Децентрализованная схема защищенного создания и хранения баз данных

М.А. Черепнёв

***Аннотация*--- В работе предложена новая схема коллективной работы для выполнения задачи защищенного создания и хранения базы данных. Такие задачи возникают при построении электронных платежных систем и систем документооборота с распределенной ответственностью, то есть когда за корректность работы базы данных отвечает вся сеть. На сегодняшний момент наиболее распространенным решением этой задачи является технология «блокчейн», о недостатках которой мы уже писали ранее. В данной работе построена схема, решающая ту же задачу, но без указанных недостатков. В построенной нами схеме у каждого абонента имеется пара открытого и секретного ключа, которые распределяются без трастового центра с помощью предложенного в статье механизма децентрализованной аутентификации. Схема построена на принципах автономии, то есть независимости от клиентского оборудования и сети, на базе которых она работает. Показано, что слабости схемы «блокчейн», описанные в нашей предыдущей работе, в данной схеме удалены. В основу построенной схемы положен протокол Шаума стираемой подписи. Поэтому, несмотря на отсутствие неотслеживаемости, в данной схеме нет возможности собирать досье на клиентов, хотя в «блокчейне» такая возможность есть. Уделено внимание стимулированию абонентов к проверке корректности работы базы. Для контроля отклика абонентов предлагается использовать сервер временных меток. Для поддержания свойства независимости от сети мы предполагаем у каждого абонента возможность выбора сети для пересылки другим абонентам. Для поддержки безопасной работы каждого клиента, мы предлагаем клиентское оборудование всегда поддерживать в режиме «online».**

Ключевые слова **--- Электронно-цифровая подпись, коллективная слепая подпись, децентрализованные схемы аутентификации.**

Статья получена 20 мая 2020.

Работа поддержана грантом РФФИ 18–29–03124 мк.

М.А.Черепнев из Московского государственного университета имени М.В.Ломоносова, РФ (e-mail: cherepniov@gmail.com)

I. Введение

Технология децентрализованного защищенного формирования и хранения базы данных может быть использована не только в платежных системах, но и для хранения юридически значимых документов при построении систем электронного документооборота на предприятиях или в сфере госуслуг. Технология «блокчейн» [1, 3] решает эту задачу с достаточно большими погрешностями [4]. Все дело в том, что известная с 15 века в открытой печати бухгалтерская технология двойной записи реализована в блокчейне так, что появились дополнительные свойства, делающие эту систему уязвимой по отношению к атакам, связанным с отсутствием аутентификации пользователей, стимула к поиску ошибок, с монопольным контролем над сетью или введением дополнительных больших вычислительных мощностей. В качестве прототипа нового протокола, лишенного этих недостатков, мы берем процедуру голосования на Новгородском вече 12-15 веков и процедуру поручительства в среде стрельцов 17 века.

Протокол защищенного формирования и хранения базы данных “блокчейн” может быть рассмотрен как протокол коллективной электронно-цифровой подписи. При этом в основе оказывается механизм случайного распределения права подписи и ответственная подпись (в основной версии PoW), то есть такая подпись, при формировании которой подписывающий тратит свои собственные ресурсы. При очевидном плюсе, связанном с уменьшением числа подписывающих при сохранении надежности, такой протокол

оказывается уязвимым относительно атак на механизм случайного распределения права подписи. Кроме того, в версии с ответственной подписью (PoW) он имеет большие непроизводительные расходы. А если в сети появляется злоумышленник, который может управлять потоками сообщений, то малое число абонентов он может легко заблокировать. Кроме того, отображаемое у клиента дерево блокчейна может быть неадекватным. Оно может быть, например, частью другого дерева или другой (более ранней) частью того же дерева. Поскольку метки времени по умолчанию не используются, то это может быть просто старая версия текущего дерева. Если ошибка (место склейки) расположено достаточно далеко от текущего блока, то найти его достаточно сложно. Значит надо вводить временные метки и вообще минимизировать влияние управления сетевым трафиком на протокол защищенного формирования и хранения базы данных. В этой работе мы предлагаем использовать для этого децентрализованный протокол коллективной слепой подписи. Мы предлагаем свою версию такого протокола. А для открытого распределения ключей --- децентрализованный протокол аутентификации.

II. Описание схемы коллективной работы

Мы предполагаем наличие нескольких сетей, связывающих различные группы абонентов так, чтобы каждый из них имел возможность выбора сети.

За основу возьмем протокол стираемой подписи Шаума [2, 5]. Он дополнительно обеспечивает невозможность собирать досье на участников обмена. Правда, нужно иметь в виду, что проверка подписи может быть осуществлена только с участием подписывающего абонента. В этом протоколе у каждого i-го участника есть секретный ключ $d_i \in Z_q^*$ и открытый ключ в виде пары (g, g^{d_i}), где вычисления проводятся в некоторой мультипликативной циклической группе порядка q с образующим элементом g. Конечно протокол Шаума не безупречен. Например, если настоящая подпись t^{d_i} отличается от опубликованной множителем маленького порядка. В этом случае подписывающий может дезавуировать эту, несовпадающую с настоящей, подпись с меньшей вероятностью, чем в общем случае. Нетрудно понять, что если указанный порядок меньше параметра безопасности в дезавуирующем протоколе Шаума, то эта вероятность будет примерно равна обратному числу к этому порядку. Однако такие простые угрозы можно преодолеть с помощью многократного применения дезавуирующего протокола, либо отождествлением таких подписей, либо объединением этих подходов. Для повышения стойкости относительно угрозы дискретного логарифмирования, протокол Шаума можно построить в группе точек на эллиптической кривой.

Теперь протокол слепой коллективной подписи. Набросок этого протокола был представлен в [4]. Прежде всего, пересылка сообщений (своих и полученных от других участников) осуществляется двум случайным абонентам из своего доверенного списка за своей подписью, используя случайно выбранную сеть из имеющихся в распоряжении абонента. Доверительный список каждый абонент строит двусторонним. То есть если А доверяет В, то В доверяет А. Проверяя подпись доверенного отправителя, абонент пересылает информацию дальше уже за своей подписью. Таким образом, на конечном получателе проверка подписи исходного отправителя не требуется. То есть происходит распараллеливание алгоритма проверки подписи, предусмотренного протоколом Шаума, а проверить подпись абонента из доверительного списка можно опираясь на его аутентифицированный открытый ключ. Сам протокол слепой подписи состоит в том, что вместо сообщения m на подпись отправляется $t = h(m)^r$, где $r \in Z_q^*$ - случайно и неразглашаемо, а h - некоторая хеш-функция. Получив подпись t^{d_i}, отправитель возводит её в степень $r^{-1}(mod\, q)$ и получает подпись $h(m)^{d_i}$. Если ему удалось за реальное время все необходимые подписи получить, то он размещает их, а также t и r в базе. Другими словами он рассылает сведение о появлении

новой записи в базе по той же схеме, то есть через двух случайных абонентов из своего доверительного списка. Теперь любой сможет проверить, что сообщение подписано, а значит получено всеми зарегистрированными пользователями. Если за реальное время собрать все подписи не удалось, то возникает ситуация "отказ в обслуживании". Здесь важно пояснить, почему именно всеми зарегистрированными пользователями. Потому, что в противном случае конкретного абонента можно обойти, и он окажется с неадекватной версией базы. А если можно обойти одного, то можно обойти и всех по очереди. То есть с метками времени ведется список зарегистрированных на данный момент абонентов (и их подписи), который каждый может проверить, как и любую запись в базе. Если абонент не работает (то есть не выдает слепые подписи) то он снимается с регистрации. Отметим здесь, что у абонентов в этой схеме нет возможности сортировать сообщения, так как они подписывают их вслепую, а сами сообщения носят случайный характер. Так что либо он подписывает все сообщения, либо начинает тормозить всю сеть, что можно определить по меткам времени в его подписях. На основании этих меток его можно снять с регистрации, разместив это сообщение как соответствующую запись в базе. Фактически зарегистрированный абонент всегда находится в состоянии «online». Для этого у него должно быть оборудование осуществляющее слепую подпись в автоматическом режиме. Благодаря этому у каждого абонента будет находиться копия общей базы, адекватная времени.

Если абонент работает, но его все время снимают с регистрации, то это значит, что он не получал соответствующее сообщение и надо менять сеть, либо то, что список доверенных лиц не достаточно большой и разнообразный (в смысле существования опосредованных связей со всеми абонентами) и тогда его нужно корректировать

Если такая подпись состоялась, то, в принципе, можно начать собирать подписи заново, но для этого надо убедить почти всех в нарушении процедуры предыдущим сборщиком (указать неверную подпись или неверный хеш).

Таким образом, процедура вычисления хеша в технологии блокчейн заменяется на протокол коллективной подписи, пусть даже долго вырабатывающий такую подпись, которую, однако, относительно легко проверить (в данном случае для тех абонентов, которые этого хотят). Необходимое время для выполнения этих процедур в сети сопоставимо.

Абоненты, ставя свои подписи вслепую, ориентируются лишь на число подписанных ими сообщений и на число записей в базе. В случае большого расхождения (то есть если часто возникает "отказ в обслуживании") абонент перестает участвовать в подписи в данной сети. Значит надо использовать другую или дополнительную сеть. Если чьи-то подписи в новой записи окажутся неверны (то есть это будет доказано протоколом Шаума), то вся запись признается недействительной. В этом месте можно возразить, что наша схема подвержена атаке с использованием монопольного управления сетью (представление неадекватной копии базы). Однако данная проблема легко преодолевается с помощью указания меток времени в подписанных записях общей базы. Если монопольный менеджер сети предоставляет группе абонентов устаревшую базу, то они не увидят в ней своих записей, и возникнет «отказ в обслуживании», в результате которого эта группа абонентов перестанет быть клиентами данной сети, и она потеряет и клиентов и возможность оказывать влияние на кого бы то ни было. Для контроля адекватности базы периодически каждый абонент должен запрашивать копию базы от абонентов из доверенного списка, и, тем самым, обменивается базой со всеми абонентами. Таким образом, монопольный менеджер сети остается перед выбором: либо обеспечит необходимый трафик для корректной работы схемы, либо потерять клиентов. Влиять на безопасность их работы он не может. При отсутствии альтернативной сети протокол «блокчейн» безопасно работать не может, а наш протокол может продолжать

работу, апираясь на корректно проведенное открытое распределение ключей с децентрализованной аутентификацией (см. ниже).

III. Основные свойства построенной схемы.

1. *Интерактивность*. Это свойство означает, что в случае корректной работы любой абонент может создать запись в базе данных, а в случае некорректной работы не сможет выдать её результат за корректную запись с коллективной подписью в её получении. Поскольку каждый зарегистрированный абонент следит за соответствием числа своих слепых подписей и числа записей в базе, находясь все время “online”, то легитимной будет только коллективная подпись всех абонентов зарегистрированных в данный момент. Эта подпись отражает доверие абонентов работе сети. То, что подписывают все, не позволяет обойти в работе ни одного абонента, хотя и требует их дисциплины и высокой надежности сети.

2. *Нулевое разглашение*. Это свойство наследуется из протокола Шаума.

IV. Описание протокола децентрализованной аутентификации.

Для работы описанного выше протокола слепой коллективной подписи, необходимо предварительное распределение ключей. Это распределение должно быть поддержано протоколом аутентификации. Аутентификация предлагается на основе идеи поручительства внутри доверенного списка. При достаточной «величине» такого списка у каждого абонента, открытое распределение ключей охватывает всю сеть через пересечения этих списков. Понятно, что чем больше этот список, тем быстрее и безопаснее этот участник сможет работать с базой. В список он заносит людей, опираясь на физическую аутентификацию и/или на проверку подписанного цифрового следа этих людей в социальных сетях, базе смс и телефонных соединений, электронных изданиях и т.д. (чем больше подписей участник обмена поставит под этими документами, тем больше доверия к его открытому ключу, и выше безопасность его работы). Заметим, что в основной версии блокчейна аутентификации нет, и это приводит к атакам с перераспределением вычислительных ресурсов в версии PoW, и крупных рейтингов в версии PoS.

V.Стойкость построенной схемы относительно критических атак на блокчейн.

1. *Нет неотслеживаемости*. Это базовое свойство, гарантирующее возможность полной проверки записей базы любому абоненту сети. В частности это гарантирует от повторной траты электронных денег, но при этом теряется важное свойство наличных денег. Конечно, при реализации различных систем документооборота открытых документов это и не важно. В предложенной схеме абонент, совершивший ошибку (например, двойную трату), может быть вычислен по регистрационным данным. Однако, предъявление ему иска невозможно ввиду свойства стираемости подписи в схеме Шаума. Фактически нарушитель рискует только тем, что он будет исключен из всех доверительных списков и не сможет работать в данной схеме. Защита от таких нарушителей держится на том, что записи, попадающие в общую базу, будут проверяться и вступят в силу только после достаточного количества проверок.

2. *Все записи защищены на одинаковом уровне*. В соответствии с этим, при работе протокола надо следить за равномерным распределением ответственности среди всех записей базы. Ошибка в одной записи не приводит как в блокчейне к дискредитации записей, которые за ней следуют. Дискредитируется только запись содержащая ошибку. Это не дает возможности, манипулируя записями, повышать угрозы для всей базы от нахождения одной ошибки. Помимо всего прочего, это позволяет правильно на каждом шаге оценить угрозы от нахождения ошибок и построить системы распределения вознаграждения с предсказуемой эффективностью.

3. *Равные полномочия всех абонентов.* Поскольку полномочия одинаковые, то ими труднее манипулировать. Мы будем добиваться равенства полномочий у всех абонентов. При этом общее количество полномочий прямо пропорционально количеству абонентов, которые этими полномочиями обладают. Если это условие не соблюдать, то может возникнуть возможность для абонентов с дополнительными полномочиями проводить атаку против абонентов с обычными полномочиями (как в случае с протоколом блокчейн в версии PoS), при этом наращивая полномочия. Это могут делать не сами владельцы дополнительных полномочий, а некоторая третья сторона, осуществляющая менеджмент полномочий. Таким образом, очень важно, чтобы полномочия абонентов были одинаковыми, и их нельзя было отделить от их собственников. То есть, чтобы было невозможно передать или передоверить свои полномочия. Понятно, что полностью добиться этого невозможно, так как абоненты свободны в своем выборе.

4. *Использование эмиссии для стимулирования строительства общей базы данных*. Созданные безошибочные блоки не могут быть признаны недействительными в случае нахождения ошибок в других блоках, как это организовано в блокчейне. Создавая безошибочный блок, абонент формирует устойчивую единицу ценности данной системы и потерять эти деньги не может. Это создает устойчивость и предсказуемость работы всей системы. Управляя распределением вознаграждения за нахождение ошибок, можно следить за уровнем безопасности работы всей базы.

5. *Стимулирование поиска ошибок*. Если эмиссию можно считать штрафом со всех, то за нахождение ошибки должен платить тот, кто её создал и те, кто её не заметил (т.е. строители следующих по времени за ошибочным блоков). Понятие штрафа представляется более удобным, чем понятие эмиссии, так как имеет более целенаправленный, адресный характер.

6. *Сведения об ошибочности блока*. Сведения об найденных ошибках каждый абонент должен иметь возможность без промедления включить в общую базу. Дальше эти сведения, также как и остальные сведения общей базы, могут быть проверены любыми другими абонентами. Если по истечении некоторого заранее оговоренного времени они не были, в свою очередь, признаны ошибочными, то нашедший ошибку абонент получает вознаграждение уже без процедуры общей подписи. Одновременно абонент совершивший ошибку выплачивает штраф (здесь без процедуры коллективной подписи, поскольку его подпись под ошибочным блоком может быть каждым проверена). Это гарантирует неотвратимость получения вознаграждения за нахождение ошибки и неотвратимость оплаты штрафа за совершение ошибки. Фактически здесь производится передача денежных средств от абонента, совершившего ошибку к абоненту, который ее нашел.

7. *Зависимость от транспорта (сети)*. Если из-за большого количества ситуаций «отказ в обслуживании» абоненты перестают пользоваться сетью, то она постепенно выбывает из списка используемых сетей. Другими словами, если данный протокол использует несколько конкурирующих сетей, то сеть, не предоставляющая абоненту возможность держать количество выданных им слепых подписей близким к количеству записей в базе, теряет этого абонента и может, в конце концов, вообще оказаться не востребованной.

8. *Зависимость от программного обеспечения, установленного на клиентском оборудовании.* Если для хранения текущих паролей и основных операций использовать защищенную смарт-карту, а большие вычисления производить на компьютере общего доступа, то эта проблема будет решена.

9. *Зависимость от вычислительных ресурсов*. Вычислительные затраты при работе этого протокола минимальны, поэтому неважно какими ресурсами обладает абонент. Если абонент подвергается атаке в сети,

связанной с увеличением количества запросов сверх нормы, то он просто отказывается от этой сети. Таким образом, борьба с нарушением абонентами лимита расходования трафика лежит на администраторах сети. Они сами должны препятствовать таким атакам, так как иначе абоненты будут вынуждены выбрать другую сеть.

10. *Зависимость от желания клиентов проверять целостность общей базы (участвовать в коллективной подписи)*. Если абонент отказывается участвовать в алгоритме слепой подписи, то он выбывает из системы. То есть исключается из общего списка. Обратное включение осуществляется при помощи прохождения абонентом процедуры регистрации. О том, что абонент отключился, становится известно из базы, где его подпись отсутствует для всех последних записей в заранее оговоренном количестве. Если это произошло не с ведома абонента, то виновата в этом сеть, и абонент её меняет. Если он отключился сам, то он исключается из списка подписантов и за ним закрепляется обязательство снова зарегистрироваться. Отключаясь от сети, абонент лишается всех преференций, которые она предоставляет. Поэтому ему это не выгодно.

11. *Наличие ошибок (закладок) в программном коде, реализующем работу системы*. Речь прежде всего идет о так зазываемых смарт контрактах. Их работа должна опираться на ответственность того, кто написал программный код. В случае нарушения работы он должен вмешаться в работу системы и скорректировать её, а также нести ответственность за материальные потери клиентов, как это принято в банковской сфере.

VI. Заключение.

Очень важно с точки зрения автора, чтобы электронно-цифровая схема не была чем-то совершенно новым, с невыясненными свойствами, а моделировала какую-то работающую, проверенную на практике схему. И не столько проверенную, сколько имеющую лучшие результаты решения соответствующих задач защиты информации среди других аналогичных систем. Так система общего равного голосования на Новгородском вече имела в свое время значительный финансовый результат. Система поручительства среди стрельцов (доверительные списки), позволила создать элиту армии, осуществляющей государственное управление на местах в 17 веке.

БИБЛИОГРАФИЯ

[1] S. Nakamoto: ”Bitcoin: A Peer-to-Peer Electronic Cash System” Available: www.bitcoin.org/bitcoin.pdf

[2] М.А. Черепнёв “Криптографические протоколы” Москва: МАКС Пресс, 2018.

[3] М.А. Черепнёв “Оценки эффективности форк-атаки на блокчейн протокол ” injoit, v.7 (2019), n.4, p.25-29.

[4] М.А. Черепнёв “Блокчейн и протокол коллективной подписи” injoit, , v.7 (2019), n.6, p.17-23.

[5] Chaum~D. Zero-knolege undeniable signatures~// LNCS, 1991, v.\,547. P.458--464.

Decentralized scheme for secure database creation and storage

M.A. Cherepniov

Abstract--- **In this paper, we propose a new collective work scheme for performing the task of secure database creation and storage. Such tasks arise when building electronic payment systems and document management systems with distributed responsibility, that is, when the entire network is responsible for the correct operation of the database. At the moment, the most common solution to this problem is the "blockchain" technology, the disadvantages of which we have already written. In this paper, a scheme is constructed that solves the same problem, but without these disadvantages. In the scheme we have built, each subscriber has a pair of public and private keys, which are distributed without a trust center using the decentralized authentication mechanism proposed in the article. The scheme is based on the principles of autonomy, that is, independence from the client hardware and network on which it operates. It is shown that the weaknesses of the "blockchain" scheme described in our previous work have been removed in this scheme. The built scheme is based on the Shaum protocol of blind signature. Therefore, despite the lack of untraceability, this scheme does not allow collecting dossiers on clients, although the "blockchain" has such a possibility. Attention is paid to encouraging subscribers to check the correctness of the database. To control the response of subscribers, we suggest using a timestamp server. To maintain the network independence property, we assume that each subscriber can choose a network to send to other subscribers. To support the secure of each client, we offer to always support the client equipment in the "online" mode.**

Key words--- **Digital signature, collective blind signature, decentralized authentication schemes.**

REFERENCES

[1] S. Nakamoto: ”Bitcoin: A Peer-to-Peer Electronic Cash System” Available: www.bitcoin.org/bitcoin.pdf

[2] M.A. Cherepnjov “Kriptograficheskie protokoly” Moskva: MAKS Press, 2018.

[3] M.A. Cherepnjov “Ocenki jeffektivnosti fork-ataki na blokchejn protokol ” injoit, v.7 (2019), n.4, p.25-29.

[4] M.A. Cherepnjov “Blokchejn i protokol kollektivnoj podpisi” injoit, , v.7 (2019), n.6, p.17-23.

[5] Chaum~D. Zero-knolege undeniable signatures~// LNCS, 1991, v.\,547. P.458--464.