DOI: 10.25586/RNU.V9187.18.06.P.63 УДК 004; 003.26

А.А. Борисов, С.А. Краснов, А.А. Нечай

ТЕХНОЛОГИЯ БЛОКЧЕЙН И ПРОБЛЕМЫ ЕЁ ПРИМЕНЕНИЯ В РАЗЛИЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Статья посвящена технологии блокчейн. Анализируется принцип ее работы. Представлены преимущества данной технологии, а также выделены информационные системы, в которых целесообразно её использование.

***Ключевые слова*:** *блокчейн, пиринговые сети, децентрализованные сети, базы данных.*

A.A. Borisov, S.A. Krasnov, A.A. Nechai

TECHNOLOGY BLOCKCHAIN AND THE PROBLEM OF ITS USE IN VARIOUS INFORMATION SYSTEMS

The article is devoted to the blockchain technology. The principle of its work is analyzed. The advantages of this technology are presented, together with the information systems in which its expedient is useful.

***Keywords*:** *blockchain, peer-to-peer networks, decentralized networks, databases.*

Впервые термин «блокчейн» был использован в 2009 году вместе с запуском системы «биткойн». С этого момента данная технология не сходит с уст крупнейших IT-компаний и IT-специалистов. О ней говорят на мировых конференциях, таких, как Money 20/20, Sibos, а также крупнейшие издания, например The Economist and Euromoney. Согласно Google Trends (рис.1), начиная с 24 февраля 2013 года вплоть до 13 января 2018 года, тема «Блокчейн» постоянно набирала популярность.

Рис. 1. Динамика популярности технологии «Блокчейн» согласно Google Trends

«Блокчейн» представляет собой журнал с фактами, реплицируемыми на несколько компьютеров внутри сети равноправных узлов (Peer2Peer). Фактами является любая информация от всевозможных денежных операций до авторских прав на контент. Узлами соответственно являются члены сети. Также блокчейн характеризуют как непрерывную цепочку блоков, выстроенную по определенным правилам и содержащую информацию.

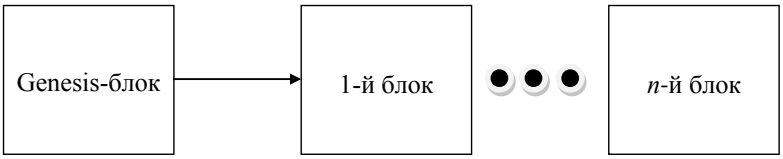

Рис. 2. Обобщённая схема блокчейна

На рис. 2 изображена обобщённая схема блокчейна. Каждый блок в цепи содержит в себе от 1-го до *n* фактов, но он не просто содержит в себе сами данные фактов, а их хэш, полученный с помощью криптографических алгоритмов. В обобщённом виде хеш-функция, благодаря которой получают хэш, выглядит следующим образом:

$$H(S) = \sum_{i=0}^{|S|-1} \alpha^{|S|-(1+i)} \times \mathrm{char}(S_i), \quad (1)$$

где S – создаваемая строка;

char (c) – функция, которая однозначно отображает каждый символ алфавита в целое число в диапазоне $\{0 \ldots \alpha - 1\}$.

Далее полученный результат уменьшают до целого числа в диапазоне от 0 до $m - 1$ с помощью остаточного деления $[H(S) \bmod m]$. Число m является большим целым числом не слишком близким к $2^i - 1$. В алгоритме, использующемся в системе “bitcoin”, число $i = 32$.

Также каждый блок обязательно содержит в себе хэш предыдущего блока и временную отметку его создания. Тем самым реализуются непрерывность и подлинность цепи. Genesis-блок содержит в себе только хэш, который генерируется по заданным правилам, и временную отметку. Он необходим для начала непрерывной цепи.

Так как данный связный список (непрерывная последовательность) реализован в одноранговой децентрализованной сети, то появляется сложная задача согласования фактов или, по-другому, разрешение конфликтов. Примером данной задачи является проблема двойного расходования.

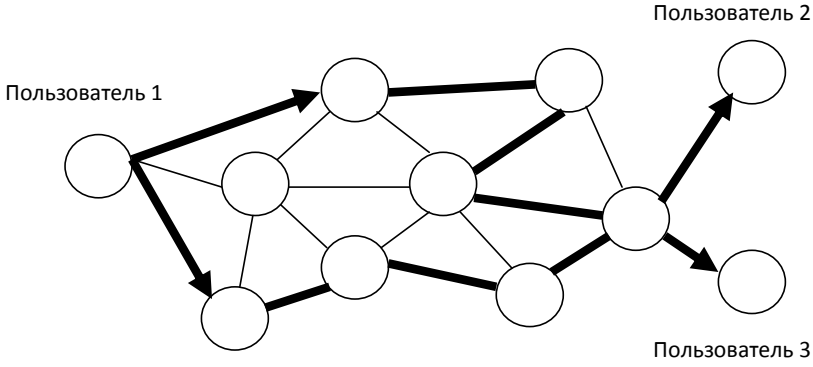

Рис. 3. Проблема двойного расходования в p2p сети

На рис. 3 изображена одноранговая сеть, в которой каждый узел является пользователем. Предположим, что «Пользователь 1» одновременно производит перевод всех своих денежных средств «Пользователю 2» и «Пользователю 3». На рис. 3 жирными линиями выделен один из возможных маршрутов движения денежных средств. Но при этом возникает проблема в определении конечного пользователя, который получит денежные средства. Например, для решения данной проблемы в реляционных базах данных используется алгоритм ссылочной целостности. В распределенной системе не имеется данного механизма, соответственно нам необходим способ, который будет согласовывать порядок фактов, происходящих внутри сети, требуется найти консенсус. Самым простым способом решения проблемы двойного расходования является упорядочивание фактов. Денежные средства получит тот пользователь, которому они первыми придут. Технология блокчейн использует механизм решения консенсуса, основанный на алгоритме доказательства выполнения работы “proof-of-work”, основанной на блоках. Данный алгоритм необходим не только для решения консенсуса, но и для защиты всей сети с помощью асимметрии затрат времени. Данная асимметрия возникает из-за того, что пользователь выполняет более длительную по времени задачу, чем проверка сервером истинности его действия. В системе bitcoin и etherium в алгоритме “proof-of-work” используется функция, основанная на деревьях Меркла (рис. 4). Дерево Меркла представляет собой полное бинарное дерево, в котором вершина всего дерева содержит хэш от всех данных, а внутренние вершины содержат сложенное хэш-значение дочерних элементов.

Общая формула проверки существования и правильности данных будет выглядеть следующим образом:

$$H_K = \begin{cases} H(L), \text{ если } K = 1 \\ H\left(H_{K-1} + A_{L\,K-1}\right), \text{ если } K \geq 2, \end{cases} \quad (2)$$

где H – используемая хэш-функция;

$\{A_{L1}, \ldots, A_{L\,K-1}\}$ – путь Меркла;

L – выбранные данные;

K – высота дерева.

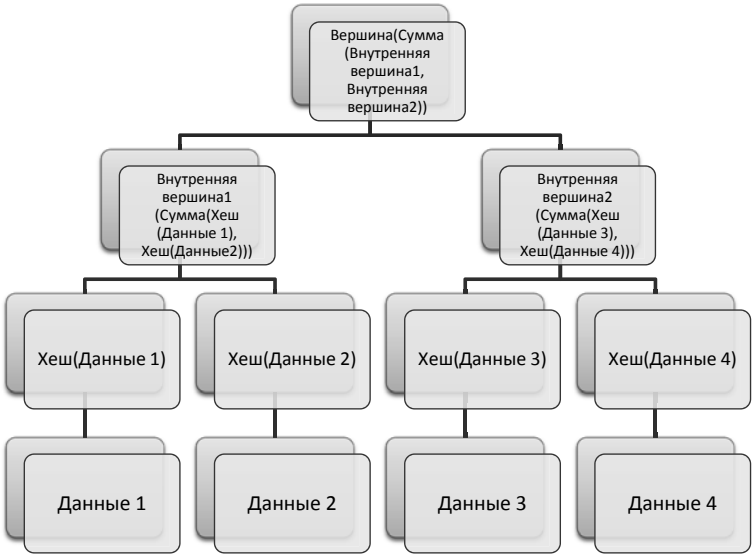

Рис. 4. Схема дерева Меркла

Проверка выполняется за $O(K) = O(\log_2 N)$, где N – количество блоков данных.

Как говорилось ранее, в блоках хранятся факты, именно благодаря блокам факты упорядочиваются, в дальнейшем цепь, состоящая из блоков, реплицируется в сети. Соответственно появляется следующая проблема: добавление фактов в блок и добавление самого блока к последовательности. Перед тем как добавить факт в блок, он попадает в область “Pending facts”, то есть он находится на рассмотрении. Локально создается блок с непроверенными фактами. Далее созданные на узлах сети локальные блоки с непроверенными фактами «соревнуются» между собой, для того чтобы быть добавленными в общую последовательность. Данное «соревнование» в разных системах реализовано по-разному. В системе “Bitcoin” задача представлена двойным SHA-256 хэшем строки из непроверенных фактов. Выбирается тот узел, у которого хэш содержит минимум n ведущих нулей. Например, при $n = 7$:

748274cdf838728dd827348fdc837ff0000127483 – отсеянный хэш;

00000002347823ff3934dccc930ff311db374e293 – выбранный хэш.

Число n меняется с определенным интервалом. Этот интервал будет регулировать сложность вычисления хэша при изменении количества узлов в сети. Данный механизм делает обнаружение ключа для проверки блоков маловероятным, соответственно делая сеть безопасной.

После того как блок выиграл, он попадает в общую цепь и реплицируется на все узлы, соответственно все остальные локально созданные последовательности из блоков с непроверенными фактами отсекаются.

Подлинность блоков в основной цепи проверяется сравнением хэша предыдущего блока, находящегося внутри блока n, с хэшем блока $n – 1$.

До этого момента блокчейн рассматривался только как хранилище для фактов, а точнее как реестр фактов, так как мы храним не сами факты, а их хэши. Но блокчейн также может исполнять программы, называемые «смарт»-контрактами. Благодаря таким контрактам отпадает необходимость совершать операции через 3-е лицо (например, нотариус). Закрепление обещания, данного двумя сторонами, происходит «технически», а не «юридически».

Исходя из всего вышесказанного, можно выделить основные условия использования данной технологии, для того чтобы в дальнейшем сделать выводы, в каких случаях её можно внедрить, а в каких она нецелесообразна.

Технология блокчейн разработана для общественных баз данных. Это означает, что изменения базы данных множеством пользователей модифицируются «транзакциями», которые должны быть приняты или отклонены. Все эти «транзакции» записываются в общий реестр, который, по сути, и будет являться блокчейном. Из первого утверждения следует, что технология блокчейн подходит для баз данных с множеством пользователей, которые генерируют «транзакции». Также данная технология необходима в случае отсутствия доверительных отношений между пользователями, так как особенности системы, такие, как проверка подлинности, отсутствие посредников, децентрализованность, прозрачность проведения «транзакций», смарт-контракты, позволяют безопасно совершать всевозможные действия внутри данной сети. Блокчейн раскрывает свой потенциал в полной мере при всех вышесказанных условиях и в случае, если «транзакции» взаимодействуют между собой. Например, «Пользователь 1» отправляет деньги «Пользователю 2», а тот в свою очередь – «Пользователю 3». В такой связке нет способа проверить транзакцию 2-го пользователя без предварительной проверки транзакции 1-го пользователя. Блокчейн необходим в вашей системе и в том случае, если необходима анонимность авторов, так как p2p сеть позволяет это реализовать в полной мере.

Данная технология очень хорошо подходит для внедрения в проекты в финансовой сфере, но существует много примеров её успешного применения и в других сфе-

рах, например цифровая идентичность, проверка подлинности и подтверждение прав доступа, рынки капитала, управление данными, авторство и права владения, средства электронного голосования, игровая индустрия.

При внедрении технологии блокчейн в свой проект нужно здраво оценивать его масштабность и потенциал. Необходимо учесть множество факторов, например: если вас устраивает реляционная база данных, то введение технологии блокчейн будет нести на себе лишние затраты человеческих и финансовых ресурсов. Технология блокчейн очень специфична, и в большинстве случаев требования проекта удовлетворяют обычные файловые хранилища, централизованные базы данных, реплицированные базы данных, а также несколько баз данных с подпиской для пользователей.

Литература

1. Smart Contracts on Bitcoin Blockchain // BitFury Group. – 2015. – Сентябрь 13 (Version 1.0)

2. Blockchain: Blueprint for a New Economy / Melanie Swan. – США : O'Reilly Media, 2015.

3. The Blockchain Explained to Web Developers, Part 1: The Theory / François Zaninotto. – Апрель 28, 2016.

4. Алгоритмы. Руководство по разработке / Стивен Скиена. – СПб. : БХВ-Петербург, 2014.

References

1. Smart Contracts on Bitcoin Blockchain // BitFury Group. – 2015. – Sentyabr' 13 (Version 1.0)

2. Blockchain: Blueprint for a New Economy / Melanie Swan. – SSHA : O'Reilly Media, 2015.

3. The Blockchain Explained to Web Developers, Part 1: The Theory / François Zaninotto. – Aprel' 28, 2016.

4. Algoritmy. Rukovodstvo po razrabotke / Stiven Skiena. – SPb. : BKHV-Peterburg, 2014.