СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Государственный стандарт Республики Беларусь. Услуги сотовой подвижной электросвязи. Требования к качеству и методы контроля : СТБ 1904–2011. Введ. 30.05.11. – Минск : Госстандарт : ОАО «Гипросвязь», 2011. – 29 с.

2. Государственная система стандартизации Республики Беларусь. Услуги передачи данных. Требования к качеству. Нормы и методы контроля.: СТБ 1962–2012. Введ. 28.05.12. – Минск : Госстандарт: Проектный и научно-исследовательский РУП «Гипросвязь»,2012. – 18 с.

3. Государственная система стандартизации Республики Беларусь. Информационные технологии. Требования к показателям качества интернет-услуг: СТБ П 2236 – 2011. Введ. от 01.03.2012 до 01.03.2014. – Минск : Госстандарт: Государственное предприятие «НИИ ТЗИ», 2011. – 12 с.

4. Об утверждении Правил оказания услуг электросвязи : постановление Совета Министров Республики Беларусь, 17 авг. 2006, № 1055 [Электронный ресурс]. – Режим доступа : https://www.beltelecom.by/sites/default/files/Doc/legalinformation/pravila_okazaniya_usl_elektrosvyazi10052042_03-11_83_11_10_2016.doc. – Дата доступа : 18.09.2022.

М.В.СТЕРЖАНОВ

АЛГОРИТМЫ КОНСЕНСУСА БЛОКЧЕЙН СИСТЕМЫ

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Блокчейн — это децентрализованная система управления реестром для записи и проверки транзакций, что позволяет двум сторонам проводить транзакции в одноранговой

(P2P) сети без участия арбитра или посредника. Находящаяся в блокчейне транзакция может описывать различные формы отношений, включая передачу права собственности или совместное использование ресурсов, где они могут быть материальными, такими как деньги, недвижимость, автомобили или нематериальные авторские права, цифровые документы, и интеллектуальная собственность и т. д.

Блокчейн обладает тремя ключевыми преимуществами:

1. Распределенность. Каждый узел обладает исчерпывающей актуальной копией данных, что позволяет восстановить базу даже, если сохраняется всего один экземпляр базы.

2. Неизменяемость данных. Блокчейн содержит всю цепочку изменений данных. Контроль целостности и корректности цепочки обеспечивается применением специальных криптографических механизмов.

3. Консенсус. Технология устойчива к мошенническому поведению одного или нескольких узлов: все операции с конфигурацией сети и с базой принимаются через консенсус узлов.

Среди основных компонентов блокчейна алгоритм консенсуса является определяющей технологией, лежащей в основе предотвращения появления ошибочных блоков и производительности системы. Каждый узел содержит свой реестр, и набор каждого реестра поддерживается одинаковым с помощью алгоритма консенсуса. То есть, механизмы консенсуса обеспечивают конвергенцию к единой, неизменяемой версии цепочки. В конце концов, любой может предоставить информацию, которая будет храниться в блокчейне, и поэтому важно, чтобы было подтверждение в форме консенсуса о том, следует ли добавлять эту информацию.

Ключевым требованием для достижения консенсуса является согласие принятия между узлами в сети одного значения данных, даже в случае сбоя некоторых узлов или их ненадежности.

Рассмотрим основные разновидности алгоритмов консенсуса [1-3]:

- «Доказательство работы» (Proof-of-work - PoW) – это механизм, который позволяет сетевым узлам конкурировать, чтобы их блок был следующим добавленным в цепочку, путем выполнения достаточно сложной вычислительной работы. В качестве примера таких действий можно требовать, чтобы хэш заголовка блока был меньше целевого значения. Для каждой попытки майнер должен вычислить хэш для всего заголовка блока. Данный механизм требует серьезных энергетических затрат: большое количество узлов производят вычисления, но в реальности только один, первый, проводит успешную работу и получает вознаграждение;

− «Доказательство доли» (Proof-of-stake - PoS) – это альтернативный механизм, который предоставляет участникам право на валидацию пропорционально их владению токенами в сети блокчейнов. Данный метод требует меньшего энергопотребления по сравнению с PoW.

Выбор узла может осуществляться случайным образом из наиболее "богатых" узлов или из наиболее старых узлов. Недостатком подхода является мотивация в концентрации средств, что может приводить к некоторой централизации сети. Однако, алгоритм предусматривает увеличение шанса на право создания блока исходя не только из количества токенов, но и времени пребывания в системе без создания блока;

− «Делегированное доказательство доли» (Delegated Proof-of-Stake - DPoS) – это вариация алгоритма PoS, созданная для минимизации издержек на поддержку блокчейн сети. Владельцы с наибольшим балансом выбирают своих представителей, каждый из которых получает право подписывать блоки в блокчейн сети;

− «Арендное доказательство доли» (Leased Proof-of-Stake - LPoS) – также является модификацией алгоритма PoS, в которой любой пользователь имеет возможность передавать свой баланс в аренду другим узлам за дополнительную прибыль;

− «Доказательство способности» (Proof-of-Capacity/ Proof-of-Space - PoC) – в данном алгоритме каждый валидатор вычисляет достаточно большой объем данных, который записывается в подсистему узла, при этом вычислительные ресурсы ограничены временем. Стратегия работы схожа с PoW, за исключением того, что потребляется дисковое хранилище вместо вычислительных возможностей;

− «Доказательство важности» (Proof-of-Importance - PoI) – значимость пользователя определяется количеством средств, имеющихся у него на балансе и количеством проведенных транзакций;

− «Доказательство деятельности» (Proof-of-Activity - PoA) – каждый валидатор блокчейн сети пробует сгенерировать заголовок блока, потом происходит рассылка в сеть и дальнейшая проверка. Узлы получают этот блок, убеждаются в его законности и добавляют этот блок в блокчейн. Плата распределяется между валидаторами и «счастливчиками»;

− «Доказательство власти» (Proof-of-Authority - PoAuth) – все транзакции и блоки проверяются посредством одобренных аккаунтов. Проведение транзакций и создание блоков проходит в автоматическом режиме;

− «Доказательство сжигания» (Proof-of-burn - PoB), основан на принципе разрешения майнерам сжигать или уничтожать токены виртуальной валюты, что дает им право писать блоки пропорционально сгоревшим монетам;

− «Практическая византийская отказоустойчивость» (Practical Byzantine Fault Tolerance - PBFT) – отвечает за эффективную работу в асинхронных сетях, позволяет достичь консенсуса, даже если некоторые узлы не отвечают или дают неверную информацию. Выбирается 2 вида узлов - лидеры и резервные. Каждый узел в сети поддерживает свое собственное внутреннее состояние, и когда он получает сообщение, он выполняет вычисления и готовит решение о новом полученном сообщении. Индивидуальное решение каждого узла отправляется лидеру, который подтверждает доверие к новому сообщению на основе решений всех узлов.

Таким образом, современные алгоритмы консенсуса имеют свои сильные и слабые стороны, поэтому возможны случаи комбинирования алгоритмов консенсуса.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Mingxiao, D. A review on consensus algorithm of blockchain. / D. Mingxiao, M. Xiaofeng, Z. Zhe // 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). – 2017. – P. 1–12.

2. Wahab, A. Survey of Consensus Protocols / A. Wahab, W. Mehmood // Distributed, Parallel, and Cluster Computing. – 2018. – P. 1–12.

3. Bano, S. SoK: Consensus in the Age of Blockchains / S. Bano, A. Sonnino, M. Al-Bassam // AFT '19: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. – 2019. – P. 183–198.