Автор:

Дмитриев Егор Андреевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

ТЕХНОЛОГИЯ БЛОКЧЕЙН

Аннотация: *в данной работе представлено описание работы технологии блокчейн.*

Ключевые слова: *блокчейн, биткойн, криптовалюта.*

Введение

Блокчейн технология – основа работы криптовалюты биткойн. В настоящее время создаются множество платформ с криптовалютами и все они также построены на технологии блокчейн.

Описание

Блокчейн – это децентрализованная распределенная вычислительная система. Если проводить аналогии, то блокчейн можно сопоставить с книгой бухгалтерского учета, которая доступа каждому участнику сети. Глядя в эту книгу, участник может видеть, какие транзакции были осуществлены. Модель представлена на рис. 1.

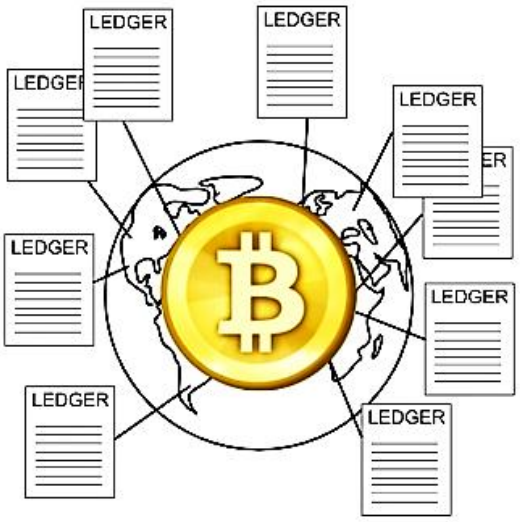

Рис. 1. Блокчейн как книга бухгалтерского учета

Каждая книга страницы – это структурированный блок, который хранит всю информацию о транзакциях. На рис.2 представлены все поля такого блока.

Field Size	Description	Data type	Comments
4	version	int32_t	Block version information (note, this is signed)
32	prev_block	char[32]	The hash value of the previous block this particular block references
32	merkle_root	char[32]	The reference to a Merkle tree collection which is a hash of all transactions related to this block
4	timestamp	uint32_t	A Unix timestamp recording when this block was created (Currently limited to dates before the year 2106!)
4	bits	uint32_t	The calculated difficulty target being used for this block
4	nonce	uint32_t	The nonce used to generate this block… to allow variations of the header and compute different hashes
?	txn_count	var_int	Number of transaction entries
?	txns	tx[]	Block transactions, in format of "tx" command

Рис. 2. Поля блока в блокчейне.

Первые шесть полей образуют заголовок блока. Хэшем заголовка называют хэш блока, то есть транзакции не участвуют в хэшировании.

Третье поле в блоке считается по определенному алгоритму. Значение данного поля есть хэш всех транзакций. Данный алгоритм проще всего представить в виде дерева на рис. 3.

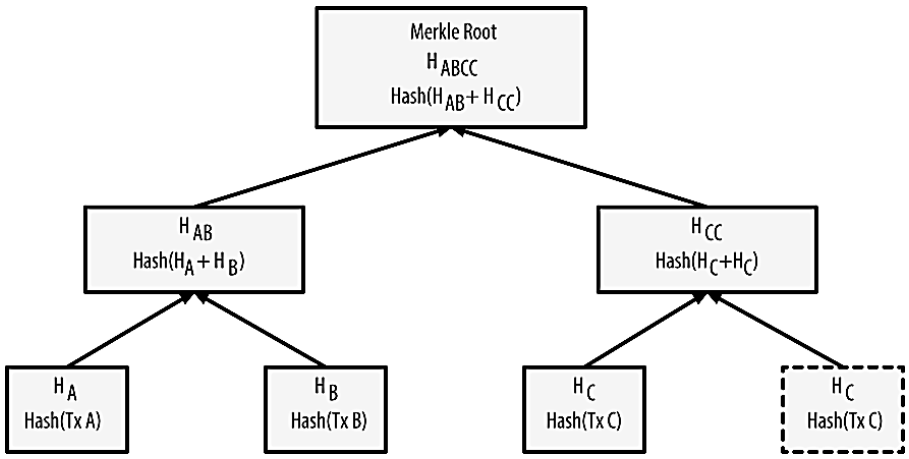

Рис. 3. Алгоритм подсчета хэша транзакций

Созданием новых блоков или по-другому майнинг занимаются майнеры. Существует механизм конечной генерации блока, который называется «Доказательство работы».

Допустим, у майнера есть список некоторое количество транзакций, из которых он собирается сгенерировать новый блок. Основная задача состоит в том, чтобы подобрать значение поля nonce заголовка блока, для того, чтобы хэш всего блока получился меньше, чем заранее заданное число target. Решения такой задачи состоит в полном переборе поля nonce, и не существует никакого алгоритма быстрой генерации. Чем меньше число N, тем сложнее подобрать значение поля. Таким образом, чем больше генерируются блоки, тем меньше становится число N, тем самым генерация нового блока занимает все больше и больше времени. На рис. 4 представлен конечный блок.

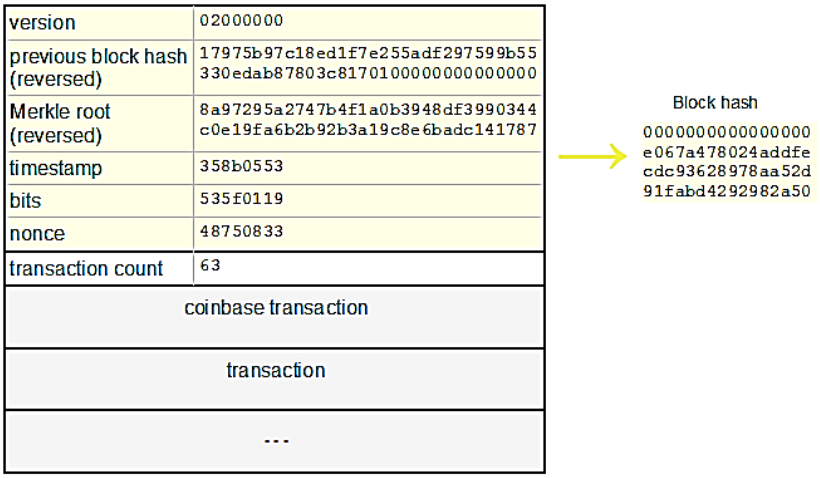

Рис. 4. Готовый блок блокчейна

При генерации нового блока майнеры получают определенную плату с транзации за трату вычислительных мощностей.

Заключение

В данной статье был рассмотрен принцип работы технологии блокчейн.

Список литературы

1. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. – 1-е изд.; Siraj Raval. – 2016. – 150 с.

2. The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. – Phil Champagne. – 2014. – 396 с.