Blockchain Architecture

# Preface

A blockchain is a mesh network of computers, not connecting to any central server, but to each other, who define and agree upon some shared state of data within constraints that all network participants adhere to. This shared state is simply a distributed state machine, each "block" making a change to the current, known, shared state.

The Bitcoin project implemented the first blockchain. Bitcoin’s blockchain is "simple", in relation to the many blockchains that exist today.

For the purposes of this article, we will reference Bitcoin's blockchain. However, the architectural components of transactions, blocks, mining, and consensus can be generalized and implemented in many different ways, leading to many different blockchain projects (usually other cryptocurrencies, or alt-coins ).

# Transactions

Transactions are the things that give a blockchain purpose, and the smallest building block of a blockchain system. Transactions generally consist of a recipient address, a sender address, and a value, not so different from a transaction on a credit card statement. In the Bitcoin network, a transaction moves the value of some bitcoin from one address to another address.

A transaction changes the state of the agreed-correct blockchain. A blockchain is a shared, decentralized, distributed state machine. All nodes (users of the blockchain system) independently hold their own copy of the blockchain, and its current known "state" is calculated by processing each transaction in order.

Transactions are bundled and delivered to each node in the form of a block. As new transactions are distributed throughout the network, they are independently verified and "processed" by each node.

This constant movement of coin is what constitutes the data within Bitcoin's (and any other) blockchain.

# Blocks

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners. Blocks contain a block header, which is the metadata that helps verify the validity of a block. This metadata contains:

version - the current version of the block structure

previous block header hash - the reference to parent block that this one is a child of

merkle root hash - a cryptographic hash of all of the transactions included in this block

time - the time that this block was created

nBits - the current difficulty that was used to create this block

nonce - a random value that the creator of a block is allowed to manipulate however they so choose

These 6 fields constitute the block header. The rest of a block contains transactions that the miner has chosen to include in the block that they created. Users create transactions and submit them to the network, where they sit in a pool waiting to be included in a block.

Архитектура Blockchain (цепочка блоков)

# Предисловие

Цепочка блоков представляет собой сеть компьютеров, не соединенных с каким-либо центральным сервером, а соединенных друг с другом, которые определяют и согласуют некоторое общее состояние данных в рамках ограничений, которые придерживаются все участники сети. Это общее состояние – просто распределенный механизм состояний, каждый «блок» вносит изменения в текущее, известное, общее состояние.

Проект Биткойн реализовал первую блочную цепочку. Биткойн «прост» по отношению к множеству цепочек, которые существуют сегодня.

Для целей этой статьи мы будем ссылаться на блокчейн Биткойна. Тем не менее, архитектурные компоненты транзакций, блоков, добычи и согласованности могут быть обобщены и реализованы по-разному, что приводит к множеству различных проектов блокчейнов (обычно других криптовалют или альтернативных монет).

# Транзакции

Транзакции - это то, что является целью цепочки блоков, и является наименьшим строительным блоком системы. Транзакции обычно состоят из адреса получателя, адреса отправителя и значения, не столь отличного от транзакции в выписке по кредитной карте. В сети Bitcoin транзакция перемещает значение некоторого биткойна с одного адреса на другой адрес.

Транзакция изменяет состояние согласованной правильной блок-цепи. Цепочка является общим, децентрализованным, распределенным механизмом состояний. Все узлы (пользователи блочной системы) независимо хранят свою собственную копию блок-цепи, а ее текущее известное «состояние» рассчитывается путем обработки каждой транзакции по порядку.

Транзакции объединяются и доставляются каждому узлу в виде блока. Поскольку новые транзакции распределены по всей сети, они независимо проверяются и обрабатываются каждым узлом.

Такое постоянное движение монеты является тем, что составляет данные в блочной цепочке Биткойна (и любой другой).

# Блоки

Блоки представляют собой структуры данных, целью которых является объединение наборов транзакций и их распределение по всем узлам сети. Блоки создаются майнерами. Блоки содержат заголовок блока, который представляет собой метаданные, которые помогают проверить достоверность блока. Эти метаданные содержат:

Версия - текущая версия структуры блока

предыдущий хеш заголовка блока - ссылка на родительский блок, что это один из дочерних элементов

криптографический хэш всех транзакций, включенных в этот блок

время - время создания этого блока

nBits - текущая сложность, которая была использована для создания этого блока

nonce - случайное значение, которое создателю блока разрешено манипулировать, однако они так выбирают

Эти 6 полей составляют заголовок блока. Остальная часть блока содержит транзакции, которые майнер выбрал для включения в созданный блок. Пользователи создают транзакции и отправляют их в сеть, где они сидят в пуле, ожидающем включения в блок.