗЛОМ ВЕРИФІКАЦІЇ КОРИСТУВАЧА, КОЛИ ВУЗОЛ ВЕРИФІКАЦІЇ ВИЗНАЧАЄ, ЩО БІОМЕТРИЧНИЙ ЦИФРОВИЙ ПІДПИС ІДЕНТИЧНИЙ ПОПЕРЕДНЬОМУ БІОМЕТРИЧНОМУ ЦИФРОВОМУ ПІДПИСУ КОРИСТУВАЧА

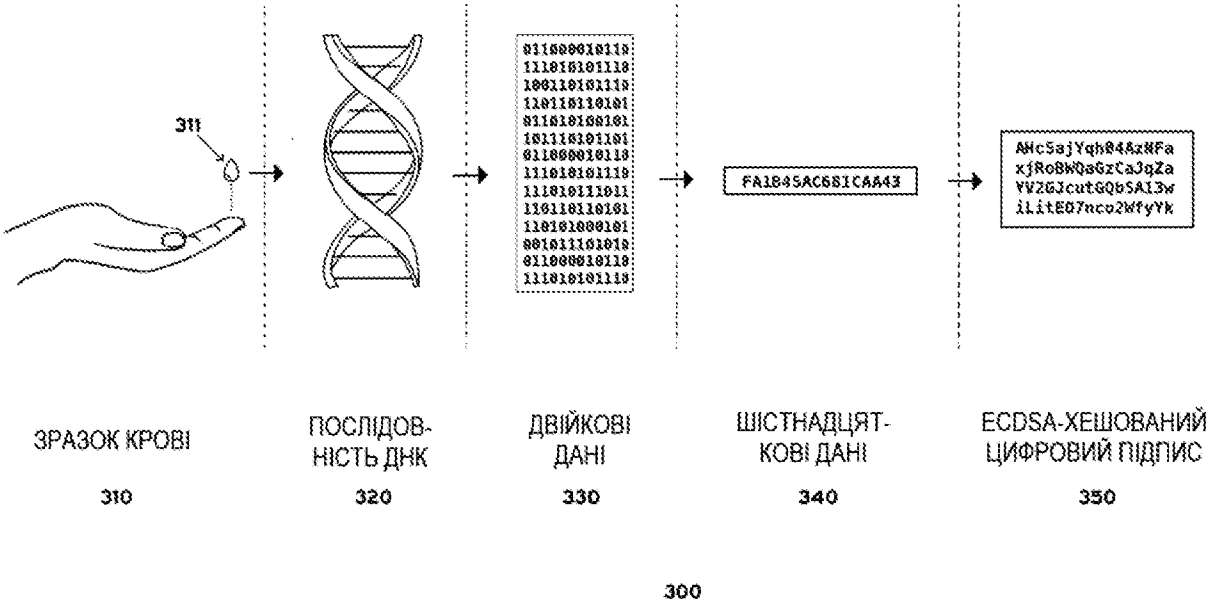
195 КІНЕЦЬ

150

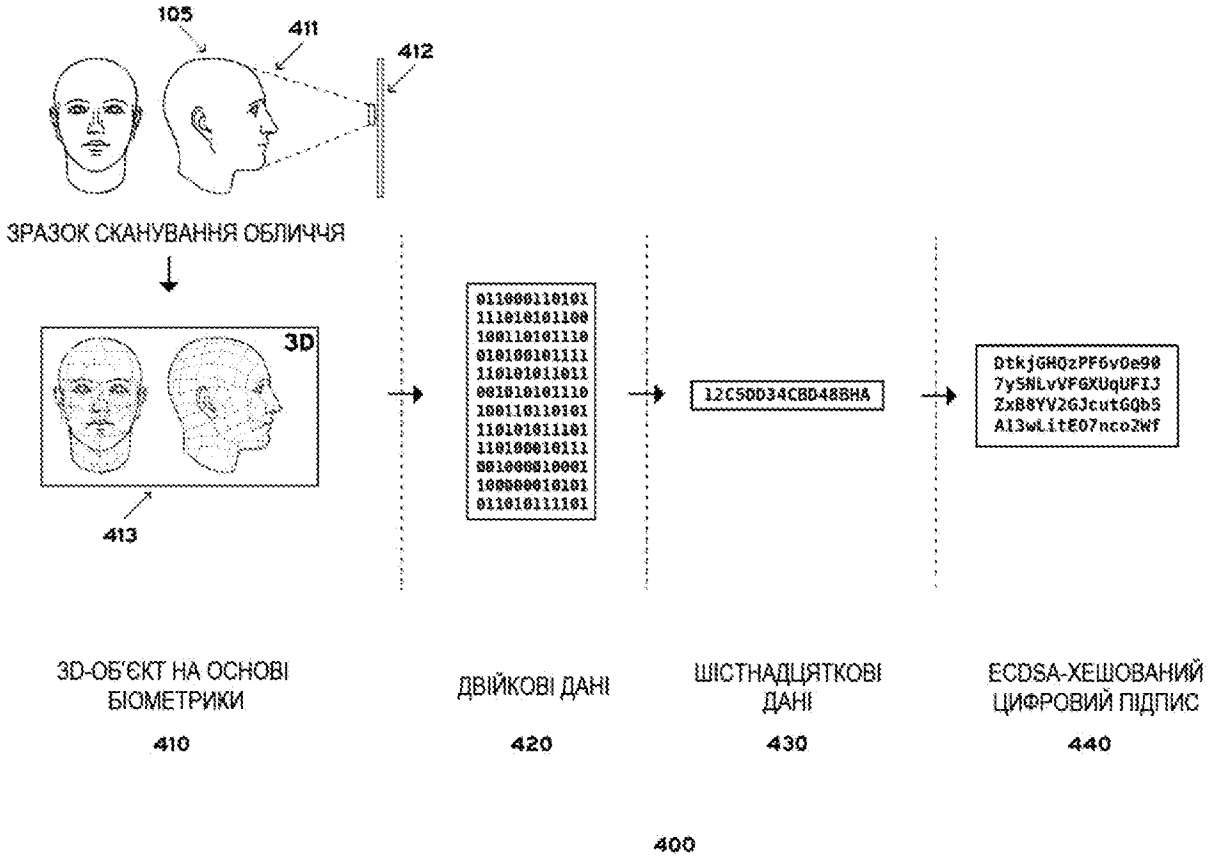
Фіг. 1B


211
F1
F2
F3
A2B02[??]9
G2A[??]38D
AA[??]D8E1
ЗРАЗОК ВІДБИТКА ПАЛЬЦЯ
210
3 Х ВІДБИТОК ПАЛЬЦЯ
220
3 Х ДВІЙКОВІ ДАНІ
230
ШІСТНАДЦЯТКОВІ ДАНІ
240
ECDSA-ХЕШОВАНИЙ ЦИФРОВИЙ ПІДПИС
250
200

Фіг. 2

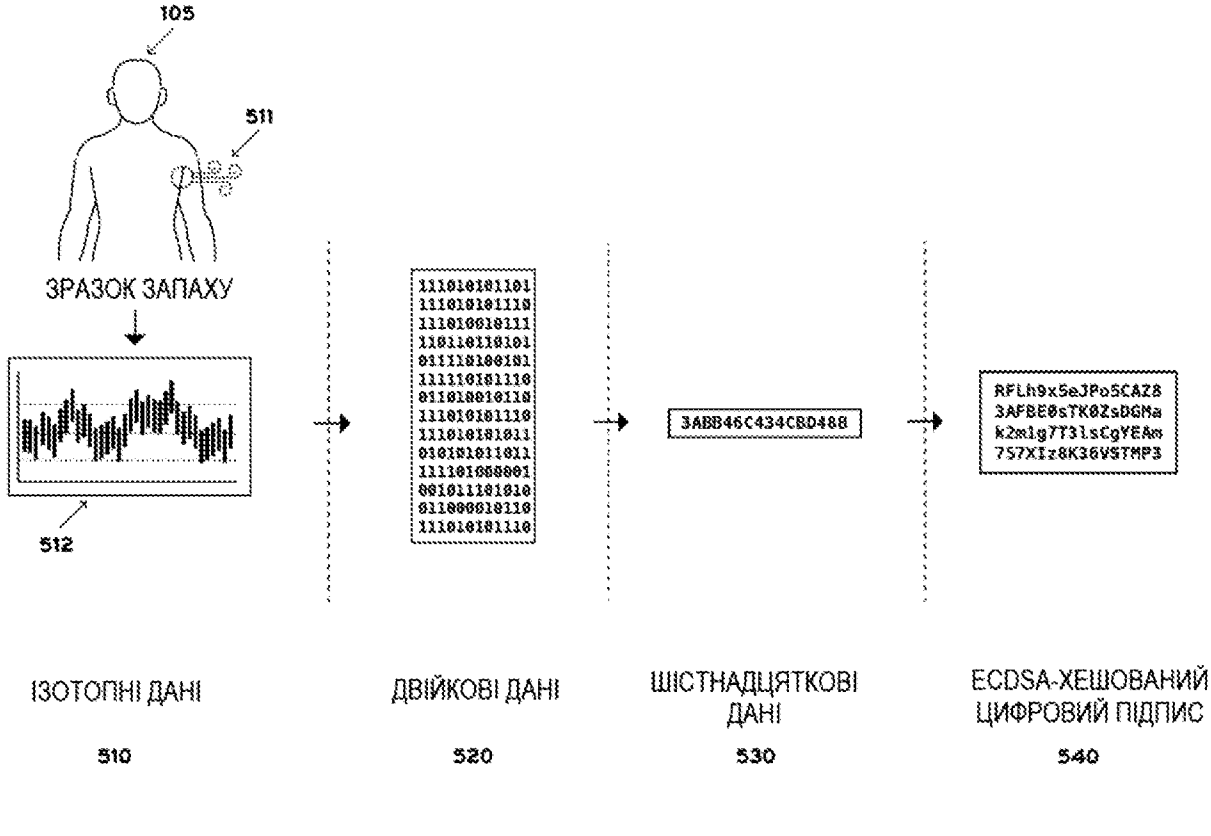

311
FA1845AC68ICAA43
ЗРАЗОК КРОВІ
310
ПОСЛІДОВ-НІСТЬ ДНК
320
ДВІЙКОВІ ДАНІ
330
ШІСТНАДЦЯТ-КОВІ ДАНІ
340
ECDSA-ХЕШОВАНИЙ ЦИФРОВИЙ ПІДПИС
350
300

Фіг. 3



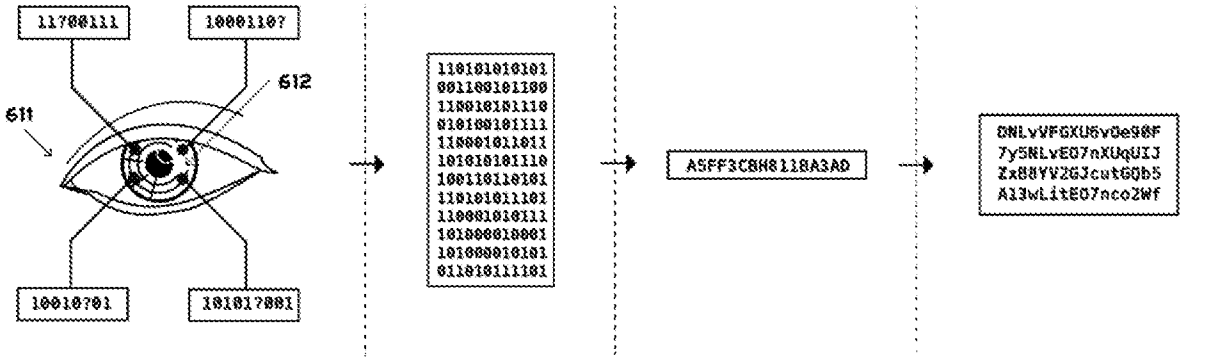
400

Фіг. 4

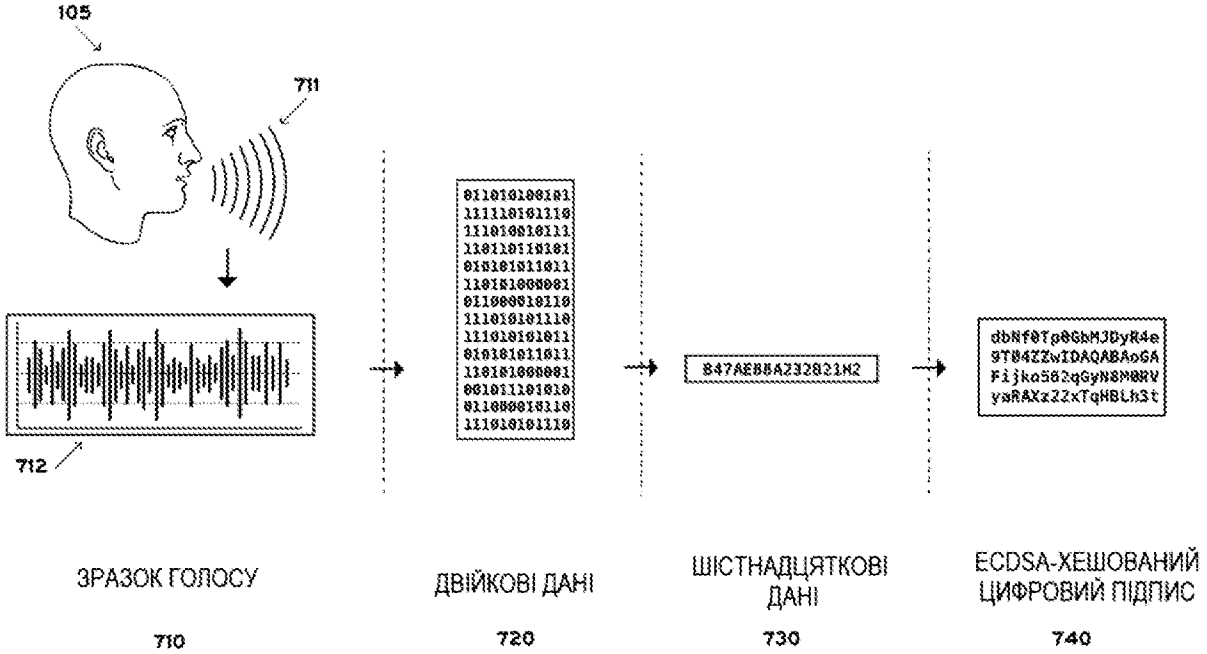


500

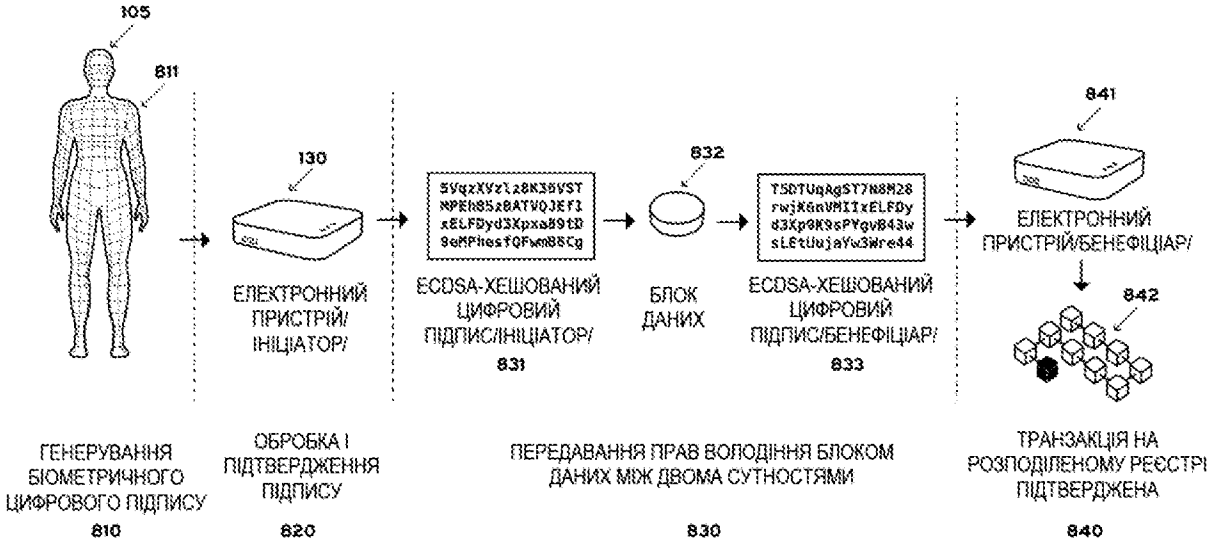
Фіг. 5


11700111
10001107
612
611
10010701
101017001
110101010101
001100101100
110010101110
010100101111
110000101011
101010101110
100110110101
110101011101
110001010111
101000010001
101000010101
011010111101
ASFF3C8H8118A3A0
8NLvVFGXU6vDeS8F
7y5NLvEG7nXUqUIJ
ZxB8YV2GJcutGDb5
Al3wLitEG7ncoZWf
СКАНУВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА
610
ДВІЙКОВІ ДАНІ
620
ШІСТНАДЦЯТКОВІ ДАНІ
630
ECDSA-ХЕШОВАНИЙ ЦИФРОВИЙ ПІДПИС
640
600

Фіг. 6

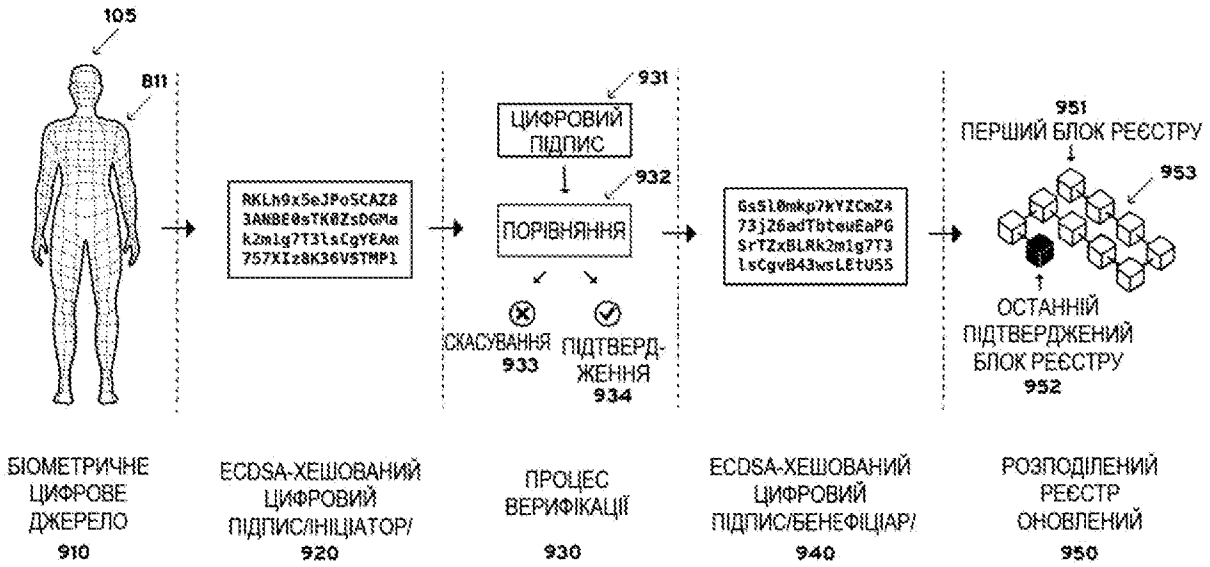

105
711
712
011010100101
111110101110
111010010111
110110110101
010101011011
110101000001
011000010110
111010101110
111010101011
010101011011
110101000001
001011101010
011000010110
111010101110
847AE88A232821M2
dbNf0Tp0GbMJDyR4e
9T04ZZwIDAQABAoGA
Fijko582qGyN8M0RV
yaRAXxZ2xTqHBLh3t
ЗРАЗОК ГОЛОСУ
710
ДВІЙКОВІ ДАНІ
720
ШІСТНАДЦЯТКОВІ ДАНІ
730
ECDSA-ХЕШОВАНИЙ ЦИФРОВИЙ ПІДПИС
740
700

Фіг. 7



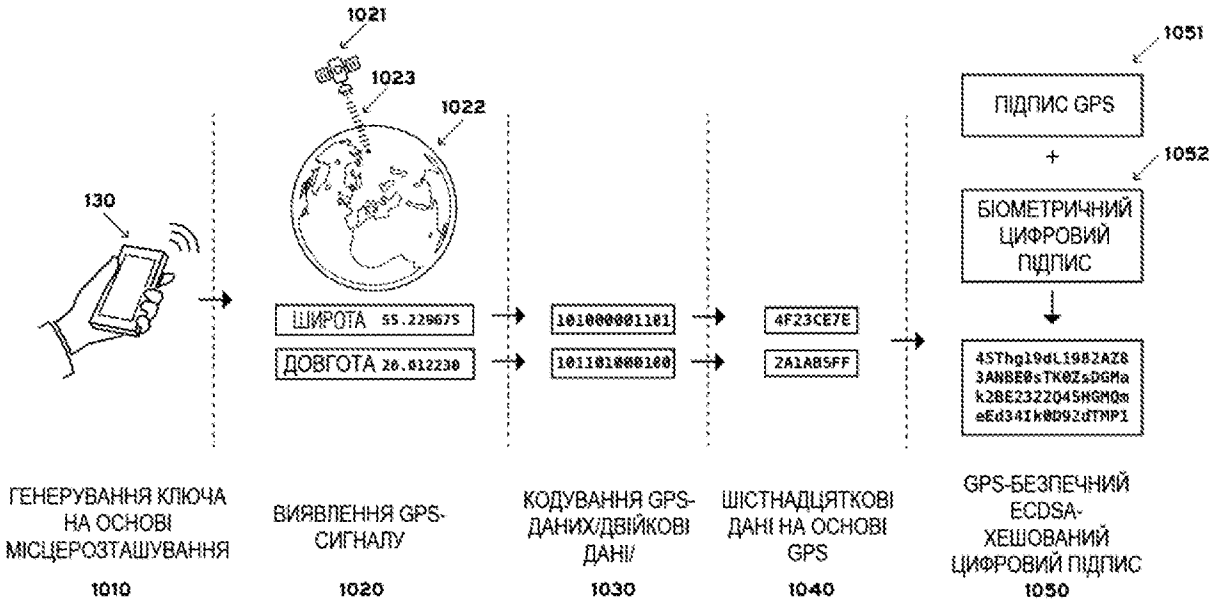
800

Фіг. 8

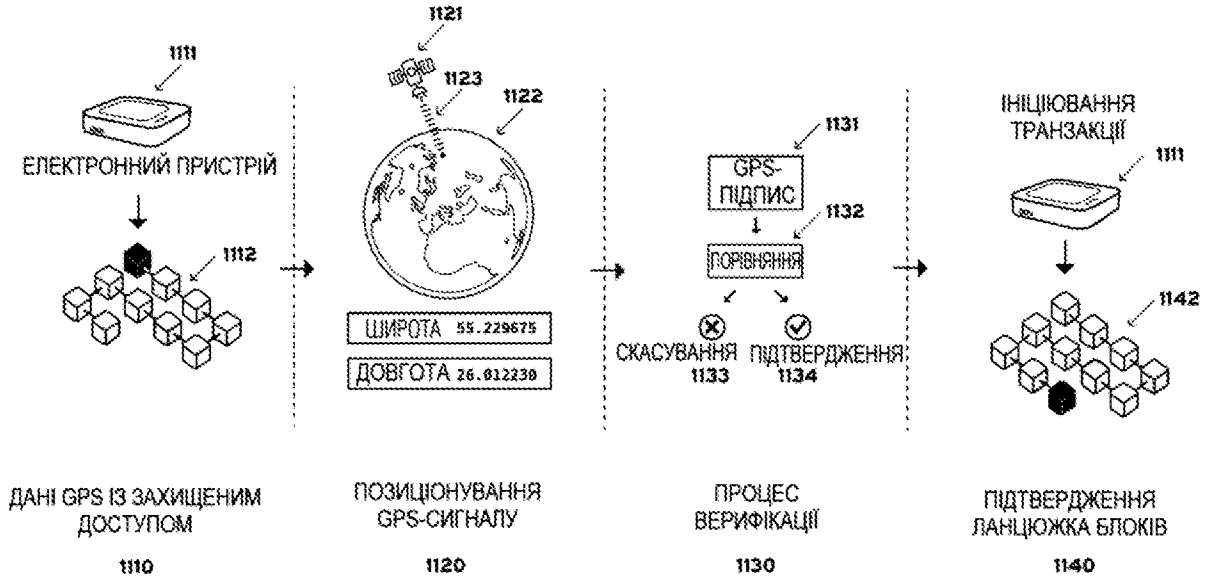


900

Фіг. 9

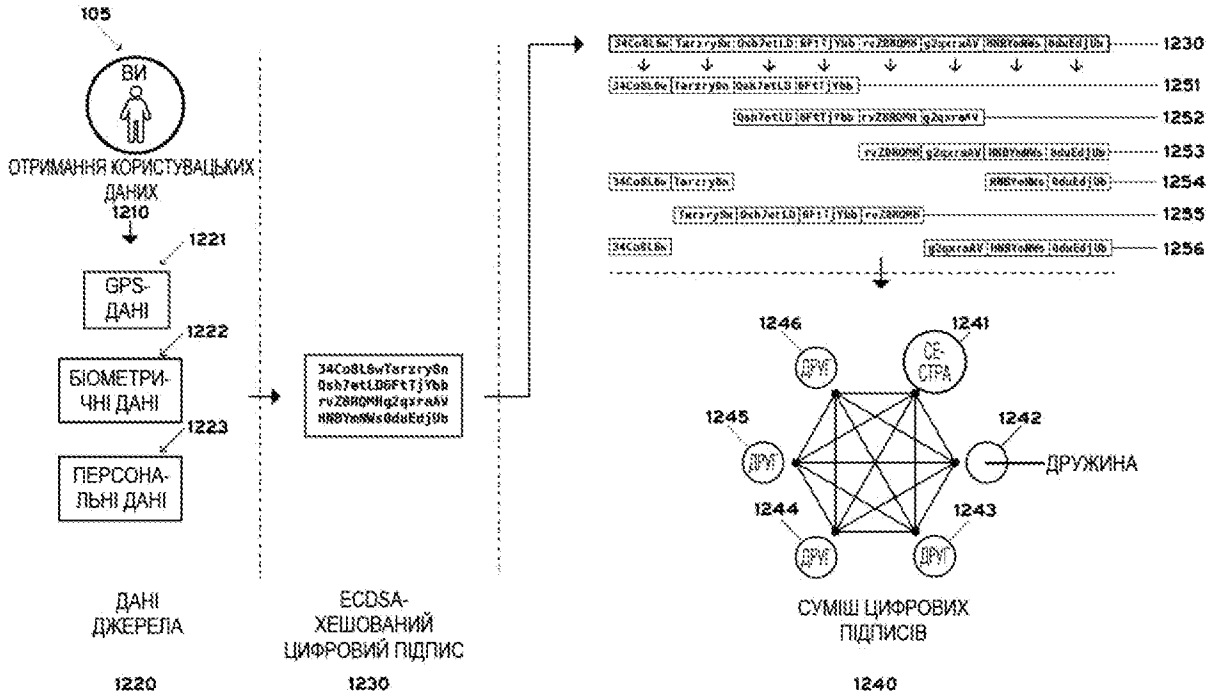


Фіг. 10 1000



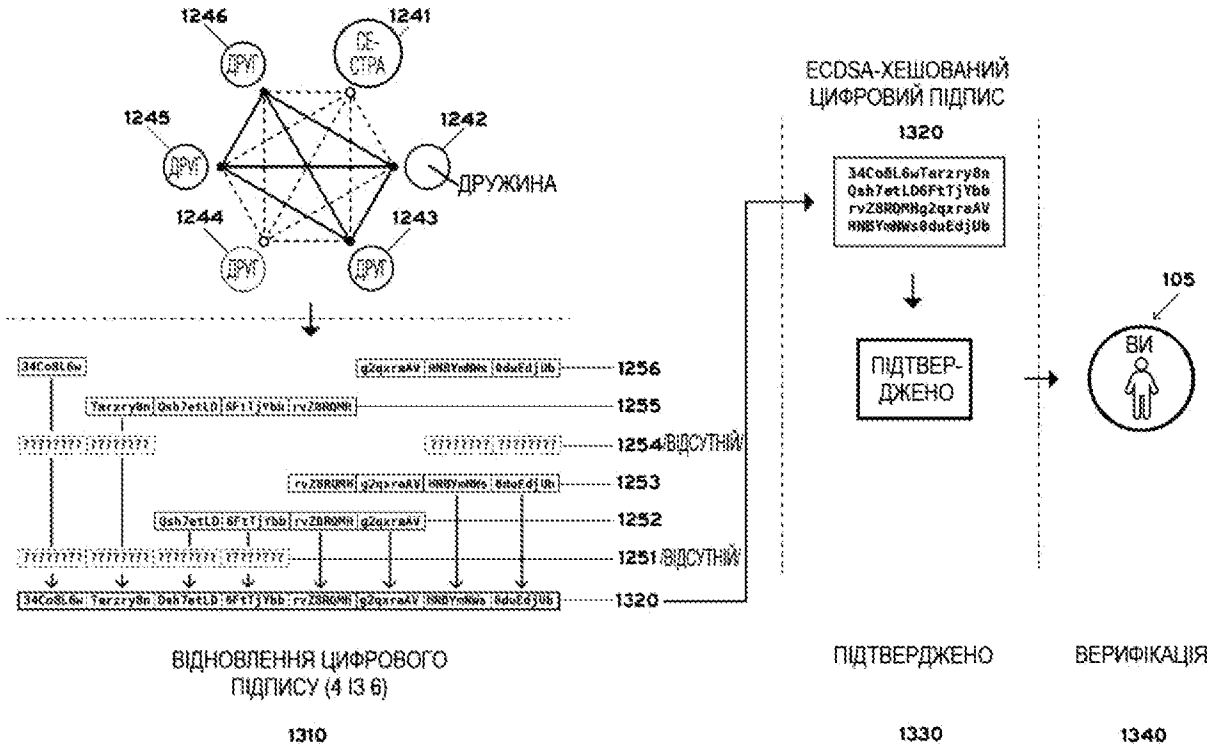
1100

Фіг. 11



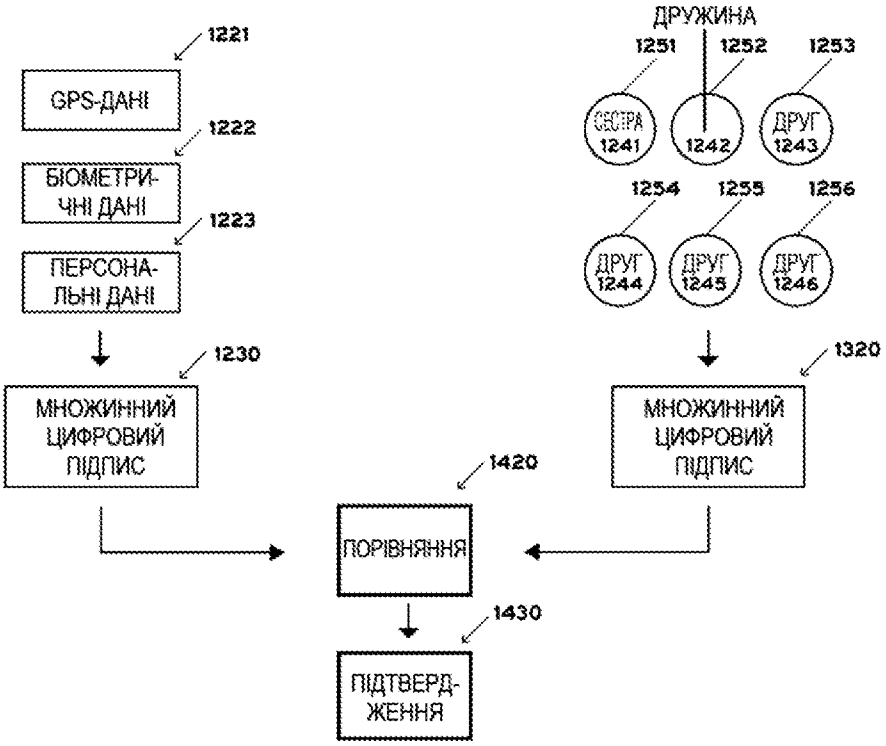
1200

Фіг. 12



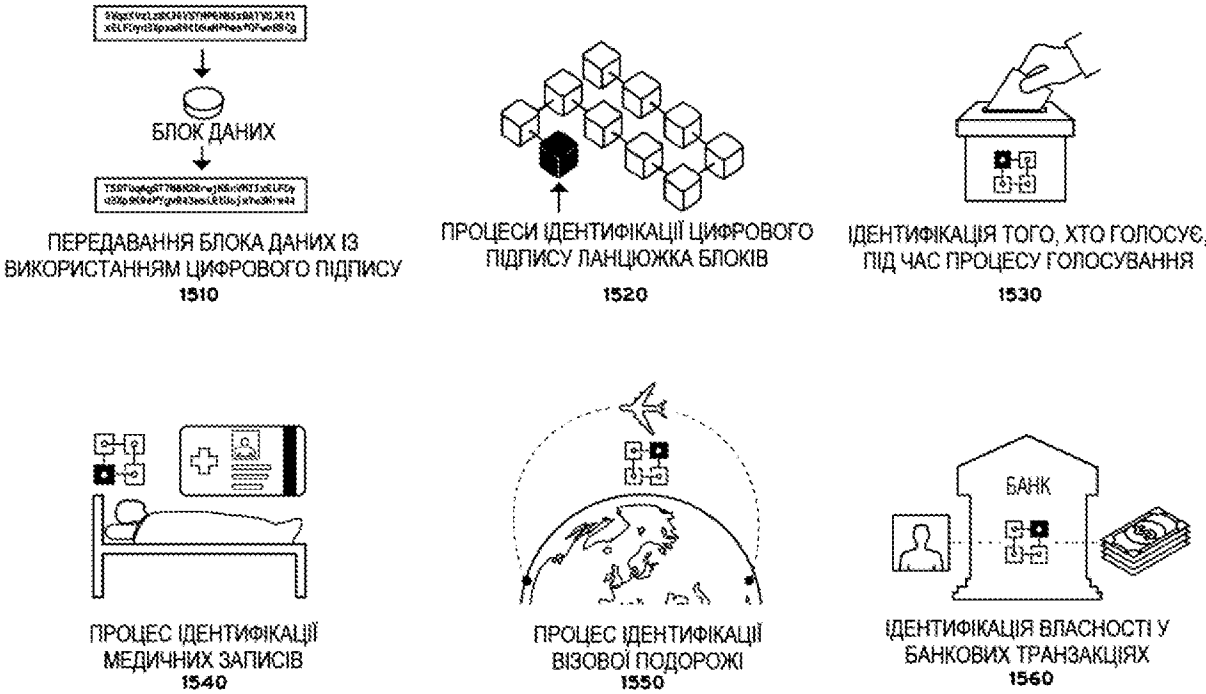
1300

Фіг. 13



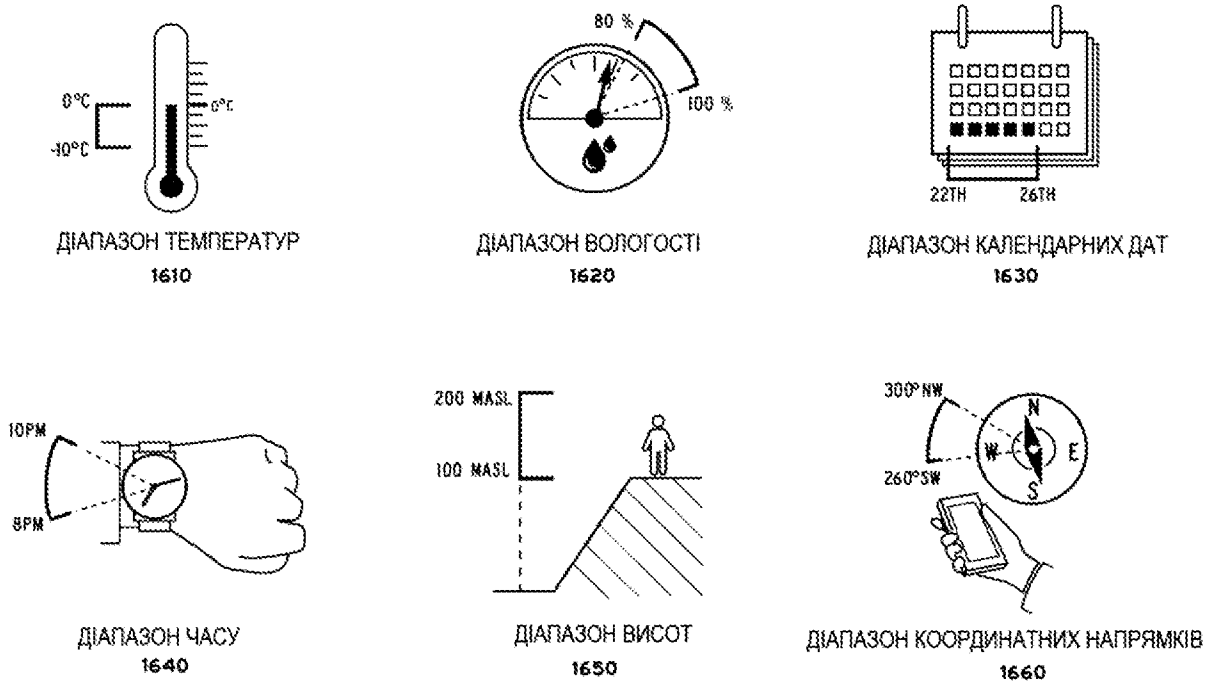
1400

Фіг. 14



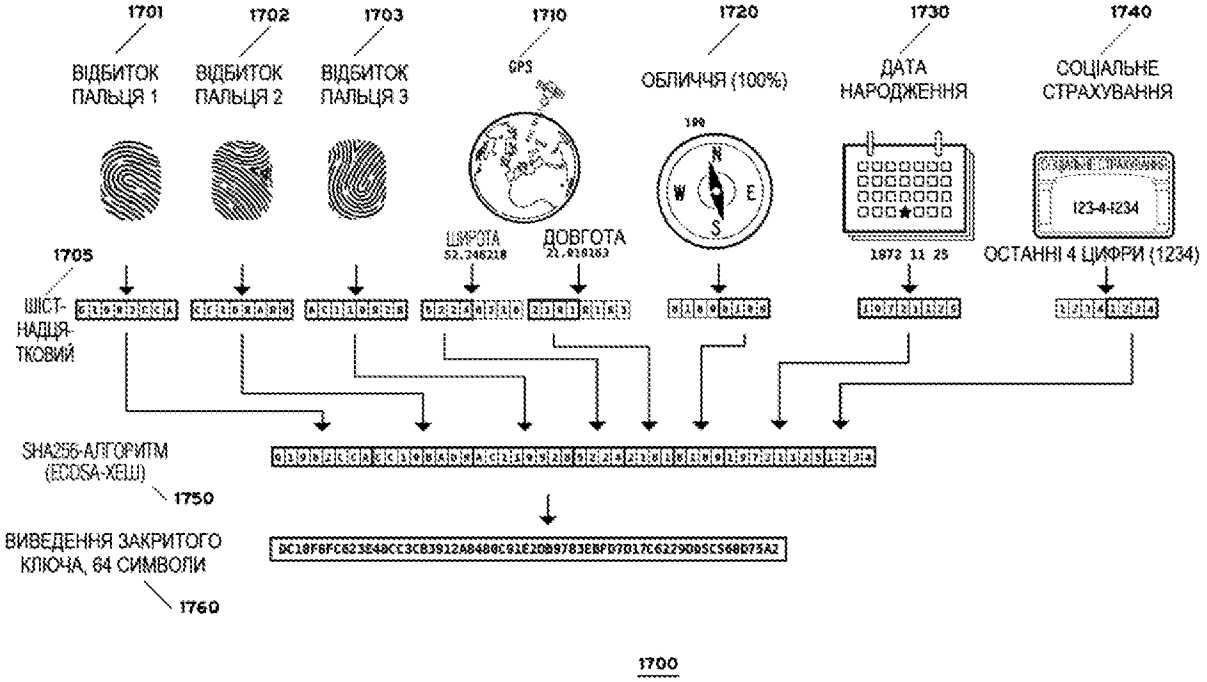
1500

Фіг. 15



1600

Фіг. 16



1700

Фіг. 17

Комп'ютерна верстка В. Юкін

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Дмитра Годзенка, 1, м. Київ – 42, 01601