

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Рассматриваются основные понятия и ключевые моменты реализации распределенной системы записи и хранения блоков фактов Блокчейн.

ВВЕДЕНИЕ

Блокчейн – это система взаимосвязанных блоков (представляемая как цепочка блоков). Каждый блок содержит в себе список проверенных фактов. Фактами могут являться любые события различных предметных областей: финансовые транзакции, записи медицинских карт, отметки о перемещении грузов. Исследователи и эксперты утверждают, что блокчейн вызовет революцию, схожую с той, которую некогда вызвал Интернет. Несмотря на то, что блокчейн создан для поддержки сети Bitcoin, сама идея блокчейна может быть определена независимо от её системы.

I. ОСНОВНЫЕ МОМЕНТЫ РЕАЛИЗАЦИИ СЕТИ ПО ПРИНЦИПУ БЛОКЧЕЙН.

Блокчейн - это распределенная система, в основе которой лежит одноранговая (пиринговая) сеть, поэтому все участники сети равноправны. Сеть, построенная по принципу блокчейна, является децентрализованной сетью, где отсутствует единый центр управления. Этот факт исключает возможность отказа или взлома сети из-за отказа или взлома нескольких её узлов. Все коммуникации внутри сети используют средства цифровой криптографии (хэш-функции, цифровые подписи, асимметричное шифрование), чтобы надежно идентифицировать отправителя и получателя, а также защитить само сообщение. Члены сети – анонимные лица, называемые узлами. Цепочка блоков с фактами реплицируется на все узлы сети. Хеш-сумма каждого нового блока в цепочке зависит от хеш-суммы предшествующего блока. Таким образом, блоки образуют тесную связь друг с другом, что исключает возможность взлома отдельных блоков, так как любой узел сети сможет обнаружить нарушение целостности цепочки.

II. ОБЩИЙ АЛГОРИТМ ОБРАБОТКИ ФАКТОВ В БЛОКЧЕЙНЕ

Блокчейн - это способ хранения фактов, разделенных на блоки. В качестве аналогии мож-

но привести бухгалтерскую книгу учета, где каждая страница - это блок, а каждая запись страницы - сам факт. Но так как блокчейн использует децентрализованные сети, то возникает вопрос определения узла, который будет присоединять новый блок с фактами к цепочке блоков (добавление новой страницы в бухгалтерскую книгу). Некоторые узлы в сети создают новые локальные блоки с неподтвержденными фактами (записи в бухгалтерской книге). Если узел быстрее остальных решает задачу или попадает под определенные критерии, то он получает возможность опубликовать его локальный блок, и все факты в этом блоке становятся подтвержденными. Новый проверенный блок посылается всем узлам в сети. Все узлы проверяют, что блок правильный, добавляют его к их копии цепи и пытаются построить новый блок с новыми неподтвержденными фактами. Схематично цепочка блоков представлена на рисунке 1

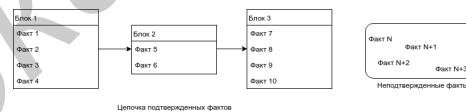


Рис. 1 – Цепочка блоков с фактами

Способы определения узла, который получает возможность разместить блок, зависят от требований и реализации конкретной сети. Например, в сети Bitcoin узлам необходимо решать сложную математическую задачу, которая решается исключительно методом перебора чисел.

III. ВЫВОДЫ

Рассмотренный подход Блокчейн в организации и хранении данных позволяет создавать гибкие и отказоустойчивые системы для обработки и хранения фактов в различных предметных областях.

Ворушенко Артём Витальевич, студент кафедры систем управления БГУИР, a.vorushenko@yandex.ru.

Научный руководитель: Шилин Леонид Юрьевич, доктор технических наук, профессор, dekfitu@bsuir.by.

Научный руководитель: Ляхор Тимофей Васильевич, магистр технических наук, ассистент, linoge@bsuir.by.

1. Свон, М. Блокчейн: Схема новой экономики / М. Свон // Олимп-Бизнес. – 2017.