(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С ДОГОВОРОМ О ПАТЕНТНОЙ КООПЕРАЦИИ (PCT)

(19) Всемирная Организация Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
09 декабря 2021 (09.12.2021)

WIPO | PCT

(10) Номер международной публикации
WO 2021/246901 A1

(51) Международная патентная классификация:
G06Q 20/30 (2012.01) *H04L 9/32* (2006.01)
G06Q 20/40 (2012.01) *H04L 29/06* (2006.01)

(21) Номер международной заявки: PCT/RU2021/000180

(22) Дата международной подачи:
28 апреля 2021 (28.04.2021)

(25) Язык подачи: Русский

(26) Язык публикации: Русский

(30) Данные о приоритете:
2020118283 03 июня 2020 (03.06.2020) RU

(71) Заявитель: АКЦИОНЕРНОЕ ОБЩЕСТВО "НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ" (AKCIONERNOE OBSHCHESTVO "NACIONAL'NAYA SISTEMA PLATEZHNYKH KART") [RU/RU]; ул. Большая Татарская, д. 11 Москва, 115184, Moscow (RU).

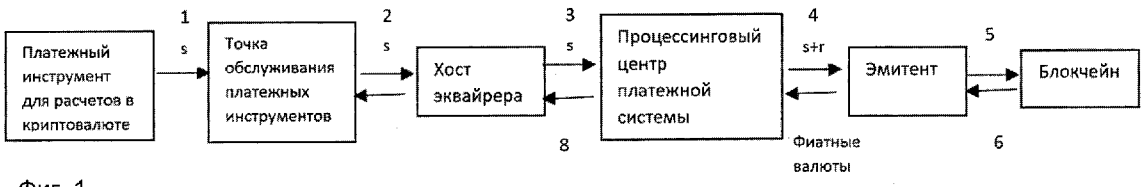
(72) Изобретатель: ГОЛДОВСКИЙ, Игорь Михайлович (GOLDOVSKIJ, Igor' Mihajlovich); Ореховый бульвар, 57, кв. 165 Москва, 115682, Moscow (RU).

(74) Агент: КИРПИЧЕНКОВ, Павел Александрович (KIRPICHENKOV, Pavel Aleksandrovich); ул. Большая Татарская, 11 Москва, 115184, Moscow (RU).

(81) Указанные государства *(если не указано иначе, для каждого вида национальной охраны)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,

(54) Title: METHOD AND SYSTEM FOR CONDUCTING NON-FIAT CURRENCY TRANSACTIONS IN A CARD INFRASTRUCTURE

(54) Название изобретения: СПОСОБ И СИСТЕМА ПРОВЕДЕНИЯ ТРАНЗАКЦИЙ НЕФИАТНЫХ ВАЛЮТ В КАРТОЧНОЙ ИНФРАСТРУКТУРЕ



Фиг. 1

1 Payment instrument for cryptocurrency settlements
2 Payment instrument point of service
3 Host of acquirer
4 Payment system processing centre
5 Issuer
6 Blockchain
7 Fiat currency

(57) **Abstract:** The invention relates to a method and system for conducting non-fiat currency transactions in a card infrastructure. The technical result consists in increased transaction security. In the present method, part of a cryptocurrency transaction signature is encrypted on a payment instrument for making cryptocurrency settlements, the key for encrypting said part being known only on the payment instrument and the issuer; data necessary to generate an authorization request, including the encrypted part of the cryptocurrency transaction signature, are transmitted to a payment instrument point of service, where an authorization request is generated and sent to a host of the acquirer, which sends said request to a processing centre of a payment system, where the number of the payment instrument for making cryptocurrency settlements is obtained, said number being used to generate the missing part of the cryptocurrency transaction signature and to route an authorization request containing both parts of the cryptocurrency transaction signature to the card issuer corresponding to the given number of the payment instrument, where a cryptocurrency transaction is generated which is sent to the address of the account of the issuer in a blockchain, from which confirmation of credit is received, then a positive response to the authorization request is sent from the issuer to the host of the acquirer.

(57) **Реферат:** Изобретение относится к способу и системе для проведения транзакций нефиатных валют в карточной инфраструктуре. Технический результат заключается в повышении безопасности проведения транзакций. В способе на платежном

[продолжение на следующей странице]

WO 2021/246901 A1

KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Указанные государства** *(если не указано иначе, для каждого вида региональной охраны)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), евразийский (AM, AZ, BY, KG, KZ, RU, TJ, TM), европейский патент (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Опубликована:

— *с отчётом о международном поиске (статья 21.3)*

инструменте для расчетов в криптовалюте зашифровывают часть подписи транзакции криптовалюты, ключ для шифрования которой известен только на платежном инструменте и эмитенте, передают данные, необходимые для формирования авторизационного запроса, в том числе зашифрованную часть подписи транзакции криптовалюты, на точку обслуживания платежных инструментов, где формируют авторизационный запрос и направляют его на хост эквайрера, который направляет его в процессинговый центр платежной системы, в котором получают номер платежного инструмента для расчетов в криптовалюте, который используют для генерации недостающей части подписи транзакции криптовалюты и маршрутизации авторизационного запроса, включающего обе части подписи транзакции криптовалюты, к эмитенту карты, соответствующему данному номеру платежного инструмента, где формируют транзакцию криптовалюты, которую направляют на адрес счета эмитента в блокчейне, от которого получают подтверждение о зачислении, затем от эмитента на хост эквайрера направляют положительный ответ на авторизационный запрос.

СПОСОБ И СИСТЕМА ДЛЯ ПРОВЕДЕНИЯ ТРАНЗАКЦИЙ НЕФИАТНЫХ ВАЛЮТ В КАРТОЧНОЙ ИНФРАСТРУКТУРЕ

Область техники

Изобретение относится к банковским платежным системам, а именно к осуществлению безналичных операций в карточных платежных системах с использованием нефиатных валют в качестве средств расчетов и предназначено для обеспечения возможности безналичной оплаты нефиатной валютой в стандартной карточной инфраструктуре приема платежных инструментов.

Уровень техники

На сегодняшний день существуют как фиатные валюты (фиатные деньги), которые относятся к централизованной платежной системе, т.е. номинальная стоимость фиатных валют устанавливается и гарантируется государством, так и нефиатные валюты (нефиатные деньги), учет внутренних расчетных единиц которой обеспечивает децентрализованная платежная система, работающая в полностью автоматическом режиме. К нефиатным валютам, рассматриваемым в контексте данного изобретения, относят криптовалюты, в основе которых лежит технология блокчейн.

В связи с ожидаемым распространением на рынке низковолатильных криптовалют, таких как TON, Libra, криптовалют центральных банков CDBC (Central Bank Digital Currency) и прочих, появляется интерес к решению задачи использования нефиатных валют, таких как криптовалюты, в существующей карточной инфраструктуре обслуживания платежных инструментов. При внедрении новой технологии в области проведения операций в карточных платежных системах с использованием нефиатных валют, таких как криптовалюты, возникает следующая проблема: магазинам невыгодно внедрять новую инфраструктуру приема новых платежных инструментов, потому что новых платежных инструментов на рынке еще мало, а новые платежные инструменты развиваются не так быстро, как хотелось бы их эмитентам, потому что их негде применять.

Предлагаемое решение позволяет убрать указанный технологический разрыв, предоставляя возможность использовать нефиатные валюты, такие как криптовалюты, для расчетов за покупки в существующей стандартной карточной инфраструктуре обслуживания платежных инструментов. При этом

предполагается, что оборудование и программное обеспечение на стороне эквайрера работает без каких-либо изменений.

Из уровня техники известна система и способ проведения платежных транзакций криптовалюты (заявка США №2015170112, G06Q 20/00, G06Q 20/38, опубликована 18.06.2015), обеспечивающие возможность оплаты товаров и/или услуг криптовалютой на точках обслуживания платежных инструментов, не принимающих криптовалюты.

Недостатком известного решения является необходимость внедрения адаптированных точек обслуживания платежных инструментов для обеспечения возможности приема и обмена криптовалюты для оплаты товаров и/или услуг.

За наиболее близкий аналог к патентуемому решению принят способ проведения транзакций криптовалюты (международная заявка №2019139655, G06Q 20/36, G06Q 20/38, опубликованная 18.07.2019), содержащий платежный инструмент для расчетов в криптовалюте, точку обслуживания платежных инструментов, хост эквайрера, процессинговый центр платежной системы и эмитент, в котором на точке обслуживания платежных инструментов принимают платежный инструмент для расчетов в криптовалюте, при этом принимают от платежного инструмента для расчетов в криптовалюте данные, необходимые для формирования авторизационного запроса, затем формируют авторизационный запрос и далее направляют его на хост эквайрера, далее на хосте эквайрера принимают вышеупомянутый авторизационный запрос, после чего направляют его в процессинговый центр платежной системы, далее на процессинговом центре платежной системы принимают вышеупомянутый авторизационный запрос, после чего направляют его эмитенту, далее от эмитента на хост эквайрера передают ответ на вышеупомянутый авторизационный запрос, указывающий, что транзакция криптовалюты авторизована.

Недостатком наиболее близкого аналога является необходимость предоставления доступа к секретным ключам платежного инструмента для расчетов в криптовалюте доверенной стороне, инициирующей транзакцию криптовалюты от лица держателя платежного инструмента для расчетов в криптовалюте.

Раскрытие изобретения

Предлагается решение, в котором проведение транзакции криптовалюты осуществляется с использованием стандартной инфраструктуры обслуживания платежных инструментов в карточных платежных системах, при этом исключается возможность генерации транзакции криптовалюты третьей стороной от лица держателя платежного инструмента для расчетов в криптовалюте. Таким образом, описываемое решение позволяет использовать нефиатные валюты, такие как криптовалюты, в основе которых лежит технология блокчейн, для расчетов в карточных платежных системах, с сохранением базового принципа блокчейна - только владелец счета в блокчейне может сгенерировать транзакцию криптовалюты со своего счета в блокчейне.

Главной проблемой реализации системы и способа для проведения безопасной транзакции нефиатных валют в стандартной карточной инфраструктуре является необходимость передачи большего по сравнению со стандартной платежной транзакцией объема данных эмитенту платежного инструмента для расчетов в криптовалюте. Известные аналоги для решения вышеуказанной проблемы предлагают модернизировать инфраструктуру точки обслуживания платежных инструментов или передавать возможность третьей стороне инициировать транзакцию криптовалюты по поручению держателя платежного инструмента для расчетов в криптовалюте. При этом нарушается базовый принцип блокчейна, который заключается в том, что операции в блокчейне может инициировать только владелец счета в блокчейне. Предложенное решение реализуется с использованием стандартной инфраструктуры обслуживания платежных инструментов в карточных платежных системах и не позволяет ни одному из участников карточной платежной системы инициировать транзакцию криптовалюты в блокчейне без - кроме непосредственного участия владельца счета в блокчейне, с которого переводится криптовалюта.

Технической проблемой, на решение которой направлено предложенное изобретение, заключается в создании системы и способа, позволяющих держателю платежного инструмента для расчетов в криптовалюте единолично инициировать транзакцию криптовалюты, используя стандартную инфраструктуру обработки операций в карточных платежных системах.

Технический результат, достигаемый при реализации данного изобретения, заключается в повышении безопасности системы и способа проведения транзакций криптовалют в стандартной карточной инфраструктуре обработки операций в карточных платежных системах, расширении арсенала платежных инструментов.

Указанный технический результат достигается в способе для проведения транзакций нефиатных валют в карточной инфраструктуре, содержащем платежный инструмент для расчетов в криптовалюте, точку обслуживания платежных инструментов, хост эквайрера, процессинговый центр платежной системы и эмитент, в котором на точке обслуживания платежных инструментов принимают платежный инструмент для расчетов в криптовалюте, при этом принимают от платежного инструмента для расчетов в криптовалюте данные, необходимые для формирования авторизационного запроса, затем формируют авторизационный запрос и далее направляют его на хост эквайрера, далее на хосте эквайрера принимают вышеупомянутый авторизационный запрос, после чего направляют его в процессинговый центр платежной системы, далее на процессинговом центре платежной системы принимают вышеупомянутый авторизационный запрос, после чего направляют его эмитенту, далее от эмитента на хост эквайрера передают ответ на вышеупомянутый авторизационный запрос, указывающий, что транзакция криптовалюты авторизована, при этом

- перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте зашифровывают часть подписи транзакции криптовалюты, при этом ключ для шифрования части подписи известен только на платежном инструменте для расчетов в крипговалюте и эмитенте, затем передают данные, необходимые для формирования авторизационного запроса, в том числе зашифрованную часть подписи транзакции криптовалюты, на точку обслуживания платежных инструментов, на точке обслуживания платежных инструментов формируют авторизационный запрос и направляют его на хост эквайрера, на хосте эквайрера принимают вышеупомянутый авторизационный запрос и направляют его в процессинговый центр платежной системы,

- на процессинговом центре платежной системы принимают вышеупомянутый авторизационный запрос от хоста эквайрера и получают

номер платежного инструмента для расчетов в криптовалюте через хост эквайрера, затем используют этот номер для генерации недостающей части подписи транзакции криптовалюты и маршрутизации авторизационного запроса, включающего обе части подписи транзакции криптовалюты, к эмитенту карты, соответствующему данному номеру платежного инструмента;

- на эмитенте от процессингового центра платежной системы принимают вышеупомянутый авторизационный запрос, включающий обе части подписи транзакции криптовалюты, затем формируют транзакцию криптовалюты, после чего направляют вышеупомянутую транзакцию криптовалюты на адрес счета эмитента в блокчейне, далее получают из блокчейна подтверждение о зачислении на адрес эмитента в блокчейне средств в криптовалюте, после чего от эмитента на хост эквайрера направляют положительный ответ на авторизационный запрос.

В частности, перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте по заранее оговоренному курсу определяют количество средств в криптовалюте, эквивалентных размеру покупки в фиатной валюте, которые необходимо передать эмитенту.

В частности, эмитент с собственным адресом счета в блокчейне выпускает платежный инструмент для расчета в криптовалюте, платежное приложение которого содержит БИН эмитента в платежной системе.

В частности, на платежный инструмент для расчетов в криптовалюте установлено платежное приложение, при помощи которого подготавливают данные для транзакции криптовалюты в блокчейне, размещают данные, необходимые для осуществления транзакции криптовалюты в тегах, используемых в стандартных ответах на команды точки обслуживания платежных инструментов, и отвечают на команды точки обслуживания платежных инструментов.

В частности, на платежный инструмент для расчетов в криптовалюте при персонализации эмитент загружает открытый и закрытый ключи, после чего открытый ключ направляют эмитенту.

Для достижения указанного технического результата предложена также и система для проведения транзакций нефиатных валют в карточной инфраструктуре, включающая платежный инструмент для расчетов в

криптовалюте, точку обслуживания платежных инструментов, хост эквайрера, процессинговый центр платежной системы и эмитент, в которой точка обслуживания платежных инструментов выполнена с возможностью приема платежных инструментов для расчетов в криптовалюте, приема от платежного инструмента для расчетов в криптовалюте данных, необходимых для формирования авторизационного запроса, формирования авторизационного запроса и его направления на хост эквайрера, хост эквайрера выполнен с возможностью приема вышеупомянутого авторизационного запроса и его направления в процессинговый центр платежной системы, процессинговый центр платежной системы выполнен с возможностью приема вышеупомянутого авторизационного запроса и его направления к эмитенту, эмитент выполнен с возможностью приема вышеупомянутого авторизационного запроса и направления на хост эквайрера ответа на вышеупомянутый авторизационный запрос, указывающий, что транзакция криптовалюты авторизована, при этом

- платежный инструмент для расчетов в криптовалюте выполнен с возможностью шифрования и передачи зашифрованной части подписи транзакции на точку обслуживания платежных инструментов, при этом ключ для шифрования подписи известен только на платежном инструменте для расчетов в криптовалюте и эмитенте,

- процессинговый центр платёжной системы выполнен с возможностью получения номера платежного инструмента для расчетов в криптовалюте через хост эквайрера, использования этого номера для генерации недостающей части подписи транзакции криптовалюты и маршрутизации авторизационного запроса, включающего обе части подписи транзакции криптовалюты, к эмитенту карты, соответствующему данному номеру платежного инструмента;

- эмитент, выполненный с возможностью приема вышеупомянутого авторизационного запроса от процессингового центра платежной системы включающего обе части подписи транзакции криптовалюты, формирования после приема вышеупомянутого авторизационного запроса транзакции криптовалюты в блокчейне, направления вышеупомянутой транзакции криптовалюты на адрес счета эмитента в блокчейне, последующего получения из блокчейна подтверждения о зачислении средств в криптовалюте на адрес счета эмитента в блокчейне, и дальнейшего направления положительного ответа на авторизационный запрос на хост эквайрера.

В частности, перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте по заранее оговоренному курсу определяют количество средств в криптовалюте, эквивалентных размеру покупки в фиатной валюте, которые необходимо передать эмитенту.

В частности, эмитент с собственным адресом счета в блокчейне выпускает платежный инструмент для расчета в криптовалюте, платежное приложение которого содержит БИН эмитента в платежной системе.

В частности, на платежный инструмент для расчетов в криптовалюте установлено платежное приложение, при помощи которого подготавливают данные для транзакции криптовалюты в блокчейне, размещают данные, необходимые для проведения транзакции криптовалюты в тегах, используемых в стандартных ответах на команды точки обслуживания платежных инструментов, и отвечают на команды точки обслуживания платежных инструментов.

В частности, на платежный инструмент для расчетов в криптовалюте при персонализации эмитент загружает открытый и закрытый ключи, после чего открытый ключ направляют эмитенту.

Благодаря использованию платежного инструмента для расчетов в криптовалюте, на котором перед передачей данных, необходимых для формируют подпись транзакции криптовалюты, затем передают данные, необходимые для формирования авторизационного запроса, в том числе часть подписи транзакции криптовалюты, на точку обслуживания платежных инструментов обеспечивается безопасность способа и системы для проведения транзакций криптовалют в карточной инфраструктуре, поскольку держатель платежного инструмента для расчетов в криптовалюте не передает доступ к криптовалюте третьим лицам, а единолично инициирует транзакцию криптовалюты. Также обеспечивается расширение арсенала платежных инструментов за счет осуществления инициирования транзакции криптовалюты с использованием стандартной инфраструктуры обработки операций в карточных платежных системах.

Благодаря приему на процессинговом центре платежной системы вышеупомянутого авторизационного запроса от хоста эквайрера, последующему определению по номеру платежного инструмента для расчетов

в криптовалюте вышеупомянутого авторизационного запроса на проведение транзакции криптовалюты, дополнению вышеупомянутого авторизационного запроса недостающей частью подписи транзакции криптовалюты и последующей передачи авторизационного запроса, включающего обе части подписи транзакции криптовалюты эмитенту обеспечивается повышение безопасности системы и способа для проведения транзакций криптовалют в карточной инфраструктуре, дополнение вышеупомянутого авторизационного запроса позволяет держателю платежного инструмента для расчетов в криптовалюте единолично инициировать транзакцию криптовалюты в условиях ограничения размера передаваемых данных для формирования транзакции криптовалюты, а также позволяет передать вышеупомянутый авторизационный запрос, включающий обе части подписи транзакции криптовалюты, эмитенту, без возможности формирования транзакции криптовалюты на процессинговом центре платежной системы. Также обеспечивается расширение арсенала платежных инструментов за счет обеспечения возможности проведения транзакций криптовалют с использованием стандартной инфраструктуры обработки операций в карточных платежных системах.

Благодаря приему на эмитенте от процессингового центра платежной системы вышеупомянутого авторизационного запроса, включающего обе части подписи транзакции криптовалюты, последующего формирования транзакции криптовалюты, направления далее вышеупомянутой транзакции криптовалюты на адрес счета эмитента в блокчейне, последующего получения из блокчейна подтверждения о зачислении на адрес эмитента в блокчейне средств в криптовалюте, и затем отправки от эмитента на хост эквайрера положительного ответа на авторизационный запрос, обеспечивается повышение безопасности системы и способа для проведения транзакций криптовалют в карточной инфраструктуре, поскольку позволяет на основе полученного авторизационного запроса, инициированного держателем платежного инструмента для расчетов в криптовалюте, сформировать и обработать транзакцию криптовалюты и направить ответ на вышеупомянутый авторизационный запрос на хост эквайрера. Также обеспечивается расширение арсенала платежных инструментов за счет возможности формирования эмитентом транзакции криптовалюты на основе данных, сформированных в условиях ограничения

размера передаваемых данных в стандартной инфраструктуре обработки операций в карточных платежных системах.

Благодаря определению перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте по заранее оговоренному курсу количества средств в криптовалюте, эквивалентных размеру покупки в валюте, которые необходимо передать эмитенту, исключается необходимость включения в систему дополнительных этапов и участников, таких как, например, валютные биржи, поскольку перевод средств с адреса счета держателя платежного инструмента для расчетов в криптовалюте осуществляется напрямую на адрес счета эмитента по заранее оговоренному курсу, в результате чего обеспечивается безопасность системы и способа проведения транзакций криптовалют в карточной инфраструктуре.

Благодаря выпуску эмитентом с собственным адресом счета в блокчейне платежного инструмента для расчетов в криптовалюте, платежное приложение которого содержит БИН эмитента в платежной системе, обеспечивается возможность определения по номеру платежного инструмента для расчетов в криптовалюте авторизационного запроса на проведение транзакции криптовалюты и его маршрутизации к эмитенту на этапе обработки авторизационного запроса процессинговым центром, что позволяет держателю платежного инструмента для расчетов в криптовалюте единолично инициировать транзакцию криптовалюты в условиях ограничения размера передаваемых данных для формирования транзакции криптовалюты через стандартную инфраструктуру обработки операций в карточных платежных системах, что дополнительно обеспечивает безопасность описываемых системы и способа и расширение арсенала платежных инструментов.

Благодаря использованию платежного инструмента для расчетов в криптовалюте с платежным приложением, при помощи которого подготавливают данные для транзакции криптовалюты в блокчейне, размещают данные для осуществления транзакции криптовалюты в тегах, используемых в стандартных ответах на команды точки обслуживания платежных инструментов, и отвечают на команды точки обслуживания платежных инструментов обеспечивается исключение доступа третьих лиц к данным держателя платежного инструмента для расчетов в криптовалюте и

возможность единоличного инициирования транзакции криптовалюты владельцем счета в условиях ограничения размера передаваемых данных через стандартную инфраструктуру обработки операций в карточных платежных системах, что повышает безопасность проведения транзакций криптовалют и так же позволяет расширить арсенал платежных инструментов, поскольку передача данных для дальнейшего формирования транзакции криптовалюты осуществляется в стандартной инфраструктуре обработки операций в карточных платежных системах.

Благодаря использованию платежного инструмента для расчетов в криптовалюте, на котором содержатся открытый и закрытый ключи и направлению открытого ключа эмитенту, обеспечивается безопасность системы для проведения транзакций криптовалюты с использованием технологии блокчейн, поскольку держателю платежного инструмента для расчетов в криптовалюте предоставляется возможность единолично инициировать транзакцию криптовалюты с использованием собственных только ему доступных открытого и закрытого ключей, а эмитенту предоставляется возможность формирования транзакции криптовалюты с использованием открытого ключа. Также обеспечивается расширение арсенала платежных инструментов в стандартной инфраструктуре обработки операций в карточных платежных системах за счет обеспечения инициирования транзакции криптовалюты с использованием открытого и закрытого ключей и формирования на эмитенте транзакции криптовалюты с использованием открытого ключа.

Ниже приведены пояснения для некоторых используемых в настоящем описании изобретения терминов.

Точка обслуживания платежных инструментов представляет собой стандартную инфраструктуру приема платежных инструментов в карточных платежных системах с технологиями контактного и/или бесконтактного считывания данных в карточных платежных системах и может быть представлена терминалом любого типа. Например, точка обслуживания платежных инструментов может быть представлена в виде штатной инфраструктуры приема карт, такой как POS-терминал, терминальное ядро и приложение, протокол подключения терминала к хосту эквайрера.

Хост эквайрера - система банка, ответственного за прием платежных инструментов в точке обслуживания платежных инструментов.

Эмитент - система банка, выпускающего в обращение платежные инструменты, в том числе платежные инструменты для расчетов в криптовалюте.

Стандартные команды точки обслуживания платежных инструментов - команды, используемые при взаимодействии точки обслуживания платежных инструментов с платежными инструментами в существующей инфраструктуре приема и обработки транзакций в карточных платежных системах. При этом в описываемом изобретении точка обслуживания платежных инструментов обменивается данными с платежным инструментом для расчетов в криптовалюте с использованием стандартных команд, используемых для обслуживания платежных инструментов в существующей инфраструктуре приема и обработки платежных инструментов в карточных платежных системах.

Платежный инструмент - банковская карта, смартфон и/или любой другой инструмент, использование которого инициирует перевод средств с адреса счета держателя платежного инструмента на адрес получателя средств. Оплата с использованием платежного инструмента может осуществляться в контактном и/или бесконтактном режиме.

В качестве платежного инструмента для расчетов в криптовалюте может выступать банковская карта, смартфон и/или любые другие инструменты, с помощью которых держателю платежного инструмента для расчетов в криптовалюте предоставляется возможность с использованием технологии блокчейн осуществлять перевод криптовалюты со своего адреса на адрес получателя. Платежный инструмент для расчетов в криптовалюте выпускается эмитентом, имеющим собственный адрес счета в блокчейне и готовым предложить своим клиентам расчеты в криптовалюте. Платежное приложение, установленное на платежном инструменте для расчетов в криптовалюте, содержит БИН эмитента в платежной системе и осуществляет диалог платежного инструмента для расчетов в криптовалюте с точкой обслуживания платежных инструментов, а также позволяет вычислять данные для передачи этих данных эмитенту платежного инструмента. Платежный инструмент для расчетов в криптовалюте выполнен с возможностью получения стандартных команд от точки обслуживания платежных инструментов, подготовки данных

для проведения транзакции криптовалюты, размещения данных в тегах стандартных сообщений и отправки указанных сообщений в ответ на команды точки обслуживания платежных инструментов.

HSM-устройство (аппаратный модуль безопасности, hardware security module) - это физическое вычислительное устройство на стороне процессингового центра платежной системы, которое позволяет формировать, хранить и управлять цифровыми ключами, а также производить криптографические вычисления с использованием ключей.

Торгово-сервисное предприятие (ТСП) - субъект хозяйственной деятельности, осуществляющий реализацию товаров, работ или услуг.

Под транзакцией криптовалюты понимается перевод криптовалюты с адреса счета отправителя на адрес счета получателя криптовалюты с применением технологии блокчейн (добавление нового блока транзакции криптовалюты в цепочке блокчейн). Например, в описании реализации данного изобретения осуществляется транзакция криптовалюты с электронного кошелька держателя платежного инструмента для расчетов в криптовалюте на электронный кошелек эмитента, эмитирующего вышеупомянутый платежный инструмент для расчетов в криптовалюте.

Под подтверждением транзакции криптовалюты понимается проверка транзакции криптовалюты на ее соответствие предъявляемым блокчейном требованиям.

Проверка валидности подписи транзакции криптовалюты - проверка подписи транзакции на соответствие стандарту, предъявляемому к подписи транзакции.

Динамические параметры транзакции - переменная часть параметров транзакции. Например, к динамическим параметрам транзакции относятся размер транзакции и валюта операции, параметры ТСП, подпись транзакции. При этом подпись транзакции - это обязательная часть динамических данных.

БИН эмитента - уникальный идентификационный номер банка-эмитента, который дает полную информацию о банке, является частью номера карты и используется для идентификации банка в рамках карточной платежной системы при авторизации, процессинге и клиринге.

Алгоритм AES (алгоритм Advanced Encryption Standard) - симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования.

ODA (Offline Data Authentication) - это криптографическая проверка подлинности данных карты в автономном режиме с использованием открытого ключа.

Счетчик ATC (Application Transaction Counter) - счетчик на стороне процессингового центра платежной системы, который увеличивается при выполнении каждой транзакции.

Подробное описание системы для проведения транзакций нефиатных валют в карточной инфраструктуре.

Владелец кошелька с криптовалютой, желающий оплачивать криптовалютой товары и услуги в ТСП, обращается к эмитенту, который эмитирует для владельца кошелька с криптовалютой платежный инструмент для расчетов в криптовалюте.

В процессе персонализации платежного инструмента для расчетов в криптовалюте эмитент загружает в платежное приложение платежного инструмента для расчетов в криптовалюте информацию о заранее оговоренных курсах обмена криптовалюты на фиатные валюты, таких как Российские Рубли, доллары США и другие.

Вместе с тем эмитент загружает на платежный инструмент для расчетов в криптовалюте стандартный набор данных, используемый в обычном EMV-приложении (приложение стандарта EMV - Europay MasterCard Visa), включая уникальный номер платежного инструмента для расчетов в криптовалюте, срок действия платежного инструмента для расчетов в криптовалюте, AIP (Application Interchange Profile), ключи для ODA (Offline Data Authentication) и др., а также адрес счета эмитента в блокчейне.

Уникальный номер платежного инструмента для расчетов в криптовалюте имеет специально выделенным префикс (БИН эмитента) - первые 6-8 цифр платежного инструмента для расчетов в криптовалюте. Присвоенный платежному инструменту для расчетов в криптовалюте номер со специально выделенным префиксом позволяет маршрутизировать транзакцию криптовалюты к эмитенту карты, а кроме того информирует процессинговый центр платежной системы о необходимости формирования дополнительных данных для проведения операции.

Так же в процессе персонализации на платежном инструменте для расчетов в криптовалюте с использованием технологии блокчейн генерируются

открытый (публичный) и закрытый ключи, требуемые для генерации параметров, необходимых для вычисления подписи платежа, после чего открытый ключ возвращают эмитенту для хранения в его базе данных. Открытый ключ требуется эмитенту для восстановления подписи транзакции криптовалюты и предварительной проверки валидности подписи транзакции криптовалюты эмитентом.

Инициирование транзакции осуществляется при взаимодействии платежного инструмента для расчетов в криптовалюте с точкой обслуживания платежных инструментов. На выпускаемом эмитентом платежном инструменте для расчетов в криптовалюте установлено платежное приложение, позволяющее получать от точки обслуживания платежных инструментов стандартные команды с параметрами транзакции, генерировать данные транзакции криптовалюты и размещать часть данных транзакции криптовалюты, включая часть подписи платежа, в тэгах. При этом указанные тэги используются в стандартных сообщениях, отправляемых от платежных инструментов стандартным образом в ответ на стандартные команды точки обслуживания платежных инструментов. Таким образом, часть данных транзакции криптовалюты отправляется от платежного инструмента для расчетов в криптовалюте к точке обслуживания платежных инструментов в стандартном формате в соответствии с применяемыми в настоящее время протоколами подключения банков к карточной платежной системе.

Обмен данными между платежным инструментом для расчетов в криптовалюте и точкой обслуживания платежных инструментов, происходит стандартным образом в результате ответов платежного инструмента для расчетов в криптовалюте на штатные APDU-команды терминала (Application Protocol Data Unit). Ответы платежного инструмента для расчетов в криптовалюте представляют собой сообщения R-APDU, содержащие объекты данных в формате TLV (Tag Length Value) со стандартными для R-APDU (команды в формате стандарта EMV) тэгами, соответствующими APDU-командам терминала. Данные, передаваемые в тегах от платежного инструмента для расчетов в криптовалюте необходимы для формирования авторизационного запроса. EMV является стандартом для взаимной работы карт IC («чип-карт») и поддерживающих IC POS терминалов и автоматических кассовых машин, и используется для аутентификации платежей кредитными и

дебетовыми платежными инструментами, где EMV является акронимом Europay, MasterCard и Visa, основоположников стандарта.

Данные, необходимые для формирования авторизационного запроса, включают в себя динамические данные, которые размещаются в тегах, формируемых на платежном инструменте для расчетов в криптовалюте и направляемых в ответах на APDU-команды терминала. Динамические параметры транзакции криптовалюты включают в себя подпись транзакции криптовалюты, которая состоит из двух частей - подпись s и значение r, используемое при проверке подписи транзакции криптовалюты. Подпись s и значение r, используемое при проверке подписи транзакции криптовалюты в бинарном представлении являются строчками из нулей и единиц длиной 32 байта каждая. Для проведения эмитентом транзакции криптовалюты в блокчейне, необходимо передать эмитенту от платежного инструмента для расчетов в криптовалюте подпись транзакции криптовалюты, состоящую из двух частей размером по 32 байта каждая. Таким образом, эмитенту необходимо передать данные размером 64 байта.

Однако на передаваемые точке обслуживания платежных инструментов от платежного инструмента для расчетов в криптовалюте данные накладываются ограничения по размеру. Так, максимальный размер передаваемых от платежного инструмента для расчетов в криптовалюте динамических данных, которые возможно передать эмитенту с использованием стандартной инфраструктуры обработки платежных инструментов в карточных платежных системах, составляет 51 байт.

Подпись транзакции криптовалюты является перевычисляемым параметром транзакции криптовалюты и представляет собой криптографическое преобразование от размера и валюты транзакции криптовалюты, адреса счета получателя, идентификатора отправителя. Существуют различные виды блокчейна. На сегодняшний день в блокчейне для создания подписи используются разные эллиптические кривые (secp256k1, ed25519 и т.п.) и разные алгоритмы формирования подписи с использованием этих кривых (ECDSA, EdDSA и т.п.). Но все подписи имеют общую структуру: (r, s). При этом значение r - это координата (абсцисса или ордината) случайной точки R циклической подгруппы группы точек эллиптической кривой, используется для проверки подписи. Значение r, используемое при проверке

подписи транзакции криптовалюты является абсциссой или ординатой случайной точки R в зависимости от используемого блокчейна. Значение s - подпись, вычисленная по алгоритму Шнорра или Эль-Гамаля в подгруппе мультипликативной группы поля GF(p) простого порядка p. Подпись s и значение r, используемое при проверке подписи транзакции криптовалюты, связаны друг с другом через параметр, который представляет собой случайное число $k \in GF(p)$. Для случайной точки R эллиптической кривой выполняется равенство $R=kG$, где G - образующая циклической подгруппы группы точек эллиптической кривой.

Поскольку размер данных, которые требуется передать от платежного инструмента для расчетов в криптовалюте для формирования авторизационного запроса больше размера данных, которые возможно передать от платежного инструмента на точку обслуживания платежных инструментов и затем на хост эквайрера, предложено передавать от платежного инструмента для расчетов в криптовалюте не весь набор данных, а только часть, содержащую динамические параметры, связанные с выполняемой операцией, которые доступны только приложению платежного инструмента для расчетов в криптовалюте.

Ключ для шифрования значения подписи s, являющейся частью подписи транзакции криптовалюты, известен только на платежном инструменте для расчетов в криптовалюте и эмитенте, выпустившем указанный платежный инструмент для расчетов в криптовалюте. Отсюда следует, что параметром, который доступен только приложению платежного инструмента для расчетов в криптовалюте, является зашифрованное значение подписи s. Таким образом, на процессинговом центре платежной системы получают динамические данные, включающие зашифрованную подпись s, но при этом на процессинговом центре платежной системы не известно значение подписи s в момент проведения операции. Это позволяет повысить безопасность системы, поскольку без значения s на процессинговом центре платежной системы невозможно восстановить подпись транзакции криптовалюты.

Данные, необходимые для формирования транзакции криптовалюты передаются от платежного инструмента для расчетов в криптовалюте к точке обслуживания платежных инструментов. Далее на точке обслуживания платежных инструментов формируют авторизационный запрос и направляют

его на хост эквайрера. Хост эквайрера принимает вышеупомянутый авторизационный запрос и передает их на процессинговый центр платежной системы.

Часть данных, необходимых для формирования транзакции криптовалюты в блокчейне, содержится в авторизационном запросе, который принимается на процессинговом центре платежной системы. Недостающая часть данных, необходимых для формирования транзакции криптовалюты в блокчейне, формируется процессинговым центром платежной системы (значение r, используемое при проверке подписи транзакции криптовалюты) и хранится в системе эмитента (например, открытый ключ платежного приложения для расчетов в криптовлюте).

Процессинговый центр направляет вышеупомянутый авторизационный запрос, включающий данные от платежного инструмента для расчетов в криптовалюте и данные, сформированные процессинговым центром платежной системы для проведения транзакции криптовалюты в блокчейне эмитенту. Эмитент по номеру платежного инструмента для расчетов в криптовалюте определяет авторизационный запрос на проведение транзакции криптовалюты. Вышеупомянутый авторизационный запрос включает, в том числе, две части подписи транзакции криптовалюты. Используя открытый ключ, полученный при персонализации платежного инструмента для расчетов в криптовалюте, на эмитенте формируют транзакцию криптовалюты в блокчейне. После получения авторизационного запроса на эмитенте восстанавливают подпись транзакции криптовалюты из авторизационного запроса, предварительно проверяют валидность подписи транзакции криптовалюты. Далее, при положительном результате проверки валидности подписи транзакции криптовалюты, эмитент добавляет размер операции, адрес счета эмитента в блокчейне и идентификатор держателя платежного инструмента для расчетов в криптовалюте. После этого эмитент направляет транзакцию криптовалюты на адрес счета эмитента в блокчейн, затем принимает из блокчейна подтверждение о зачислении на адрес счета эмитента в блокчейне средств в криптовалюте, эквивалентных размеру покупки, после чего в стандартном режиме направляет положительный ответ на авторизационного запрос на хост эквайрера, указывающий, что покупка одобрена.

В дальнейшем, изобретение поясняется чертежами.

На фиг. 1 представлено схематичное изображение заявленной системы для проведения транзакций нефиатных валют в карточной инфраструктуре.

На фиг. 2 представлена блок-схема способа проведения транзакций нефиатных валют в карточной инфраструктуре.

Подробное описание реализации способа заявленного технического решения.

Для инициирования транзакции с использованием платежного инструмента для расчетов в криптовалюте платежный инструмент для расчетов в криптовалюте принимают на точке обслуживания платежных инструментов. Далее в автоматическом режиме осуществляется диалог платежного инструмента для расчетов в криптовалюте и точки обслуживания платежных инструментов, результатом которого является передача данных от платежного устройства для расчетов в криптовалюте на точку обслуживания платежных инструментов, необходимых для формирования авторизационного запроса. Все упомянутые в описании команды и объекты данных определены в стандарте EMV (команды и объекты в формате стандарта Europay MasterCard Visa).

При приеме платежного инструмента для расчетов в криптовалюте на точке обслуживания платежных инструментов, на платежном инструменте для расчетов в криптовалюте с помощью команды Select по стандартному AID (Application Identifier) точкой обслуживания платежных инструментов выбирается платежное приложение для расчетов в криптовалюте с использованием технологии блокчейн. Далее в объекте FCI Template читают PDOL (Processing Data Object List), содержащий размер и валюту транзакции криптовалюты и затем передают платежному инструменту для расчетов в криптовалюте команду GPO (Get Processing Options) с параметрами транзакции криптовалюты, запрашиваемыми PDOL.

Платежный инструмент для расчетов в криптовалюте формирует данные транзакции криптовалюты, которые включают в себя динамические данные, включающие часть подписи транзакции криптовалюты, размер и валюту транзакции криптовалюты, адрес счета получателя, идентификатор отправителя и пр. На платежном инструменте зашифровывают часть подписи транзакции криптовалюты при помощи ключа для шифрования значения подписи s.

Точка обслуживания платежных инструментов командами Read Record читает объекты:

- Track 2 Equivalent Data (Tag 57, 19 байт)
- PAN Sequence # (5F34, 1 байт)

Точка обслуживания платежных инструментов с помощью команды Generate AC получает данные:

- ATC (9F36, 2 байта)
- ARQC (9F26, 8 байт)
- IAD(9F10, 32 байта)
- ICC Dynamic Number (9F4C, 8 байт)

При осуществлении обмена данными между платежным инструментом для расчетов в криптовалюте и точкой обслуживания платежных инструментов, зашифрованное значение части подписи транзакции криптовалюты (подписи s) длиной 32 байта передается от платежного инструмента для расчетов в криптовалюте на точку обслуживания платежных инструментов в поле данных объекта IAD.

Данные, необходимые для формирования транзакции криптовалюты размещаются платежным приложением платежного инструмента для расчетов в криптовалюте в тегах и затем передаются на точку обслуживания платежных инструментов. Далее на основании данных, полученных от платежного инструмента для расчетов в криптовалюте на точке обслуживания платежных инструментов, формируют авторизационный запрос и направляют на хост эквайрера.

Хост эквайрера в автоматическом режиме осуществляет операции приема данных о транзакциях от точки обслуживания платежных инструментов, обрабатывает авторизационные запросы и передает их на процессинговый центр платежной системы. Далее, хост эквайрера направляет авторизационный запрос, включающий перечисленные ниже данные, сгенерированные платежным инструментом для расчетов в криптовалюте в процессинговый центр платежной системы.

Track 2 Equivalent Data (Tag 57, 19 байт)

PAN Sequence # (5F34, 1 байт)

ARQC (9F26, 8 байт)

IAD (9F10, 32 байта)

Все перечисленные данные могут использоваться для хранения части подписи транзакции криптовалюты. Например, подпись s размером 32 байта может быть передана в поле данных объекта IAD. При этом в объекте Track 2 Equivalent Data для передачи данных эмитенту могут использоваться только 10 байт. Таким образом, общий объем данных, передаваемых эмитенту платежным инструментом, составит 51 байт.

Процессинговый центр платежной системы в автоматическом режиме принимает от хоста эквайрера авторизационный запрос, содержащий данные, сгенерированные платежным инструментов для расчетов в криптовалюте.

При получении авторизационного запроса на процессинговом центре платежной системы принимают сгенерированные на платежном инструменте для расчетов в криптовалюте данные, включая часть подписи транзакции криптовалюты (подпись s) длиной 32 байта. Далее на процессинговом центре платежной системы вычисляют недостающую часть подписи транзакции криптовалюты - значение r, используемое при проверке подписи транзакции криптовалюты.

Поскольку значение r, используемое при проверке подписи транзакции криптовалюты в зависимости от используемого блокчейна, является абсциссой или ординатой случайной точки R циклической подгруппы группы точек эллиптической кривой, на процессинговом центре платежной системы вычисляют значение случайной точки R циклической подгруппы группы точек эллиптической кривой. Для случайной точки R эллиптической кривой выполняется равенство R=kG, где G - образующая циклической подгруппы группы точек эллиптической кривой, известна на процессиноговом центре платежной системы, параметр k, представляет собой случайное число. При этом процессинговый центр платежной системы может вычислить значение R, но не может получить значение k в явном виде. Это достигается реализацией в HSM-устройстве отдельной функции расчета точки R. Подпись s и значение r, используемое при проверке подписи транзакции криптовалюты, связаны друг с другом через вышеупомянутый параметр k.

Для вычисления значения r, используемого при проверке подписи транзакции криптовалюты, на процессинговом центре платежной системы вычисляется значение вышеупомянутого параметра k. Значение вышеупомянутого параметра k вычисляется с использованием закрытого ключа

размером 256 бит, известного в приложении платежного инструмента для расчетов в криптовалюте и на HSM-устройстве процессингового центра платежной системы путем применения алгоритма AES сначала к значению счетчика транзакций криптовалюты ATC, а потом дополнительного к ATC значения. В результате конкатенации полученных значений получится двоичное представление k размером 256 бит.

Далее на процессинговом центре платежной системы по номеру платежного инструмента для расчетов в криптовалюте выводится ключ для генерации вышеупомянутого параметра k и значение счетчика транзакций криптовалюты ATC. Зная значение параметра k вычисляют значение r, используемое при проверке подписи транзакции криптовалюты. Значение r, используемое при проверке подписи транзакции криптовалюты является ординатой или абсциссой точки R в зависимости от используемого блокчейна. Полученное значение r, используемое при проверке подписи транзакции криптовалюты, добавляют его в вышеупомянутый авторизационный запрос. По одному из вариантов реализации, для передачи значения r, используемого при проверке подписи транзакции криптовалюты, можно выделить отдельный тег и добавить этот объект данных в ПЛ-055 сообщения 0100.

После вычисления части подписи транзакции криптовалюты процессинговый центр платежной системы передает эмитенту вышеупомянутый авторизационный запрос, включающий обе части подписи транзакции криптовалюты.

Эмитент в автоматическом режиме принимает авторизационный запрос от процессингового центра платежной системы, определяет по номеру платежного инструмента для расчетов в криптовалюте авторизационный запрос на проведение транзакции криптовалюты. Вышеупомянутый авторизационный запрос включает, в том числе две части подписи транзакции криптовалюты. Используя открытый ключ, полученный при персонализации платежного инструмента для расчетов в криптовалюте, на эмитенте формируют транзакцию криптовалюты в блокчейне. Транзакцию криптовалюты в блокчейне формируют следующим образом. После получения авторизационного запроса на эмитенте, включающего две части подписи транзакции криптовалюты, на эмитенте восстанавливают подпись транзакции криптовалюты из авторизационного запроса, предварительно проверяют валидность подписи

транзакции криптовалюты. Далее, при положительном результате проверки валидности подписи транзакции криптовалюты, эмитент дополняет транзакцию криптовалюты: добавляет размер операции, адрес счета эмитента в блокчейне и идентификатор держателя платежного инструмента для расчетов в криптовалюте. После этого эмитент направляет вышеупомянутую транзакцию криптовалюты на адрес счета эмитента в блокчейн.

Далее эмитент в автоматическом режиме принимает из блокчейна подтверждение о зачислении на адрес счета эмитента в блокчейне средств в криптовалюте, эквивалентных размеру покупки, после чего в стандартном режиме направляет положительный ответ на авторизационного запрос на хост эквайрера, указывающий, что покупка одобрена.

Таким образом, предлагаемое решение предполагает исключение доступа третьих лиц к инициированию в стандартной инфраструктуре обработки операций в карточных платежных системах транзакций криптовалюты со счета владельца платежного инструмента для расчетов в криптовалюте, что повышает безопасность системы и способа проведения транзакций нефиатных валют в карточной инфраструктуре и позволяет расширить арсенал платежных инструментов.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ для проведения транзакций нефиатных валют в карточной инфраструктуре, содержащий платежный инструмент для расчетов в криптовалюте, точку обслуживания платежных инструментов, хост эквайрера, процессинговый центр платежной системы и эмитент, в котором на точке обслуживания платежных инструментов принимают платежный инструмент для расчетов в криптовалюте, принимают от платежного инструмента для расчетов в криптовалюте данные, необходимые для формирования авторизационного запроса, формируют авторизационный запрос и направляют его на хост эквайрера, на хосте эквайрера принимают вышеупомянутый авторизационный запрос и направляют его в процессинговый центр платежной системы, на процессинговом центре платежной системы принимают вышеупомянутый авторизационный запрос и направляют его эмитенту, после чего от эмитента на хост эквайрера передают ответ на вышеупомянутый авторизационный запрос, указывающий, что транзакция криптовалюты авторизована, при этом

- перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте зашифровывают часть подписи транзакции криптовалюты, при этом ключ для шифрования части подписи известен только на платежном инструменте для расчетов в криптовалюте и эмитенте, затем передают данные, необходимые для формирования авторизационного запроса, в том числе зашифрованную часть подписи транзакции криптовалюты, на точку обслуживания платежных инструментов, на точке обслуживания платежных инструментов формируют авторизационный запрос и направляют его на хост эквайрера, на хосте эквайрера принимают вышеупомянутый авторизационный запрос и направляют его в процессинговый центр платежной системы,

- на процессинговом центре платежной системы принимают вышеупомянутый авторизационный запрос от хоста эквайрера и получают номер платежного инструмента для расчетов в криптовалюте через хост эквайрера, затем используют этот номер для генерации недостающей части подписи транзакции криптовалюты и маршрутизации авторизационного запроса, включающего обе части подписи транзакции криптовалюты, к эмитенту карты, соответствующему данному номеру платежного инструмента;

- на эмитенте от процессингового центра платежной системы принимают вышеупомянутый авторизационный запрос, включающий обе части подписи транзакции криптовалюты, затем формируют транзакцию криптовалюты, после чего направляют вышеупомянутую транзакцию криптовалюты на адрес счета эмитента в блокчейне, далее получают из блокчейна подтверждение о зачислении на адрес эмитента в блокчейне средств в криптовалюте, после чего от эмитента на хост эквайрера направляют положительный ответ на авторизационный запрос.

2. Способ для проведения транзакций нефиатных валют в карточной инфраструктуре по п.1, отличающийся тем, что перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте по заранее оговоренному курсу определяют количество средств в криптовалюте, эквивалентных размеру покупки в валюте, которые необходимо передать эмитенту.

3. Способ для проведения транзакций нефиатных валют в карточной инфраструктуре по п.1, отличающийся тем, что эмитент с собственным адресом счета в блокчейне выпускает платежный инструмент для расчета в криптовалюте, платежное приложение которого содержит БИН эмитента в платежной системе.

4. Способ для проведения транзакций нефиатных валют в карточной инфраструктуре по п.1, отличающийся тем, что на платежный инструмент для расчетов в криптовалюте установлено платежное приложение, при помощи которого подготавливают данные для транзакции криптовалюты в блокчейне, размещают данные, необходимые для осуществления транзакции криптовалюты в тегах, используемых в стандартных ответах на команды точки обслуживания платежных инструментов, и отвечают на команды точки обслуживания платежных инструментов.

5. Способ для проведения транзакций нефиатных валют в карточной инфраструктуре по п.1, отличающийся тем, что на платежный инструмент для расчетов в криптовалюте при персонализации эмитент загружает открытый и закрытый ключи, после чего открытый ключ направляют эмитенту.

6. Система для проведения транзакций нефиатных валют в карточной инфраструктуре включает платежный инструмент для расчетов в криптовалюте, точку обслуживания платежных инструментов, хост эквайрера, процессинговый

центр платежной системы и эмитент, в которой точка обслуживания платежных инструментов выполнена с возможностью приема платежных инструментов для расчетов в криптовалюте, приема от платежного инструмента для расчетов в криптовалюте данных, необходимых для формирования авторизационного запроса, формирования авторизационного запроса и его направления на хост эквайрера, хост эквайрера выполнен с возможностью приема вышеупомянутого авторизационного запроса и его направления в процессинговый центр платежной системы, процессинговый центр платежной системы выполнен с возможностью приема вышеупомянутого авторизационного запроса и его направления к эмитенту, эмитент выполнен с возможностью приема вышеупомянутого авторизационного запроса и направления на хост эквайрера ответа на вышеупомянутый авторизационный запрос, указывающий, что транзакция криптовалюты авторизована, при этом

- платежный инструмент для расчетов в криптовалюте выполнен с возможностью шифрования и передачи зашифрованной части подписи транзакции на точку обслуживания платежных инструментов, при этом ключ для шифрования подписи известен только на платежном инструменте для расчетов в криптовалюте и эмитенте,

- процессинговый центр платёжной системы выполнен с возможностью получения номера платежного инструмента для расчетов в криптовалюте через хост эквайрера, использования этого номера для генерации недостающей части подписи транзакции криптовалюты и маршрутизации авторизационного запроса, включающего обе части подписи транзакции криптовалюты, к эмитенту карты, соответствующему данному номеру платежного инструмента;

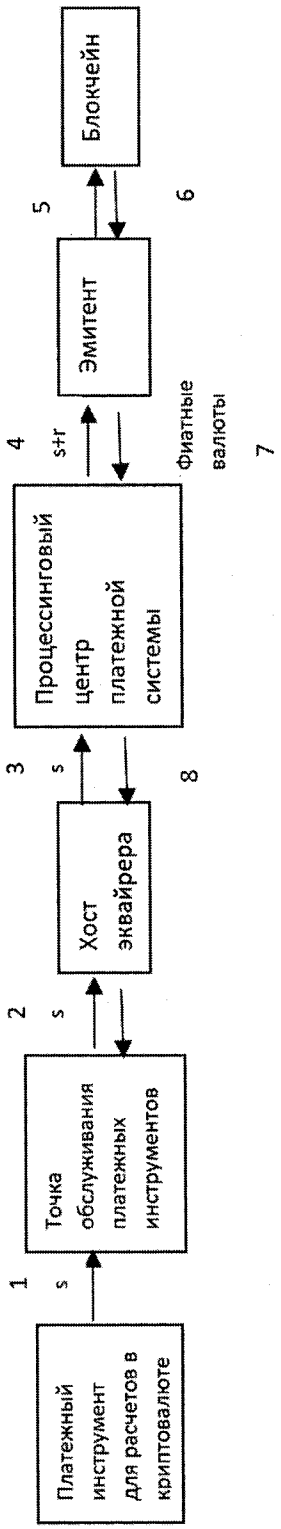
- эмитент, выполненный с возможностью приема вышеупомянутого авторизационного запроса от процессингового центра платежной системы включающего обе части подписи транзакции криптовалюты, формирования после приема вышеупомянутого авторизационного запроса транзакции криптовалюты в блокчейне, направления вышеупомянутой транзакции криптовалюты на адрес счета эмитента в блокчейне, последующего получения из блокчейна подтверждения о зачислении средств в криптовалюте на адрес счета эмитента в блокчейне, и дальнейшего направления положительного ответа на авторизационный запрос на хост эквайрера.

7. Система для проведения транзакций нефиатных валют в карточной инфраструктуре по п.6, отличающаяся тем, что перед передачей данных, необходимых для формирования авторизационного запроса, на платежном инструменте для расчетов в криптовалюте по заранее оговоренному курсу определяют количество средств в криптовалюте, эквивалентных размеру покупки в валюте, которые необходимо передать эмитенту.

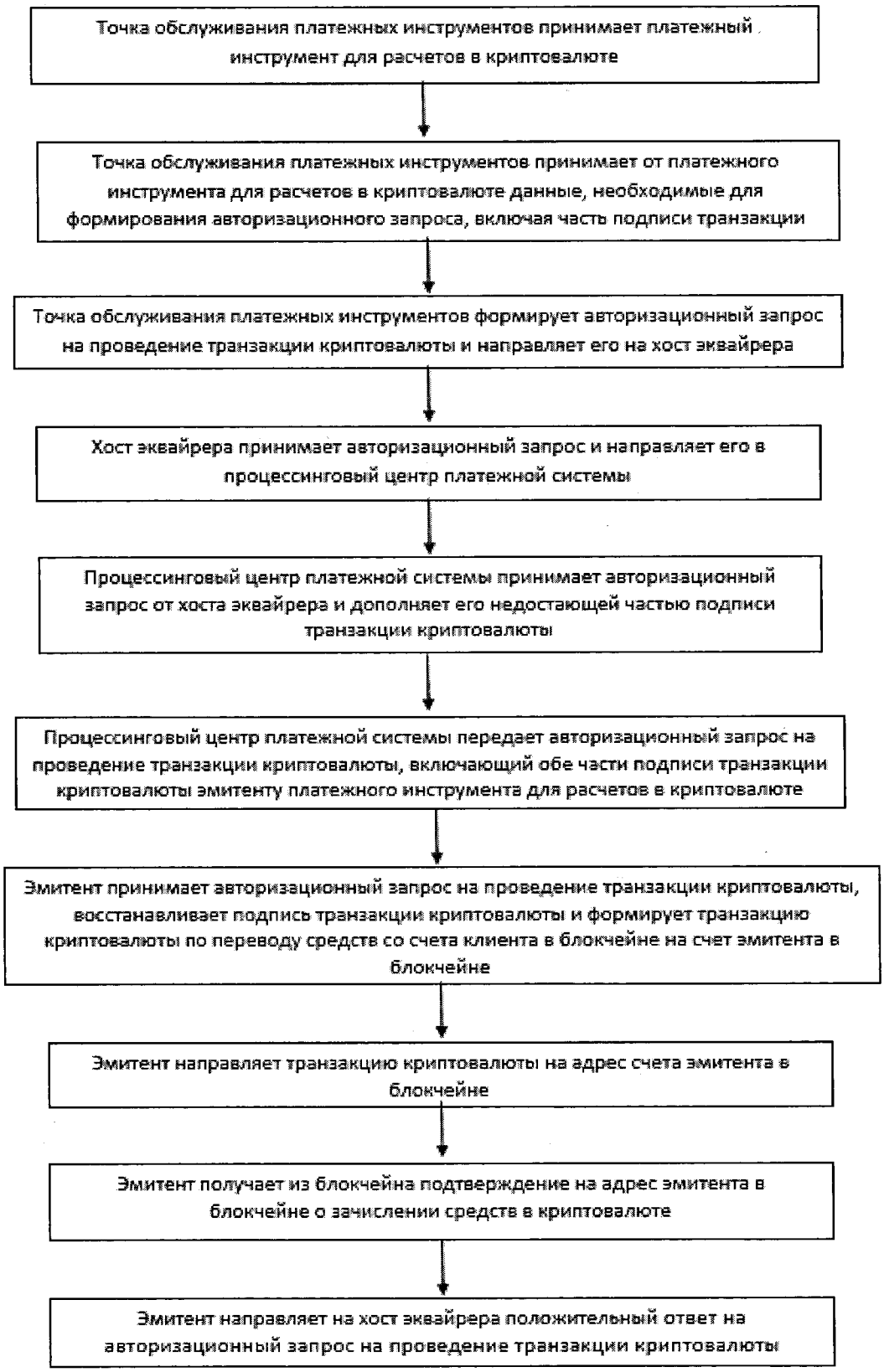
8. Система для проведения транзакций нефиатных валют в карточной инфраструктуре по п.6, отличающаяся тем, что эмитент с собственным адресом счета в блокчейне выпускает платежный инструмент для расчета в криптовалюте, платежное приложение которого содержит БИН эмитента в платежной системе.

9. Система для проведения транзакций нефиатных валют в карточной инфраструктуре по п.6, отличающаяся тем, что на платежный инструмент для расчетов в криптовалюте установлено платежное приложение, при помощи которого подготавливают данные для транзакции криптовалюты в блокчейне, размещают данные, необходимые для проведения транзакции криптовалюты в тегах, используемых в стандартных ответах на команды точки обслуживания платежных инструментов, и отвечают на команды точки обслуживания платежных инструментов.

10. Система для проведения транзакций нефиатных валют в карточной инфраструктуре по п.6, отличающаяся тем, что на платежный инструмент для расчетов в криптовалюте при персонализации эмитент загружает открытый и закрытый ключи, после чего открытый ключ направляют эмитенту.


Платежный инструмент для расчетов в криптовалюте
Точка обслуживания платежных инструментов
Хост эквайрера
Процессинговый центр платежной системы
Эмитент
Блокчейн
1
s
2
s
3
s
4
s+r
5
6
7
8
Фиатные валюты

Фиг. 1


Точка обслуживания платежных инструментов принимает платежный инструмент для расчетов в криптовалюте
Точка обслуживания платежных инструментов принимает от платежного инструмента для расчетов в криптовалюте данные, необходимые для формирования авторизационного запроса, включая часть подписи транзакции
Точка обслуживания платежных инструментов формирует авторизационный запрос на проведение транзакции криптовалюты и направляет его на хост эквайрера
Хост эквайрера принимает авторизационный запрос и направляет его в процессинговый центр платежной системы
Процессинговый центр платежной системы принимает авторизационный запрос от хоста эквайрера и дополняет его недостающей частью подписи транзакции криптовалюты
Процессинговый центр платежной системы передает авторизационный запрос на проведение транзакции криптовалюты, включающий обе части подписи транзакции криптовалюты эмитенту платежного инструмента для расчетов в криптовалюте
Эмитент принимает авторизационный запрос на проведение транзакции криптовалюты, восстанавливает подпись транзакции криптовалюты и формирует транзакцию криптовалюты по переводу средств со счета клиента в блокчейне на счет эмитента в блокчейне
Эмитент направляет транзакцию криптовалюты на адрес счета эмитента в блокчейне
Эмитент получает из блокчейна подтверждение на адрес эмитента в блокчейне о зачислении средств в криптовалюте
Эмитент направляет на хост эквайрера положительный ответ на авторизационный запрос на проведение транзакции криптовалюты

Фиг. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 2021/000180

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/30 (2012.01); G06Q 20/40 (2012.01); H04L 9/32 (2006.01); 04L 29/06 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 20/00-20/40, G06F 21/00-21/46, H04L 9/00-9/32, 29/00-29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019/139655 A1 (VISA INTERNATIONAL SERVICE SERVICE ASSOCIATION) 18.07.2019	1-10
A	US 2019/0156301 A1 (CORNELL UNIVERSITY) 23.05.2019	1-10
A	WO 2018/102057 A1 (MASTERCARD INTERNATIONAL INCORPORATED 2000) 07.06.2018	1-10
A	WO 2019/133578 A1 (AKAMAI TECHNOLOGIES, INC.) 04.07.2019	1-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 August 2021 (06.08.2021)	19 August 2021 (19.08.2021)
Name and mailing address of the ISA/ RU	Authorized officer
Facsimile No.	Telephone No.

ОТЧЕТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Номер международной заявки

PCT/RU 2021/000180

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ

G06Q 20/30 *(2012.01)*
G06Q 20/40 *(2012.01)*
H04L 9/32 *(2006.01)*
H04L 29/06 *(2006.01)*

Согласно Международной патентной классификации МПК

B. ОБЛАСТЬ ПОИСКА

Проверенный минимум документации (система классификации с индексами классификации)

G06Q 20/00-20/40, G06F 21/00-21/46, H04L 9/00-9/32, 29/00-29/08

Другая проверенная документация в той мере, в какой она включена в поисковые подборки

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)

PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Информационно-поисковая система ФИПС

C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ:

Категория*	Цитируемые документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	WO 2019/139655 A1 (VISA INTERNATIONAL SERVICE SERVICE ASSOCIATION) 18.07.2019	1-10
A	US 2019/0156301 A1 (CORNELL UNIVERSITY) 23.05.2019	1-10
A	WO 2018/102057 A1 (MASTERCARD INTERNATIONAL INCORPORATED 2000) 07.06.2018	1-10
A	WO 2019/133578 A1 (AKAMAI TECHNOLOGIES, INC.) 04.07.2019	1-10

☐ последующие документы указаны в продолжении графы C.

☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:

"A" документ, определяющий общий уровень техники и не считающийся особо релевантным

"D" документ, цитируемый заявителем в международной заявке

"E" более ранняя заявка или патент, но опубликованная на дату международной подачи или после нее

"L" документ, подвергающий сомнению притязание(я) на приоритет, или который приводится с целью установления даты публикации другого ссылочного документа, а также в других целях (как указано)

"O" документ, относящийся к устному раскрытию, использованию, экспонированию и т.д.

"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета

"T" более поздний документ, опубликованный после даты международной подачи или приоритета, но приведенный для понимания принципа или теории, на которых основывается изобретение

"X" документ, имеющий наиболее близкое отношение к предмету поиска; заявленное изобретение не обладает новизной или изобретательским уровнем, в сравнении с документом, взятым в отдельности

"Y" документ, имеющий наиболее близкое отношение к предмету поиска; заявленное изобретение не обладает изобретательским уровнем, когда документ взят в сочетании с одним или несколькими документами той же категории, такая комбинация документов очевидна для специалиста

"&" документ, являющийся патентом-аналогом

Дата действительного завершения международного поиска	Дата отправки настоящего отчета о международном поиске
06 августа 2021 (06.08.2021)	19 августа 2021 (19.08.2021)
Наименование и адрес ISA/RU: Федеральный институт промышленной собственности, Бережковская наб., 30-1, Москва, Г-59, ГСП-3, Россия, 125993 Факс: (8-495) 531-63-18, (8-499) 243-33-37	Уполномоченное лицо: Д.М. Старшинов Телефон № 499-240-60-15