



УКРАЇНА

(19) **UA**
(51) МПК(11) **128858**(13) **C2**

G06Q 20/08 (2012.01)
G06Q 20/10 (2012.01)
G06Q 20/22 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

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

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

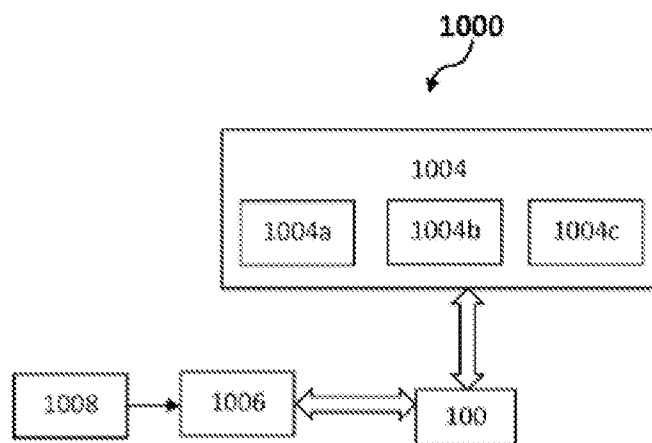
(21) Номер заявки: а 2019 00002 (22) Дата подання заявки: 12.05.2017 (24) Дата, з якої є чинними права інтелектуальної власності: 14.11.2024 (31) Номер попередньої заявки відповідно до Паризької конвенції: 201621021488 (32) Дата подання попередньої заявки відповідно до Паризької конвенції: 22.06.2016 (33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку: IN (41) Публікація відомостей про заявку: 11.03.2019, Бюл.№ 5 (46) Публікація відомостей про державну реєстрацію: 13.11.2024, Бюл.№ 46 (86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ: PCT/IB2017/052793, 12.05.2017	(72) Винахідник(и): Асбе Діліп (IN), Раджендран Нараянан (IN), Палагірі Сатіш (IN), Шарма Анубхав (IN) (73) Володілець (володільці): НАТІОНАЛ ПЕЙМЕНТС КОРПОРАТІОН ОФ ІНДІА, 1001A, B Wing, 10th Floor, The Capital, Bandra-Kurla Complex, Bandra (East), Mumbai, Maharashtra 400051, India (IN) (74) Представник: Кістерський Кирило Арсенійович, реєстр. №207 (56) Перелік документів, взятих до уваги експертизою: NPCI. UNIFIED PAYMENT INTERFACE - API and Technology Specifications - Version 1.0 (DRAFT)., FEBRUARY 2015 US 8700527 B2, 15.04.2014
---	---

(54) СИСТЕМА ЕЛЕКТРОННИХ ПЛАТЕЖІВ І СПОСІБ ЇХ ЗДІЙСНЕННЯ**(57) Реферат:**

Цей винахід описує систему електронних платежів і спосіб їх здійснення. Цей винахід належить до області систем електронних платежів. Система електронних платежів спрощує відправлення та прийом грошей простим способом з використанням користувацьких пристроїв. Вона являє собою уніфікований платіжний інтерфейс (UPI) і надає можливість користувачам оплачувати та отримувати/інкасувати платежі з рахунків причетних фізичних/юридичних осіб. Система за цим винаходом надає можливість здійснення платіжних транзакцій між платником і отримувачем платежу без необхідності обов'язкового надання банківської інформації та реквізитів банківського рахунку один одного. Вона усуває ризик зберігання реквізитів рахунку покупця та може використовуватися покупцями, які не мають кредитної/дебетової карти. Вона забезпечує конфіденційність платіжної транзакції та спрощує встановлення багатьох утиліт, оплату готівкою у разі доставки, у разі розділення/спільного використання рахунків, у разі оплати/переказу грошей продавцеві. Система електронних платежів за цим винаходом працює

UA 128858 C2

через різні інтерфейси, за допомогою яких запити на платіж можуть бути згенеровані в інтернет-інтерфейсі та авторизовані в мобільному інтерфейсі (інструмент додатка).



Фіг. 1

Цей винахід відноситься до систем електронних платежів.

Вираз "zareestrovaniy korystuvach", використовуваний надалі в описі цього винаходу, відноситься до особи, яка використовує систему електронних платежів (EPS) за цим винаходом для здійснення транзакцій у системі електронних платежів. Zareestrovanim korystuvachem може

бути платник, тобто особа, яка хоче Відправити/Заплатити гроші, використовуючи EPS, або їм може бути отримувач платежу, тобто особа, яка отримує/інкасує гроші, використовуючи EPS.

Вираз "korystuvats'kyi prystriy", використовуваний надалі в описі цього винаходу, відноситься до пристрою, що використовується zareestrovanim korystuvachem, при цьому

korystuvats'kyi prystriy включає, але не обмежується цим, мобільний телефон, лептоп,

планшет, iPad, КПК, ноутбук, нетбук, інтелектуальний пристрій, смартфон, персональний

комп'ютер, портативний пристрій і таке інше.

Вираз "platizhni tranzaktsii", використовуваний надалі в описі цього винаходу, відноситься як до фінансових, так і до нефінансових транзакцій. Фінансові транзакції включають запити на інкасацію/pull-запити, запити на оплату/push-запити та комерційні платежі. Нефінансові транзакції включають, але не обмежуються цим, реєстрацію мобільного банкінгу, генерацію одноразового пароля (OTP), перевірку балансу, установку або зміну PIN-коду, реєстрацію скарг та перевірку статусу транзакції.

Вираз "Sistema operatora platizhnogo servisu (PSPS)", використовуваний надалі в описі цього винаходу, відноситься до Банку, Платіжного банку або до будь-якої іншої юридичної особи, регульованої централізовано або державою, якій дозволено залучати покупців і надавати платіжні сервіси (кредитові/дебетові) покупцям (фізичним або юридичним особам). PSPS надає інструменти відповідних додатків, до яких zareestrovani korystuvachi можуть отримати доступ на своїх користувачьких пристроях для виконання push- або pull-платежів. PSPS надає інструмент для електронної обробки фінансових і нефінансових транзакцій.

Вираз "vidpravnik", використовуваний надалі в описі цього винаходу, відноситься до zareestrovano korystuvacha, який відправляє запит на оплату/push-запит або запит на інкасацію грошей/pull-запит, використовуючи користувачький пристрій за цим винаходом. Відправником може бути платник або отримувач платежу.

Вираз "otrimuvach", використовуваний надалі в описі цього винаходу, відноситься до zareestrovano korystuvacha, який отримує запит на користувачькому пристрої на інкасацію грошей/pull-запит або запит на оплату грошей/push-запит, використовуючи користувачький пристрій за цим винаходом. Отримувачем може бути отримувач платежу або платник.

Вирази "unikalnyi identifikator (ID)" або "virtualna platizhna adresa (VPA)", використовувані надалі в описі цього винаходу, відносяться до унікального ідентифікатора, пов'язаного із zareestrovanim korystuvachem. Унікальний ID або Віртуальна платіжна адреса (VPA) використовуються для здійснення платіжних транзакцій. Вони можуть бути створені zareestrovanim korystuvachem для здійснення платіжної(их) транзакції(й).

Вираз "unifikoivaniy platizhnyi interfeys (UPI)", використовуваний надалі в описі цього винаходу, відноситься до інтерфейсної системи, яка забезпечує інтерфейс між системами PSPS для здійснення фінансових і нефінансових платіжних транзакцій, включаючи платіжні транзакції та розрахункові платежі.

Вираз "Dodatek operatora platizhnogo servisu (PSPA)", використовуваний надалі в описі цього винаходу, відноситься до інструменту додатка, який забезпечується кожною PSPS. Інструмент PSPA може бути забезпечений на Інтернет-порталі або в магазині ігор і/або в мобільному Інтернеті, або за допомогою інших засобів для взаємодії з PSPS за допомогою UPI.

Вираз "informatsiyni dani pro korystuvacha", використовуваний надалі в описі цього винаходу, відноситься до даних, які відносяться до zareestrovano korystuvacha, включаючи VPA zareestrovano korystuvacha, дані облікового запису та інші нефінансові дані. Інформаційні дані про користувача використовуються для автентифікації zareestrovano korystuvacha.

Ці терміни та визначення доповнюють терміни та визначення, що існують у цій галузі техніки.

Останніми роками фінансові транзакції все частіше здійснюються за допомогою портативних пристроїв, тобто традиційних мобільних телефонів і смартфонів. Нині доступні різні способи оплати за допомогою портативних пристроїв. Ці способи оплати вимагають знання номера рахунку отримувача платежу та додаткових даних, які стосуються банку отримувача платежу. У разі онлайн-платежів платнику необхідно зайти на Інтернет-портал свого банку за допомогою Інтернет-банкінгу або мобільного банкінгу для здійснення фінансових транзакцій. На сьогодні багато користувачів все ще нечасто користуються фінансовими транзакціями онлайн/електронними транзакціями, оскільки банківські Інтернет-портали для Інтернет-банкінгу

або мобільного банкінгу незручні або складні у користуванні, а для введення даних й авторизації вимагається тривалий час.

У деяких випадках для виконання платежу використовується номер мобільного телефону отримувача платежу. Проте за такого способу вкрай важливо для платника знати банківські реквізити отримувача платежу і/або номер мобільного телефону, оскільки мобільний банкінг прив'язаний до номера SIM-карти. Під час здійснення усіх таких транзакцій платіж спрямовується платником отримувачу платежу. Отримувач платежу залежить виключно від платника, який здійснює транзакції, а платник залежить від Інтернет-порталу свого банку, що реалізовує платіжний сервіс. Деякі користувачі схильні міняти свої номери мобільних телефонів, і у таких випадках платнику складно відстежувати ці зміни. Крім того, у деяких випадках платник й отримувач платежу можуть не захотіти розкривати свої банківські реквізити та особисті дані один одному.

Відповідно, існує необхідність в обмеженні вищезгаданих недоліків і в тому, щоб запропонувати ефективну, просту та зручну у користуванні систему та спосіб здійснення транзакцій у системі електронних платежів.

Далі представлено деякі з цілей цього винаходу, яким задовольняє щонайменше один варіант його здійснення, описаний у цьому документі:

Ціллю цього винаходу є усунення однієї або більше проблем попереднього рівня техніки або, щонайменше, забезпечення прийнятної альтернативи.

Ціллю цього винаходу є забезпечення системи електронних платежів, яка є простою у користуванні.

Іншою ціллю цього винаходу є забезпечення системи електронних платежів, яка має уніфікований платіжний інтерфейс (UPI).

Ще однією ціллю цього винаходу є забезпечення системи електронних платежів, яка надає можливість користувачам здійснювати pull-платежі/інкасувати платежі з рахунків причетних фізичних/юридичних осіб після того, як запитувана юридична особа авторизує такі платежі.

Ще однією ціллю цього винаходу є спрощення системи електронних платежів як для платників, так і для отримувачів платежів шляхом скорочення етапів авторизації та підвищення функцій безпеки.

Ще однією ціллю цього винаходу є забезпечення системи електронних платежів, яка надає можливість виконувати платіжні транзакції між платником й отримувачем платежу без необхідності обов'язкового надання банківської інформації та реквізитів банківського рахунку один одного.

Крім того, ціллю цього винаходу є забезпечення системи електронних платежів, яка надає можливість користувачу відправляти та отримувати гроші за допомогою віртуальної платіжної адреси.

Ще однією ціллю цього винаходу є забезпечення системи електронних платежів, яка усуває залежність користувача від Інтернет-порталу свого банку або мобільного додатку для Інтернет-банкінгу, або мобільного банкінгу, і дозволяє користувачу використовувати для здійснення платіжних транзакцій Інтернет-портал іншого банку і/або мобільні додатки, відмінні від його банківського рахунку.

Інші цілі та переваги цього винаходу стануть очевидними з нижченаведеного опису, який жодним чином не обмежує об'єм цього винаходу.

Система електронних платежів (EPS) і спосіб їх здійснення передбачені для спрощення здійснення платіжних транзакцій між множиною користувачів. Система містить оперативний запам'ятовуючий пристрій, операційний процесор, множину Систем операторів платіжного сервісу (PSPS), виконаних з можливістю реєстрації користувачів і виконаних з додатковою можливістю реєстрації їх в EPS, множину користувацьких пристроїв, інструменти Додатків операторів платіжного сервісу (PSPAs) і Уніфікований платіжний інтерфейс (UPI). Оперативний запам'ятовуючий пристрій зберігає набір заздалегідь заданих правил дій, які використовуються операційним процесором для отримання набору команд управління роботою системи. Кожна PSPS містить локальний запам'ятовуючий пристрій, що зберігає інформаційні дані про користувача, які відносяться до користувачів, зареєстрованих у PSPS, щонайменше одну пошукову таблицю, яка спрощує співставлення даних, введених покупцем, інформаційних даних про користувача та про зареєстрованого користувача, і PSPS-сервер. Кожен користувацький пристрій з множини користувацьких пристроїв пов'язаний з одним із зареєстрованих користувачів і зареєстрований в якості частини інформаційних даних про користувача. Кожен інструмент PSPA пов'язаний і розміщений на своєму ресурсі PSPS-сервером системи PSPS, зареєстрованої в EPS, і містить елементи, які завантажуються та зберігаються у користувацькому пристрої зареєстрованого користувача, незалежно від того, чи зареєстрований

цей користувач у PSPS, пов'язаний з інструментом PSPA, чи ні. Кожен інструмент PSPS спрощує генерацію та отримання сигналів за даними про транзакцію, які відносяться до запитів на платіж від зареєстрованих користувачів, і до кредитових і/або дебетових рахунків зареєстрованих користувачів на підставі цих запитів. Завантажені елементи кожного інструменту PSPA містять модуль реєстрації та модуль створення віртуальної платіжної адреси (VPA). Модуль реєстрації дозволяє проводити реєстрацію користувацького пристрою у зареєстрованій PSPS, пов'язаний з інструментом PSPA, у взаємно-однозначній відповідності. Модуль створення VPA дозволяє зареєстрованому користувачу створювати унікальний VPA, який включає ідентифікацію PSPS, в якій зареєстрований цей користувач, і надалі надає можливість користувацькому пристрою відправляти унікальний VPA на локальний запам'ятовуючий пристрій системи PSPS, у якій зареєстрований користувач, в якості частини інформаційних даних про користувача від зареєстрованого користувача. UPI спрощує реєстрацію PSPS в EPS і надалі спрощує кероване вибіркове переміщення сигналів за даними про транзакцію між системами PSPS для здійснення платежу від одного зареєстрованого користувача до іншого зареєстрованого користувача в однакових або різних системах PSPS. UPI містить модуль розрахунків, який взаємодіє з множиною систем PSPS для періодичного співставлення кредитових і дебетових транзакцій та генерації інструкцій по чистому кредиту та дебету між зареєстрованими системами PSPS.

Нижче систему електронних платежів і спосіб їх здійснення за цим винаходом буде описано за допомогою супровідних матеріалів, на яких:

На Фіг. 1 представлено блок-схему системи електронних платежів (EPS) відповідно до одного варіанту здійснення цього винаходу;

На Фіг. 2A представлено схему, яка показує виконання транзакції за типом клієнт-клієнт з використанням EPS відповідно до одного варіанту здійснення цього винаходу, представленого на Фіг. 1;

На Фіг. 2B представлено схему, яка показує інший варіант виконання транзакції за типом клієнт-клієнт з використанням EPS відповідно до одного варіанту здійснення цього винаходу, представленого на Фіг. 1;

На Фіг. 3 представлено діаграму процесу виконання платіжної транзакції, здійснюваної у разі інкасованого платежу, що здійснюється за допомогою EPS, як показано на Фіг. 2A;

На Фіг. 4 представлено діаграму процесу, яка показує виконання платіжної транзакції, здійснюваної у разі прямого платежу, що здійснюється за допомогою EPS, як показано на Фіг. 2B;

На Фіг. 5 представлено діаграму процесу, яка показує платіжну транзакцію між водієм таксі та його пасажиром, здійснювану за допомогою EPS, як показано на Фіг. 1;

На Фіг. 6 представлено діаграму процесу, яка показує платіжну транзакцію з переказу платежу, здійснювану за допомогою EPS, як показано на Фіг. 1;

На Фіг. 7 представлено діаграму процесу, яка показує трибічну комерційну транзакцію, здійснювану між покупцем і продавцем, які мають однакову PSPS, відповідно до одного варіанту здійснення цього винаходу, представленого на Фіг. 1;

На Фіг. 8A, 8B, 8C, 8D і 8E представлено різні зображення, які відображаються на зареєстрованому користувацькому пристрої з використанням інструменту PSPA системи EPS, як показано на Фіг. 1.

Список позицій та їх позначень, використовуваних в описі та на графічних матеріалах:

Позиція	Позначення
1000	Система електронних платежів (EPS)
100, 500, 600, 700	Уніфікований платіжний інтерфейс (UPI)
100A	Модуль розрахунків
100b	Приймач
100c	Аналізатор
100d	Екстрактора ідентифікатора
100e	Передатчик
1002a	Оперативний запам'ятовуючий пристрій
1002b	Операційний процесор
1004	Система оператора платіжного сервісу (PSPS)
1004a	Локальний запам'ятовуючий пристрій
1004b	Щонайменше одна пошукова таблиця
1004c	PSPS-сервер
1006	Користувацький пристрій

Позиція	Позначення
1008	Інструмент Додатка оператора платіжного сервісу (PSPA)
1008a	Модуль реєстрації
1008b	Модуль створення віртуальної платіжної адреси (VPA)
102, 502, 702	Користувацький пристрій Отримувача платежу
104, 504, 604	Користувацький пристрій Платника
106, 506, 606	PSPS Отримувача платежу
108, 508, 608	PSPS Платника
110, 510, 610, 706	Банк-ремітент/Емітент/банк Платника
112, 512, 612, 708	Банк-бенефіціар/Еквайєр/банк Отримувача платежу
704	PSPS (загальні PSPS) Продавця/Покупця
710	Покупець

Нижче наведено опис цього винаходу з посиланням на супровідні графічні матеріали, які ілюструють, але не обмежують обсяг і сферу застосування цього винаходу. Цей опис наведено виключно в якості прикладу та ілюстрації.

5 Кілька років тому власникам банківських рахунків дозволялося використовувати свої дебетові/пластикові карти для здійснення грошових транзакцій тільки в авторизованих банкоматах, що належать банку власника рахунку. Зі збільшенням потреб користувачів, клієнтів і покупців банківських послуг було розроблено нову модель, яка передбачала розширення доступу до банкоматів, надаючи можливість власникам банківських рахунків використовувати банкомати, що належать будь-яким банкам. Нині будь-яка особа може використовувати будь-який банкомат по всьому світу, незалежно від свого конкретного банку. Це спрощує встановлення універсальної взаємної високої мобільності між банкоматами та дебетовими/пластиковими картами у різних мережах, які виконують обробку транзакцій та розрахунок коштів між учасниками транзакції.

15 У цьому винаході розглядається взаємодія банківських мобільних додатків і/або банківських Інтернет-порталів у разі здійснення платіжних транзакцій. Використовуючи систему за цим винаходом, користувачі і/або покупці банківських послуг не обмежені використанням Інтернет-порталів і/або мобільних Інтернет-сайтів банків, в яких вони тримають свій рахунок (рахунки). У той же час, користувачі (як платник, так і отримувач платежу) і/або покупці можуть вибирати Інтернет-портал або мобільний Інтернет-сайт будь-якого банку для здійснення своїх платіжних транзакцій, не знаючи реквізитів банківського рахунку іншого користувача/особи. Користувачам (платнику або отримувачу платежу) необхідно знати тільки унікальний ID або віртуальну платіжну адресу (VPA) для здійснення транзакцій у системі фінансових/електронних платежів.

20 Як показано на супровідних графічних матеріалах, на Фіг. 1 представлено блок-схему системи електронних платежів (1000) (що надалі називається EPS), яка спрощує здійснення платіжних транзакцій між множиною користувачів. Платіжні транзакції включають як фінансові, так і нефінансові транзакції, при цьому фінансові транзакції включають запити на інкасацію/pull-запити, запити на оплату/push-запити та комерційні платежі, а нефінансові транзакції включають реєстрацію мобільного банкінгу, генерацію одноразового пароля (OTP), установку або зміну PIN-коду, перевірку статусу транзакції, реєстрацію скарг і таке інше.

25 EPS (1000) містить оперативний запам'ятовуючий пристрій (1002a), операційний процесор (1002b), множину Систем операторів платіжного сервісу (PSPS), множину користувацьких пристроїв, інструменти Додатка оператора платіжного сервісу (PSPA), Уніфікований платіжний інтерфейс (UPI) (100).

35 Оперативний запам'ятовуючий пристрій (1002a) виконаний з можливістю зберігання набору заздалегідь заданих правил дій. Оперативний запам'ятовуючий пристрій (1002a) може включати будь-який машинопрочитуваний носій, відомий у цій галузі техніки, у тому числі, наприклад, енергозалежний запам'ятовуючий пристрій, такий як статичний запам'ятовуючий пристрій з довільною вибіркою (SRAM) і динамічний запам'ятовуючий пристрій з довільною вибіркою (DRAM), і/або енергонезалежний запам'ятовуючий пристрій, такий як постійний запам'ятовуючий пристрій (ROM), програмований ROM з можливістю електричного стирання, флеш-пам'ять, жорсткі диски, оптичні диски та стрічки для магнітного запису або хмарну систему зберігання (хмарне зберігання). В одному варіанті здійснення цього винаходу оперативний запам'ятовуючий пристрій (1002a) виконаний з можливістю зберігання заздалегідь заданих правил дій, які відносяться до транзакцій у системі електронних платежів, до передачі та прийому запитів на платіж і таке інше.

Операційний процесор (1002b) виконаний з можливістю взаємодії з оперативним запам'ятовуючим пристроєм (1002a) для прийому та обробки заздалегідь заданих правил дій

для отримання набору команд управління роботою системи. Операційний процесор (1002b) може бути реалізований у вигляді одного або більше мікропроцесорів, мікрокомп'ютерів, мікроконтролерів, цифрових сигнальних процесорів, центральних обчислювальних блоків, машин станів, логічних схем і/або будь-яких пристроїв, які оброблюють сигнали на підставі операційних інструкцій. Окрім інших функціональних можливостей, операційний процесор (1002b) виконаний з можливістю виклику та виконання заздалегідь заданого набору правил дій, який зберігається в оперативному запам'ятовуючому пристрої (1002a), для управління модулями EPS 1000.

Множина Систем операторів платіжного сервісу (PSPS) реєструються в EPS (1000) і виконані з можливістю реєстрації користувачів. Кожна PSPS (1004) містить локальний запам'ятовуючий пристрій (1004a), щонайменше одну пошукову таблицю (1004b) і PSPS-сервер (1004c). Локальний запам'ятовуючий пристрій (1004a) зберігає інформаційні дані про користувача, які відносяться до користувачів, зареєстрованих у PSPS (1004). В одному варіанті здійснення цього винаходу дані про користувача включають віртуальну платіжну адресу (VPA), дані облікового запису та інші нефінансові дані зареєстрованого користувача для спрощення автентифікації зареєстрованого користувача. Щонайменше одна пошукова таблиця (1004b) спрощує співставлення даних, введених покупцем, інформаційних даних про користувача та про зареєстрованого користувача.

Кожен користувацький пристрій (1006) з множини користувацьких пристроїв пов'язаний з одним із зареєстрованих користувачів і реєструється в якості частини інформаційних даних про користувача. Кожен із зареєстрованих користувачів використовує зареєстрований користувацький пристрій для генерації сигналів за даними про транзакцію, які відносяться до запитів на платежі за допомогою інструменту PSPA.

Кожен інструмент PSPA (1008) із інструментів PSPA пов'язаний і розміщений на своєму ресурсі PSPS-сервером (1004c) системи PSPS (1004), зареєстрованої у зазначеній EPS (1000), і містить елементи, які завантажуються та зберігаються у користувацькому пристрої (1006) зареєстрованого користувача, незалежно від того, чи зареєстрований цей користувач у PSPS, пов'язаний з інструментом PSPA (1008), чи ні. Кожен інструмент PSPS (1008) спрощує генерацію та прийом сигналів за даними про транзакцію, які відносяться до запитів на платіж, що поступають від вищезазначених зареєстрованих користувачів, і до кредитових і/або дебетових рахунків зареєстрованих користувачів на підставі цих запитів. Завантажувані елементи кожного інструменту PSPA (1008) містять модуль реєстрації (1008a) і модуль створення віртуальної платіжної адреси (VPA) (1008b). Модуль реєстрації (1008a) дозволяє проводити реєстрацію користувацького пристрою (1006) у зареєстрованій PSPS (1004), пов'язаній з інструментом PSPA (1008), у взаємно-однозначній відповідності. Модуль створення VPA (1008b) надає можливість зареєстрованому користувачу створювати унікальний VPA, який включає ідентифікацію PSPS, в якій зареєстрований цей користувач, і додатково надає можливість користувацькому пристрою (1006) передавати унікальний VPA на локальний запам'ятовуючий пристрій (1004a) системи PSPS (1004), в якій зареєстрований користувач, в якості частини інформаційних даних про користувача від зареєстрованого користувача.

UPI (100) спрощує реєстрацію PSPS (1004) в EPS (1000) і додатково спрощує кероване вибіркове переміщення сигналів за даними про транзакцію між системами PSPS для здійснення платежу від одного зареєстрованого користувача до іншого зареєстрованого користувача в однакових або різних системах PSPS. UPI (100) містить модуль розрахунків (100a), який взаємодіє з множиною систем PSPS для періодичного співставлення кредитових і дебетових транзакцій, і генерації інструкцій з чистого кредиту та дебету між зареєстрованими системами PSPS. В одному варіанті здійснення цього винаходу модуль розрахунків (100a) є сервером розрахунків.

Для того щоб спростити кероване переміщення даних про транзакцію, UPI (100) додатково містить приймач (100b), аналізатор (100c), екстрактор (100d) і передавач (100e). Приймач (100b) приймає сигнали за даними про транзакцію, які відносяться до запитів на платіж від зареєстрованих користувацьких пристроїв через будь-який з інструментів PSPA. Кожен запит на платіж містить VPA першого зареєстрованого користувача, VPA другого зареєстрованого користувача та суму транзакції, таким чином, ці VPA включають інформацію, яка відноситься до систем PSPS, в яких зареєстровані перший зареєстрований користувач і другий зареєстрований користувач. Аналізатор (100c) аналізує сигнали за даними про транзакцію для отримання проаналізованих сигналів. Потім за допомогою екстрактора ідентифікатора (100d) з проаналізованих сигналів отримується та ідентифікується інформація, яка відноситься до PSPS першого зареєстрованого користувача та до PSPS другого зареєстрованого користувача. Потім передавач (100e) передає сигнали за даними про транзакцію ідентифікованим відповідним

PSPS для того, щоб спростити списання кредитового платежу з рахунку першого зареєстрованого користувача на рахунок другого зареєстрованого користувача або зарахування дебетового платежу на рахунок першого зареєстрованого користувача з рахунку другого зареєстрованого користувача, у залежності від змісту цих проаналізованих сигналів.

5 На Фіг. 2A і 2B супровідних графічних матеріалів представлено схеми, які показують виконання транзакції за типом клієнт-клієнт з використанням UPI (100) для платіжних транзакцій. UPI (100) є інтерфейсом, що має множину серверів.

В одному варіанті здійснення цього винаходу UPI (100) має сервер транзакцій, сервер авторизації, UPI-сервер і сервер розрахунків. Сервер транзакцій оброблює сигнали за даними про транзакцію, сервер авторизації авторизує зареєстрованих користувачів, а UPI-сервер оброблює збережений набір правил дій для ідентифікації зареєстрованих систем PSPS. UPI (100) взаємодіє з банками на підставі інструкцій/запитів від PSPS, створених за допомогою інструментів PSPA. UPI (100) здійснює обробку транзакцій та розрахунків платежів. В одному варіанті здійснення цього винаходу обробка транзакцій виконується за допомогою сервера транзакцій. Розрахункові платежі між банками та системами PSPS здійснюються з використанням сервера розрахунків у кінці дня. В одному варіанті здійснення цього винаходу PSPS-сервер розміщує на своєму ресурсі інструмент PSPA, який може використовуватися зареєстрованими користувачами для передачі запитів на платіж. Запит на платіж може бути запитом на оплату/push-запитом або запитом на інкасацію/pull-запитом.

20 Запит на pull-платіж є запитом, за яким фізичній/юридичній особі необхідно інкасувати платіж від іншої фізичної/юридичної особи. Запит на push-платіж є запитом, за яким фізичній/юридичній особі необхідно заплатити певну суму іншій фізичній/юридичній особі. В одному варіанті здійснення цього винаходу етапи, які надають можливість користувачу здійснити push-платіж або pull-платіж, включають такі:

- 25 а. Реєстрація у PSPS;
- б. Реєстрація у мобільному банкінгу та генерація PIN-коду UPI для транзакцій (якщо до цього моменту він не був зареєстрований);
- в. Завантаження інструменту PSPA, наданого будь-яким PSPS, на користувацький пристрій, і створення профілю зареєстрованого користувача шляхом надання даних облікового запису за допомогою пароля/PIN-логіна з використанням інструменту PSPA;
- 30 д. Створення VPA в якості унікального ID з використанням інструменту PSPA так, щоб прив'язати VPA до будь-яких реквізитів банківського рахунку (рахунків) користувача, з використанням системи за цим винаходом; і
- е. Передача push-запитів або pull-запитів/даних про транзакцію за допомогою інструменту PSPA.

35 PSPS є банком, який надає інструмент PSPA і який може бути зареєстрований в EPS (1000) для того, щоб використовувати UPI (100). На вищезгаданому етапі "а" "реєстрації в PSPS" користувачі реєструються у банку на власний вибір шляхом відкриття рахунку у банку. Якщо користувач вже має рахунок у банку, він може зареєструватися у мобільному банкінгу, надавши необхідні дані, включаючи дані про свій користувацький пристрій, для того, щоб зареєструвати користувацький пристрій. Після завершення реєстрації, користувач може завантажувати інструменти PSPA, як зазначено на етапі "с" вище. Користувач (наприклад, платник або отримувач платежу) використовує свій користувацький пристрій для доступу до інструменту PSPA на власний вибір, незалежно від того, чи має він рахунок у банку, який надає інструмент PSPA. На етапі "d" користувач повинен створити VPA. Зображення створення VPA представлено на Фіг. 8A. Оскільки користувач зареєстрований у своєму банку, він надає такі самі дані для того, щоб користуватися інструментом PSPA. Номер рахунку користувача автоматично відображається на екрані створення VPA, як показано на Фіг. 8A. Таким чином, користувачу не потрібно пам'ятати реквізити свого рахунку. Потім користувачу пропонується створити новий VPA або використовувати зареєстровані ним VPA (якщо він створив VPA раніше). В одному варіанті здійснення цього винаходу, якщо користувач зареєстрований у банку "xyz", то його VPA має код розширення "@xyz". Правила дій з визначення коду розширення адрес VPA для конкретної PSPS визначаються UPI (100) і/або PSPS, що зберігається на UPI-сервері і/або на PSPS-сервері. Таким чином, VPA матиме ім'я користувача, вибране користувачем з кодом розширення, пов'язаним з PSPS, в якій користувач зареєстрований. Тому, у випадку "abc@xyz", "abc" є унікальним ім'ям/ім'ям користувача, обраним користувачем, а "xyz" є ім'ям PSPS користувача. Інші приклади включають Унікальне ім'я@HDFC, Унікальне ім'я@SBI, Унікальне ім'я@Corporation, Унікальне ім'я@PNB і таке інше. Потім користувач PSPS зберігає дані про свою VPA та інші нефінансові дані, створені з використанням інструменту PSPA, на локальному запам'ятовуючому пристрої PSPS. В одному варіанті здійснення цього винаходу

користувач реєструє, щонайменше в одному банку, такі дані облікового запису, як ім'я облікового запису користувача, номер облікового запису, номер Aadhaar (Aadhaar – унікальний персональний номер системи ідентифікації громадян і резидентів Індії), код IFSC (IFSC – код фінансової системи Індії) і таке інше, використовуючи інструмент PSPA, який потрібен для ідентифікації банківського рахунку користувача для здійснення платіжної транзакції. У разі успішного створення VPA, користувач може використовувати VPA під час передачі запитів на push-платіж або pull-платіж/даних про транзакцію за допомогою інструменту PSPA. Крім того, користувач також може використовувати Номер облікового запису разом з IFSC, номером Aadhaar, номером Aadhaar + номер IIN (IIN – об'єднана інформаційна мережа) і номером мобільного телефону, а також разом з ідентифікаційним номером платіжної системи "Мобільні гроші" (MMID), або разом тільки з номером свого мобільного телефону (у тому числі і в той момент, коли він підключений до системи) для оплати за допомогою UPI (100).

Після завершення процесу реєстрації та створення VPA користувачі (платники та одержувачі платежів) мають відповідні VPA. Для здійснення платіжних транзакцій платник або одержувач платежу використовує VPA/унікальний ID, не знаючи назв банків або реквізити банківського рахунку іншої особи. Дані VPA і банківські дані усіх користувачів підтримуються відповідними локальними запам'ятовувачими пристроями та оброблюються відповідними PSPS-серверами, і вони не повинні використовуватися спільно з UPI (100).

Платіжні транзакції включають транзакції інкасації (запит на інкасацію) і транзакції оплати (запит на оплату). Інструмент PSPA надає зареєстрованому користувачу різні опції на екрані дисплея його користувацького пристрою для здійснення платіжних транзакцій, як показано на Фіг. 8B. Для оплати платежу або отримання грошей користувач може вибирати будь-яку опцію з наступних: оплата на VPA, інкасування платежу з VPA, оплата з використанням QR-коду (QR-код – код швидкого реагування), оплата з використанням номера облікового запису в IFSC, оплата на Aadhaar, оплата на номер мобільного телефону. UPI (100) за допомогою інструменту PSPA також спрощує відстежування користувачем історії своїх транзакцій в UPI. Він також дозволяє користувачу управляти користувацькими VPA. Якщо користувач хоче управляти своїми VPA, він може вибрати опцію "управляти", що відображається на екрані, як показано на Фіг. 8B, у відповідь для користувача інструментом його PSPA відображається зображення, показане на Фіг. 8E. Потім користувач може вибрати: створення VPA, зміну існуючого VPA або видалення існуючого VPA.

Коли отримувач платежу хоче інкасувати гроші у платника (тобто Отримати гроші або здійснити Інкасовану транзакцію, або зробити запит на Інкасацію) (Фіг. 2A), отримувач платежу використовує користувацький пристрій отримувача платежу (102) для того, щоб отримати доступ і управління інструментом PSPA для надання VPA/унікального ID платника разом з сумою, яку отримувач хоче інкасувати у платника (етап 1). В одному варіанті здійснення цього винаходу зображення, що відображається для отримувача платежу, представлено на Фіг. 8D. Це зображення відображається у разі ініціації запиту на інкасацію (тобто "інкасувати з VPA", як показано на Фіг. 8B). У разі інкасації з VPA, VPA користувача/отримувача платежу завантажується автоматично, оскільки користувач вже зареєстрований. Потім отримувачу платежу необхідно ввести VPA платника, суму, яку необхідно інкасувати, і коментарі, якщо такі є. Отримувачу також надається опція електронної інкасації платежу негайно або в зазначений час. Як тільки запит на інкасацію відправляється, він перевіряється PSPS отримувача платежу (106). Перевірений запит спрямовується в UPI (100) разом із зареєстрованими банківськими реквізитами отримувача платежу та VPA/унікальним ID платника через PSPS отримувача платежу (106) (етап 2). UPI (100) ідентифікує PSPS платника (108) на підставі коду розширення VPA платника та відправляє запит на інкасацію до PSPS платника (108) (етап 3). PSPS платника (108) передає запит на інкасацію платнику через його інструмент PSPA з використанням користувацького пристрою платника (104). Платник приймає запит на інкасацію та надає дані автентифікації, якщо він згоден виконати запит на інкасацію, тобто, якщо він згоден сплатити запитувану суму отримувачу платежу. Платник проходить автентифікацію системою PSPS платника (108) перед здійсненням транзакції з використанням засобу автентифікації (на фігурах не показано). Засіб автентифікації включає PIN-код UPI, біометричне сканування, іридо-сканування та таке інше. Одне з підтверджень автентифікації надається платником для продовження транзакції. Банківські реквізити платника, зареєстровані в інструменті PSPA платника та PSPS платника (108), за допомогою користувацького пристрою платника (104) передаються на UPI-сервер (100) (етап 4). Тепер в UPI (100) є банківські реквізити як платника, так і отримувача платежу на підставі їх адрес VPA/унікальних ID. UPI (100) використовує банківські реквізити для зв'язку з банком-ремітентом (110) (тобто, з банком-платником) і для дебетування бажаної суми (етап 5 і 6), а потім для зв'язку з банком-

бенефіціаром (112) (тобто, з банком отримувача платежу) для кредитування цієї суми для того, щоб завершити транзакцію (етап 7 і 8). Після успішної транзакції UPI (100) відправляє інформацію про успішну транзакцію інструментам PSPA отримувача платежу (етап 9a, 9b і 10) і платника, до яких отримали доступ користувацький пристрій отримувача платежу (102) і користувацький пристрій платника (104) відповідно, при цьому вікно з даними про транзакцію спливає на дисплеях відповідних користувацьких пристроїв за допомогою відповідних інструментів PSPA.

Виконання транзакції у зв'язку із запитом на інкасацію/pull-запитом включає наступні етапи (Фіг. 3):

Етап 301 – Отримувач платежу ініціює транзакцію за допомогою інструменту свого PSPA на користувацькому пристрої отримувача платежу (102).

Етап 302 – Користувацький пристрій отримувача платежу (102) ініціює запит на Інкасацію у PSPS отримувача платежу (106).

Етап 303 – PSPS отримувача платежу (106) перевіряє дані отримувача платежу та перевіряє автентифікацію першого фактора.

Етап 304 – PSPS отримувача платежу (106) відправляє запит на Інкасацію в UPI (100).

Етап 305 – UPI (100) оброблює адресу платника двома способами:

a. Якщо адреса має глобальні ідентифікатори (наприклад, номер Мобільного телефону, унікальний ID, номер облікового запису та таке інше), то PSPS робить запит UPI (100) про повідомлення у черзі за допомогою інтерфейсу прикладного програмування (API) за цим номером мобільного телефону або за номером Aadhaar, або за номером облікового запису та IFSC.

b. Якщо Адреса має віртуальну адресу, запропоновану PSPS платника (108), то UPI (100) відправляє запит у PSPS платника (108) на трансляцію адреси.

Етап 306 – У випадку етапу 305b PSPS платника (108) відправляє повідомлення платнику, який приймає або відхиляє запит на підставі правил дій, встановлених на його стороні.

Етап 307 – У випадку етапу 305b, у разі ухвалення запиту на Інкасацію, PSPS платника (108) ініціює запит на користувацький пристрій платника (104) на введення підтверджень автентифікації платника. Платник надає підтвердження автентифікації на користувацькому пристрої платника (104).

Етап 308 – У випадку етапу 305b PSPS платника (108) завантажує дані платника та відповідає UPI (100).

Етап 309 – UPI (100) відправляє дебетовий запит на дебетування рахунку постачальника (110).

Етап 310 – Постачальник рахунку автентифікує Платника на підставі наданих підтверджень.

Етап 311 – Постачальник рахунку дебетує рахунок Платника.

Етап 312 – Постачальник рахунку відправляє Дебетову відповідь у UPI (100).

Етап 313 – UPI (100) відправляє Кредитовий запит постачальнику кредитового рахунку (112).

Етап 314 – Постачальник рахунку кредитує рахунок на підставі даних Отримувача платежу.

Етап 315 – Постачальник рахунку відправляє Кредитову відповідь у UPI (100).

Етап 316 – UPI (100) відправляє Підтверджувальну відповідь у PSPS платника (108).

Етап 317 – UPI (100) відправляє відповідь на платіж у PSPS отримувача платежу (106).

Етап 318 – PSPS отримувача платежу (106) повідомляє отримувача платежу.

Коли платник хоче відправити гроші отримувачу платежу (тобто, Сплатити гроші або Сплатити транзакцію, або зробити Push-запит) (Фіг. 2B), платник використовує користувацький пристрій платника (104) для того, щоб отримати доступ і управління інструментом PSPA для надання авторизованого VPA отримувача платежу разом з сумою, яку платник хоче відправити отримувачу платежу (етап 1). В одному варіанті здійснення цього винаходу зображення, яке відображається для отримувача платежу, представлене на Фіг. 8C. Це зображення відображається у разі ініціації push-запиту/запиту на оплату (тобто "Сплатити на VPA", як показано на Фіг. 8B). Під час оплати на VPA, VPA користувача/платника завантажується автоматично, оскільки користувач вже зареєстрований в інструменті PSPA з даними про свою PSPS. Потім платнику необхідно ввести VPA отримувача платежу, суму, яку необхідно інкасувати, і коментарі, якщо такі є. Після відправлення запиту на оплату, платник може бути автентифікований PSPS платника (108) перед здійсненням транзакції з використанням засобу автентифікації. Засіб автентифікації включає PIN-код UPI, біометричне сканування, іридо-сканування та таке інше. Одне з підтверджень автентифікації надається платником. Автентифікація платника спрямовується в UPI (100) разом із зареєстрованими банківськими реквізитами платника та VPA отримувача платежу за допомогою PSPS платника (108) (етап 2). UPI (100) ідентифікує PSPS отримувача платежу (106) на підставі коду розширення VPA

отримувача платежу та відправляє запит на PSPS отримувача платежу (106) (етап 3). PSPS отримувача платежу (106) авторизує банківські реквізити, зареєстровані в інструменті PSPA отримувача платежу, у PSPS отримувача платежу (106) за допомогою користувацького пристрою отримувача платежу (102), і повертає банківські реквізити на UPI-сервер (100) (етап 4). Тепер у UPI (100) є банківські реквізити як платника, так і отримувача платежу на підставі їх адрес VPA/унікальних ID. UPI (100) використовує банківські реквізити для зв'язку з банком-ремітентом (110) (тобто, з банком платника) і дебетування бажаної суми (етап 5 і 6), а потім для зв'язку з банком-бенефіціаром (112) (тобто, з банком отримувача платежу) для кредитування цієї суми для того, щоб завершити транзакцію (етап 7 і 8). Після успішної транзакції, UPI (100) відправляє інформацію про успішну транзакцію інструментам PSPA платника (етап 9а, 9б і 10) і отримувача платежу, до яких отримали доступ користувацький пристрій платника (104) і користувацький пристрій отримувача платежу (102) відповідно, при цьому вікно з даними про транзакцію спливає на дисплеях відповідних користувацьких пристроїв за допомогою відповідних інструментів PSPA.

У кінці дня, коли усі фінансові та нефінансові транзакції завершені, UPI (100) виконує розрахунок усіх платіжних транзакцій, які були здійснені між усіма системами PSPS, зареєстрованими в EPS (1000). В одному варіанті здійснення цього винаходу платник використовує інструмент PSPA, який відрізняється від інструменту PSPA отримувача платежу. В іншому варіанті здійснення цього винаходу платник використовує такий самий інструмент PSPA, що й отримувач платежу.

Виконання транзакції у зв'язку із запитом на оплату/push-запитом включає наступні етапи (Фіг. 4):

Етап 401 – Платник ініціює транзакцію за допомогою інструменту свого PSPA на користувацькому пристрої платника (104).

Етап 402 – Платник надає підтвердження автентифікації на користувацькому пристрої платника (104).

Етап 403 – Користувацький пристрій платника (104) ініціює запит на Оплату у PSPS платника (108).

Етап 404 – PSPS платника (108) перевіряє дані платника та перевіряє автентифікацію першого фактора.

Етап 405 – PSPS платника (108) відправляє запит на оплату в UPI (100).

Етап 406 – UPI (100) оброблює Адресу платника наступними двома способами:

а. Якщо адреса має глобальні ідентифікатори (наприклад, номер Мобільного телефону, унікальний ID, номер облікового запису та таке інше), то адреса отримувача платежу може бути оброблена центральним картографом UPI (100).

б. Якщо адреса має віртуальну адресу, запропоновану PSPS отримувача платежу (106), то UPI (100) відправляє запит у PSPS отримувача платежу (106) на трансляцію адреси.

Етап 407 – у випадку 406b PSPS отримувача платежу (106) приймає або відхиляє запит на підставі правил дій, встановлених на його стороні.

Етап 408 – у випадку 406b, у разі ухвалення запиту на Оплату, PSPS отримувача платежу (106) завантажує дані платника та відповідає UPI (100).

Етап 409 – UPI (100) відправляє дебетовий запит на дебетування рахунку постачальника (114).

Етап 410 – Постачальник рахунку автентифікує Платника на підставі наданих підтверджень.

Етап 411 – Постачальник рахунку дебетує рахунок Платника.

Етап 412 – Постачальник рахунку відправляє Дебетову відповідь у UPI (100).

Етап 413 – UPI (100) відправляє Кредитовий запит постачальникові кредитового рахунку (112).

Етап 414 – Постачальник рахунку кредитує рахунок на підставі даних Одержувача платежу.

Етап 415 – Постачальник рахунку відправляє Кредитову відповідь у UPI (100).

Етап 416 – UPI (100) відправляє Підтверджувальну відповідь у PSPS отримувача платежу (106).

Етап 417 – UPI (100) відправляє відповідь на платіж у PSPS платника (108).

Етап 418 – PSPS платника (108) повідомляє платника.

EPS (1000) використовує різні способи автентифікації. В одному варіанті здійснення цього винаходу EPS (1000) використовує спосіб двофакторної автентифікації з одним кліком, як показано у Таблиці 1 нижче:

Таблиця 1

Автентифікація	Реєстрація	Авторизовано	Транзакція	Авторизовано
1-й фактор	Мобільний пристрій/Номер (вихідне зашифроване SMS-повідомлення)	PSPS	Відбиток пристрою	PSPS
2-й фактор	OTP	Емітент	PIN-код UPI або біометричні характеристики	Емітент

В одному варіанті здійснення цього винаходу кожна PSPS (1004) містить модуль автентифікації (на фігурах не показано), виконаний з можливістю забезпечення двохфакторної автентифікації. Модуль автентифікації містить автентифікатор першого фактора та автентифікатор другого фактора. Автентифікатор першого фактора приймає заздалегідь зареєстрований унікальний номер, формує користувача, зареєстрованого у PSPS (1004), для перевірки та зв'язку зареєстрованого користувача із зареєстрованим користувацьким пристроєм (1006) шляхом співставлення прийнятого від зареєстрованого користувача заздалегідь зареєстрованого унікального номера з інформаційними даними про користувача, які зберігаються на локальному запам'ятовуючому пристрої (1004a), таким чином забезпечуючи перший фактор автентифікації. Автентифікатор другого фактора виконаний з можливістю прийому PIN-коду UPI і/або біометричних характеристик, введених зареєстрованим користувачем, для автентифікації зареєстрованого користувача шляхом співставлення прийнятого PIN-коду UPI і/або введених біометричних характеристик з інформаційними даними про користувача, таким чином забезпечуючи автентифікацію другого фактора.

Як видно з Таблиці 1, для автентифікації першого фактора під час реєстрації в інструменті PSPA зашифроване SMS-повідомлення ініціюється користувацьким пристроєм/мобільним телефоном користувача та передається у PSPS, в якій зареєстрований користувач. PSPS перевіряє унікальний номер (номер мобільного телефону або міжнародний ідентифікатор апаратури мобільного зв'язку (IMEI) і таке інше) користувацького пристрою (цей унікальний номер заздалегідь зберігається в якості інформаційних даних про користувача за допомогою PSPS під час реєстрації користувача) і зв'язує унікальний номер з обліковим записом користувача. Якщо покупець зареєстрований у мобільному банкінгу, то він використовуватиме свій PIN-код UPI або біометричні характеристики у автентифікації другого фактора. Якщо покупець хоче зареєструватися у мобільному банкінгу, то він може встановити PIN-код UPI, використовуючи останні 6 цифр дебетової карти та дату закінчення терміну дебетової карти разом з OTP, створеним Емітентом, або будь-які інші аналогічні відповідні перевіірочні дані. У подальшій транзакції відбиток пристрою може використовуватися для авторизації системою PSPS. Під час автентифікації другого фактора PIN-код UPI або біометричні характеристики запитуються у користувача, авторизованого Емітентом у подальшій транзакції, для автентифікації користувача.

Фіг. 5 супровідних графічних матеріалів показує діаграму виконання, яка ілюструє платіжну транзакцію, що здійснюється між водієм таксі та його пасажиром. У типовому варіанті здійснення система за цим винаходом використовується водієм таксі для інкасації оплати за послуги, надані їм своєму пасажирові/покупцю. Коли таксі прибуває на місце призначення, водій таксі (у даному випадку отримувач платежу) може використовувати свій користувацький пристрій (502), щоб отримати/інкасувати платіж (плату за послуги таксі) від пасажирів з використанням системи за цим винаходом. Пасажир надає свій VPA, який вводиться водієм таксі в інструмент PSPA отримувача платежу разом із запитом на інкасування на користувацькому пристрої водія таксі (502). VPA разом з даними рахунку водія таксі надається UPI (500) системою PSPS (506) водія таксі (отримувача платежу) (етап 51). UPI (500) ідентифікує PSPS/банк пасажирів (платника) за допомогою VPA і направляє запит на інкасацію у PSPS пасажирів (508) (етап 52). PSPS пасажирів (508) відправляє повідомлення про запит на інкасацію інструменту PSPA пасажирів на користувацькому пристрої пасажирів (504) (етап 53) на підставі того, які підтвердження автентифікації надаються пасажиром для ухвалення запиту на інкасацію (етап 54). В одному варіанті здійснення цього винаходу автентифікація надається шляхом введення PIN-коду UPI з використанням інструменту PSPA на користувацькому пристрої пасажирів (504). Після отримання підтвердження від пасажирів (отримувача платежу)

PSPS пасажир (508) перевіряє дані про пасажирів та відправляє фінансові дані UPI (500) для дебетування банківського рахунку пасажирів (платників) (етап 55). Потім дебетовий запит відправляється PSPS/банку пасажирів (ремітенту) (510) і запитувана сума списується за дебетом з банківського рахунку пасажирів (ремітенту) (510) (етап 56 і 57) за допомогою UPI (500). Потім UPI (500) відправляє кредитовий запит PSPS водія таксі/банку (бенефіціару) (512) на кредитування потрібної суми (етап 58) і отримує повідомлення про успішне кредитування від PSPS водія таксі/банку (бенефіціара) (512) про успішне кредитування (етап 59). Потім підтвердження про успішну транзакцію передається за допомогою UPI (500) пасажирів (платників) (етап 50a) і водію таксі (отримувачу платежу) (50b) за допомогою інструментів своїх відповідних PSPA.

EPS (1000) за цим винаходом може використовуватися постачальником (доставка їжі, доставка одягу та таке інше) для того, щоб уникнути проблем, пов'язаних з оплатою готівкою у разі доставки (COD). Вона забезпечує двофакторну автентифікацію з одним кліком, при цьому транзакція може бути авторизована шляхом введення тільки PIN-коду UPI.

На Фіг. 6 наведено діаграму виконання, яка показує платіжну транзакцію з переказу грошей, здійснювану за допомогою EPS (1000), яка використовується відправником (платником) для здійснення push-платежу. Відправник використовує свій користувацький пристрій (604) для введення запиту на оплату, включаючи VPA отримувача (отримувача платежу) і PIN-код UPI банку-емітента разом з сумою, яка має бути відправлена до банку отримувача (етап 61). Потім реквізити рахунку відправника, PIN-код UPI і VPA отримувача надаються UPI (600) за допомогою PSPS відправника (608) з використанням інструменту свого PSPA (етап 62). UPI (600) ідентифікує дестриптор/дані PSPS отримувача (отримувача платежу/бенефіціара) і відправляє запит на оплату у PSPS отримувача (606) (етап 63). PSPS отримувача (606) відповідає на фінансову адресу бенефіціара (тобто фінансову адресу отримувача платежу) (етап 64). На підставі відповіді UPI (600) відправляє реквізити рахунку відправника (платника) і PIN-код разом з дебетовим запитом у PSPS/банк відправника (610) (етап 65) і отримує успішну дебетову відповідь (етап 66). У разі отримання дебетової відповіді UPI (600) відправляє кредитовий запит у PSPS/банк отримувача/отримувача платежу (612) (етап 67) і отримує успішну кредитову відповідь (етап 68). Потім підтвердження про успішну транзакцію відправляється у PSPS отримувача/отримувача платежу (етап 69) і відправнику за допомогою PSPS (608) відправника та його користувацького пристрою (604) (етап 60).

Платник /відправник/продавець і отримувач платежу/отримувач/покупець можуть мати однакові PSPS. На Фіг. 7 наведено діаграму виконання, яка показує трибічну комерційну транзакцію між покупцем і продавцем, у яких є однакова PSPS. Покупець (710) зареєстрований в UPI (700) системи за цим винаходом за допомогою інструменту PSPA на своєму користувацькому пристрої (702). Оскільки PSPS (704) покупця та продавця однакові, то віртуальні адреси як продавця, так і покупця доступні у PSPS (704). Коли запит (push-запит або pull-запит) виконується з використанням інструменту PSPA, то запит відправляється в PSPS (704), який (у даному випадку) є загальним як для продавця, так і для покупця (етап 71). В одному варіанті здійснення цього винаходу запит містить довідковий ID (VPA користувача), суму та ID продавця. Оскільки віртуальні адреси доступні в PSPS (704), то фінансові адреси, що лежать в основі віртуальних адрес, надаються в UPI (700) за допомогою PSPS (704) (етап 72). Потім UPI (700) відправляє дебетовий запит емітенту/PSPS платника/банку (706) (етап 73) і приймає дебетову відповідь (етап 74) на підставі push-запиту або pull-запиту. Потім UPI (700) відправляє кредитовий запит еквайєру/PSPS отримувача платежу/банку (708) (етап 75) і отримує відповідь про успішний кредит від еквайєра/PSPS/банка отримувача платежу (708) (етап 76). UPI (700) передає успішну транзакцію користувачу за допомогою його користувацького пристрою (702) з використанням PSPS (704) (етап 77 і 78).

Цей винахід передбачає спосіб здійснення електронних платежів, який спрощує здійснення платіжних транзакцій між множиною користувачів. Цей спосіб включає наступні етапи:

- зберігання в оперативному запам'ятовуючому пристрої набору заздалегідь заданих правил дій;
- обробка операційним процесором заздалегідь заданих правил дій для отримання набору команд управління роботою системи;
- реєстрація користувачів у множині Систем операторів платіжного сервісу (PSPS), виконаних з можливістю реєстрації в Системі електронних платежів (EPS) (1000), причому кожна PSPS включає наступні етапи:
 - зберігання на локальному запам'ятовуючому пристрої інформаційних даних про користувача, які відносяться до користувачів, зареєстрованих у PSPS,

- спрощення за допомогою щонайменше однієї пошукової таблиці співставлення даних, введених покупцем, інформаційних даних про користувача та про зареєстрованого користувача, і

- надання PSPS-сервера;

5 - прив'язування кожного користувацького пристрою з множини користувацьких пристроїв до одного з зареєстрованих користувачів і реєстрація в якості частини інформаційних даних про користувача;

10 - зв'язування та розміщення на своєму ресурсі кожного інструменту Додатка оператора платіжного сервісу (PSPA) з множини інструментів PSPA за допомогою PSPS-сервера системи PSPS, зареєстрованої в EPS, і зберігання елементів, що завантажуються та зберігаються у користувацькому пристрої зареєстрованого користувача, незалежно від того, чи зареєстрований цей користувач у PSPS, пов'язаний з інструментом PSPA, чи ні, і додаткове спрощення за допомогою кожного інструменту PSPA генерації та прийому сигналів за даними про транзакцію, які відносяться до запитів на платіж від зареєстрованих користувачів, а також до кредитових і/або дебетових рахунків зареєстрованих користувачів на підставі запитів, причому

15 завантажувані елементи кожного інструменту PSPA включають етапи:

- дозвіл, за допомогою модуля реєстрації, реєстрації користувацького пристрою у зареєстрованій PSPS, пов'язаний з інструментом PSPA, у взаємно-однозначній відповідності, і

20 - надання можливості, за допомогою модуля створення віртуальної платіжної адреси (VPA), зареєстрованому користувачу створити унікальний VPA, який включає ідентифікацію PSPS, в якій зареєстрований цей користувач, і додаткове надання можливості користувацькому пристрою передавати унікальний VPA на локальний запам'ятовуючий пристрій PSPS, в якій користувач зареєстрований, в якості частини інформаційних даних про користувача від зареєстрованого користувача;

25 і

- спрощення, за допомогою Уніфікованого платіжного інтерфейсу (UPI), реєстрації PSPS в EPS і керованого вибіркового переміщення сигналів за даними про транзакцію між системами PSPS для здійснення платежу від одного зареєстрованого користувача до іншого зареєстрованого користувача в однакових або різних системах PSPS, причому, UPI включає

30 етапи:

- надання модуля розрахунків, виконаного з можливістю взаємодії з множиною систем PSPS для періодичного співставлення кредитових і дебетових транзакцій та генерації інструкцій з чистого кредиту та дебету між зареєстрованими системами PSPS.

UPI додатково включає наступні етапи:

35 - прийом отримувачем сигналів за даними про транзакцію, які відносяться до запитів на платіж від зареєстрованих користувацьких пристроїв за допомогою будь-якого з інструментів PSPA, причому кожен запит містить VPA першого зареєстрованого користувача, VPA другого зареєстрованого користувача та суму транзакції;

40 - аналіз аналізатором сигналів за даними про транзакцію для отримання проаналізованих сигналів,

- отримання та ідентифікацію з проаналізованих сигналів, за допомогою екстрактора ідентифікатора, інформації, яка відноситься до PSPS першого зареєстрованого користувача та PSPS другого зареєстрованого користувача,

45 - передача передавачем сигналів за даними про транзакцію ідентифікованим відповідним системам PSPS для спрощення списання кредитового платежу з рахунку першого зареєстрованого користувача на рахунок другого зареєстрованого користувача або зарахування дебетового платежу на рахунок першого зареєстрованого користувача з рахунку другого зареєстрованого користувача, вибірково, на підставі змісту цих проаналізованих сигналів.

50 Кожна PSPS додатково містить етап надання двохфакторної автентифікації модулем автентифікації. Етап надання двохфакторної автентифікації включає наступні етапи:

55 - прийом, за допомогою автентифікатора першого фактора, заздалегідь зареєстрованого унікального номера від користувача, зареєстрованого в PSPS, для перевірки та зв'язку зареєстрованого користувача із зареєстрованим користувацьким пристроєм шляхом співставлення прийнятого від зареєстрованого користувача заздалегідь зареєстрованого унікального номера з інформаційними даними про користувача, що зберігаються на локальному запам'ятовуючому пристрої, таким чином забезпечуючи автентифікацію першого фактора, і

- прийом, за допомогою автентифікатора другого фактора, PIN-коду UPI і/або біометричних характеристик, введених зареєстрованим користувачем, для автентифікації зареєстрованого користувача шляхом співставлення прийнятого PIN-коду UPI і/або введених біометричних

характеристик з інформаційними даними про користувача, таким чином забезпечуючи автентифікацію другого фактора.

Навіть якщо покупець і продавець використовують однакову PSPS, вони обоє можуть мати безліч різних інструментів PSPA на своїх користувацьких пристроях. Для прикладу, Набір інструментальних засобів розробки програм (SDK) PSPA вбудований в інструмент PSPA продавця, і різні інструменти PSPA доступні покупцеві. У тому випадку, коли продавець має намір/створює запит, на користувацькому пристрої клієнта відображаються усі інструменти UPI PSPA з тим, щоб покупець міг вибрати однаковий з продавцем інструмент PSPA. Як показано на Фіг. 7, у даному прикладі віртуальні адреси як продавця, так і покупця також доступні у PSPS, а транзакція відбувається так само, як описано вище.

EPS (1000), передбачена у цьому винаході, може використовуватися Реальними магазинами/Продавцями для здійснення транзакцій, включаючи оплату Постачальникам овочевої продукції, плату за Продукти в магазині, оплату за проїзд у Таксі/Автомобілі/Автобусі/Поїзді/оплату за Авіапереліт, оплату у Ресторанах/Магазинах/за Заправку бензину, оплату за навчання різним Учбовим закладам, оплату за Проїзд у пунктах збору мита під час подорожей, оплату Постачальникам молочної продукції/Рознощикам газет, пожертвування Довірчому фонду/Храму/Фонду взаємодопомоги/НБО, оплату у Торговому центрі та таке інше. EPS (1000) також може використовуватися для здійснення оплати комунальних послуг, включаючи оплату різних рахунків, таких як рахунки за електрику, воду, телефон, кредитну карту та таке інше, для виставлення та оплати рахунків за ремонт квартири, для виставлення та оплати рахунків за навчання в школі, для сплати страхової премії, погашення кредиту у розстрочку, погашення автокредиту за допомогою зовнішнього інтерфейсу комп'ютера (EMI) і таке інше.

Крім того, онлайн-продавці також можуть використовувати EPS (1000) для здійснення транзакцій в Електронній комерції, включаючи COD-платежі, для платежів у Вбудованому додатку (In-App), в онлайн-трейдингу, за мобільне поповнення рахунку за газетним оголошенням з використанням додатка "Scan N Pay", в Електронній комерції (Інкасація/Оплата) – Платіж за допомогою UPI після оформлення замовлення, для платежів за бронювання квитків у кіно та таке інше. Крім того, вона також може використовуватися для здійснення транзакцій у разі Безпосереднього з'єднання двох пристроїв для переказу грошей (як Оплата, так і Отримання грошей), для платежів фізичній особі/друзям, для розділення рахунків з друзями, для виплати заробітної плати водієві, для платежів на номер Aadhaar/номер мобільного телефону на підставі внутрішнього переказу на інший банківський рахунок.

Цей винахід, описаний вище, має ряд технічних переваг, включаючи, але не обмежуючись цим, реалізацію системи електронних платежів, яка:

- спрощує відправлення та отримання грошей простим способом з використанням користувацьких пристроїв;
- забезпечує уніфікований платіжний інтерфейс (UPI);
- надає можливість користувачу отримувати/інкасувати платежі з рахунків причетних фізичних/юридичних осіб;
- проста у користуванні, як для платників, так і для отримувачів платежів;
- надає можливість здійснення платіжних транзакцій між платником і отримувачем платежу без необхідності обов'язкового надання банківської інформації та реквізитів банківського рахунку один одного;
- надає можливість користувачу відправляти та отримувати гроші за допомогою віртуальної платіжної адреси;
- забезпечує безпечне здійснення платежів на підставі єдиного/унікального ідентифікатора;
- усуває ризик зберігання віртуальної адреси покупця, як на картках;
- може використовуватися покупцями, які не мають кредитної/дебетової карти;
- підходить для Електронної комерції та Мобільної комерції;
- вирішує проблему інкасації COD;
- забезпечує можливість здійснення платежів за покупки у Вбудованому додатку (IAP);
- забезпечує конфіденційність шляхом спільного використання тільки Віртуальної адреси та ніякої іншої конфіденційної інформації;
- спрощує встановлення багатьох утиліт у разі оплати готівкою під час доставки/ у разі розділення/спільного використання рахунків/у разі оплати/переказу грошей продавцеві;
- авторизує транзакцію шляхом введення тільки PIN-коду UPI або біометричних характеристик, або ID користувача (UID), або шляхом проведення іридо-сканування та таке інше; і

- працює за допомогою різних інтерфейсів, де запит на платіж може бути згенерований на Інтернет-інтерфейсі та авторизований на Мобільному інтерфейсі (App).

Варіанти здійснення цього винаходу та різні ознаки й детальний опис їх переваг пояснюються з посиланням на необмежуючі варіанти здійснення цього винаходу, представлені у вищенаведеному описі. Детальний опис добре відомих компонентів і способів обробки опущені у цьому документі, щоб надмірно не ускладнювати розуміння варіантів здійснення цього винаходу. Використовувані у цьому документі приклади призначені лише для спрощення розуміння способів практичної реалізації варіантів здійснення цього винаходу та для додаткового надання фахівцями у цій галузі техніки можливості практичної реалізації варіантів здійснення винаходу, описаних у цьому документі. Відповідно, ці приклади не слід тлумачити як такі, що обмежують об'єм варіантів здійснення винаходу, описаних у цьому документі.

Наведений вище опис конкретних варіантів здійснення цього винаходу настільки повно розкриває загальний характер варіантів здійснення винаходу, описаних у цьому документі, що інші можуть, застосовуючи знання існуючого рівня техніки, легко модифікувати і/або адаптувати для різних застосувань такі конкретні варіанти здійснення цього винаходу, не відходячи від загальної концепції, і, отже, такі адаптації та модифікації слід тлумачити згідно з сенсом і серією еквівалентів розкритих варіантів здійснення цього винаходу. Слід розуміти, що використовувана у цьому документі фразеологія або термінологія призначена для опису, а не для обмеження. Таким чином, хоча варіанти здійснення винаходу описані у цьому документі з точки зору переважних варіантів здійснення цього винаходу, фахівці у цій галузі техніки зрозуміють, що варіанти здійснення винаходу, описані у цьому документі, можуть бути практично реалізовані з модифікацією у межах суті та обсягу варіантів здійснення винаходу, які описані у цьому документі.

ФОРМУЛА ВИНАХОДУ

1. Система електронних платежів (EPS) (1000) для спрощення здійснення платіжних транзакцій між множиною користувачів, яка містить:

множину систем операторів платіжного сервісу (PSPS), виконаних з можливістю реєстрації користувачів і з додатковою можливістю реєстрації у зазначеній EPS (1000), причому кожна PSPS (1004) містить:

локальний запам'ятовуючий пристрій (1004a), виконаний з можливістю зберігання інформаційних даних про користувача, які належать до користувачів, зареєстрованих у зазначеній PSPS (1004),

щонайменше одну пошукову таблицю (1004b), виконану з можливістю спрощення співставлення даних, введених покупцем, інформаційних даних про користувача та про зареєстрованого користувача, і PSPS-сервер (1004c);

множину користувацьких пристроїв, причому кожен користувацький пристрій (1006) зв'язаний з одним з вищезгаданих зареєстрованих користувачів і зареєстрований як частина інформаційних даних про користувача;

множину інструментів додатка оператора платіжного сервісу (PSPA), причому кожен інструмент PSPA (1008) зв'язаний та розміщений на своєму ресурсі PSPS-сервером (1004c) системи PSPS (1004), зареєстрованої в EPS (1000), і містить елементи, які завантажуються та зберігаються в користувацькому пристрої (1006) зареєстрованого користувача,

кожен інструмент PSPA (1008) виконаний з можливістю забезпечення доступу зареєстрованого користувача до зазначеного інструменту (1008) незалежно від того, чи він тримає рахунок у банку, який надає інструмент PSPA з додатковою можливістю для того, щоб дозволити вказаному користувачеві використовувати зазначений інструмент (1008) для передачі або прийому запитів на платіж, причому

кожен інструмент PSPA (1008) виконаний з можливістю спрощення генерації та прийому сигналу за даними про транзакцію, які належать до запитів на платежі від зазначених зареєстрованих користувачів, а також до кредитових і/або дебетових рахунків зазначених зареєстрованих користувачів на підставі зазначених запитів, причому

зазначені завантажувані елементи кожного інструменту PSPA (1008) містять:

модуль реєстрації (1008a), виконаний з можливістю дозволу реєстрації користувацького пристрою (1006) у зареєстрованій PSPS (1004), пов'язаний з інструментом PSPA (1008), у взаємно-однозначній відповідності, і

модуль створення віртуальної платіжної адреси (VPA) (1008b), виконаний з можливістю створення для зареєстрованого користувача унікального VPA, який містить ідентифікацію PSPS, в якій зареєстрований цей користувач, і вказаний VPA пов'язаний з реквізитами банківського

рахунку (рахунків) користувача, при цьому вказаний модуль (1008b) створення VPA додатково надає можливості користувацькому пристрою (1006) передавати зазначений унікальний VPA на локальний запам'ятовуючий пристрій (1004a) системи PSPS (1004), в якій користувач зареєстрований, як частини інформаційних даних про користувача від зареєстрованого користувача;

уніфікований платіжний інтерфейс (UPI) (100), виконаний з можливістю спрощення реєстрації PSPS (1004) у зазначеній EPS (1000) і з додатковою можливістю спрощення керованого вибіркового переміщення сигналів за даними про транзакцію між системами PSPS для здійснення платежу від одного зареєстрованого користувача до іншого зареєстрованого користувача в однакових або різних системах PSPS, причому зазначений UPI (100) містить: модуль розрахунків (100a), виконаний з можливістю взаємодії з зазначеною множиною систем PSPS для періодичного співставлення кредитових і дебетових транзакцій і генерації інструкцій з чистого кредиту та дебету між зареєстрованими системами PSPS, оперативний запам'ятовуючий пристрій (1002a), виконаний з можливістю зберігання набору заздалегідь заданих правил дій, причому зазначений набір заздалегідь визначених правил належить до транзакцій в системі електронних платежів, передачі та прийому запитів на платіж; операційний процесор (1002b), виконаний з можливістю взаємодії із зазначеним оперативним запам'ятовуючим пристроєм (1002a) для прийому та обробки зазначених заздалегідь заданих правил дій для отримання набору команд управління роботою системи для роботи із зазначеними модулями.

2. Система (1000) за п. 1, яка **відрізняється** тим, що зазначений UPI (100) додатково містить: приймач (100b), виконаний з можливістю прийому сигналів за даними про транзакцію, які належать до запитів на платежі від зареєстрованих користувацьких пристроїв за допомогою будь-якого з інструментів PSPA, причому кожен запит містить VPA першого зареєстрованого користувача, VPA другого зареєстрованого користувача та суму транзакції; аналізатор (100c), виконаний з можливістю аналізу зазначених сигналів за даними про транзакцію для отримання проаналізованих сигналів; екстрактор ідентифікатора (100d), виконаний з можливістю отримання та ідентифікації з проаналізованих сигналів інформації, яка належить до PSPS першого зареєстрованого користувача та до PSPS другого зареєстрованого користувача; і передавач (100e), виконаний з можливістю передачі зазначених сигналів за даними про транзакцію ідентифікованим відповідним системам PSPS для спрощення списання кредитового платежу з рахунку першого зареєстрованого користувача на рахунок другого зареєстрованого користувача або зарахування дебетового платежу на рахунок першого зареєстрованого користувача з рахунку другого зареєстрованого користувача, вибірково, на підставі змісту даних проаналізованих сигналів.

3. Система (1000) за п. 1, яка **відрізняється** тим, що кожна PSPS (1004) додатково містить модуль автентифікації, виконаний з можливістю надання двофакторної автентифікації, який містить:

автентифікатор першого фактора, виконаний з можливістю прийому заздалегідь зареєстрованого унікального номера, від зареєстрованого користувача у вищезгаданій PSPS (1004) для перевірки та зв'язку зареєстрованого користувача із зареєстрованим користувацьким пристроєм (1006) шляхом співставлення прийнятого від зареєстрованого користувача заздалегідь зареєстрованого унікального номера з інформаційними даними про користувача, які зберігаються на зазначеному локальному запам'ятовуючому пристрої (1004a), таким чином забезпечуючи автентифікацію першого фактора, і

автентифікатор другого фактора, виконаний з можливістю прийому PIN-коду UPI і/або біометричних характеристик, введених зареєстрованим користувачем, для автентифікації зареєстрованого користувача шляхом співставлення прийнятого PIN-коду UPI і/або введених біометричних характеристик з вищезгаданими інформаційними даними про користувача, таким чином забезпечуючи автентифікацію другого фактора.

4. Система (1000) за п. 2, яка **відрізняється** тим, що зазначений UPI (100) додатково містить сервер транзакцій для обробки сигналів за даними про транзакцію, сервер авторизації для авторизації користувача та UPI-сервер для обробки збереженого набору правил дій для ідентифікації зареєстрованих систем PSPS.

5. Спосіб здійснення електронних платежів для спрощення здійснення платіжних транзакцій між множиною користувачів, який включає наступні етапи:

реєстрація користувачів у множині систем операторів платіжного сервісу (PSPS) для реєстрації у системі електронних платежів (EPS) (1000), причому кожна PSPS включає наступні етапи:

зберігання на локальному запам'ятовуючому пристрої інформаційних даних про користувача, які належать до користувачів, зареєстрованих у зазначеній PSPS;
спрощення за допомогою щонайменше однієї пошукової таблиці співставлення даних, введених покупцем, інформаційних даних про користувача та про зареєстрованого користувача, і

5 надання PSPS-сервера;

зв'язування кожного користувацького пристрою з множини користувацьких пристроїв з одним із зазначених зареєстрованих користувачів і реєстрація як частини інформаційних даних про користувача;

10 зв'язування та розміщення на своєму ресурсі кожного інструменту додатка оператора платіжного сервісу (PSPA) з множини інструментів PSPA за допомогою PSPS-сервера системи PSPS, зареєстрованої у зазначеній EPS, вказаними інструментами PSPA зберігання елементів, які завантажуються та зберігаються в користувацькому пристрої зареєстрованого користувача, кожен інструмент PSPA виконаний з можливістю забезпечення зареєстрованому користувачеві доступу до зазначеного інструменту (1008) незалежно від того, чи він тримає рахунок у банку,
15 який надає інструмент PSPA, і додатково виконаний з можливістю дозволу зазначеному користувачу використовувати зазначений інструмент (1008) для передачі або прийому запитів на платіж і додаткове спрощення генерації та прийому сигналів за даними про транзакцію, які належать до вказаних запитів на платежі від зазначених зареєстрованих користувачів, а також до кредитових і/або дебетових рахунків зазначених зареєстрованих користувачів на підставі зазначених запитів, причому зазначені завантажувані елементи кожного інструменту PSPA включають наступні етапи:

дозвіл, за допомогою модуля реєстрації, реєстрації користувацького пристрою у зареєстрованій PSPS, пов'язаний з інструментом PSPA, у взаємно-однозначній відповідності, і

25 надання можливості, за допомогою модуля створення віртуальної платіжної адреси (VPA), зареєстрованому користувачу створювати унікальний VPA, який містить ідентифікацію PSPS, в якій зареєстрований цей користувач, пов'язуючи зазначений VPA з даними банківського рахунку (рахунків) користувача, і додаткове надання можливості користувацькому пристрою передавати вищезгаданий унікальний VPA на локальний запам'ятовуючий пристрій системи PSPS, в якій користувач зареєстрований, як частину інформаційних даних про користувача від зареєстрованого користувача;

спрощення, за допомогою уніфікованого платіжного інтерфейсу (UPI), реєстрації PSPS у зазначеній EPS і керованого вибіркового переміщення сигналів за даними про транзакцію між системами PSPS для здійснення платежу від одного зареєстрованого користувача до іншого зареєстрованого користувача в однакових або різних системах PSPS, причому UPI включає наступний етап:

надання модуля розрахунків для взаємодії із зазначеною множиною систем PSPS для періодичного співставлення кредитових і дебетових транзакцій та генерації інструкцій з чистого кредиту та дебету між зареєстрованими системами PSPS.

6. Спосіб за п. 5, який **відрізняється** тим, що зазначений UP1 додатково включає:

40 прийом отримувачем сигналів за даними про транзакцію, які належать до запитів на платежі від зареєстрованих користувацьких пристроїв за допомогою будь-якого з інструментів PSPA, причому кожен запит містить VPA першого зареєстрованого користувача, VPA другого зареєстрованого користувача та суму транзакції;

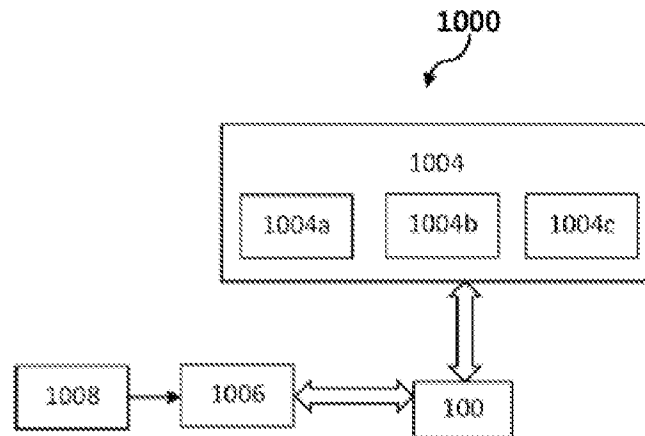
45 аналіз аналізатором зазначених сигналів за даними про транзакцію для отримання проаналізованих сигналів, отримання та ідентифікація з проаналізованих сигналів, за допомогою екстрактора ідентифікатора, інформації, яка належить до PSPS першого зареєстрованого користувача і PSPS другого зареєстрованого користувача, передачу передавачем зазначених сигналів за даними про транзакцію ідентифікованим відповідним системам PSPS для спрощення списання кредитового платежу з рахунку першого зареєстрованого користувача на рахунок другого зареєстрованого користувача або зарахування дебетового платежу на рахунок першого зареєстрованого користувача з рахунку другого зареєстрованого користувача, вибірково, на підставі змісту цих проаналізованих сигналів.

7. Спосіб за п. 5, який **відрізняється** тим, що кожна PSPS додатково включає

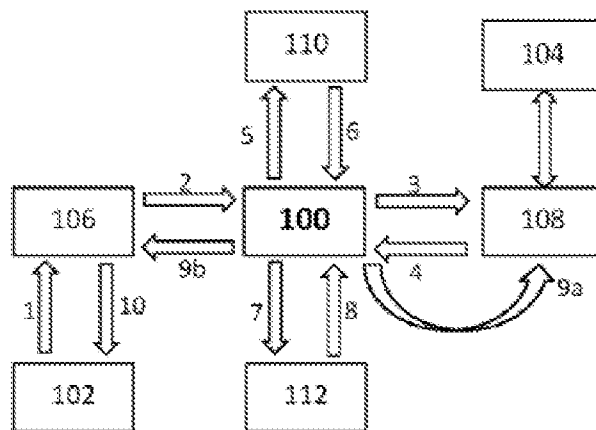
55 забезпечення двофакторної автентифікації модулем автентифікації, причому зазначений етап забезпечення двофакторної автентифікації включає наступні етапи:

прийом, за допомогою автентифікатора першого фактора, заздалегідь зареєстрованого унікального номера від користувача, зареєстрованого у зазначеній PSPS, для перевірки та зв'язку зареєстрованого користувача із зареєстрованим користувацьким пристроєм, шляхом співставлення прийнятого від зареєстрованого користувача заздалегідь зареєстрованого унікального номера з інформаційними даними про користувача, які зберігаються на

- 5 зазначеному локальному запам'ятовуючому пристрої, таким чином забезпечуючи автентифікацію першого фактора, і прийом, за допомогою автентифікатора другого фактора, PIN-коду і/або біометричних характеристик, введених зареєстрованим користувачем, для автентифікації зареєстрованого користувача шляхом співставлення прийнятого PIN-коду і/або введених біометричних характеристик з зазначеними інформаційними даними про користувача, таким чином забезпечуючи автентифікацію другого фактора.



Фіг. 1



Фіг. 2A

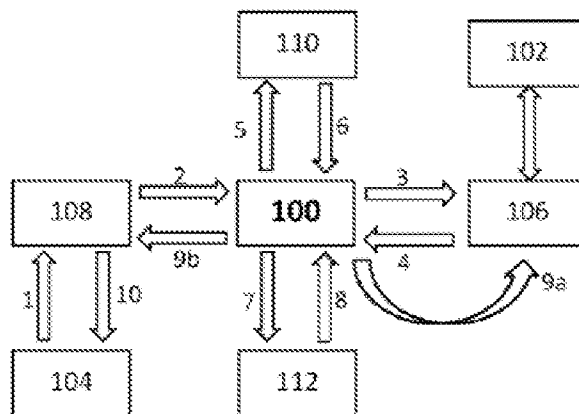


Fig. 2B

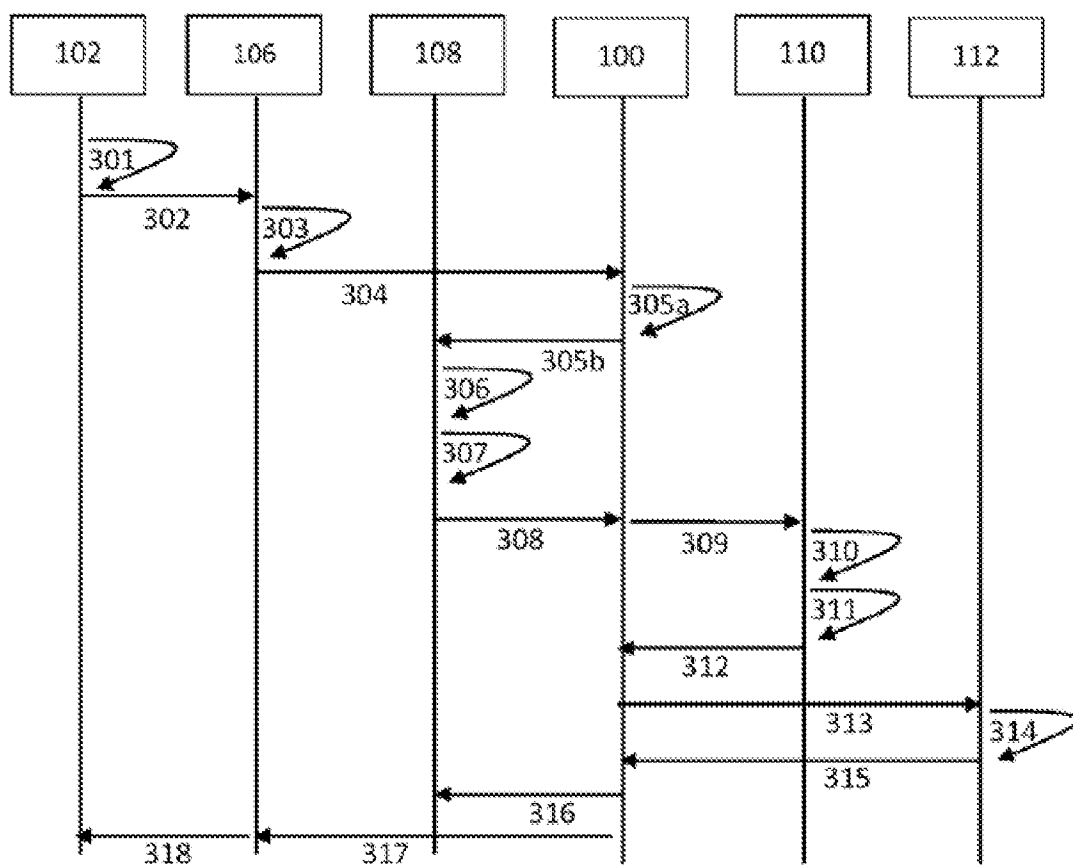


Fig. 3

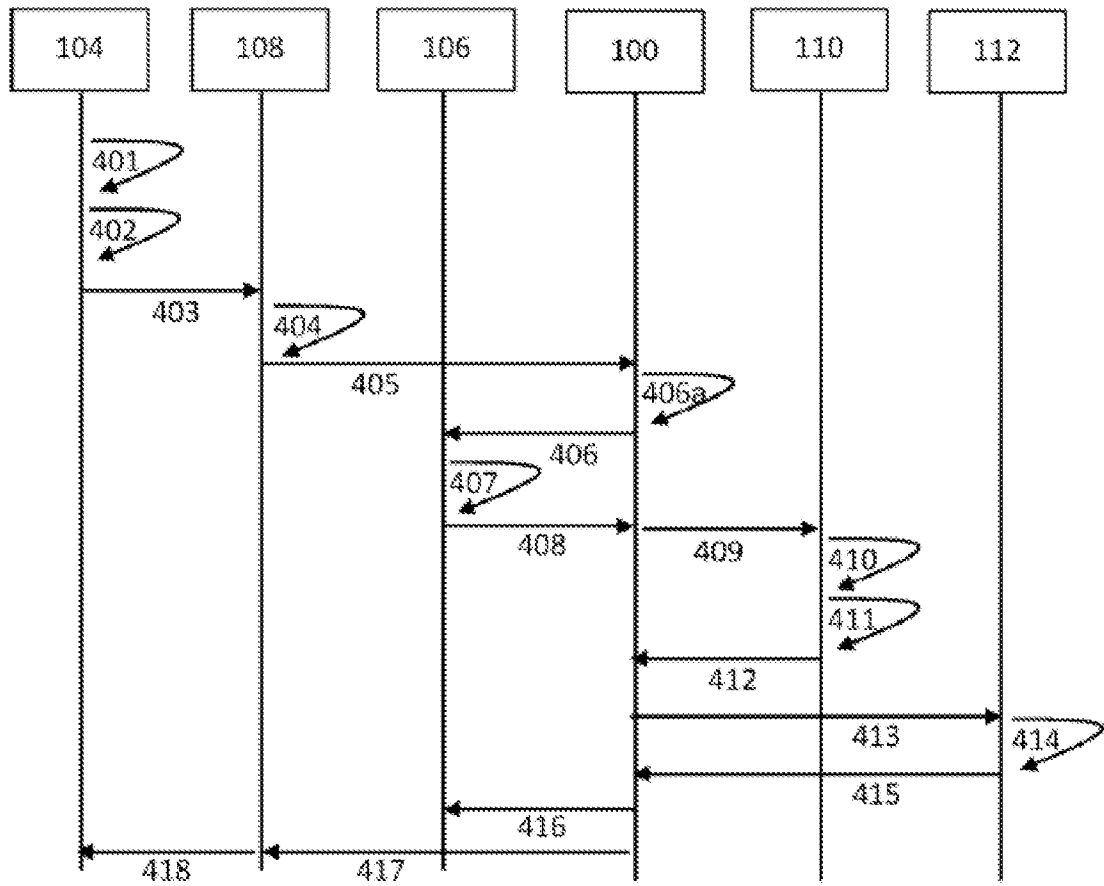


Fig. 4

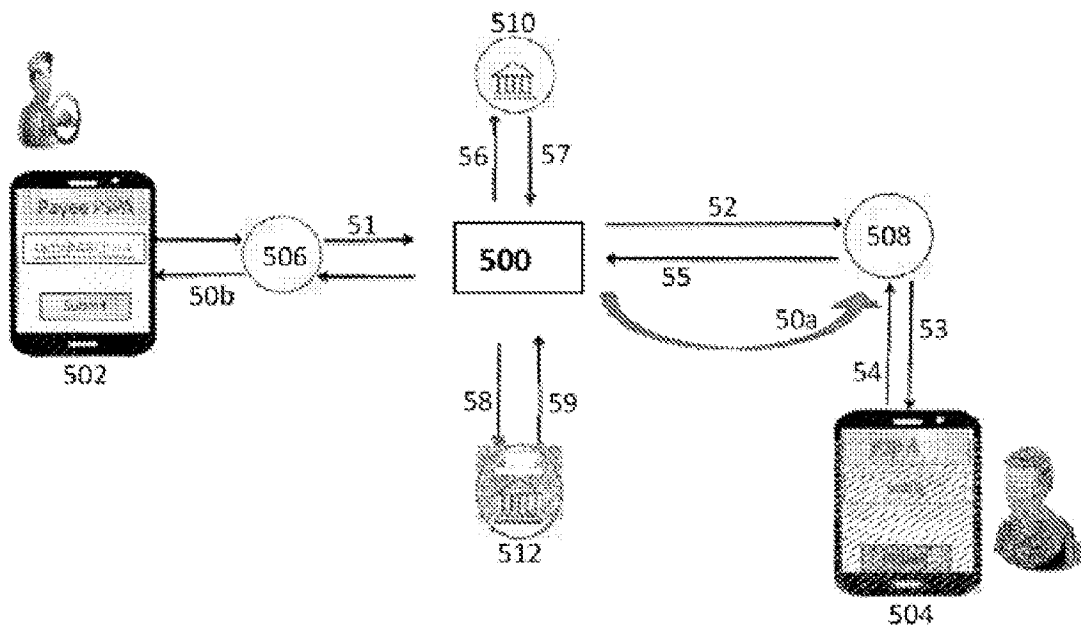
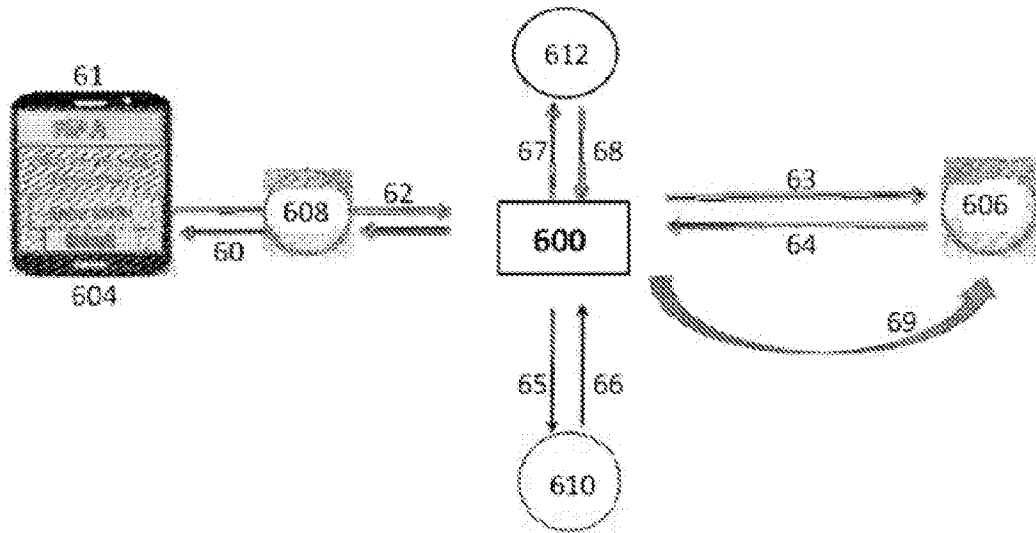
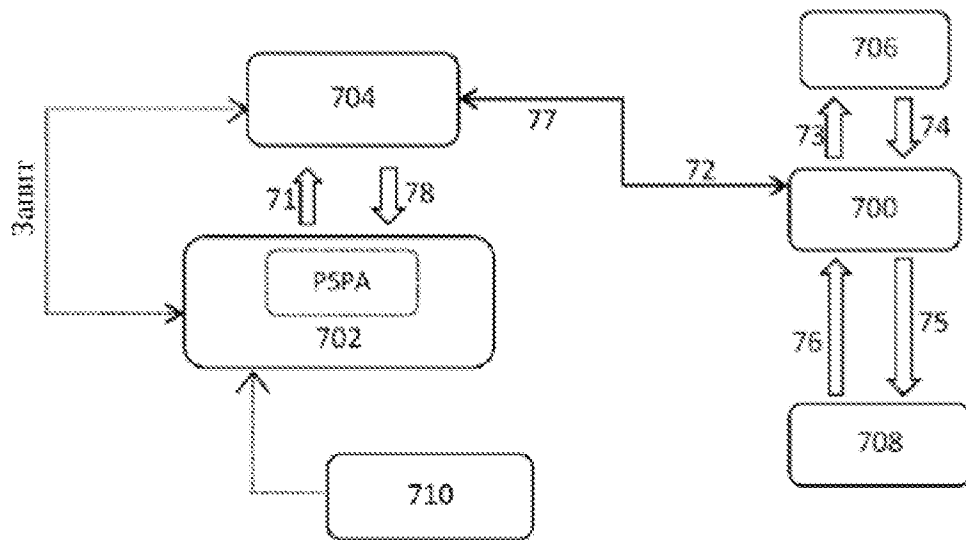


Fig. 5



Фіг. 6



Фіг. 7