УДК 004.056.53

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ОДНОРАНГОВЫХ СЕТЯХ.

© Буслаев А.А., Лёзин И.А.

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

e-mail: buslaew.ar@mail.ru

Различают два типа сетей – одноранговую и сеть на основе сервера. Сети обеих разновидностей выполняют поставленные перед ними задачи, но делают это по-разному.

Одноранговая сеть – это тип компьютерных сетей, в которых все узлы имеют равные возможности и выполняют одинаковые функции без централизованного контроля или иерархии. Каждый узел в такой сети является как клиентом, так и сервером, способным обмениваться ресурсами и информацией с другими узлами [1]. На рисунке 1 представлен пример одноранговой сети.

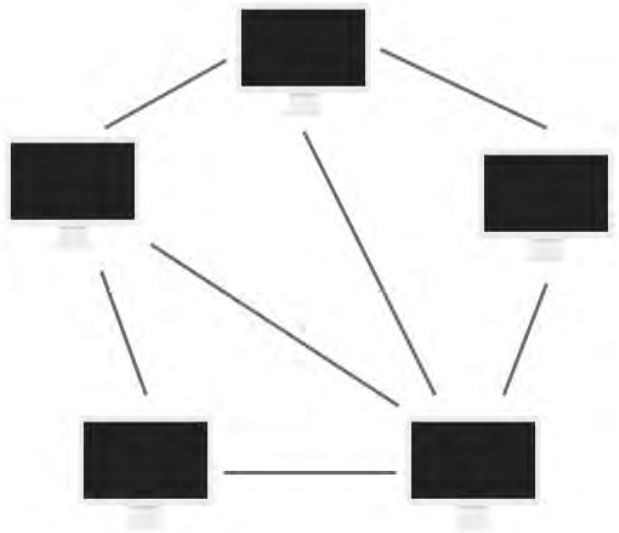

Рисунок 1 – Пример одноранговой сети

Децентрализованные приложения – это особая разновидность интернет-приложений, основанных на одноранговой сети (peer-to-peer network) и имеющих открытый исходный код. Ни один узел сети не имеет полного контроля над ДП. Структура и способ хранения данных ДП зависят от его функционального назначения. Например, Bitcoin использует структуру данных в виде блокчейна. Узлом одноранговой сети может стать любой компьютер, подключенный к Интернету. В структуре ДП нет главного сервера, который координирует узлы и принимает решение о достоверности данных. Для решения этой сложной задачи предназначены особые протоколы консенсуса. Протоколы консенсуса разрабатывают под конкретную структуру данных ДП. Например, Bitcoin для достижения консенсуса использует протокол доказательства работы (proof-of-work protocol, PoW).

Сам же блокчейн представляет собой структуру данных, применяемую для создания децентрализованного регистра. Блокчейн состоит из блоков (block), особым образом соединенных в цепочку (chain). Блок содержит набор транзакций, хеш

предыдущего блока, метку времени (время создания блока), сумму отчисления майнеру за блок и т. д. Поскольку каждый блок содержит хеш предыдущего блока, они связаны в цепочку. Каждый узел сети хранит полную копию блокчейна. Для поддержания безопасности блокчейна применяют протоколы с доказательством выполнения работы (proof-of-work, PoW), с доказательством владения долей (proof-of-stake, PoS) и некоторые другие. Добавление блока происходит по-разному – в зависимости от протокола. В случае с протоколом proof-of-work блок создается при помощи процедуры, которая называется майнингом и обеспечивает безопасность добавления блока. Майнер должен решить сложную математическую задачу и затратить дорогостоящие вычислительные ресурсы [2]. На рисунке 2 представлен алгоритм работы технологии блокчейн.

Рисунок 2 – Алгоритм работы технологии блокчейн

А так выглядит формула для вычисления сложности задачи в сети Ethereum:

$$CBD = PBD + \left(\frac{PBD}{2048}\right) * Max\left(1 - \left\lfloor\frac{CBT - PBT}{10}\right\rfloor, -99\right) + 2^{\left(\left\lfloor\frac{CBN}{100000}\right\rfloor - 2\right)}$$

Здесь:

- CBD: сложность текущего блока.
- PBD: сложность предыдущего блока.
- CBT: временная метка текущего блока.
- PBT: временная метка предыдущего блока.
- CBN: номер текущего блока.

Формула учитывает несколько факторов, включая разницу во времени между текущим и предыдущим блоками, а также номер текущего блока, для расчета новой сложности текущего блока. Это позволяет регулировать сложность в зависимости от изменений во времени генерации блоков и обеспечивает более стабильную скорость генерации блоков в блокчейне.

Таким образом, блокчейн и одноранговые сети представляют инновационные децентрализованные технологии, способствующие безопасной и прозрачной передаче данных и обеспечивающие участникам равные права и возможности.

Библиографический список

1. Прасти Нараян Блокчейн. Разработка приложений / пер. с англ. СПб.: БХВ-Петербург, 2018. 256 с.

2. Ватаманюк А.И. Создание, обслуживание и администрирование сетей на 100 %. СПб.: Питер, 2010. 288 с.