



УКРАЇНА

(19) UA (11) 50483 (13) A

(51) G 07 F 19/00, G 07 F 7/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВИНАХІДвидається під
відповідальність
власника
патенту

(54) СПОСІБ ЗДІЙСНЕННЯ ПЛАТЕЖІВ З ВИКОРИСТАННЯМ ЦИФРОВИХ СЕРТИФІКАТІВ (ВАРІАНТИ)

1

(21) 2002010572

(22) 23 01 2002

(24) 15 10 2002

(46) 15 10 2002, Бюл. № 10, 2002 р.

(72) Кандауров Євген Валентинович

(73) Кандауров Євген Валентинович

(57) 1 Спосіб здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцеві цифрового сертифіката як платіжного засобу та перевірку продавцем дійсності цифрового сертифіката, який відрізняється тим, що як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, яку передають продавцю разом з адресою комірки збереження цифрової купюри, до якої продавець повинен передати здачу, а перевірку продавцем дійсності цифрової купюри здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після перевірки дійсну цифрову купюру розмінюють на цифрову купюру покупця та цифрову купюру продавця, після чого повертають обидві купюри продавцю та залишають у продавця цифрову купюру, що йому належить, а цифрову купюру покупця передають за адресою комірки збереження цифрової купюри, потім передають цифрову купюру покупця до системи банків цифрових купюр, де її перевіряють на дійсність, дійсну цифрову купюру обмінюють на нову цифрову купюру покупця, яку повертають до комірки збереження цифрової купюри, після чого з неї надсилають покупцеві шифроване повідомлення про здійснені операції.

2 Спосіб за п 1, який відрізняється тим, що перевірку дійсності цифрової купюри здійснюють по базі дійсних цифрових купюр у банку цифрових купюр.

3 Спосіб за п 1, який відрізняється тим, що при розміні цифрової купюри спочатку генерують замість переданої цифрової купюри цифрову купюру покупця та цифрову купюру продавця, сумарний номінал яких дорівнює номіналу переданої купюри, після чого заносять цифрову купюру покупця та цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

2

4 Спосіб за п 1, який відрізняється тим, що при обміні цифрової купюри покупця спочатку генерують замість переданої цифрової купюри нову цифрову купюру покупця, номінал якої дорівнює номіналу переданої цифрової купюри покупця, після чого заносять нову цифрову купюру покупця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

5 Спосіб за п 1, який відрізняється тим, що шифроване повідомлення про здійснені операції надсилають покупцеві через термінал продавця.

6 Спосіб за п 1, який відрізняється тим, що шифроване повідомлення про здійснені операції надсилають безпосередньо покупцеві.

7 Спосіб здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцеві цифрового сертифіката як платіжного засобу та перевірку продавцем дійсності цифрового сертифіката, який відрізняється тим, що як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, та спочатку передають продавцеві адресу комірки збереження цифрової купюри та повідомляють номінал цифрової купюри, яку покупець бажає отримати, потім передають запит від продавця за вказаною адресою комірки збереження цифрової купюри, з якої, при наявності необхідної суми, надсилають продавцеві запит ключа доступу, потім від продавця передають запит покупцеві, від якого передають ключ доступу продавцеві, та потім, від нього, до комірки збереження цифрової купюри, після чого з неї передають цифрову купюру до системи банків цифрових купюр, де її розмінюють на цифрову купюру продавця і цифрову купюру покупця, потім повертають обидві цифрові купюри до комірки збереження цифрової купюри, де залишають цифрову купюру покупця, потім передають продавцеві цифрову купюру продавця, а перевірку продавцем дійсності цифрової купюри, що йому передана, здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після перевірки дійсну цифрову купюру обмінюють на нову цифрову купюру продавця, яку повертають продавцеві, після чого з комірки збереження цифрової купюри надсилають покупцеві

(13) A

(11) 50483

(19) UA

шифроване повідомлення про здійснені операції

8 Спосіб за п 7, який **відрізняється** тим, що як ключ доступу використовують одноразовий ключ доступу

9 Спосіб за будь-яким з пп 7 або 8, який **відрізняється** тим, що при розміні цифрової купюри спочатку генерують замість переданої цифрової купюри цифрову купюру покупця та цифрову купюру продавця, сумарний номінал яких дорівнює номіналу переданої купюри, після чого заносять цифрову купюру покупця та цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр

10 Спосіб за будь-яким з пп 7 або 8, який **відрізняється** тим, що перевірку дійсності цифрової купюри здійснюють по базі дійсних цифрових купюр у банку цифрових купюр

11 Спосіб за будь-яким з пп 7 або 8, який **відрізняється** тим, що при обміні цифрової купюри продавця спочатку генерують замість переданої цифрової купюри продавця нову цифрову купюру продавця, номінал якої дорівнює номіналу переданої цифрової купюри продавця, після чого заносять нову цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру продавця вилучають з бази дійсних цифрових купюр у банку цифрових купюр

12 Спосіб за п 7, який **відрізняється** тим, що шифроване повідомлення про здійснені операції над-

силають покупцеві через термінал продавця

13 Спосіб за п 7, який **відрізняється** тим, що шифроване повідомлення про здійснені операції надсилають безпосередньо покупцеві

14 Спосіб здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцеві цифрового сертифіката як платіжного засобу та перевірку продавцем дійсності цифрового сертифіката, який **відрізняється** тим, що як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, яку передають продавцю, а перевірку продавцем дійсності цифрової купюри здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після перевірки дійсну цифрову купюру обмінюють на нову цифрову купюру, потім повертають продавцеві нову цифрову купюру

15 Спосіб за п 14, який **відрізняється** тим, що перевірку дійсності цифрової купюри здійснюють по базі дійсних цифрових купюр у банку цифрових купюр

16 Спосіб за п 14, який **відрізняється** тим, що при обміні цифрової купюри спочатку генерують замість переданої цифрової купюри нову цифрову купюру, номінал якої дорівнює номіналу переданої цифрової купюри, після чого заносять нову цифрову купюру до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр

Винахід належить до повних банківських систем, зокрема до способів здійснення готівкових платежів. Спосіб за даним винаходом може бути використаний як альтернатива для розрахунків, які здійснюють готівкою за допомогою паперових купюр, монет, векселів, тощо

З рівня техніки відомо спосіб оплати товарів і послуг за допомогою готівки, а також кредитних карток як платіжних інструментів, які є альтернативою готівці

Використання кредитних карток при оплаті товарів і послуг "на місці" та через інтернет має наступні недоліки

1 При здійсненні покупки "на місці", власник кредитної картки повинен пред'явити її у установі продавця. При цьому інформація яку несе кредитна картка (номер, термін дії картки тощо) може бути у подальшому використана працівниками установи продавця у корисливих цілях

2 При здійсненні покупки через мережу інтернет, власник кредитної картки повинен надати данні про номер картки, термін її дії та інші відомості для можливості перевірки дійсності цієї картки. Ця інформація, теж може бути незаконно використана власниками сайту у корисливих цілях

Також, з рівня техніки, відомо безпечні способи організації віддалених покупок та покупок "на місці"

Прикладом може бути платіжна система E-

cash, що розроблена голландською фірмою Digi-Cash і призначена для проведення інтернет платежів, та як альтернатива готівці

Відомо платіжна система Mondex, яка призначена для здійснення розрахунків електронною готівкою. У системі Mondex носієм платіжного засобу є запрограмована смарт-карта. Недоліком цієї системи є те, що її реалізація дуже дорого коштує, а саме, покупцю необхідно придбати смарт-карту, а продавцю пристрій для обробки та зчитування інформації з смарт-карти. Це призводить до багато мільярдних витрат на реалізацію цієї системи

Також відомо система PayCash, яка розроблена банком "Тавричним" та групою компаній "Алкор" (Санкт-Петербург, Росія) у 1998 році. Система PayCash задумана як засіб проведення платежів у рамках всесвітньої мережі Інтернет

Традиційні платіжні системи, будучи дуже недосконалим засобом здійснення платежів поза Інтернетом, перестають відповідати більшості вимог, пропонованих до них, як тільки ці системи починають застосовуватися в Інтернеті

Шість головних недоліків традиційних платіжних систем стосовно до Інтернету

неприйнятна ризикованість,

відсутність приватності,

низька швидкість транзакції в порівнянні із середньою швидкістю передачі в Інтернеті звичайної інформації,

складність,
висока собівартість транзакції,
суттєві обмеження за допомогою традиційних платіжних систем можливо проводити тільки мікроплатежі, які є збитковими, у зв'язку з чим, ведення певних видів електронної комерції, заснованих на мікроплатежах, є абсолютно нерациональним

Результати спроб модифікації традиційних платіжних систем за допомогою створення "Інтернет-побридів" - наприклад, онлайн-ових систем "банк-клієнт", авторизаційних центрів, і ін. - не витримують ні економічної, ні технічної критики

навіть після модифікації безпека систем залишається неприйнятно низькою в порівнянні з можливими фінансовими втратами,

приватність не може бути забезпечена належною мірою,

не може бути досягнута висока швидкість здійснення платежів,

алгоритм здійснення платежів залишається занадто складним,

собівартість транзакції в модифікованих системах залишається вкрай високою,

здійснення мікроплатежів продовжує залишатися нерациональним через збитковість таких операцій

У силу домінування в Інтернеті традиційних платіжних систем, електронна комерція щомісяця втрачає мільйони доларів упущеного прибутку

Найбільш близьким до винаходу є спосіб проведення платежів через систему PayCash (www.paycash.kiev.ua), який включає передачу покупцем продавцю цифрового сертифікату як платіжного засобу, перевірку продавцем дійсності цифрового сертифікату та повідомлення покупця про проведення операції

В основі системи PayCash лежить технологія електронної (цифрової) готівки, запропонована Девідом Чаумом (David Chaum, система "eCash") Електронна (цифрова) готівка - це грошові зобов'язання на пред'явника, що емітовані банківською чи іншою структурою у формі електронних (цифрових) сертифікатів, що можуть бути використані для розрахунків через мережу Інтернет і забезпечуються звичайними грошовими коштами на момент пред'явлення зобов'язання його емітенту

З погляду користувача (продавця чи покупця), система PayCash - це сукупність електронних Гаманців, кожний з яких є захищеною клієнтською програмою, що дозволяє переказувати і одержувати електронну готівку з інших Гаманців, зберігати її в Інтернет-банку, конвертувати, виводити із системи на банківські рахунки чи в інші платіжні системи, тощо

Здійсненні розрахунків через систему PayCash проводять наступним чином

1 Гаманець продавця відсилає Гаманцю покупця вимогу заплатити, що містить підписаний електронним цифровим підписом текст договору

2 Гаманець покупця пред'являє своєму хазяїну текст договору Якщо покупець погоджується платити (при достатній кількості грошей у покупця), то Гаманець покупця відправляє Гаманцю продавця електронні гроші і підписаний електронним цифровим підписом покупця договір

3 Гаманець продавця приймає платежі тільки на підставі договорів, переданих потенційним покупцям Для Гаманця можна визначити період протягом якого він буде приймати платежі по відсланих договорах Таким чином Магазин може видаляти зі своєї бази даних застарілі неоплачені замовлення Після перевірки цих умов Гаманець магазину відсилає електронні гроші в банк для авторизації

5 Банк, одержавши електронні гроші від продавця, проводить їхню авторизацію й, у випадку успіху, зараховує відповідну суму грошей на рахунок продавця в системі PayCash Повідомлення про це передається продавцю разом з електронним чеком для покупця

6 Одержавши відповідь з банку, Гаманець продавця передає магазину дані авторизації і повідомлення про успішне зарахування грошей на рахунок продавця Електронний чек з банку передається Гаманцю покупця

Зазначений спосіб має такі недоліки

По-перше, для того, щоб стати учасником, покупцю, необхідно мати спеціальне устаткування (комп'ютер) та програмне забезпечення (сучасний оглядач WWW (Internet Explorer, Netscape Navigator версії 3.0 чи новіший та програму розпакування ZIP-архівів)

По-друге, платіжним засобом у цьому способі є цифровий банківський сертифікат, що у загальному понятті є електронною цифровою готівкою, яка забезпечена звичайними грошовими коштами Носієм цифрового банківського сертифікату є електронний Гаманець Недоліком цього платіжного засобу є те, що він залежить від свого носія як фізичного, так і програмного

Крім того, спосіб забезпечує проведення платежів у рамках всесвітньої мережі Інтернет Тобто застосування способу обмежується тільки Інтернетом та цей спосіб є не придатним для здійснення покупок "на місці"

В основу винаходу поставлена задача створити спосіб здійснення готівкових платежів з використанням платіжних засобів інших ніж готівка, який би забезпечував надійну захищеність приватних платежів, забезпечував розрахунки платіжними засобами незалежними від свого носія як фізичного, так і програмного та виключав необхідність наявності у покупця програмного забезпечення і спеціального устаткування, крім того забезпечував здійснення платежів як у всесвітній мережі Інтернет так і "на місці"

Поставлена задача вирішується тим, що у першому варіанті способу здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцю цифрового сертифікату як платіжного засобу та перевірку продавцем дійсності цифрового сертифікату, згідно з винаходом як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, яку передають продавцю разом з адресою комірки збереження цифрової купюри, до якої продавець повинен передати задачу, а перевірку продавцем дійсності цифрової купюри здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після переві-

рки, дійсну цифрову купюру розмінюють на цифрову купюру покупця та цифрову купюру продавця, після чого повертають обидві купюри продавцю, та залишають у продавця цифрову купюру, що йому належить, а цифрову купюру покупця передають за адресою комірки збереження цифрової купюри, потім передають цифрову купюру покупця до системи банків цифрових купюр, де її перевіряють на дійсність, дійсну цифрову купюру обмінюють на нову цифрову купюру покупця, яку повертають до комірки збереження цифрової купюри, після чого з неї надсилають покупцеві шифроване повідомлення про здійснені операції.

У першому варіанті способу перевірку дійсності цифрової купюри можуть здійснювати по базі дійсних цифрових купюр у банку цифрових купюр.

Крім того, за першим варіантом способу, при розміні цифрової купюри спочатку генерують замість переданої цифрової купюри цифрову купюру покупця та цифрову купюру продавця, сумарний номінал яких дорівнює номіналу переданої купюри, після чого заносять цифрову купюру покупця та цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

Додатково, за першим варіантом способу, при обміні цифрової купюри покупця спочатку генерують замість переданої цифрової купюри нову цифрову купюру покупця, номінал якої дорівнює номіналу переданої цифрової купюри покупця, після чого заносять нову цифрову купюру покупця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

Крім того, у першому варіанті способу, шифроване повідомлення про здійснені операції можуть надсилати покупцеві через термінал продавця або безпосередньо покупцю.

У другому варіанті способу поставлена задача вирішується тим, що у способі здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцеві цифрового сертифікату як платіжного засобу та перевірку продавцем дійсності цифрового сертифікату, згідно з винаходом як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, та спочатку передають продавцеві адресу комірки збереження цифрової купюри та повідомляють номінал цифрової купюри яку покупець бажає отримати, потім передають запит від продавця за вказаною адресою комірки збереження цифрової купюри, з якої, при наявності необхідної суми, надсилають продавцеві запит ключа доступу, потім від продавця передають запит покупцеві, від якого передають ключ доступу продавцеві, та потім, від нього, до комірки збереження цифрової купюри, після чого з неї передають цифрову купюру до системи банків цифрових купюр, де її розмінюють на цифрову купюру продавця і цифрову купюру покупця, потім повертають обидві цифрові купюри до комірки збереження цифрової купюри, де залишають цифрову купюру покупця, потім передають продавцеві цифрову купюру продавця, а перевірку продавцем

дійсності цифрової купюри, що йому передана, здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після перевірки, дійсну цифрову купюру обмінюють на нову цифрову купюру продавця, яку повертають продавцеві, після чого з комірки збереження цифрової купюри надсилають покупцеві шифроване повідомлення про здійснені операції.

У другому варіанті способу як ключ доступу базано використовують одноразовий ключ доступу.

Також, у другому варіанті способу при розміні цифрової купюри спочатку генерують замість переданої цифрової купюри цифрову купюру покупця та цифрову купюру продавця, сумарний номінал яких дорівнює номіналу переданої купюри, після чого заносять цифрову купюру покупця та цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

Крім того, за другим варіантом способу, перевірку дійсності цифрової купюри можуть здійснювати по базі дійсних цифрових купюр у банку цифрових купюр.

Додатково, за другим варіантом способу, при обміні цифрової купюри продавця спочатку генерують замість переданої цифрової купюри продавця нову цифрову купюру продавця, номінал якої дорівнює номіналу переданої цифрової купюри продавця, після чого заносять нову цифрову купюру продавця до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру продавця вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

Крім того, у другому варіанті способу, шифроване повідомлення про здійснені операції можуть надсилати покупцеві через термінал продавця або безпосередньо покупцю.

У третьому варіанті способу поставлена задача вирішується тим, що у способі здійснення платежів з використанням цифрових сертифікатів, який включає передачу покупцем продавцеві цифрового сертифікату як платіжного засобу та перевірку продавцем дійсності цифрового сертифікату, згідно з винаходом як цифровий сертифікат використовують цифрову купюру, що являє собою згенеровану цифрову послідовність, яку передають продавцю, а перевірку продавцем дійсності цифрової купюри здійснюють шляхом відправлення цифрової купюри до системи банків цифрових купюр, де її перевіряють на дійсність, після перевірки, дійсну цифрову купюру обмінюють на нову цифрову купюру, потім повертають продавцеві нову цифрову купюру.

У третьому варіанті способу перевірку дійсності цифрової купюри можуть здійснювати по базі дійсних цифрових купюр у банку цифрових купюр.

Додатково, у третьому варіанті способу при обміні цифрової купюри спочатку генерують замість переданої цифрової купюри нову цифрову купюру, номінал якої дорівнює номіналу переданої цифрової купюри, після чого заносять нову цифрову купюру до бази дійсних цифрових купюр у банку цифрових купюр, а передану цифрову купюру

чають з бази дійсних цифрових купюр у банку цифрових купюр

Використання цифрової купюри у обох варіантах способу за даним винаходом, забезпечує легкість та захищеність здійснення платежів

Наявність операцій перевірки, обміну та розміну цифрової купюри у банку цифрових купюр, забезпечує надійний захист від можливого втручання третіх осіб

Використання одноразового ключа доступу до комірки збереження, тобто ключа доступу яким можливо скористатися тільки один раз, у способі за даним винаходом виключає можливість повторного звертання до комірки збереження цифрової купюри як третіх осіб, так і самого покупця за цим одноразовим ключем доступу, що у свою чергу забезпечує надійність та захищеність комірки збереження цифрової купюри від несанкціонованого втручання

У даному винаході використовуються такі терміни

Під терміном "цифрова купюра" розуміється унікальна цифрова послідовність, яка містить дві основні частини

- номінал або вартість (аналогічно з купюрою готівки),

- унікальна частина

Відмінною ознакою цифрової купюри є те, що вона не залежить від носія інформації як фізичного, так і програмного. Цифрова купюра не має обмеження на величину номіналу, її можна обробляти та перетворювати різноманітними математичними функціями, передавати через мережу Інтернет, по телефону тощо. Крім того, вона може бути обмінена на купюру того ж номіналу або розмінена на кілька купюр з можливістю дрібності розміну. Наприклад купюру номіналом 100 доларів США можливо розмінати на купюри номіналом 77,12 та 22,88 доларів США.

Ще однією відмінною особливістю цифрової купюри від звичайних паперових купюр є те, що цифрова купюра є лише цифровою послідовністю у той час як паперові гроші треба виготовляти з дорогого паперу застосовуючи спеціальні фарби та спеціальне обладнання, а це коштує дуже дорого.

Цифрова купюра призначена для використання як платіжний засіб на пред'явника, аналогічно готівці та іншим цінним паперам. Вона забезпечується звичайними грошовими коштами та цілком емулює якості звичайних готівкових засобів, додаючи до них більш високий ступінь захищеності, приватності, але головне - економічності власне платіжної системи.

Під терміном "система банків цифрових купюр" розуміють будь-яку установу яка включає один або кілька банків цифрових купюр (група банків цифрових купюр), може керувати ним / ними та підтримувати його / їх функціонування, має або може утворювати безпечні канали обміну інформацією з покупцями, продавцями та комірками збереження, може приймати та передавати, по цих безпечних каналах, цифрові купюри та іншу інформацію.

Під терміном "банк цифрових купюр" розуміють інформаційну базу даних, яка зберігає у собі дійсні цифрові купюри. Банк цифрових купюр

(БЦК) є блоком системи банків цифрових купюр (СБЦК). Кількість БЦК у СБЦК необмежена і залежить від номіналу цифрових купюр, валют, що використовуються і т.п. Банк цифрових купюр має наступні функції:

- зберігати базу дійсних цифрових купюр,
- перевіряти цифрові купюри, що пред'являються, на дійсність,
- обмінювати та розмінювати цифрові купюри, що пред'являються,
- генерувати нові цифрові купюри,
- вилучати старі цифрові купюри.

Під терміном "комірка збереження цифрової купюри" розуміють електронний гаманець дистанційного керування, що програмується. Комірка збереження цифрової купюри існує незалежно від системи банків цифрових купюр і може бути розміщена у прийнятному для покупця та/або продавця місці. Комірка збереження цифрової купюри має наступні функції:

- приймати цифрову купюру та інформацію, що її супроводжує,
- автоматично відправляти на перевірку та обмін до банку цифрових купюр цифрові купюри, що надійшли,
- зберігати цифрові купюри,
- у відповідь на дистанційний запит видавати цифрову купюру зазначеного номіналу,
- надавати доступ до інформації про рух коштів у комірці.

Спосіб платежів, що заявляється пояснюється малюнками.

На фіг 1 зображено динаміку першого варіанту способу здійснення платежів,

на фіг 2 зображено динаміку другого варіанту способу здійснення платежів,

на фіг 3 зображено динаміку третього варіанту способу здійснення платежів.

Покупець 1 та продавець 2 використовують систему банків цифрових купюр (СБЦК) 3 для перевірки та обміну / розміну цифрових купюр. Комірка збереження цифрової купюри (КЗЦК) 4 існує як посередник між покупцем 1 / продавцем 2 та СБЦК 3 та використовується для перевірки дійсності та зберігання цифрової купюри.

Спосіб платежів, що заявляється здійснюється таким чином:

Перший варіант способу здійснення платежів

Схематично цей спосіб зображено на фіг 1.

Припустимо, що покупець 1 хоче придбати будь-який товар або замовити послуги у продавця 2 на визначену суму. Покупець 1 має цифрову купюру (ЦК) та бажає розрахуватися цією купюрою. Тоді, покупець передає продавцю ЦК та адресу КЗЦК 4 до якої продавець 2 повинен передати заду (крок К1 на фіг 1).

Продавець 2, отримавши купюру безпосередньо від покупця 1, передає ЦК до СБЦК 3 для розміну та перевірки (крок К2 на фіг 1), де перевіряють дійсність цифрової купюри по базі дійсних ЦК, та при підтвердженні дійсності цифрової купюри, її розмінюють на цифрову купюру продавця (ЦК_{продавця}) та цифрову купюру покупця (ЦК_{покупця}) які потім заносять до бази дійсних цифрових купюр у банку цифрових купюр, а передану ЦК вилучають з бази дійсних цифрових купюр у банку цифрових купюр.

Після цього з СБЦК 3 передають ці купюри продавцю 2 (крок К3 на фіг 1), потім продавець передає ЦК_{покупця} до КЗЦК 4 вказаної покупцем (крок К4 на фіг 1). КЗЦК 4 передає ЦК_{покупця} до СБЦК 3 (крок К5 на фіг 1) де перевіряють дійсність ЦК_{покупця} по базі дійсних цифрових купюр та при підтвердженні дійсності цифрової купюри, її обмінюють на нову ЦК_{покупця} яку заносять до бази дійсних цифрових купюр, а передану ЦК вилучають з бази дійсних цифрових купюр у банку цифрових купюр, потім повертають замість переданої купюри нову ЦК_{покупця} до КЗЦК 4 (крок К6 на фіг 1). Як підтвердження проведених операцій з КЗЦК 4 надсилають покупцю 1 шифроване повідомлення через термінал продавця 2 (крок К7-1 на фіг 1) або безпосередньо покупцю 1 (крок К7-2 на фіг 1).

За цим способом покупцю, для розрахунку з продавцем, достатньо тільки передати продавцю цифрову купюру як оплату товару або послуги. Цей варіант способу здійснення платежів є зручними для розрахунків у мережі інтернет та "на місці", наприклад, у супермаркеті, магазині тощо.

Другий варіант способу здійснення платежів

Схематично цей спосіб зображено на фіг 2

Припустимо, що покупець 1 хоче придбати будь-який товар або замовити послуги у продавця 2 на визначену суму. Але покупець 1 не має "на руках" ЦК, а знає лише адресу КЗЦК 4 де зберігається ЦК. Тоді, покупець 1 передає продавцю 2 реквізити КЗЦК 4 та повідомляє номінал ЦК яку він хоче отримати (крок К8 на фіг 2).

Продавець 2, отримавши цю інформацію від покупця, передає запит до КЗЦК 4 (крок К9 на фіг 2). Якщо вказана покупцем 1 сума знаходиться у КЗЦК 4, то, у відповідь, КЗЦК 4 надсилає запит ключа доступу (крок К10 на фіг 2). Продавець 2 передає запит КЗЦК 4 покупцю 1 (крок К11 на фіг 2), потім покупець 1 передає продавцю 2 ключ доступу (крок К12 на фіг 2). Після отримання продавцем 2 ключа доступу продавець 2 передає цей ключ доступу до КЗЦК 4 (крок К13 на фіг 2). В свою чергу, КЗЦК 4 передає ЦК, що знаходиться у неї до СБЦК 3 для розміну та перевірки (крок К14 на фіг 2), де перевіряють дійсність ЦК по базі дійсних ЦК у банку цифрових купюр, де при підтвердженні дійсності ЦК, розмінюють передану ЦК на цифрову купюру продавця (ЦК_{продавця}) та цифрову купюру покупця (ЦК_{покупця}), потім заносять ці купюри до бази дійсних цифрових купюр, а передану купюру вилучають з бази дійсних цифрових купюр у банку цифрових купюр. Після цього СБЦК 3 передає ці купюри до КЗЦК 4 (крок К15 на фіг 2), потім КЗЦК 4 передає ЦК_{продавця} до продавця 2 та залишає у себе ЦК_{покупця} (крок К16 на фіг 2). Продавець 1 передає ЦК_{продавця} до СБЦК 3 (крок К17 на фіг 2) де перевіряють дійсність ЦК_{продавця} по базі дійсних ЦК у банку цифрових купюр, де при підтвердженні дійсності ЦК_{продавця}, генерують замість переданої купюри нову ЦК_{продавця} яку потім заносять до бази дійсних цифрових купюр, а передану ЦК вилучають з бази дійсних цифрових купюр. Після цього СБЦК 3 повертає нову ЦК_{продавця} продавцю 2 (крок К18 на фіг 2).

Як підтвердження проведених операцій КЗЦК 4 надсилає шифроване повідомлення покупцю 1 через термінал продавця 2 (крок К19-1 на фіг 2)

або безпосередньо покупцю 1 (крок К19-2 на фіг 2).

Цей варіант способу зручно використовувати, коли покупець не має "на руках" цифрову купюру, а знає тільки адресу комірки збереження цифрової купюри де зберігається цифрова купюра.

За цим варіантом способу, покупцю, для розрахунку з продавцем, достатньо тільки передати продавцю адресу комірки збереження цифрової купюри де зберігається цифрова купюра якою він бажає розрахуватися за товари або послуги.

Здійснення платежів за цим варіантом є зручними для розрахунків у мережі інтернет та "на місці", наприклад, у супермаркеті, магазині тощо.

Третій варіант способу здійснення платежів

Схематично цей спосіб зображено на фіг 3

Припустимо, що покупець 1 хоче придбати будь-який товар або замовити послуги у продавця 2 на визначену суму. Покупець 1 має цифрову купюру (ЦК) та бажає розрахуватися цією купюрою. Тоді, покупець 1 передає продавцю 2 ЦК (крок К20 на фіг 3). Продавець 2, отримавши купюру безпосередньо від покупця 1, передає ЦК до СБЦК 3 для перевірки та обміну (крок К21 на фіг 3), де її перевіряють по базі дійсних ЦК у банку цифрових купюр, та при підтвердженні дійсності цифрової купюри, її обмінюють на нову цифрову купюру яку потім заносять до бази дійсних цифрових купюр, а передану ЦК вилучають з бази дійсних цифрових купюр у банку цифрових купюр. Після цього з СБЦК 3 передають цю купюру продавцю 2 (крок К22 на фіг 3).

Цей варіант способу зручно використовувати, коли покупець тільки має "на руках" цифрову купюру, а також, продавець і покупець не мають будь-якої комірки збереження цифрової купюри за посередництвом якої було б можливо здійснити перевірку дійсності цифрової купюри.

За цим варіантом способу, продавець передає цифрову купюру безпосередньо до СБЦК.

Цей варіант способу здійснення платежів є зручними для розрахунків у мережі інтернет та "на місці", наприклад, у супермаркеті, магазині тощо.

Перевірка, обмін та розмін цифрової купюри у СБЦК є критичними аспектами способу за даним винаходом. Використання СБЦК забезпечує можливість розрахунку платіжними засобами іншими ніж готівка, забезпечує надійну захищеність приватних платежів та виключає необхідність наявності у покупця програмного забезпечення і спеціального устаткування.

Використання цифрової купюри забезпечує можливість розрахунку платіжними засобами незалежними від свого носія як фізичного, так і програмного.

Завдяки використанню СБЦК, де перевіряють, обмінюють та розмінюють ЦК покупець та продавець захищені від можливого шахрайства.

Вищенаведені варіанти способу здійснення платежів є зручними та безпечними для віддалених розрахунків (наприклад у мережі Інтернет тощо) та "на місці", наприклад, у супермаркеті, магазині тощо.

Обмін цифровими купюрами та інформацією можливо здійснювати через закриті канали зв'язку, мережу Інтернет, телефон або інші придатні

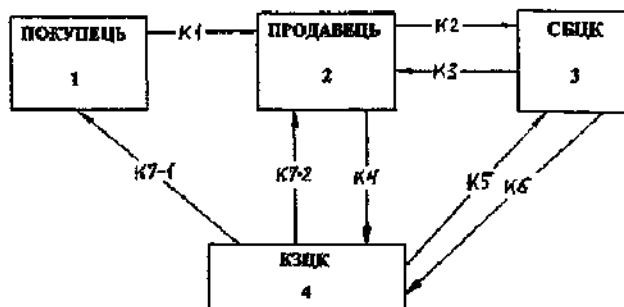
канали зв'язку

Для здійснення способу за даним винаходом можуть бути застосовані усі сучасні методи криптографії (з закритим та відкритим ключом)

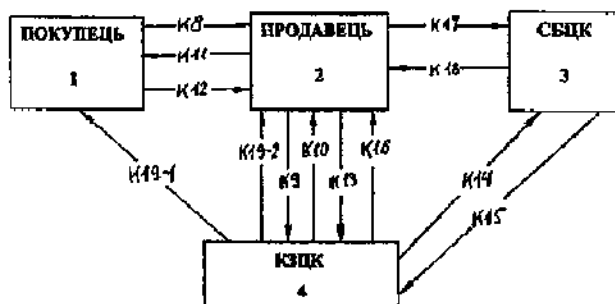
Для реалізації апаратного та програмного забезпечення системи банків цифрових купюр може бути використано спеціалізований сервер за допомогою стандартних операційних систем фірми

Майкрософт (операційних систем сімейства UNIX або Windows NT, Windows 2000)

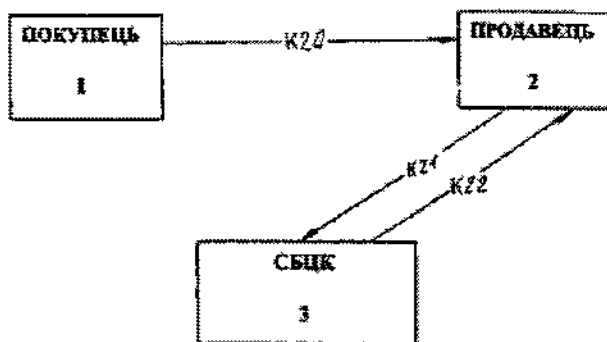
Найкраще реалізувати СБЦК у вигляді так званої "чорної скрині". Така реалізація забезпечує високий рівень безпеки та захист від несанкціонованого втручання третіх осіб у процеси перевірки, обміну та розміну цифрових купюр



Фиг 1



Фиг 2



Фиг 3