УДК 003.26

А. М. Кудин, д-р. техн. наук, с. н. с.
Физико-технический институт Национального технического университета Украины «Киевский политехнический институт имени И. Сикорского», г. Киев

БЛОКЧЕЙН И КРИПТОВАЛЮТЫ НА ОСНОВАНИИ «ДОКАЗАТЕЛЬСТВА ТОЧНОСТИ»

Предложен новый метод построения цепочки блоков транзакций (blockchain) на основании общей теории оптимальных алгоритмов. Метод позволяет улучшить оценки скорости и стойкости при сохранении децентрализации внесения изменений в цепочки блоков транзакций.

Ключевые слова: *цепочка блоков транзакций, криптовалюты, доказательство на основе работы, доказательство на основе ставок, биткоин, общая теория оптимальных алгоритмов.*

Введение. Одними из последних тенденций развития технологий распределенных вычислений и электронной наличности являются «блокчейн» и его производные (криптовалюты, интеллектуальные контракты). Актуальность развития этих технологий [1] объясняется принципиальной возможностью использования блокчейна как основы распределенной децентрализованной целостностной технологии обработки информации для решения самого широкого рода прикладных задач: от децентрализованного выпуска и обращения электронной наличности («криптовалюты»), аутентификации и электронного нотариата до распределенного подписания контрактов и электронных выборов. С другой стороны технологии блокчейна — реализация последних достижений теории вычислительной сложности алгоритмов и криптологии. Само появление одной из распространенных технологий работы блокчейна — технологии «доказательства проделанной работы (англ. — proof-of-works)» — обязано решению задач от DoS-атак и спама [2, с. 139–147]. Именно это делает исследование аспектов практической стойкости блокчейна и теоретических основ его построения и анализа одной из самых актуальных задач информационных технологий и криптологии.

Известными и актуальными проблемами применения данных технологий являются скорость выполнения транзакций при сохранении децентрализации, нагрузки на вычислительные ресурсы и сохранения доверия к алгоритму консенсуса [3]. Это фундаментальные проблемы данных технологий, связанные с децентрализацией. Для их решения обычно применяются различные алгоритмы «майнинга»

новых блоков в цепочке [4, с. 7–8]. В статье предлагается принципиально новый подход к задаче майнинга — подтверждения транзакций, основанный на балансе — точность/сложность.

Технологии блокчейн и его производные. Основным направлением развития блокчейн является применение новых алгоритмов распределенного соглашения при генерации очередного блока в цепочке блоков транзакций. Недостатками существующих алгоритмов «proof-of-works» является их ограничения по скорости и сложности осуществления транзакций, связанных с формированием «вычислительных пулов» майнингов, высокой ценой майнинга и принципиальной неточностью описания сложности вычислительной способности участников блокчейна. Кроме этого постоянный рост вычислительной сложности «майнинга» начинает ограничивать децентрализацию. Именно это вызывает переходы к другим алгоритмам соглашения при формировании и верификации новых блоков в блокчейне, таких как «proof-of-stake» или «proof-of-activity» [5]. Но простой переход к консенсусу «наличию долей-ставок» ведет к снижению стойкости протокола консенсуса [3], а тривиальное объединение подходов «proof-of-works» и «proof-of-stake» на базе самих «stake-ставок» слабо осуществимо на практике [6].

Постановка задачи построения эффективного алгоритмам соглашения при формировании и верификации новых блоков в блокчейне состоит в том, чтобы построить одностороннее преобразование, стойкое к последовательной централизации (при увеличении вычислительных ресурсов одного или сообщества узлов права по согласованию растут линейно) и атаки «накопления ставок».

Идея предлагаемого в статье алгоритма в том, чтобы для вычисления сложной функции требовались не только вычислительные ресурсы, но и информация о входных данных (заданных неполно и неточно), позволяющая решить задачу с требуемой точностью. Для пояснения идеи остановимся на кратком описании алгоритма функционирования блокчейн при использовании технологии соглашения «proof-of-works», удобное для дальнейшего анализа.

1. Алгоритм обеспечения целостности информации. Для обеспечение целостности используется результат вычисления хеш-кода по методу двоичного дерева Меркла [7, с. 40–45] (рисунок). Таким образом, для верификации целостности i-го блока данных уровнях иерархии и «корень хеш-дерева», т. е. кортеж

$$< (h_n^i, h_n^{i+1}), (h_{n-1}^i, h_{n-1}^{i+1}), ..., (h_1^i, h_1^{i+1}), h_0 > .$$

Всего для верификации блока данных необходимо не более $O(\log_2 n)$ операций и хэш-кодов. Общий принцип построения конструкции «цепочки блоков транзакций» — blockchain показан на рисунке.

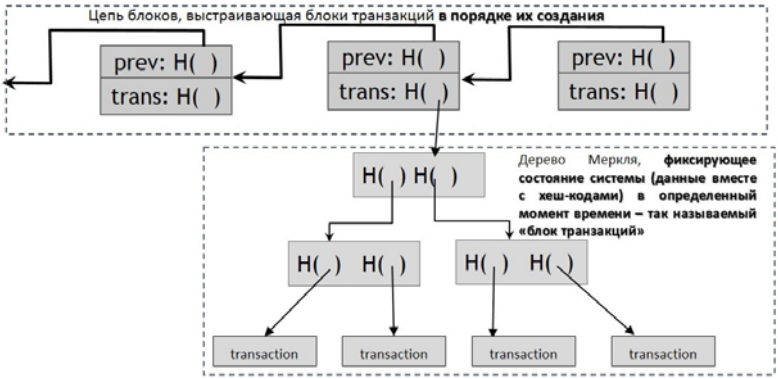

Рисунок. *Общий принцип построения конструкции «цепочки блоков транзакций» — blockchain*

2. Алгоритм добавления нового блока в блокчейн при применении протокола соглашения «proof-of-works».

2.1. Новые транзакции получают все участники протокола соглашения.

2.2. Все участники протокола соглашения генерируют блок транзакций по определенным правилам (например, генерируют и проверяют правильность построения дерева Меркля и цифровые подписи каждой транзакции).

2.3. Все участники протокола формируют «цифровую пломбу» блока путем решения вычислительно сложной задачи. Известным примером такой задачи является вычисление хэш-кода от заданных данных (так называемой «хэш-головоломки»), а именно задачи найти такое значение $nonce$, чтобы значение хэш-кода $h(nonce \,||\, hcode_{i-1} \,||\, block_i) < t$, где $hcode_{i-1}$ — хэш-код предыдущего блока, $block_i$ — данные текущего блока, t — некоторый порог, одинаковый для всех участников протокола. Известно, что для сильной хэш-функции эта задача решается только методом прямого перебора по всем значениям $nonce$.

2.4. Участники протокола проверяют цифровую пломбу участника, который сформировал ее раньше всех и при правильности проверки добавляют этот блок в цепочку блока транзакций.

Алгоритм соглашения на основании «доказательства точности». Для решения проблем протоколов согласования, изложенных выше, предлагается изменить вычисление функции формирования «цифровой пломбы» (пункт 2.3 алгоритма добавления нового блока в блокчейн при применении протокола соглашения «proof-of-works») таким образом, чтобы необходимые входные данные были заданы

неполно и неточно, а значение функции требовалось вычислить с точностью, задаваемой некоторым порогом. Информация о входных данные располагаются на нескольких ресурсах за доступ к которым конкурируют участники протокола соглашения. Последнее свойство позволяет уравнивать шансы участников протокола с высокопроизводительными и малопроизводительными вычислительными ресурсами в борьбе за право генерации нового блока.

Теоретической основой построения и оценки стойкости протокола соглашения на основании «доказательства точности» предлагается выбрать общую теорию оптимальных алгоритмов [8, с. 18–42], которая связывает существование и сложность алгоритмов с точностью задания входных данных. Введем следующие обозначения. Пусть заданы множества X, Y. Пусть 2^Y — класс всех подмножеств множества Y. Аналогично подходу, предложенному автором в работе [9, с. 248–249] для построения однонаправленного преобразования рассматривается оператор $S: X \times R_+ \to 2^Y$, где $R_+ = [0, \infty)$, называемый оператором решения и обладающий двумя свойствами:

$S(x,0) \neq \varnothing, \forall x \in X$, $\delta_1 \leq \delta_2 \Rightarrow S(x,\delta_1) \subset S(x,\delta_1), \forall \delta_1, \delta_2 \in R_+, x \in X$.

Для заданного $\varepsilon \geq 0$ элемент $y \in Y$, удовлетворяющий условию $y \in S(x,\varepsilon)$ называется ε-приближением. Задача поиска ε-приближения рассматривается при условии отсутствия полной (и, в общем случае, точной) информации об элементе x, о котором известна некоторая информация $N(x)$, где: $N: X \to Y$ — информационный оператор в терминологии общей теории оптимальных алгоритмов, а Y — образ множества X. Зная $N(x)$ необходимо найти ε-приближение к x.

Если множество $V(N,x) = \{\widetilde{x} \in X : N(\widetilde{x}) = N(x)\}$ всех элементов $\widetilde{x}$ неотличимых с помощью информационного оператора N от x состоит из одного элемента, то оператор N устанавливает взаимнооднозначное соответствие между множествами X и Y, и называется полным (и неполным в противном случае). Оператор решения, примененный к неполному информационному оператору, порождает множество $A(N,x,\varepsilon) = \bigcap_{\widetilde{x} \in V(N,x)} S(\widetilde{x},\varepsilon)$, при этом для некоторых $\delta_1 \leq \delta_2 \Rightarrow A(N,x,\delta_1) \subset A(N,x,\delta_2)$.

Тогда $r(N,x) = \inf\{\delta : A(N,x,\delta) \neq \varnothing\}$ и $r(N) = \sup_{x \in X} r(N,x)$ определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе.

В работе [8, с. 26] доказано, что на классе идеальных алгоритмов $\Phi(N): N(x) \to G$ с введенными определениями локальной $e(\varphi, N, x) =$

$= \inf\{\delta : \varphi(N(X) \in A(N, x, \delta)\}$ и глобальной $e(\varphi, N) = \sup_{x \in X} e(\varphi, N, x)$ погрешностей информация $N(X)$ позволяет найти ε-приближение для произвольного $x \in X$ тогда и только тогда, когда выполняется одно из условий:

$$r(N) < \varepsilon,$$

$$r(N) = \varepsilon, \exists \varphi : \varphi(N(x)) \in S(x, e(\varphi, N), \forall x \in X .$$

Используя приведенные выше неравенства можно вычислить порог точности вычисления функции «цифрового пломбирования» блоков, который позволит регулировать свойства стойкости протокола и скорости генерации нового блока при условии сохранения децентрализации протокола.

Выводы. Рассмотрен новый метод построения цепочки блоков транзакций (blockchain) на основании общей теории оптимальных алгоритмов. Метод позволяет улучшить оценки скорости и стойкости внесения изменений в цепочки блоков транзакций.

Список использованной литературы:

1. Satoshi N. Как технология блокчейн поможет человечеству. Режим доступа: www.bitnovosti.com/2014/10/02/blockchain-pomozhet-chelovechestvu.
2. Dwork C., Naor M. Pricing via processing or combatting junk mail. Annual International Cryptology Conference CRYPTO 1992: Advances in Cryptology. CRYPTO' 92. P. 139–147.
3. Andrew Poelstra Distributed Consensus from Proof of Stake is Impossible. https://download.wpsoftware.net/bitcoin/old-pos.pdf.
4. Fan Zhang, Ittay Eyal, Robert Escriva, Ari Juels, Robbert van Renesse REM: Resource-Efficient Mining for Blockchains. https://eprint.iacr.org/2017/179.pdf.
5. Ray Patterson Alternatives for Proof of Work, Part 1: Proof Of Stake / https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison.
6. Ray Patterson Alternatives for Proof of Work, Part 2: Proof of Activity, Proof of Burn, Proof of Capacity, and Byzantine Generals. https://bytecoin.org/blog/-proof-of-activity-proof-of-burn-proof-of-capacity/
7. Ralph C. Merkle Secrecy, authentication, and public key systems. Ph.D. thesis, Electrical Engineering, Stanford, 1979. 182 p.
8. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. М.: Мир, 1988. 184 с.
9. Кудин А. М. Однонаправленные функции с информационно невычислимой лазейкой. *Прикладная радиоэлектроника.* Том. 11. № 2. С. 246–249.

A new method of blockchain generation is proposed.

Key words: *blockchain, cryptocurrency, bitcoin, proof-of-work, proof-of-stake, general optimal algorithms theory.*

Получено 21.03.2017