01.01.00. Математика

УДК 004.42

С.В. Дьяченко
доцент кафедры информатики и математики, к.физ.-мат.н.,
филиал «КубГУ» в г. Новороссийске
S.V. Dyachenko
candidate of physical and mathematical Sciences associate Professor
of the Department of Informatics and mathematics of the Kuban state University
branch in Novorossiysk (900-243-68-09 svdnov@mail.ru)
Е.Г. Бойко
студент направления подготовки «Прикладная математика и информатика»,
филиала «КубГУ» в г. Новороссийске
E.G. Boyko
student of the direction "Applied mathematics and Informatics" Department of
Informatics and mathematics of the Kuban state University branch
in Novorossiysk (900-243-68-09 svdnov@mail.ru)

ТЕХНОЛОГИИ ОБРАБОТКИ ТРАНЗАКЦИЙ В BLOCKCHAIN

Аннотация. В статье описываются два наиболее популярных механизма достижения консенсуса в блокчейне - Proof-of-Work (PoW), использующийся в сети добываемых монет (таких как Bitcoin, Litecoin, Ethereum и др.), то есть монет, требующих внушительные вычислительные мощности для проведения транзакций в сети, и Proof-of-Stake - использующийся в сети предварительно созданных монет (таких, как Ripple), то есть монет, транзакции, в сети которых не нуждаются в вычислительных мощностях. Описаны принципы работы этих двух механизмом, их преимущества и недостатки, включая слабые места и уязвимости в безопасности. Так же рассматриваются гибридные механизмы (PoI, PoA и др.). Понимание такого важного звена системы, как механизмы достижения консенсуса, помогает лучше разобраться во внутреннем устройстве самой системы блокчейн, системе валидации транзакций и характеристиках, влияющих на скорость сети (и транзакций соответственно), что поможет в проектировании и разработке приложений и проектов, связанных с блокчейном. Такими проектами могут быть новые криптовалюты, криптовалютные кошельки, боты для торговли на биржах или системы, прогнозирующие изменения курса криптовалют на основе статистических данных и машинного обучения. Понимание принципов работы этих механизмов позволяет более детально смотреть на внутренние процессы той или иной криптовалюты. При помощи машинного обучения и открытых источников (API пулов для майнинга и торговых бирж) возможно обучить модель машинного обучения находить закономерности, которые будут так или иначе влиять на курс.

Annotation. The article describes two of the most popular consensus – building mechanisms in blockchain-Proof-of-Work (PoW), which is used in the network of mined coins (such as Bitcoin, Litecoin, Ethereum, etc.), that is, coins that require impressive computing power for transactions in the network, and Proof-of - Stake-which is used in the network of pre-created coins (such as Ripple), that is, transactions in the network do not need computing power. The principles of operation of these two mechanisms, their advantages and disadvantages, including weaknesses and vulnerabilities, are described. Hybrid mechanisms (PoI, PoA, etc.) are also considered. Understanding such an important part of the system as consensus-building mechanisms helps to better understand the internal structure of the blockchain system itself, the transaction validation system and the characteristics that affect the network speed (and transactions, re-

spectively), which will help in the design and development of applications and projects related to blockchain. Such projects can be new cryptocurrencies, cryptocurrency wallets, bots for trading on exchanges or systems that predict changes in the rate of cryptocurrencies based on statistics and machine learning. Understanding the principles of these mechanisms allows to look in more detail at the internal processes of a cryptocurrency. With the help of machine learning and open sources (API pools for mining and trading exchanges), it is possible to train the machine learning model to find patterns that will affect the course one way or another.

Ключевые слова: искусственный интеллект, машинное обучение, криптовалюта, blockchain, курсы криптовалют.

Key words: artificial intelligence, machine learning, cryptocurrency, blockchain, cryptocurrency courses.

В статье анализируются достоинства и недостатки технологий обработки транзакций в blockchain PoW и PoS с целью создания программ машинного обучения для прогнозирования изменений курсов криптовалюты.

Для работы любой криптовалюты необходима возможность обмена этой криптовалютой между её держателями, ведь сама по себе валюта (в том числе и фиатная) – фидуциальный механизм, который имеет какую-то ценность только тогда, когда держатели в эту ценность верят и наделяют ей валюту. Без возможности обмена и торговли любой объект теряет финансовую ценность, поэтому крайне важно обеспечить надежный и быстрый механизм оборота. Любая (почти) криптовалюта строится на механизме Blockchain – изначально реплицированной распределенной базы данных, созданной для запуска Bitcoin. Blockchain представляет из себя выстроенную по особому алгоритму непрерывную, последовательную цепочку блоков (контейнеров с данными), хранимую независимо друг от друга на распределенных узлах сети, то есть является распределенным реестром, содержащим в себе все когда либо совершенные операции с криптовалютой.

Так как Blockchain – децентрализованная система, крайне важным её механизмом является безопасное децентрализованное создание и обработка транзакций. А вот реализация этого механизма у разных криптовалют может отличаться.

Условно, можно поделить все криптовалюты на добываемые (процесс добычи называется майнинг – от англ. mining – добыча) и предварительно созданные. К добываемым относятся Bitcoin, Litecoin, Ethetium, Monero, ZCash и другие, к предварительно созданным относятся Ripple, Stellar, EOS, NEO. В сети каждой криптовалюты необходимо проверять транзакции, чтобы убедиться, что криптовалюта не была потрачена дважды. Группа транзакций объединяется в блок, который после проверки присоединяется к другим, ранее проверенным блокам. Таким образом, осуществляется «прозрачность» сети. За саму «проверку» начисляется награда, и наиболее популярные механизмы проверки и награды это Proof-of-Work (PoW) и Proof-of-Stake (PoS).

Proof-of-Work

Proof-of-Work (доказательство выполнения работы) – это механизм достижения консенсуса (он достигается, когда все участники сети подтверждают достоверность транзакций и идентичность информации на всех узлах), используемый для подтверждения (обработки и добавления в последовательность блоков) транзакций и создания новых блоков. Этот механизм позволяет конкурировать майнерам (сверхмощным ЭВМ с множеством GPU или ASIC) за завершение транзакций в сети и вознаграждение. Награда майнерам зачисляется за верно сгенерированный и подтвержденный блок, и состоит из комиссии, взымаемой со всех транзакций в блоке. Таким образом, майнер получает награду только в случае, если хеш предыдущего блока подобран верно, транзакции обработаны и сгруппированы в новый блок, блоку присвоен хеш, содержащий в себе хеш прошлого блока,

и в другой цепи блоков не появилось больше блоков, чем в цепи блоков, обрабатываемых майнером (в этом случае наиболее длинная цепь блоков считается достоверной, а менее длинная обнуляется и считается недействительной, транзакции из блоков менее длинной сети встают в очередь для формирования нового блока).

Этот механизм считается безопасным, поскольку делает практически невозможным «Атаку 51%», и формирование блоков зависит от совокупной мощности каждого майнера, а не от количества монет у какого-либо держателя (модель PoS). Таким образом, держатели большого количества монет не имеют власти над сетью и не могут манипулировать транзакциями (что и является некоторого рода реализацией «Атаки 51%»), а совершить подобное, используя мощности майнера (то есть собрать в один узел сети мощность 51% майнеров этой сети) крайне ресурсозатратно и практически нереализуемо, поэтому Proof-of-Work считают безопасной моделью проверки транзакций и начисления награды. Однако, у этой модели достаточно много минусов.

Самым очевидным и серьезным минусом является очень высокая стоимость этой модели, поскольку математические расчеты (которые становятся все более сложными) являются крайне ресурсозатратными. Оборудование потребляет огромное количество электроэнергии и по сути, сама по себе работа является бесполезной, поскольку производится исключительно для обработки транзакций в сети (а не научных расчетов, моделирования поведения частиц и т.д.). Так же оборудование работает 24 часа в сутки и выделяет огромное количество тепла, которое необходимо эффективно отводить и охлаждать оборудование, что делает промышленную или домашнюю добычу криптовалюты (майнинг) достаточно проблемным процессом. Еще одной проблемой этой модели является незаконное распространение добытчиков на утройства пользователей без их ведома, то есть умышленное заражение злоумышленниками большого количества вычислительной техники (компьютеры, смартфоны, сетевое оборудование) с целью майнинга криптовалюты, от чего сильно снижается производительность техники, и пользователи сталкиваются с неудобствами.

Чтоб сделать процесс создания транзакций менее ресурсоемким, была создана новая модель Proof-of-Stake (доказательство доли владения), которая позволяет обойтись без ресурсоемкого процесса добычи монеты майнерами и подразумевает единовременный выход всех токенов (монет) в сеть и на торговую площадку.

Proof-of-Stake

Proof-of-Stake – это механизм, при котором вероятность формирования нового блока участником сети пропорциональна доле, которую составляют принадлежащие этому участнику токены (монеты) этой криптовалюты от общего количества токенов в данной валюте. Так как такая криптовалюта создается единожды и все токены валюты доступны сразу, большая вероятность формирования блока будет у юнитов, содержащих большую долю токенов. Например, держатель, владеющий 2% всех токенов валюты, будет генерировать 2% новых блоков. Этот механизм позволяет создавать блоки участникам, просто купившим определенное количество токенов валюты, и не требует никаких вычислительных мощностей, а, следовательно, и энергозатрат. Так же этот механизм позволяет использовать алгоритмы теории игр для эффективного противодействия централизации (захвата одного участника, с наибольшим количеством токенов на аккаунте, контроля над всеми транзакциями).

Однако из этого следуют и очевидные недостатки. Все-таки, теоретически, сценарий накапливания критического количества токенов такой криптовалюты для захвата контроля над формированием блоков более легко реализуем, чем захват критического количества вычислительной мощности в механизме PoW.

Например, некоторые криптовалюты (например, Ripple) вызывают серьезное опасение у криптовалютного сообщества, по причине того, что около половины всех выпущенных токенов находится под контролем разработчиков криптовалюты (достаточно узкого круга лиц), и, по факту, данная криптовалюта централизована.

Существуют гибридные технологии, например Proof-of-Importance (PoI – доказательство важности, используется криптовалютой NEM), на вероятность формирования блока в котором влияет количество единиц криптовалюты на балансе, активность аккаунта и время нахождения аккаунта в сети; Proof-of-Activity (PoA – доказательство активности); множество других, менее популярных и более специфических технологий, например Proof-of-Capacity (PoC – доказательство выделенного объема, используется для майнинга путем предоставления сети свободного дискового пространства) и т.д., однако основными двумя технологиями являются PoW и PoS. И после того, как какая-либо добываемая криптовалюта исчерпает количество токенов, выдаваемых в награду за майнинг, скорее всего, PoW для этой криптовалюты будет заменен на PoS (вероятное будущее Ethereum и Litecoin), а, значит, транзакции в сети этой криптовалюты продолжат обрабатываться и криптовалюта продолжит жить.

Как в случае с PoW, возможно на основании количества юнитов в сети прогнозировать скорость транзакций, а, следовательно, и популярность валюты, что напрямую отражается на её курсе, так и в случае с PoS – количество держателей монеты формирует скорость транзакций, что, аналогично, при некоторых обстоятельствах поможет спрогнозировать тенденции изменения курса. Понимание принципов работы этих механизмов позволяет более детально смотреть на внутренние процессы той или иной криптовалюты. При помощи машинного обучения и открытых источников (API пулов для майнинга и торговых бирж) возможно обучить модель машинного обучения находить закономерности, которые будут так или иначе влиять на курс.

Источники:

1. С. Равал, "Децентрализованные приложение — Технология Blockchain в действии" — СПб., Питер, 2017. — 191 с.
2. Андреас М. Антонопулос, "Овладение биткойном" — СПб., Питер, 2014. — 298 с.
3. Мелани Свэн, "Блокчейн: сценарий новой экономики" — М., Наука, 2015. — 153 с.

Sources:

1. S. Raval, "Decentralized application - Blockchain technology in action" - St. Petersburg, Peter, 2017. - 191 p.
2. Andreas M. Antonopoulos, "Mastering bitkoynom" - St. Petersburg, Peter, 2014. - 298 p.
3. Melanie Swan, "Blokchein: the scenario of a new economy" - M., Nauka, 2015. - 153 p.