INSIDE BITCOIN'S BLOCKCHAIN

HEADER

The block header is hashed twice to create the fingerprint which is referred to in the next block.

Technical data

Includes a Magic ID, a version number (to specify which set of protocol rules this block conforms to), the size of this block.

Previous block hash

2x SHA256 hash of previous block header (excluding magic ID & block size). This is the link that creates the chain of blocks.

Merkle Root

Distills all the transactions in the block into a single hash.

Timestamp

Approximate timestamp of when the block was created. Used to figure out mining difficulty re-targets i.e if the network is making blocks too quickly or too slowly.

Difficulty target

Related to mining and how hard it is to successfully mine the block

Nonce

A random number. One of the things you can change when mining to create different hashes, while searching for a suitable hash.

TECHNICAL DATA

Version number

Can be used for specifying which set of protocol rules this transaction confirms to.

Transaction lock time

Something which may be used in future for "future dating" a transaction, like writing a post-dated cheque.

Input count

How many inputs are in this transaction.

Output count

How many outputs does this transaction create.

INPUT

(Technical) Input script length

How much data is in the input.

(Technical) Sequence number

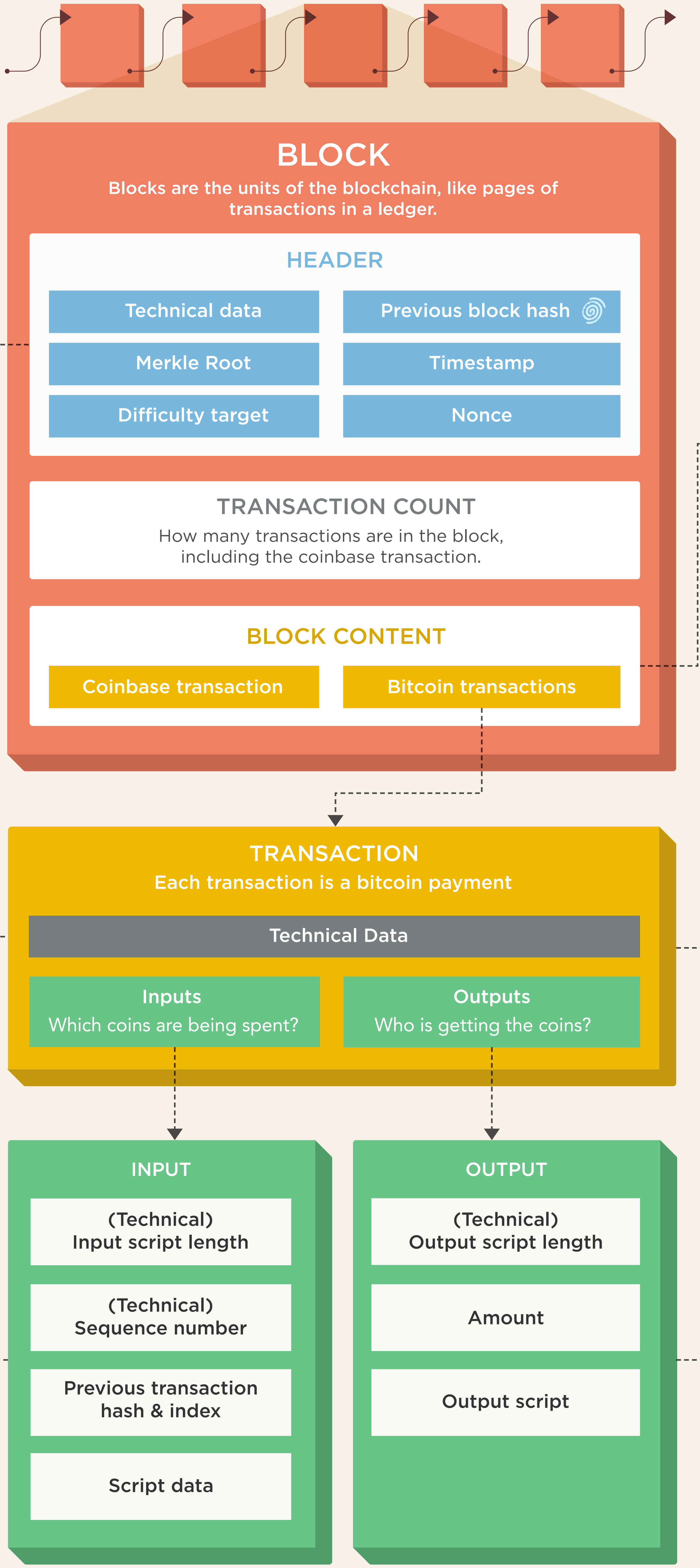
Not really used.

Previous transaction hash & index

This identifies where the coins are coming from, by specifying an output from a previous transaction.

Script data

This is where you "prove" you own the coins and you are allowed to spend it, by signing with the private key of the address that the bitcoins are in.



BLOCK

Blocks are the units of the blockchain, like pages of transactions in a ledger.

HEADER

Technical data | Previous block hash | Merkle Root | Timestamp | Difficulty target | Nonce

TRANSACTION COUNT

How many transactions are in the block, including the coinbase transaction.

BLOCK CONTENT

Coinbase transaction | Bitcoin transactions

TRANSACTION

Each transaction is a bitcoin payment

Technical Data

Inputs
Which coins are being spent?

Outputs
Who is getting the coins?

INPUT

(Technical) Input script length

(Technical) Sequence number

Previous transaction hash & index

Script data

OUTPUT

(Technical) Output script length

Amount

Output script

www.bitsonblocks.net

Designed by www.fractalphia.com

BLOCK CONTENT

Coinbase transaction

The bit where you get to pay yourself the mining reward (currently 25 BTC) plus the fees from the transactions included in the block.

It's a special transaction where there are no 'inputs' or 'from' addresses.

Bitcoin transactions

This is the main payload of the block. Contains bitcoin payments.

Transaction | Transaction | Transaction | Transaction

FOLLOWING THE MONEY

Bank accounts vs cryptocurrencies

Bank accounts mix money up. When you pay someone, you don't specify "use those pounds which I earned from my salary" or "use those pounds which I received for my birthday". Money is treated equally once it hits your account, and is untraceable.

On the other hand, with cryptocurrencies, you need to specify exactly which incoming deposits you are spending. This makes every transaction traceable, right back to the creation of the coins.

Inputs and Outputs

Every bitcoin transaction references some incoming deposits as inputs, and spends them entirely as new outputs, with change returned to one of your addresses.

This is like paying £43.50 by taking three £20 banknotes from your wallet and creating two new banknotes: £43.50 and £16.50. You hand over the £43.50 banknote and keep the £16.50 banknote. You can then spend the £16.50 later in one go. The other person can spend the £43.50 later in one go.

Inputs: 3 x £20

Outputs: £43.50 (payment), £16.50 (change)

OUTPUT

(Technical) Output script length

How much data is in this output

Amount

How many bitcoins (actually, Satoshis) are being sent.

Output script

Who (which address/es) are the bitcoins being sent to? Which signatures are needed to re-spend these coins?