(19) Евразийское патентное ведомство

(21) 202092857 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2021.12.31

(22) Дата подачи заявки
2020.12.23

(51) Int. Cl. ***G07C 13/00*** (2006.01)
G06F 17/40 (2006.01)
H04L 9/32 (2006.01)
G06F 21/62 (2013.01)

(54) СПОСОБ И СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ

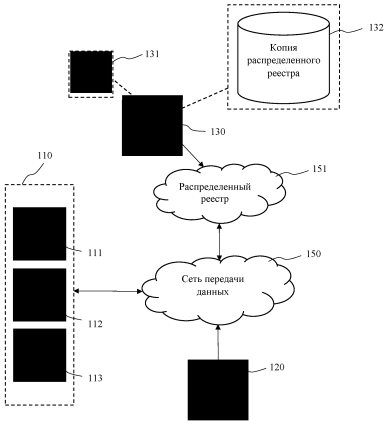
(31) **2020119904**
(32) **2020.06.16**
(33) **RU**

(71) Заявитель:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Кяжин Сергей Николаевич, Попов Владимир Александрович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области компьютерных технологий, в частности к способам и системам электронного анонимного голосования, использующим технологии распределенного реестра. Технический результат заключается в повышении безопасности электронного голосования за счет анонимизации голосующих, исключения возможности влияния на ход и результаты голосования со стороны организатора, а также открытости в распределенном реестре результатов голосования. Заявленный результат достигается за счет компьютерно-реализуемого способа электронного голосования в распределенном реестре, содержащего этапы, на которых с помощью центра сертификации формируют сертификат открытого ключа для каждого устройства пользователя, участвующего в сессии голосования в распределенном реестре; на устройстве организатора формируют сессию для голосования с заданными параметрами, передают от устройства организатора на узел сети распределенного реестра параметры сессии голосования; записывают в распределенный реестр параметры сессии голосования; осуществляют регистрацию участников голосования в сессии голосования, при которой генерируют на каждом из устройств участников пару закрытого VS и открытого VP ключей для связываемой кольцевой подписи; передают от устройств участников открытые ключи VP для соответствующего идентификатора сессии голосования; выполняют аутентификацию устройств пользователей на основе сертификатов открытых ключей; осуществляют логикой смарт-контракта проверку допустимости участия в сессии голосования с помощью проверки наличия сертификатов открытых ключей в параметрах сессии голосования для соответствующего идентификатора сессии голосования и наличия отметки о регистрации для сертификатов открытых ключей; записывают в распределенный реестр открытые ключи VP и отметки о регистрации для соответствующих сертификатов открытых ключей; с помощью центра сертификации формируют анонимный сертификат открытого ключа для каждого устройства пользователя, допущенного к соответствующей сессии голосования; осуществляют голосование участников, при котором каждое устройство получает список всех открытых ключей VP участников текущей сессии голосования для генерирования ответов устройствами участников и вычисления связываемой кольцевой подписи.



202092857 A1

202092857 A1

МПК: G06Q 50/22; G06Q 50/26

СПОСОБ И СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное техническое решение относится к области компьютерных технологий, в частности, к способам и системам электронного анонимного голосования, использующим технологии распределенного реестра.

УРОВЕНЬ ТЕХНИКИ

[0002] Очное голосование обладает определенными недостатками, среди которых:

- отсутствие возможности объективной проверки корректности результатов;
- возможность подачи сфабрикованного голоса организатором вместо полноправного участника;
- возможность повторного голосования при условии сговора организатора и участника.

[0003] Системы электронного голосования решают частично описанные проблемы, однако добавляют новые. Например, часто попытки сделать голосование анонимным приводят к ухудшению возможности проверки.

[0004] Для обеспечения анонимности в ряде решений используют технологию связываемой кольцевой подписи. Значение связываемой кольцевой подписи к сообщению вычисляется одним участником группы с использованием открытых ключей всех участников группы и секретного ключа подписывающего участника. Проверка подписи осуществляется с использованием открытых ключей всех участников группы. При этом: по значению подписи невозможно понять, кто из участников группы является ее автором (но известно, что кто-то из указанной группы); по двум значениям подписи (к одному или разным сообщениям) можно понять, разные у них авторы или один (при этом в последнем случае неизвестно, кто именно).

[0005] Пример такого подхода описан в работе Liu J.K. et al. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. Information Security and Privacy. ACISP 2004. Lecture Notes in Computer Science, vol 3108. 2004. Pp. 325-335.

[0006] Для обеспечения возможности проверки корректности результатов голосования в ряде решений используют технологии распределенного реестра. Системы распределенного реестра можно разделить на две группы в зависимости от контроля доступа участников: открытые системы (общедоступны для любых участников) и системы с контролируемым доступом (разграничение прав доступа регламентируется администратором).

[0007] В качестве аналога предлагаемого решения можно рассмотреть систему электронного голосования, известную из работы Kirillov D. et al. Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain. Computational Science and Its Applications. Lecture Notes in Computer Science, vol 11620. 2019. Pp. 509-521. Данное решение предполагает использование системы распределенного реестра, допускающей возможность работы центра сертификации в режиме анонимизации участников, однако применяемая технология подписи вслепую может привести к возможности подачи сфабрикованного голоса организатором.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0008] Решаемой технической проблемой, присущей известным из уровня техники решениям, является анонимизация голосующих при сохранении возможности проверки корректности результатов голосования, а также невозможности подачи сфабрикованного голоса организатором.

[0009] Технический результат заключается в повышении безопасности электронного голосования за счет анонимизации голосующих, исключения возможности влияния на ход и результаты голосования со стороны организатора, а также открытости в распределенном реестре результатов голосования.

[0010] Заявленный результат достигается за счет компьютерно-реализуемого способа электронного голосования в распределенном реестре, содержащего этапы, на которых:

- с помощью центра сертификации формируют сертификат открытого ключа для каждого устройства пользователя, участвующего в сессии голосования в распределенном реестре;
- на устройстве организатора формируют сессию для голосования, параметры которой содержат по меньшей мере идентификатор сессии и перечень упомянутых сертификатов открытых ключей устройств пользователей,

- передают от устройства организатора на узел сети распределенного реестра параметры сессии голосования;
- записывают в распределенный реестр параметры сессии голосования;
- осуществляют регистрацию участников голосования в сессии голосования, при которой
    - генерируют на каждом из устройств участников пару закрытого VS и открытого VP ключей для связываемой кольцевой подписи;
    - передают от устройств участников на упомянутый узел сети распределенного реестра упомянутые открытые ключи VP для соответствующего идентификатора сессии голосования;
    - выполняют аутентификацию устройств пользователей на основе сертификатов открытых ключей;
    - осуществляют логикой смарт-контракта проверку допустимости участия в сессии голосования с помощью проверки наличия сертификатов открытых ключей в параметрах сессии голосования для соответствующего идентификатора сессии голосования и наличия отметки о регистрации для сертификатов открытых ключей;
    - записывают в распределенный реестр открытые ключи VP и отметки о регистрации для соответствующих сертификатов открытых ключей;
- с помощью центра сертификации формируют анонимный сертификат открытого ключа для каждого устройства пользователя, допущенного к соответствующей сессии голосования;
- осуществляют голосование участников, при котором
    - каждое устройство получает список всех открытых ключей VP участников текущей сессии голосования;
    - формируют на каждом из устройств участников ответы для текущей сессии голосования;
    - вычисляют на каждом из упомянутых устройств участников значение связываемой кольцевой подписи на основании сформированных ответов,

секретного ключа VS участника и всех открытых ключей VP участников текущей сессии голосования;

- передают от устройств участников на узел сети распределенного реестра сформированные ответы, а также значение связываемой кольцевой подписи;
- выполняют аутентификацию устройств пользователей на основе анонимных сертификатов открытых ключей;
- осуществляют логикой смарт-контракта проверку значения связываемой кольцевой подписи, используя сформированные ответы и открытые ключи VP участников текущей сессии голосования, и проверку факта осуществленной ранее передачи результатов голосования данным участником, используя проверенное значение связываемой кольцевой подписи и значения подписей, записанные ранее в распределенный реестр;
- записывают в распределенный реестр ответы соответственно значению связываемой кольцевой подписи.

[0011] В одном из частных примеров реализации способа, после проверки допустимости участия пользователя в сессии голосования, открытый ключ VP и сертификат открытого ключа устройства пользователя связываются для соответствующего идентификатора сессии голосования.

[0012] В другом частном примере реализации способа, с помощью центра сертификации формируется сертификат открытого ключа для устройства организатора, на основе которого выполняется аутентификация устройства организатора.

[0013] В другом частном примере реализации способа, сертификаты открытых ключей хранятся в центре сертификации, на устройствах пользователей и на узлах сети распределенного реестра.

[0014] В другом частном примере реализации способа, сеть распределенного реестра представляет собой блокчейн-сеть.

[0015] В другом частном примере реализации способа, блокчейн-сеть содержит упорядочивающие узлы, формирующие блоки для записи в реестр.

[0016] В другом частном примере реализации способа, блокчейн-сеть выполнена с помощью системы Hyperledger Fabric.

[0017] Заявленный технический результат также достигается за счет системы электронного голосования в распределенном реестре, которая содержит:

центр сертификации, выполненный с возможностью

формирования сертификатов открытых ключей для устройств пользователей, участвующих в сессии голосования в распределенном реестре;

формирования анонимных сертификатов открытых ключей для устройств пользователей, допущенных к соответствующей сессии голосования;

устройство организатора, выполненное с возможностью

формирования сессии для голосования, параметры которой содержат по меньшей мере идентификатор сессии и перечень упомянутых сертификатов открытых ключей устройств пользователей;

передачи на узел сети распределенного реестра параметров сессии голосования ;

по меньшей мере одно устройство пользователя, участвующего в сессии голосования, выполненное с возможностью

генерации пары закрытого VS и открытого VP ключей для связываемой кольцевой подписи;

передачи на узел сети распределенного реестра открытого ключа VP для соответствующего идентификатора сессии голосования;

формирования ответов для текущей сессии голосования;

получения списка всех открытых ключей VP участников текущей сессии голосования;

вычисления значения связываемой кольцевой подписи на основании сформированных ответов, секретного ключа VS участника и всех открытых ключей VP участников текущей сессии голосования;

передачи на узел сети распределенного реестра сформированных ответов и значения связываемой кольцевой подписи;

по меньшей мере один узел сети распределенного реестра, выполненный с возможностью

осуществления аутентификации устройств пользователей на основе сертификатов открытых ключей и анонимных сертификатов открытых ключей;

хранения распределенного реестра;

записи в распределенный реестр параметров сессии голосования;

записи в распределенный реестр открытых ключей VP и отметок о регистрации для соответствующих сертификатов открытых ключей;

осуществления логикой смарт-контракта проверки допустимости участия пользователя в сессии голосования с помощью проверки наличия сертификата открытого ключа в параметрах сессии голосования для соответствующего идентификатора сессии голосования и наличия отметки о регистрации для сертификата открытого ключа;

осуществления логикой смарт-контракта проверки значения связываемой кольцевой подписи с использованием сформированных ответов участника и всех открытых ключей VP участников текущей сессии голосования и проверки факта осуществленной ранее передачи результатов голосования данным участником с использованием проверенного значения связываемой кольцевой подписи и значений подписей, записанных ранее в распределенный реестр;

записи в распределенный реестр ответов соответственно значению связываемой кольцевой подписи.

[0018] В одном из частных примеров заявленной системы, после проверки допустимости участия пользователя в сессии голосования, открытый ключ VP и сертификат открытого ключа устройства пользователя связываются для соответствующего идентификатора сессии голосования.

[0019] В другом частном примере заявленной системы, центр сертификации выполнен с возможностью формирования сертификата открытого ключа для устройства организатора.

[0020] В другом частном примере заявленной системы, узел распределенного реестра выполнен с возможностью осуществления аутентификации устройства организатора на основе сертификата открытого ключа.

[0021] В другом частном примере заявленной системы, сертификаты открытых ключей хранятся в центре сертификации, на устройствах пользователей и на узлах сети распределенного реестра.

[0022] В другом частном примере заявленной системы, сеть распределенного реестра представляет собой блокчейн-сеть.

[0023] В другом частном примере заявленной системы, блокчейн-сеть содержит упорядочивающие узлы, формирующие блоки для записи в реестр.

[0024] В другом частном примере заявленной системы, блокчейн-сеть выполнена с помощью системы Hyperledger Fabric.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0025] Фиг. 1А иллюстрирует общую схему заявленного решения.

[0026] Фиг. 1Б иллюстрирует схему взаимодействия устройств – участников голосования.

[0027] Фиг. 2 иллюстрирует блок-схему выполнения заявленного способа.

[0028] Фиг. 3 иллюстрирует схему процесса регистрации участников голосования.

[0029] Фиг. 4 иллюстрирует схему процесса голосования участниками.

[0030] Фиг. 5 иллюстрирует общий вид вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0031] Как представлено на Фиг. 1А, общая схема заявленного решения включает в себя следующие элементы. Устройства участников голосования (110), центр сертификации (120), узел (130) распределенного реестра, содержащий смарт-контракт (131) и копию распределенного реестра (132). Все элементы системы объединены сетью передачи данных (150), например, Интернет, а также сетью распределенного реестра (151).

[0032] В качестве сети распределенного реестра (151) может применяться различный тип блокчейн протоколов (блокчейн сети). Предлагаемое техническое решение предполагает использование системы с контролируемым доступом, то есть все участники и

их права известны заранее. Пример такой системы — Hyperledger Fabric. В предлагаемом решении система распределенного реестра используется для того, чтобы обеспечить невозможность цензуры и возможность проверки результатов как непосредственными участниками, так и внешними наблюдателями.

[0033] Сеть передачи данных (150) может быть организована с помощью любого известного подхода, обеспечивающего информационный обмен для используемых устройств, например, посредством принципов связи: WAN, LAN, WLAN, Wi-Fi, GSM и т.п.

[0034] В качестве центра сертификации (120) используется вычислительный узел, например, серверное приложение или сервер, обеспечивающий заданный функционал. Программный компонент, реализуемый с помощью центра (120), может быть создан на основе исполняемого кода системы распределенного реестра, либо на основе внешнего исполняемого кода. Центр сертификации (120) может работать в двух режимах: стандартный (выпуск, учет и отзыв криптографических сертификатов пользователей (110)) и режим анонимизации участников с сохранением атрибутов (выпуск, учет и отзыв анонимных криптографических сертификатов с атрибутами). В заявленном решении для обеспечения процесса голосования используется единственный атрибут — вхождение пользователя (110) в список пользователей системы. Валидность данного атрибута проверяется центром сертификации (120).

[0035] В качестве устройств участников голосования (110) могут применяться любые технические средства, обеспечивающие обработку требуемых данных и обладающие заданным функционалом для работы через сеть передачи данных (150). Таким устройствами могут являться: смартфоны, компьютеры, ноутбуки, игровые приставки, умные устройства (телевизоры, носимые устройства) и т.п.

[0036] Устройства (110) содержат исполняемый процессором устройства программный компонент, который необходим для взаимодействия пользователей (110) с сетью распределенного реестра (151) и центром сертификации (120).

[0037] Как показано на Фиг. 1Б, устройства (110) распределяются на роли в системе для осуществления процесса голосования (111 - 113), в частности, такими ролями являются: организатор (111), голосующие (121 – 12n) и наблюдатель (113).

[0038] Устройство организатора (111) обеспечивает инициализацию сессии голосования. Организатор (111) составляет перечень вопросов и перечень участников

голосования, определяет сроки регистрации и голосования. Устройства участников голосования (121 – 12n) обеспечивают регистрацию в требуемой сессии голосования, а также непосредственно голосование. Наблюдатель (113) следит за корректностью работы системы.

[0039] Узел сети распределенного реестра (130) (один или более) представляет собой вычислительный узел с программным компонентом, который может быть создан на основе исполняемого кода системы распределенного реестра (например, указанной выше системы Hyperledger Fabric). Узел сети распределенного реестра (130) содержит копию распределенного реестра (132), смарт-контракт (131) и среду исполнения программного кода смарт-контрактов. Смарт-контракт (131) представляет собой программную логику, реализующую функционал процесса голосования.

[0040] Также архитектура решения может включать в себя один или несколько упорядочивающих узлов сети распределенного реестра (не показан на Фиг. 1А). Программный компонент такого узла может быть сформирован на основе исполняемого кода системы распределенного реестра. Упорядочивающий узел обеспечивает упорядочивание изменений в реестре.

[0041] На Фиг. 2 представлен общий процесс выполнения заявленного способа (200) электронного голосования. Перед началом создания сессии голосования определяются права для устройств пользователей (110), перечень узлов (130), выполняется настройка центра сертификации (120), загрузка смарт-контракта (131). Дополнительно может определяться перечень упорядочивающих узлов.

[0042] На первом этапе (201) осуществляется формирование сертификатов открытых ключей для устройств пользователей (110), участвующих в сессии голосования. Сертификаты открытых ключей формируются центром сертификации (120). Для каждого пользователя (110) создается пара открытого и секретного ключа (Pi, Si), где i — номер пользователя.

[0043] Сертификат открытого ключа может храниться в центре сертификации, на узлах сети распределенного реестра, на устройстве пользователя, секретный ключ — например, в личном хранилище пользователя, доступ к которому реализован с помощью устройства (110) пользователя и управляется специализированным приложением. Каждый элемент

взаимодействия пользователя под номером i с сетью распределенного реестра подразумевает аутентификацию по сертификату, который содержит открытый ключ Pi.

[0044] На этапе (202) выполняется создание сессии голосования с параметрами допуска устройств участников (121 – 12n), для чего на устройстве организатора (111) формируют сессию для голосования, параметры которой содержат идентификатор сессии (ID) и перечень сертификатов открытых ключей устройств пользователей Pj, j = 1,…,n. Также параметрами сессии голосования могут выступать такие данные, как: перечень вопросов, сроки регистрации и голосования и т.п.

[0045] Параметры сессии голосования на этапе (203) передаются от устройства организатора (111) на узел распределенного реестра (130). В результате обработки полученных параметров в сети распределенного реестра (151) выполняется их запись в распределенный реестр (132) .

[0046] На этапе (204) осуществляется регистрация участников голосования (121 – 12n) в сессии голосования, сформированной устройством организатора (111). Процесс регистрации участников голосования будет рассмотрен более подробно с отсылкой к Фиг. 3.

[0047] На первом этапе (301) регистрации устройств участников (121 – 12n) сессии голосования выполняется генерация пары открытого и секретного ключей для голосования (VPj, VSj), j — номер участника (121 – 12n), которые будут использоваться в схеме связываемой кольцевой подписи. Далее на этапе (302) каждое из зарегистрированных устройств отправляет открытый ключ VPj и ID сессии голосования, в котором он хочет принять участие, на узел распределенного реестра (130) посредством сети передачи данных (150).

[0048] Узел (130) выполняет аутентификацию устройств пользователей (этап 303) на основе сертификатов открытых ключей.

[0049] Затем смарт-контракт (131) выполняет проверку (этап 304), что текущий пользователь (121 – 12n) имеет право участвовать в сессии голосования с соответствующим ID. Для этого на этапе (305) должно соблюдаться условие наличия соответствующего открытого ключа Pj в перечне параметров, сформированных устройством организатора (111). При успешной валидации в сети распределенного реестра (151) выполняется запись в реестр (132) ключа для голосования VPj соответствующего устройства участника (121 – 12n) (этап 306). Если запись

соответствующего ключа Pj отсутствует в параметрах сессии, то пользователь не допускается к сессии голосования (этап 307). При доступе или отказе в доступе может формироваться соответствующее уведомление, отображаемое на устройстве пользователя (121 – 12n).

[0050] На этапе (205) с помощью центра сертификации (120) осуществляется формирование анонимных сертификатов открытого ключа для каждого устройства пользователя (121 – 12n), допущенного к соответствующей сессии голосования.

[0051] Каждый участник (121 – 12n), который зарегистрировал свой ключ VPj для сессии голосования, на этапе (205) взаимодействует с центром сертификации (120), который работает в режиме анонимизации участников с сохранением атрибутов, для получения анонимного сертификата с атрибутами, выдача которого будет означать, что владелец сертификата входит в список пользователей системы. Взаимодействие может выполняться через программное приложение, установленное на устройстве (121 – 12n).

[0052] Процесс голосования будет описан подробнее с отсылкой на Фиг. 4. На первом этапе голосования (401) каждым из допущенных устройств (121 – 12n) выполняется загрузка открытых ключей всех устройств (121 – 12n) VPj, j = 1,…,n, для соответствующей сессии голосования. Это требуется для последующего вычисления связываемой кольцевой подписи.

[0053] Каждый участник с помощью своего устройства формирует на этапе (402) ответы на вопросы и вычисляет для полученного в результате формирования ответов сообщения значение связываемой кольцевой подписи с помощью секретного ключа участника VSj, j — номер участника, и множества всех загруженных открытых ключей для голосования VPj, j = 1,…,n (этап 403).

[0054] Далее на этапе (404) сформированные ответы в сессии голосования отправляются от каждого из устройств (121 – 12n) на узел (130) в виде сообщения, содержащего ответы и значение связываемой кольцевой подписи. На этапе (405) выполняется аутентификация каждого устройства (121 – 12n) с помощью анонимного сертификата.

[0055] Логикой смарт-контракта (131) проверяется, верна ли связываемая кольцевая подпись (этап 406), с использованием открытых ключей для голосования всех участников (121 – 12n) VPj, j = 1,…,n. Также для каждого значения связываемой кольцевой подписи выполняется проверка факта осуществления ранее голосования

соответствующим участником (121 – 12n), что проверяется возможностью связывания текущего значения подписи с одним из записанных ранее в распределенный реестр.

[0056] Если значение связываемой кольцевой подписи верное, то на этапе (407) выполняется запись (или перезапись, если участник ранее голосовал) ее значения и ответов участника (121 – 12n) в распределенный реестр (132). До окончания процедуры голосования участник (121 – 12n) может получить другой анонимный сертификат и отправить новое сообщение для изменения своего решения. Подсчёт результатов голосования происходит одновременно, после учёта каждого голоса.

[0057] Далее рассмотрим подробнее принцип работы связываемой кольцевой подписи. Пусть имеется группа устройств участников голосования (121 – 12n), у каждого устройства имеется ключ подписи VPj (открытый) и ключ проверки подписи VSj (секретный), $j = 1, \ldots, n$. Также есть некоторое сообщение m, которое требуется подписать.

[0058]

[0059] Кольцевая подпись от имени группы участников сессии голосования вычисляется с помощью алгоритма *Sign*(*m, VP1*, ..., *VPn, VSk*), который принимает на вход сообщение m, открытые ключи всех участников группы *VP1*, ..., *VPn* и секретный ключ *VSk* подписывающего участника, возвращает значение кольцевой подписи σ.

[0060] Значение кольцевой подписи проверяется с помощью алгоритма *Verify*(*m, VP1*, ..., *VPn,* σ) , который принимает на вход сообщение m, открытые ключи всех участников сессии голосования *VP1*, ..., *VPn* и значение подписи σ, возвращает значение “да” или “нет”.

[0061] Таким образом, кольцевая подпись позволяет одному из участников группы подписать сообщение от имени группы, при этом по значению подписи не будет известно, кто именно из участников группы его подписал.

[0062] У связываемой кольцевой подписи, которая используется в предлагаемом решении, алгоритмы принимают такие же параметры, но имеются следующие отличия:

– алгоритм вычисления подписи *Sign*(*m, VP1*, ..., *VPn, VSk*) внутри себя содержит функцию *TagGen*(*VP1*, ..., *VPn, VSk*) , которая возвращает идентификатор, который

не зависит от сообщения и по которому нельзя восстановить VSk или VPk (этот идентификатор является частью значения подписи σ);

– появляется дополнительная возможность по двум значениям подписи понять, разные у них авторы или один (но по-прежнему неизвестно, какой).

[0063] В предлагаемом решении связываемая кольцевая подпись используется для обеспечения двух свойств. В-первых, она позволяет обеспечить невозможность определить, какой участник как проголосовал, благодаря базовому свойству — неизвестно, кто из голосующих поставил подпись под сообщением с голосом, но точно известно, что кто-то из группы участников для соответствующей ID сессии.

[0064] Во-вторых, она позволяет защититься от ситуации, когда один из голосующих проголосует дважды, благодаря дополнительному свойству — если голосующий отправит два сообщения с голосом, можно будет понять, что это был один и тот же человек, но неизвестно, кто именно.

[0065] Все запросы, направляемые в сеть распределенного реестра (150), по умолчанию подписываются обыкновенной подписью, для этого используются сертификаты открытого ключа (либо обыкновенные, либо анонимные), выданные центром сертификации (120). Чтобы работать с кольцевой подписью, используются ключи, которые не связаны ни с обычными сертификатами, ни с анонимными. Пользователи на этапе регистрации (204) генерируют новые ключи и отправляют их в сеть, а на этапе голосования (206) вычисляют значения связываемой кольцевой подписи с использованием упомянутых ключей и отправляют их в сеть внутри запроса, подписанного обыкновенной подписью.

[0066] На Фиг. 5 представлен пример общего вида вычислительного устройства (500), на базе которого может быть реализовано заявленное решение, в частности вычислительные устройства, и элементы, выполняющие вычислительную обработку информации.

[0067] В общем случае, устройство (500) содержит объединенные общей шиной информационного обмена (510) один или несколько процессоров (501), средства памяти, такие как ОЗУ (502) и ПЗУ (503), интерфейсы ввода/вывода (504), устройства ввода/вывода (505), и устройство для сетевого взаимодействия (506). В общем случае устройство (500) может представлять собой сервер, серверный кластер, мейнфрейм, суперкомпьютер, или иной тип пригодного вычислительного устройства.

[0068] Процессор (501) (или несколько процессоров, многоядерный процессор и т.п.) может выбираться из ассортимента устройств, широко применяемых в настоящее время, например, таких производителей, как: Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором или одним из используемых процессоров в устройстве (500) также необходимо учитывать графический процессор, например, GPU NVIDIA или Graphcore, тип которых также является пригодным для полного или частичного выполнения заявленного способа, а также может применяться для обучения и применения моделей машинного обучения в различных информационных системах.

[0069] ОЗУ (502) представляет собой оперативную память и предназначено для хранения исполняемых процессором (501) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (502), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.). При этом, в качестве ОЗУ (502) может выступать доступный объем памяти графической карты или графического процессора.

[0070] ПЗУ (503) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

[0071] Для организации работы компонентов устройства (500) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (504). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

[0072] Для обеспечения взаимодействия пользователя с устройством (500) применяются различные средства (505) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор, мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

[0073] Средство сетевого взаимодействия (506) обеспечивает передачу данных посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (506) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

[0074] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА

1. Компьютерно-реализуемый способ электронного голосования в распределенном реестре, содержащий этапы, на которых:

- с помощью центра сертификации формируют сертификат открытого ключа для каждого устройства пользователя, участвующего в сессии голосования в распределенном реестре;
- на устройстве организатора формируют сессию для голосования, параметры которой содержат по меньшей мере идентификатор сессии и перечень упомянутых сертификатов открытых ключей устройств пользователей,
- передают от устройства организатора на узел сети распределенного реестра параметры сессии голосования;
- записывают в распределенный реестр параметры сессии голосования;
- осуществляют регистрацию участников голосования в сессии голосования, при которой
    - генерируют на каждом из устройств участников пару закрытого VS и открытого VP ключей для связываемой кольцевой подписи;
    - передают от устройств участников на упомянутый узел сети распределенного реестра упомянутые открытые ключи VP для соответствующего идентификатора сессии голосования;
    - выполняют аутентификацию устройств пользователей на основе сертификатов открытых ключей;
    - осуществляют логикой смарт-контракта проверку допустимости участия в сессии голосования с помощью проверки наличия сертификатов открытых ключей в параметрах сессии голосования для соответствующего идентификатора сессии голосования и наличия отметки о регистрации для сертификатов открытых ключей;
    - записывают в распределенный реестр открытые ключи VP и отметки о регистрации для соответствующих сертификатов открытых ключей;

- с помощью центра сертификации формируют анонимный сертификат открытого ключа для каждого устройства пользователя, допущенного к соответствующей сессии голосования;
- осуществляют голосование участников, при котором
    - каждое устройство получает список всех открытых ключей VP участников текущей сессии голосования;
    - формируют на каждом из устройств участников ответы для текущей сессии голосования;
    - вычисляют на каждом из упомянутых устройств участников значение связываемой кольцевой подписи на основании сформированных ответов, секретного ключа VS участника и всех открытых ключей VP участников текущей сессии голосования;
    - передают от устройств участников на узел сети распределенного реестра сформированные ответы, а также значение связываемой кольцевой подписи;
    - выполняют аутентификацию устройств пользователей на основе анонимных сертификатов открытых ключей;
    - осуществляют логикой смарт-контракта проверку значения связываемой кольцевой подписи, используя сформированные ответы и открытые ключи VP участников текущей сессии голосования, и проверку факта осуществленной ранее передачи результатов голосования данным участником, используя проверенное значение связываемой кольцевой подписи и значения подписей, записанные ранее в распределенный реестр;
    - записывают в распределенный реестр ответы соответственно значению связываемой кольцевой подписи.

2. Способ по п.1, характеризующийся тем, что после проверки допустимости участия пользователя в сессии голосования, открытый ключ VP и сертификат открытого ключа устройства пользователя связываются для соответствующего идентификатора сессии голосования.

3. Способ по п.1, характеризующийся тем, что с помощью центра сертификации формируется сертификат открытого ключа для устройства организатора, на основе которого выполняется аутентификация устройства организатора.

4. Способ по п.1, характеризующийся тем, что сертификаты открытых ключей хранятся в центре сертификации, на устройствах пользователей и на узлах сети распределенного реестра.

5. Способ по п.1, характеризующийся тем, что сеть распределенного реестра представляет собой блокчейн-сеть.

6. Способ по п.5, характеризующийся тем, что блокчейн-сеть содержит упорядочивающие узлы, формирующие блоки для записи в реестр.

7. Способ по п.5 характеризующийся тем, что блокчейн-сеть выполнена с помощью системы Hyperledger Fabric.

8. Система электронного голосования в распределенном реестре, содержащая:

центр сертификации, выполненный с возможностью

формирования сертификатов открытых ключей для устройств пользователей, участвующих в сессии голосования в распределенном реестре;

формирования анонимных сертификатов открытых ключей для устройств пользователей, допущенных к соответствующей сессии голосования;

устройство организатора, выполненное с возможностью

формирования сессии для голосования, параметры которой содержат по меньшей мере идентификатор сессии и перечень упомянутых сертификатов открытых ключей устройств пользователей;

передачи на узел сети распределенного реестра параметров сессии голосования ;

по меньшей мере одно устройство пользователя, участвующего в сессии голосования, выполненное с возможностью

генерации пары закрытого VS и открытого VP ключей для связываемой кольцевой подписи;

передачи на узел сети распределенного реестра открытого ключа VP для соответствующего идентификатора сессии голосования;

формирования ответов для текущей сессии голосования;

получения списка всех открытых ключей VP участников текущей сессии голосования;

вычисления значения связываемой кольцевой подписи на основании сформированных ответов, секретного ключа VS участника и всех открытых ключей VP участников текущей сессии голосования;

передачи на узел сети распределенного реестра сформированных ответов и значения связываемой кольцевой подписи;

по меньшей мере один узел сети распределенного реестра, выполненный с возможностью

осуществления аутентификации устройств пользователей на основе сертификатов открытых ключей и анонимных сертификатов открытых ключей;

хранения распределенного реестра;

записи в распределенный реестр параметров сессии голосования;

записи в распределенный реестр открытых ключей VP и отметок о регистрации для соответствующих сертификатов открытых ключей;

осуществления логикой смарт-контракта проверки допустимости участия пользователя в сессии голосования с помощью проверки наличия сертификата открытого ключа в параметрах сессии голосования для соответствующего идентификатора сессии голосования и наличия отметки о регистрации для сертификата открытого ключа;

осуществления логикой смарт-контракта проверки значения связываемой кольцевой подписи с использованием сформированных ответов участника и всех открытых ключей VP участников текущей сессии голосования и проверки факта осуществленной ранее передачи результатов голосования данным участником с использованием проверенного значения связываемой

кольцевой подписи и значений подписей, записанных ранее в распределенный реестр;

записи в распределенный реестр ответов соответственно значению связываемой кольцевой подписи.

9. Система по п.8, характеризующаяся тем, что после проверки допустимости участия пользователя в сессии голосования, открытый ключ VP и сертификат открытого ключа устройства пользователя связываются для соответствующего идентификатора сессии голосования.

10. Система по п.8, характеризующаяся тем, что центр сертификации выполнен с возможностью формирования сертификата открытого ключа для устройства организатора.

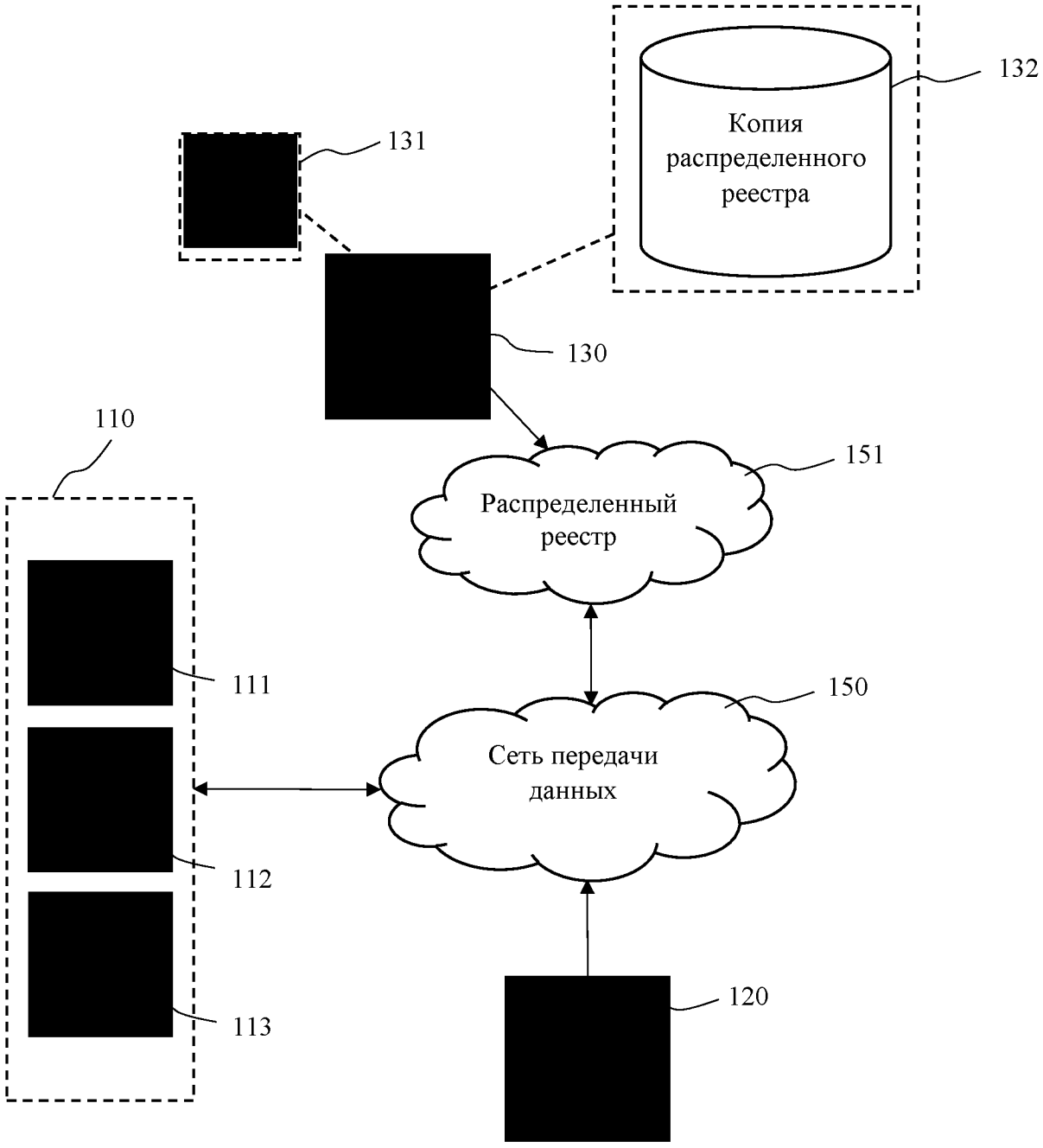
11. Система по п.8, характеризующаяся тем, что узел распределенного реестра выполнен с возможностью осуществления аутентификации устройства организатора на основе сертификата открытого ключа.

12. Система по п.8, характеризующаяся тем, что сертификаты открытых ключей хранятся в центре сертификации, на устройствах пользователей и на узлах сети распределенного реестра.

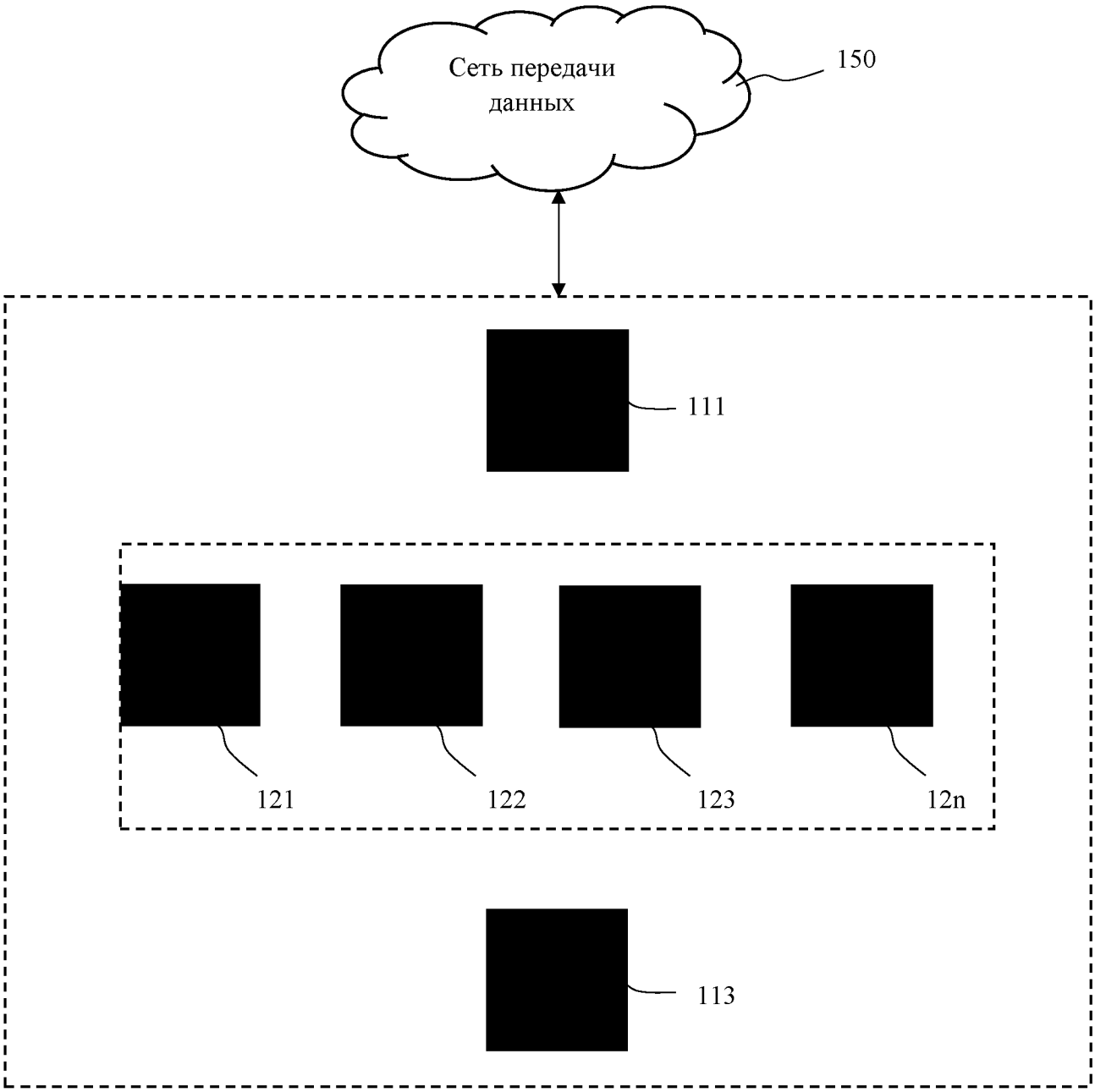
13. Система по п.8, характеризующаяся тем, что сеть распределенного реестра представляет собой блокчейн-сеть.

14. Система по п.13, характеризующаяся тем, что блокчейн-сеть содержит упорядочивающие узлы, формирующие блоки для записи в реестр.

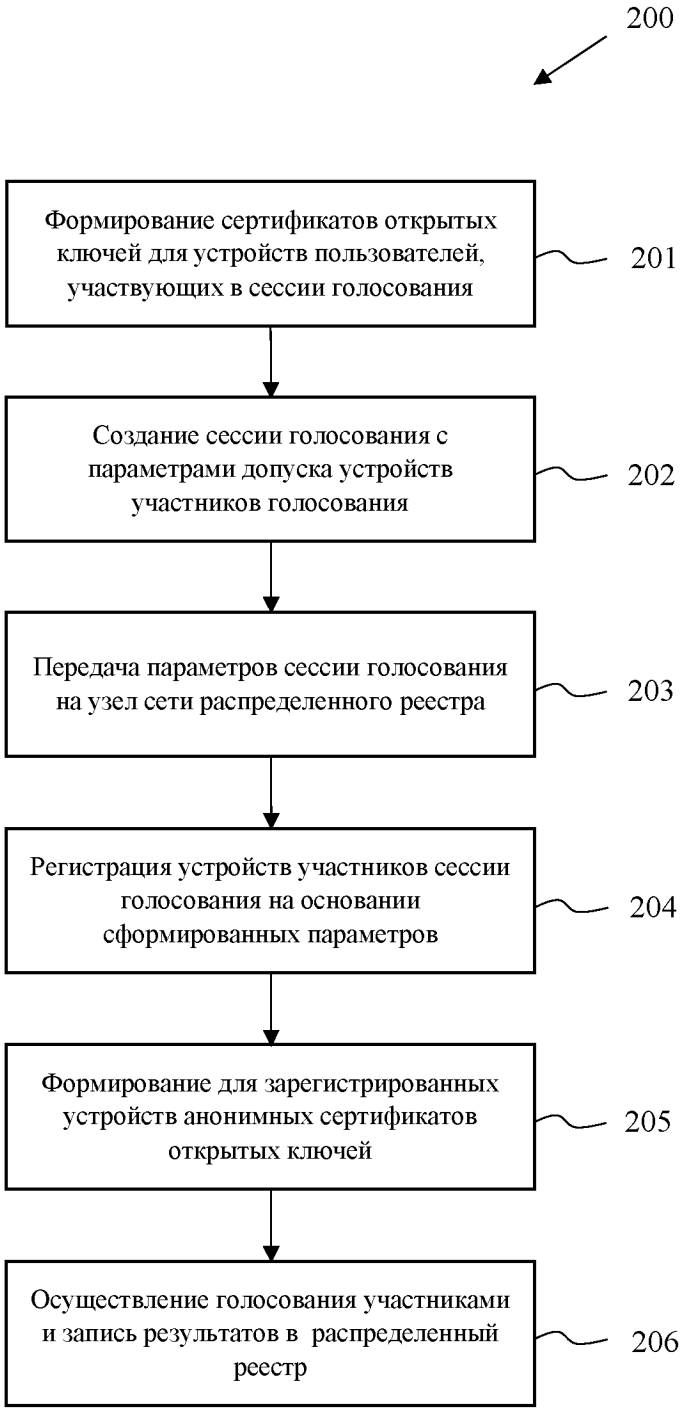
15. Система по п.13, характеризующаяся тем, что блокчейн-сеть выполнена с помощью системы Hyperledger Fabric.


Копия распределенного реестра
132
131
130
110
151
Распределенный реестр
111
150
Сеть передачи данных
112
113
120

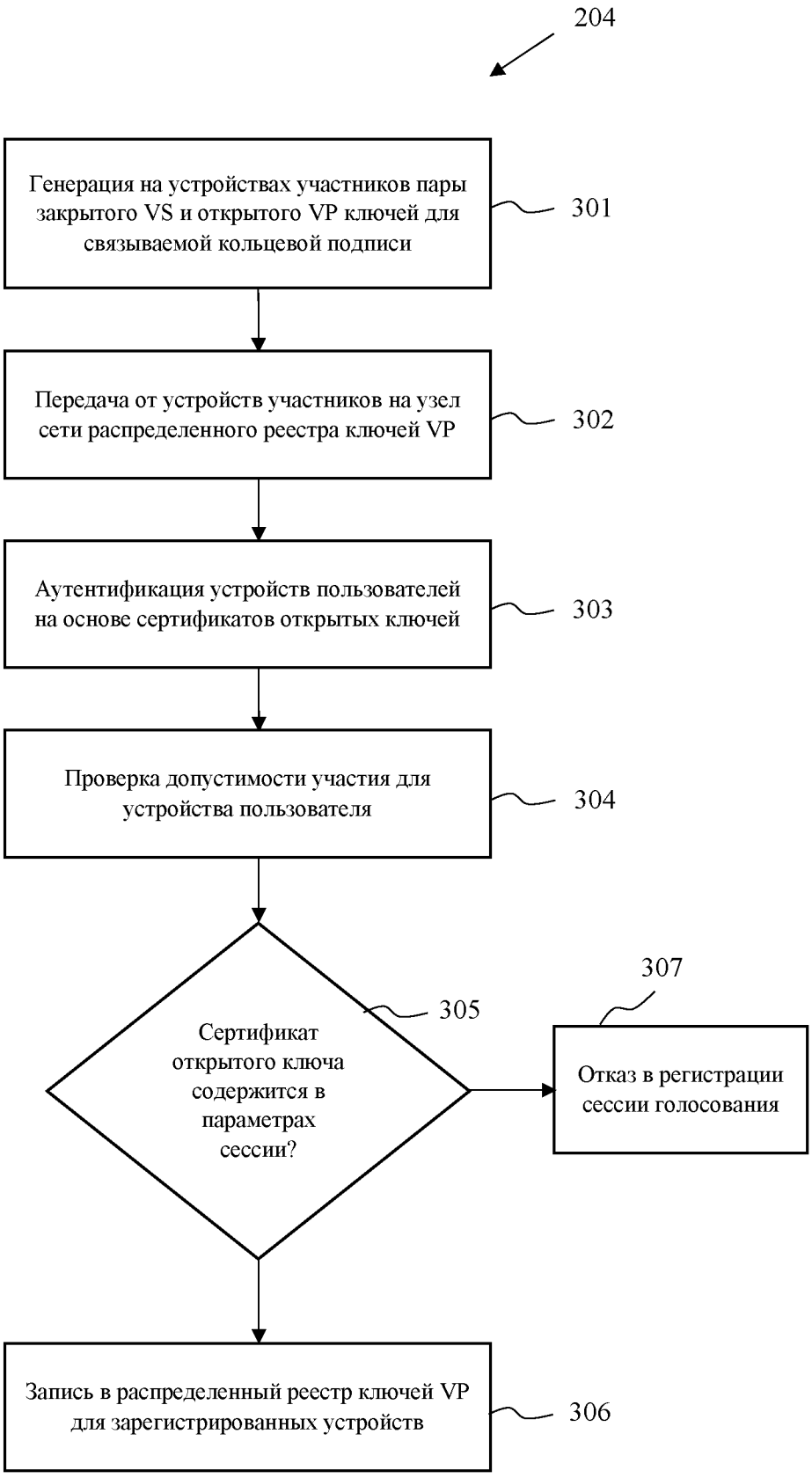
Фиг. 1А



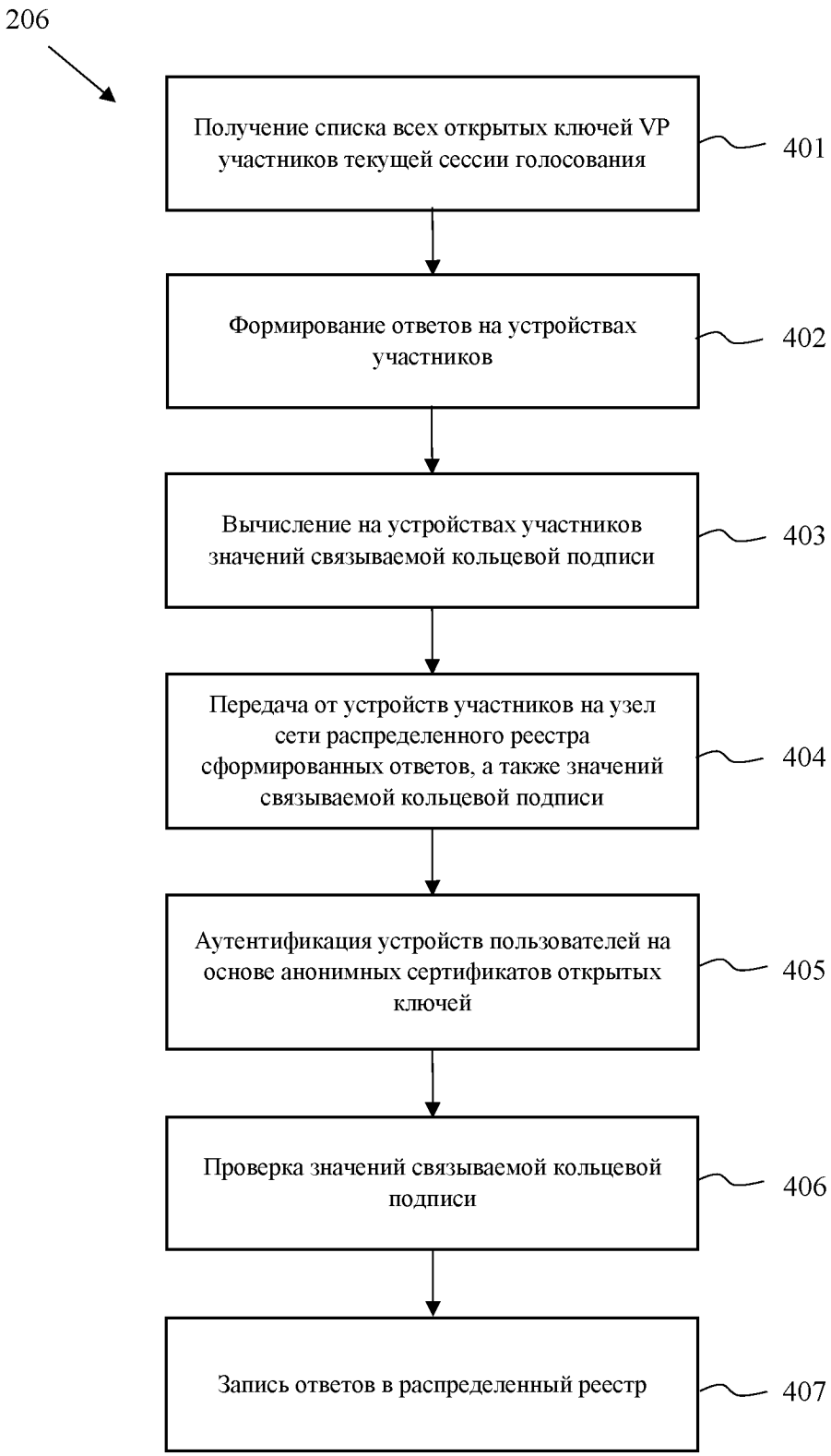
Фиг. 1Б


200
Формирование сертификатов открытых ключей для устройств пользователей, участвующих в сессии голосования
201
Создание сессии голосования с параметрами допуска устройств участников голосования
202
Передача параметров сессии голосования на узел сети распределенного реестра
203
Регистрация устройств участников сессии голосования на основании сформированных параметров
204
Формирование для зарегистрированных устройств анонимных сертификатов открытых ключей
205
Осуществление голосования участниками и запись результатов в распределенный реестр
206

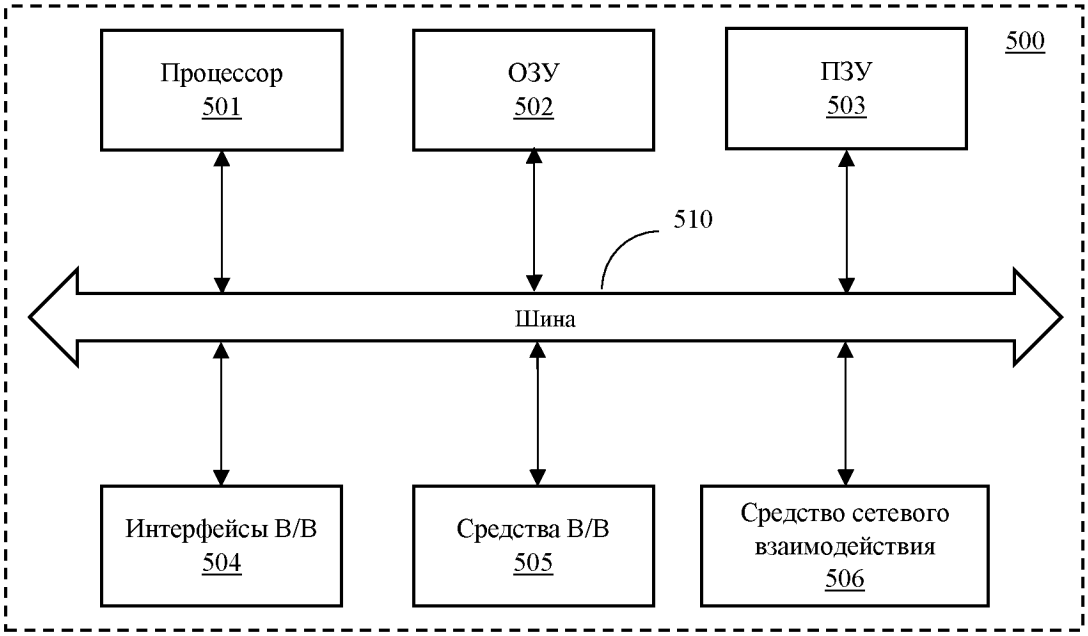
Фиг. 2


204
Генерация на устройствах участников пары закрытого VS и открытого VP ключей для связываемой кольцевой подписи
301
Передача от устройств участников на узел сети распределенного реестра ключей VP
302
Аутентификация устройств пользователей на основе сертификатов открытых ключей
303
Проверка допустимости участия для устройства пользователя
304
Сертификат открытого ключа содержится в параметрах сессии?
305
307
Отказ в регистрации сессии голосования
Запись в распределенный реестр ключей VP для зарегистрированных устройств
306

Фиг. 3


206
Получение списка всех открытых ключей VP участников текущей сессии голосования
401
Формирование ответов на устройствах участников
402
Вычисление на устройствах участников значений связываемой кольцевой подписи
403
Передача от устройств участников на узел сети распределенного реестра сформированных ответов, а также значений связываемой кольцевой подписи
404
Аутентификация устройств пользователей на основе анонимных сертификатов открытых ключей
405
Проверка значений связываемой кольцевой подписи
406
Запись ответов в распределенный реестр
407

Фиг. 4


500
Процессор
501
ОЗУ
502
ПЗУ
503
510
Шина
Интерфейсы В/В
504
Средства В/В
505
Средство сетевого
взаимодействия
506

Фиг. 5

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки: **202092857**

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

G07C 13/00 *(2006.01)*
G06F 17/40 *(2006.01)*
H04L 9/32 *(2006.01)*
G06F 21/62 *(2013.01)*

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G07C 13/00, G06F 17/00-17/40, H04L 9/00-9/32, 29/00-29/06, G06F 16/00-16/22, 21/00-21/62, G06Q 10/00-10/06

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
ESP@CENET, K-PION, PAJ, RUPTO, USPTO, WIPO, GOOGLE, ЕАПАТИС

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X Y	US2017/0109955 A1, (FOLLOW MY VOTE, INC.), 20.04.2017 название, реферат, абзацы [0002], [0005]-[0007], [0016]-[0023], [0025], [0027], п.п. 1, 8 формулы	1-6, 8-14 7, 15
Y	WO2020/008445 A1, (SCYTALE TECHNOLOGIES LTD), 09.01.2020 абзац [0015]	7, 15
A	KR20200008413 A, (IUCF HYU et al), 28.01.2020	1-15
A	CN109286497 A, (GUIYANG ACADEMY OF INFORMATION TECH INSTITUTE OF SOFTWARE CHINESE ACADEMY OF SCIENCES GUIYANG BRANCH et al), 29.01.2019	1-15

☐ последующие документы указаны в продолжении

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"
«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: **02/09/2021**

Уполномоченное лицо:
Заместитель начальника отдела механики, физики и электротехники

М.Н. Юсупов