Блокчейн и протокол коллективной подписи

М.А. Черепнёв

***Аннотация*--- В работе протокол защищенного формирования и хранения базы данных “блокчейн” рассмотрен как протокол коллективной электронно-цифровой подписи. При этом в основе оказывается механизм случайного распределения права подписи и ответственная подпись, то есть такая подпись, при формировании которой подписывающий тратит свои собственные ресурсы. При очевидном плюсе, связанном с уменьшением числа подписывающих и сохранении надежности, такой протокол оказывается уязвимым от атак на механизм случайного распределения права подписи. Кроме того, 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 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 подписи. Мы предлагаем свою версию такого протокола. Посчитано матожидание и дисперсия времени создания одного блока блокчейна, а также показано, что вероятность того, что это время окажется близко ко времени реализации в сети протокола коллективной подписи мала.**

Ключевые слова **--- Электронно-цифровая подпись, коллективная подпись, Блокчейн, независимость протоколов от сети.**

I. Введение

Технология блокчейн в настоящее время приобрела большую популярность. По-существу эта технология решает задачу согласованного построения и защищенного хранения базы данных в сети со многими пользователями. Важным преимуществом при этом является то, что для решения этих задач не требуется аутентификация пользователей. Стойкость блокчейна держится на том, что право изменить базу распределяется случайным механизмом и за это право каждый пользователь платит своими ресурсами (например, компьютерным временем).

База строится по принципу цепи, поэтому далекие от текущего блока её части гарантированы ресурсами, затраченными несколькими пользователями.

В версии с PoW случайное распределение прав среди участников сети делается при помощи распараллеливания вычислительно трудной, но хорошо масштабируемой задачи получения хеш значения с фиксированным количеством нулей в конце двоичной записи результата. Поэтому нельзя атаковать протокол блокчейн, сконцентрировав вычислительные ресурсы в одном узле, или контролируя лишь малое число узлов.

Таким образом, фактически, получается система коллективной подписи без трастового центра, в которой за достоверность базы данных отвечает вся сеть. Основными составными частями её являются механизм случайного выбора абонента, который вносит изменения и его ответственная подпись (т.е. требующая существенных его собственных затрат). Механизм случайного выбора позволяет как бы “размазать

ответственность” за ведение базы по всем абонентам. Таким образом, никто конкретно за целостность этой базы не отвечает, а отвечает вся сеть. Правда, если наряду с блокчейном используются открытые ключи абонентов, то их приходится использовать без аутентификации, поскольку в противном случае обычно требуется трастовый центр и преимущество децентрализованности пропадает.

Ответственный характер подписи защищает от влияния на базу данных случайных, не заинтересованных в её развитии абонентов. Хотя при этом возникает и слабость, связанная с нежеланием абонентов заниматься обслуживанием сети. При этом указанная затрата ресурсов является явно не производительной.

Будем рассматривать протокол блокчейн как схему для коллективной подписи, в которой отсутствует трастовый центр.

Целью данной статьи является выявление слабостей протокола блокчейн и некоторые предложения по их преодолению.

II. Определение блокчейна

Дерево блокчейна состоит из блоков (совокупностей записей). Ветвь дерева блокчейна, вообще говоря, может начинаться с любого его блока. Блоки в дереве связаны при помощи вычисления хеш-функций в соответствии со следующей процедурой:

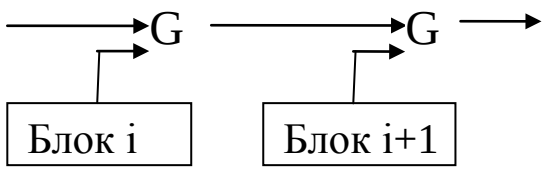

Рис. 1 Дерево блокчейна

Процедура G состоит из следующих действий:

1. Выбор наибольшей ветви дерева блокчейна и её последнего блока.
2. Проверка целостности выбранной ветви и содержания нового блока, вычисление хеш значения h этого содержания.
3. Вычисление хеш-функции, которая имеет два входа (h и результат применения предыдущей процедуры в данной цепи) и один выход.

Хеш-функция, используемая на втором этапе, обычно таже, что и на третьем (SHA 256 для Bitcoin) и применяется несколько раз, чтобы результат существенно зависел от всего содержания блока.

III. Плюсы и минусы блокчейна.

1. *Нет неотслеживаемости*. Это гарантирует от повторной траты электронных денег, но при этом теряется важное свойство наличных денег. Конечно, при реализации различных систем документооборота открытых документов это не важно. Это свойство мы принимаем.
2. *Старые записи менять труднее новых*. Это делает старые записи лучше защищенными. Однако это же ведёт к забвению старых данных и к невозможности исправить ошибку, даже если она установлена. Ведет также к переполнению памяти т.к. в цепи приходится хранить маловажную информацию, которая связана с важной. Это свойство нам кажется лишним, и в новой предлагаемой системе его нет. В обычном протоколе коллективной подписи ошибку можно исправлять независимо от других записей.
3. *Возможность работы с offline клиентами*. Впрочем, здесь остается главная проблема оценки адекватности базы при очередном включении. А именно, при отключении “честных” игроков (вольному или невольному) может быть заложена ошибка, которую в дальнейшем будет трудно найти и ещё труднее исправить. В обычном протоколе коллективной подписи все записи в смысле стойкости равноценны.
4. *Использование эмиссии для стимулирования строительства общей базы данных*. В реальных протоколах электронных денег (Bitcoin) этого все равно оказывается недостаточно и аудитом (проверкой целостности) и майнингом (созданием новых блоков) занимаются сами организаторы сети, то есть она, по существу, перестает быть децентрализованной. В иностранной литературе это называется “затуханием энергии” [1]. Исправление (нахождение)

ошибки, очевидно, нужно также стимулировать, чтобы аудит был привлекательным. 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 за ошибочным блоков). Штраф должен быть подписан при помощи протокола коллективной подписи и только тогда принят к исполнению. Понятие штрафа представляется более удобным, чем понятие эмиссии.

5. *Возможность применения различных протоколов консенсуса*. Отметим, что правило длинных цепочек, как составная часть всех известных на сегодня протоколов консенсуса, само собой не подразумевает избавления от ошибочных блоков. И даже может быть использовано злоумышленниками для подтверждения и, в дальнейшем, забвения ошибочных блоков. Нам представляется, что получение сведений об ошибочности блока должны быть обязательно простимулированы и надежно переданы всем абонентам.

6. *Зависимость от транспорта (сети)*. Для решения этой проблемы мы предлагаем использовать протокол коллективной подписи для каждой записи базы. Некоторый такой протокол мы предлагаем в этой статье.

7. *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.

8. *Зависимость от вычислительных ресурсов*. Ответственность подписывающего более естественно поддержать штрафами, которые, конечно, нужно подтверждать протоколом коллективной подписи.

9. *Зависимость от желания клиентов проверять целостность общей базы (участвовать в коллективной подписи).* На примере уже достаточно продолжительно работающей блокчейн-системы Bitcoin [1] известно, что “энергия затухает”. То есть клиенты склонны отказываться от проверки целостности базы и даже от её строительства. Даже несмотря на стимулирование этих процессов, просто исходя из несоответствия этой работы их реальным целям участия, что приводит к вырождению всей системы в централизованную, контролируемую весьма ограниченным числом участников. Таким образом, деятельность, связанная с аудитом и строительством базы, должна опираться на естественные потребности клиентов. Для того, чтобы не иметь возможности навредить работе сети, клиенты должны подписывать все входящие сообщения вне зависимости от их содержания.

9. *Невнятное стимулирование поиска ошибок*. Прежде всего, система должна позволять довести сведения о найденной ошибке до каждого участника. Вознаграждение для нашедшего ошибку должно состоять из штрафа с того, кто эту ошибку сделал, а также с тех, кто её до этого не замечал. Помимо разового вознаграждения, клиент, нашедший ошибку, должен получить увеличение рейтинга, ведущее к новым возможностям использования базы. В тоже время клиенты допустившие, или не замечавшие ошибку должны получить снижение своего рейтинга, что, в конечном счете, может привести к исключению из числа пользователей. Таким образом, клиенты должны обладать возможностями для выполнения таких функций, то есть из реализация должна быть достаточно простой вычислительной задачей.

10. *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.

IV. Примеры децентрализованных систем управления.

В качестве примера можно привести систему математических публикаций, которая имеет схожую структуру с блокчейном. А

именно, естественные логические связи приводят к тому, что найденные ошибки в доказательствах теорем ведут к снижению индекса цитирования публикаций опирающихся на них результатов. Своим трудом по созданию новой статьи автор голосует за цитированные статьи. То есть это ответственная коллективная подпись, в которой количество подписывающих уменьшено по сравнению с общим числом абонентов за счет увеличения ответственности каждого подписывающего.

Ещё один пример – Новгородская республика и её система денежного обращения. Примерно с 1120г. по середину 15 века, когда в Новгороде укрепились немецкие купцы (до этого были голландские) прекратился ввоз европейских серебряных монет. Торговля осуществлялась исключительно при помощи серебряных гривен и европейских марок. И то и другое представляет собой серебряные слитки, изготавливаемые участнивами обмена самостоятельно (ответственная подпись). А высшим органом власти было новгородское вече (схема коллективного голосования). Все это вместе представляло собой торговую биржу при порте, способном принимать суда морского класса. База данных, при этом, это список участников вече, их рейтинги (там были верхние и нижние), последние торговые операции, цены (в частности указанные в “Русской правде”), налоги и т.д.

Все это можно объединить как использование энергии желания участвовать в процессе с новыми возможностями связи, рекламы, коллективного разума, коллективного использования материальных ценностей, новых знаний и т.д.

Один из наиболее естественных стимулов, способных заставить клиентов работать над базой данных, а не просто использовать её – это возможность исключения из числа пользователей, а также рейтинги, дающие дополнительные возможности, позволяющие участвовать в контроле, а возможно и исключении других пользователей. В любом случае, представляется, что работа над базой должна поддерживаться не разовыми преференциями, а долговременным увеличением возможностей её использования. Таким образом, работа в базе должна быть естественным образом связана с жизнью клиентов. Это может быть торговая биржа или сеть обмена знаниями эффективность работы в которых влияет на качество жизни клиентов.

V. Блокчейн как схема коллективной подписи.

Правило длинных цепочек подразумевает процедуру построения цепи, требующую много времени для одного, или небольшого числа абонентов. Таким образом, она может быть сложной вычислительной задачей, допускающей эффективное распараллеливание, либо её просто невозможно выполнить малым числом абонентов (например, электронное голосование с получением почти всех подписей). 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 может быть заменена на протокол коллективной подписи пусть даже долго вырабатывающий такую подпись, которую легко проверить.

VI. Использование схемы коллективной подписи вместе с технологией блокчейн.

Для достижения независимости работы блокчейна от транспорта (сети) предлагается использовать децентрализованную схему коллективной подписи. Время создания такой подписи обычно не более нескольких секунд и значит, её работа не затормозит работу блокчейна вцелом, в котором время создания нового блока в общей базе около 10 минут. Оценим матожидание и дисперсию времени создания нового блока в общей базе, опираясь на модель [2].

Рассмотрим биты в двоичной записи значения хеш-функции блокчейна как случайные величины, принимающие значение

0 или 1 с вероятностью ½. Тогда вероятность того, что эта запись заканчивается на k нулей равна $1/2^k$, а матожидание времени T, за которое такое значение можно получить, равно $C\cdot 2^k$, для некоторой константы C . Для вычисления дисперсии имеем:

$$D(T) = M(T-M(T))^2 = M(T^2) - (M(T))^2 =$$

$$\frac{C^2}{2^k}\sum_{i=1}^{\infty} i^2\left(1-\frac{1}{2^k}\right)^{i-1} = \frac{C^2}{2^k}\left(zf''(z)+f'(z)\right) =$$

при $f(z) = \sum_{i=1}^{\infty} z^i = \frac{z}{1-z}$, $z = 1-\frac{1}{2^k}$,

$$= \frac{C}{2^k}\left(\frac{(1-\frac{1}{2^k})2}{1/2^{3k}} + \frac{1}{1/2^{2k}}\right) = C^2(2^{2k+1}-2^k).$$

Отметим, что это значение больше квадрата матожидания.

Оценим также вероятность того, что время окажется в 1000 раз меньше матожидания. Это соответствует тому, что при среднем значении времени 10 мин., оно окажется 0,6 сек., то есть будет сравнимо со временем, необходимым для реализации в сети протокола коллективной подписи. Такая вероятность равна

$$\frac{1}{2^k} + \left(1-\frac{1}{2^k}\right)\frac{1}{2^k} + \ \ldots + \ \left(1-\frac{1}{2^k}\right)^{2^{k-10}-1}\frac{1}{2^k} =$$

$$\frac{1}{2^k}\left(\frac{1-\left(1-\frac{1}{2^k}\right)^{2^{k-10}}}{1/2^k}\right) = 1-\left(1-\frac{1}{2^k}\right)^{2^{k-10}}$$

$$\approx \left(1-e^{-2^{-10}}\right) \approx 10^{-3}.$$

Таким образом, дополнительное подключение к блокчейну протокола коллективной подписи не вызовет существенной задержки работы всего протокола вцелом, так как возможные сбои редки и их можно нейтрализовать повторением последних шагов.

VII. Децентрализованные протоколы коллективной подписи.

В этом разделе представим некоторый протокол коллективной подписи, не требующий общего центра. Правда мы будем считать, что все участники обмена имеют открытые e_i и закрытые d_i ключи. Если не предполагать наличие трастового центра, который их раздает, то можно, например, каждой паре присвоить вес в зависимости от того, какая доля записей общей базы данных была подписана этими ключами. Коллективная подпись будет считаться состоявшейся, если сумма долей всех подписавших близка, в некотором смысле, к единице. Инициатива по сбору подписей исходит от “сборщика” или создателя записи (транзакции), который заинтересован в её вхождении в общую базу данных. При этом, если он успеет собрать подписи в течение, скажем, одной секунды, то запись вместе с меткой времени и их коллективной подписью принимается в базу. Если не успел, то возникает ситуация платеж не прошёл и нужно начинать процедуру коллективной подписи заново с новой меткой времени. И так пока не пройдет. Если несколько раз не проходит, то возникает ситуация “отказ в обслуживании” сети. Таким образом, если сеть как транспорт, или как совокупность подписывающих, не смогла удовлетворить временным ограничениям, то подпись не состоится и нужно ждать другого момента, когда они будут готовы к формированию подписи. Протокол устроен таким образом, что на момент подписи подписывающий абонент не видит сообщения (слепая подпись). Таким образом, он только фиксирует для сборщика то, что он это сообщение получил. Пусть t – сообщение (транзакция). Вычисления проводятся в циклической группе порядка q.

На первом этапе сборщик выбирает случайное $r \in_R Z_q^*$ и вычисляет $c = t^r$. Затем он делает общую рассылку, в которую помещает c под своей подписью. Каждый i-й участник обмена, проверив подпись отправителя, подписывает c, вычисляя c^{d_i}, и возвращает это отправителю. Получив от всех, отправитель делает общую рассылку, включив в неё r, метку времени и свою подпись этой пары. Каждый абонент после проверки метки времени и подписи отправляет сборщику свое z_i . Получив все c^{d_i}, сборщик вычисляет $t^{d_i} = c^{d_i r^{-1}(mod\ q)}$, и размещает их, а также t и r, в базе. Сведения о появлении в общей базе

новой записи рассылаются по той же схеме. Таперь любой сможет проверить, что сообщение подписано, а значит получено большинством участников сети.

VIII. Заключение.

Рассматривая блокчейн как децентрализованный протокол коллективной подписи, получаем преимущество в том, что эти подписи ответственные и право подписи предоставляется случайным механизмом, что позволяет существенно снизить необходимое для относительной стойкости число подписывающих (в Bitcoin их шесть, см. [1]). При использовании протокола консенсуса PoW для получения обоих этих свойств используется вычислительно сложная, но легко масштабируемая задача вычисления хеша с фиксированным количеством нулей в конце записи результата. В протоколе консенсуса PoS для случайного распределения права подписи применяется отдельный механизм, основанный на рейтингах участников. В любом случае остается зависимость от транспорта (сети) и большие непроизводительные расходы машинного времени.

В данной статье мы предлагаем отказаться от идеи ответственной подписи в пользу общей коллективной подписи и предлагаем пример децентрализованного протокола коллективной полписи, независимого от транспорта. Для получения независимости от транспорта в работе обычного блокченйна наш протокол можно применять без существенного увеличения времени общей работы с сохранением положительных свойств этой схемы.

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] Черепнев М. А. Оценка эффективности Fork-атаки на протокол “блокчейн” //International Journal of Open Information Technologies. – 2019. – Т. 7. – №. 4.- С.25-29.

Статья получена 05.04.2019.
Работа поддержана грантом РФФИ 18–29–03124 мк.
М.А.Черепнев – Московский государственный университет имени М.В.Ломоносова, РФ (e-mail: cherepniov@gmail.com)

Blockchain and the common signature protocol

M.A. Cherepniov

Abstract **- We consider protocol of secure construction and storage of database, named "blockchain". This protocol may be considered as a common electronic signature scheme. In this case, the main parts are mechanisms of random distribution of rights to sign and responsible signature. We investigate responsible signature as a signature protocol in which signer spend its own resources. An adventure is a minimization of a number of signers with the same reliability. But such protocols have vulnerability against the mechanism of random distribution of rights to sign, and have large non-production costs. To the other hand, if somebody can manage internet traffic, he can block traffic of a not big number of participants. Blockchain tree, that client can see, may be out of date or wrong. It may be a part of another tree, or another (earlier) part of the same tree. If error (the place of gluing) is situated rather far from the current block, then it is difficult to find it. So it's necessary to use timestamps and take action to minimize the influence of internet control on the protocol of secure construction and storage of database. In this work we propose to apply the common electronic signature protocol, that uses on the telephone conferences, but such that not uses a trust center. We propose our own version of such a protocol. We obtain average value and dispersion of the construction block time and show that the probability that this time will be close to common signature protocol realization time is small.**

Key words**---blockchain, common signature protocol, independence from traffic control.**

REFERENCES

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

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

[3] Cherepnev M. A. Ocenka jeffektivnosti Fork-ataki na protokol "blokchejn" //International Journal of Open Information Technologies. – 2019. – T. 7. – #. 4.- S.25-29.