the Availability Digest

www.availabilitydigest.com
@availabilitydig

So You Want to Mine Bitcoins?

April 2014

Bitcoins is a digital currency that made its debut in 2009. We described in some detail how bitcoins work in our earlier article entitled "Mt. Gox, Largest Bitcoin Exchange, Goes Belly Up."[1]

Bitcoin mining is the way in which new bitcoins are minted (digitally, that is). Mining involves packaging bitcoin transactions into blocks and appending them to the bitcoin block chain that records every bitcoin transaction. For each block that a miner adds to the block chain, he is rewarded with 25 bitcoins. At today's price of about $600 USD, this amounts to $15,000. Sounds like a fast way to make a lot of money.

The backup service iDrive decided to try its hand at bitcoin mining. iDrive backs up its customers' files overnight, which leaves most of its 3,000 quad-core servers idle during the day. It put 600 of its servers to work during the day mining bitcoins.[2] After a bit of experience, it calculated that it would earn around 0.4 of a bitcoin per year – about $240!

The Bitcoin Infrastructure

How can mining for bitcoins be so difficult? The answer is that the algorithm for creating a legitimate block of transactions is very difficult to calculate, and its difficulty is raised as time goes on. To understand this, we must first understand a bit about the structure of the bitcoin network.

The Bitcoin Peer-to-Peer Network

The bitcoin infrastructure comprises a large number of peer-to-peer nodes worldwide that cooperate to manage bitcoins. Every bitcoin transaction is sent to each node in the network. Available to each node is the bitcoin block chain, a sequence of blocks that contains every bitcoin transaction that ever occurred since bitcoins were introduced in 2009.

Some of these nodes are mining nodes run by miners. Their job is to package a set of transactions into a block and append them to the block chain. For this effort, they receive as compensation some bitcoins as well as any transaction fees offered by the parties to the transaction.

A miner may be an individual, an organization, or a group of participants that form a *mining pool* and share the profits based on their relative contribution of processing power to the pool.

---

[1] Mt. Gox, Largest Bitcoin Exchange, Goes Belly Up, *Availability Digest*; March 2014.
http://www.availabilitydigest.com/public_articles/0903/bitcoins.pdf

[2] Mining Experiment: Running 600 Servers for a Year Yields 0.4 Bitcoin, *Data Center Knowledge*; February 24, 2014.
http://www.datacenterknowledge.com/archives/2014/02/24/mining-experiment-running-600-servers-year-yields-0-4-bitcoin/

The Block Chain

The block chain is a linked series of transaction blocks that hold every bitcoin transaction made since the currency's introduction in 2009. Each block is protected by a hash value to prevent it from being subsequently modified. Furthermore, the hash for each block includes the hash of the previous block. This guarantees the proper ordering of blocks.

Including the hash from the previous block has an additional advantage. The older a block becomes, the more likely that it is secure, since a hacker would have to modify all subsequent blocks in order for the block chain to remain viable.

A Transaction

A bitcoin transaction specifies that a certain number of bitcoins (or more likely, microbitcoins –µbitcoins, currently worth about USD 0.06 cents) be transferred from one party to another. The transaction is secured via a digital signature using public key encryption. The sender encrypts the transaction with its private key and sends it to the public key of the receiver. The receiver decrypts the transaction via its private key to get the encrypted transaction sent by the sender, and then further decrypts the transaction with the sender's public key.

The transaction is sent from the sender to the receiver via the bitcoin peer-to-peer network, which also ensures that all nodes in the network receive the transaction.

The amount sent to the receiver may be less than the receiver is specified to get. The difference is a transaction fee that is given to the successful miner.

The transaction is only a proposed transaction until it has been included in a transaction block that has been added to the block chain.

A Transaction Block

A transaction block is a group of transactions that are protected by a hash. The SHA-256 hash algorithm is used, which creates a 256-bit hash value to be appended to the group of transactions. The group of transactions yields only one value for the hash. It is virtually impossible (without immense computing power) to determine the transactions from the hash.

A miner has access to every transaction generated, since all transactions are sent to all bitcoin nodes. In addition, he knows which transactions have already made it to the block chain. He selects a group of transactions that have not yet been added to the block chain, typically starting with the earliest transaction that is available. A typical number of transactions in a block is about four hundred, though there is no requirement for any number of transactions to be included. Typical transaction size ranges from 200 to 1,000 bytes.[3]

A miner can skip transactions if he wants. For instance, he can skip transactions that do not pay a transaction fee. These transactions will be picked up in later blocks by other miners. Therefore, there is an incentive for the parties to a transaction to pay an incentive fee, since their transaction is not recognized by the bitcoin network until it has been added to the block chain.

A key to the transaction block is the header that is created for it. The header includes:

- Version - The software version number used to create the block.
- Prev_block -The hash value of the previous block to which this block will be appended.
- Merkle_root - The root of a Merkle tree containing a hash of all of the transactions.

[3] Bitcoin Block Explorer
http://blockexplorer.com/

- Timestamp - A time stamp recording when the block was created.
- Bits - The difficulty target for this block.
- Nounce – The nounce used to create this block (described later).

It is only the header that is hashed by the block hash. Thus, the block may include any number of transactions; and the time to calculate the hash does not depend upon the number of transactions in the block. Therefore, a miner has no incentive to limit the number of transactions in a block, though the block size is limited to one megabyte.

Merkle Tree

The transactions are organized as a Merkle tree when they are added to the block. A Merkle tree separates the transactions into "leaves" and creates a hash for each leaf. The leaf hashes are then aggregated and hashed. These hashes are then aggregated into another hash until the root of the Merkle tree is reached. This root hash is stored in the header.

Submitting a Block

When a miner has successfully found a hash for his block, he submits it to the network. It is sent to every node in the network, which must verify that the hash is correct. If the majority of the nodes in the network agree that the block is correct, it is added to the block chain. At this point, all miner nodes start working on the next set of transactions.

In the unlikely event that two miners arrive at correct solutions at the same time, the block chain will fork with each of these blocks. However, the bitcoins network has procedures for correcting these forks and leaving the block chain as one contiguous chain.

As mentioned earlier, a transaction is not recognized until it has been included in a block appended to the block chain. Until this time, it is a proposed transaction. In fact, many participants wait until other blocks have been added to ensure that this block has not been hacked (a hacker would have to hack all subsequent blocks before he could hack a block). It is typical to wait until the block is followed by at least five other blocks before the transaction is recognized.

Difficulty

So why is mining so difficult? It is because the network imposes a level of difficulty on the calculation of the block hash. Specifically, the network requires that a certain number of initial bits in the 256-bit hash be zero. The more zeros, the more difficult it is to find a hash value that complies with the difficulty level.

The rate at which blocks are generated depends upon two factors – the level of difficulty and the combined computing power of all of the miners. As time goes on, the number of miners and the computing power they have available to them continues to increase, increasing the rate of block creation.

The bitcoin network strives to keep the block generation constant. It does this by adjusting the level of difficulty (the number of leading zeroes in the hash). Specifically, it attempts to set the block generation rate to 2,016 blocks per two-week period. This is equivalent to one block every ten minutes. Every two weeks, the bitcoin network determines the number of blocks that have been generated in the previous two weeks. If more than 2,016 blocks have been generated, it increases the level of difficulty by increasing the number of required leading zeros in the hash. If less than this number of blocks has been generated, it decreases the difficulty (the level of difficulty is almost always increased).

If a miner calculates an illegitimate hash, he must try again. In order to do this, the miner must change the data that is being hashed. Remember that it is only the block header that is being hashed. The first step is to change the *nounce* stored in the header. The nounce is a 32-bit number that can be changed for each hash attempt (perhaps by incrementing it). However, the 32-bit nounce with about 4×10^9 combinations

has fallen a long way behind the number of tries that it takes to currently calculate a suitable hash. Therefore, something else must change in the header once all nounce values have been tried and failed. This is typically done by restructuring the Merkle tree so that the Merkle root in the header changes. The nounce values are then run through again. This procedure continues until a valid hash is found or until another miner has completed a block to add to the block chain. At this time, all miners begin the hashing process over, using the remaining transactions that have yet to be added to the block chain.

How complex is this calculation today? It is estimated that the total hash computing capacity in the bitcoin network is 50,000 gigahashes/second (Ghash/s), or 5×10^{16} hashes per second.[4] Since a new block is found every 10 minutes (600 seconds), the calculation of a hash currently requires about $600 \times 5 \times 10^{16} = 3 \times 10^{19}$ attempted hash calculations. Of course, this is across the entire bitcoin network, and the same hash attempt is made by many miner nodes before a solution is found. It is not possible to determine the number of miner nodes in the bitcoin network.

In terms of estimating the difficulty for a single mining node, the current difficulty as of this writing is that the first sixteen hexadecimal digits must be zero.[5] Thus, there are $16^{16} = 2 \times 10^{19}$ hash values that do not meet this criterion. On the average, half of these hashes must be calculated before a miner node finds a solution. This is about 10^{19} hash calculations. Even with a processing power of a terahash/sec. (Thash/s), it would take $10^{19}/10^{15} = 10{,}000$ seconds to arrive at a legitimate hash value for a block of transactions. This is 2.8 hours, much longer than the average ten minutes that it will take some miner in the network to randomly find a solution.

Computing Power

How can a miner gather enough computing power to effectively mine bitcoin transactions? In the early days, normal CPUs (desktops and laptops) were used. They were able to achieve about two megahash/sec (Mhash/s). per core.[6]

It was then discovered that Graphics Processing Units (GPUs) used in PCs were much more efficient than CPUs. GPUs could achieve one hundred Mhash/s of hashing speed.

Soon, even this power became miniscule compared to the size of the task. ASICs were designed to provide extraordinary hashing power. An ASIC (application-specific integrated circuit) is a special chip designed specifically for bitcoin mining. The processing power that ASICs bring to the network has made them extremely popular among miners and mining pools. Today's ASICs can provide hash rates of hundreds of thousands of Mhash/s, and some are being released that provide a few million Mhash/s (Thash/s).

Many ASICs can be grouped together, and large groups used by mining pools can achieve hundreds of Thash/s of hashing power.

The more powerful ASIC devices cost several thousand dollars each, and each consumes several kilowatts of power.

Decreasing Rewards for Mining

The bitcoin network is designed to create a steady stream of bitcoins, but this stream is ultimately to come to an end. In 2017, the 25-bitcoin block reward will be cut in half. Every four years after that, it will be cut in half again. In 2040, the bitcoin reward will be terminated and there will be no more bitcoins created. However, miners will still earn their transaction fees.

---

[4] Bitcoin Wisdom
https://bitcoinwisdom.com/bitcoin/difficulty

[5] Block Explorer
http://blockexplorer.com/q/hextarget

[6] Mining hardware comparison, Bitcoin Wiki
https://en.bitcoin.it/wiki/Mining_Hardware_Comparison

There currently are about 12 million bitcoins in circulation with a value of about $7 billion USD. The ultimate bitcoin limit in 2040 is estimated to be about 21 million bitcoins.

The Future of Bitcoins

There are several interesting observations to be made about bitcoins.

Reduction in the Number of Miners

As the bitcoin reward diminishes over the next few years and the difficulty level is raised, it is expected that miners will start to drop out of the network. This means that the difficulty level will eventually go down unless the increase in per-miner compute capacity increases.

Value of a Bitcoin

There is a limit to the number of bitcoins that will be generated, currently estimated at 21 million bitcoins. At $1,000 per bitcoin, this is a total value of USD 21 billion dollars. This amount is trivial compared to the total currency value of most nations. If bitcoins really take off, there will be millions of participants worldwide. Twenty-one billion dollars is not nearly enough to handle the level of transactions that this group will generate. Therefore, many predict that the value of bitcoins will increase by a large factor. Of course, if bitcoins don't make it into the mainstream, they may ultimately be worth nothing.

Transaction Rate

Currently, the bitcoin transaction rate is limited to one block every ten minutes. At an average of 400 transactions per block, this is a rate of 40 transactions per minute. This pales in comparison to the thousands of transactions per second that Visa and other payment processors handle. It is not clear how bitcoins is going to modify its algorithms to handle a transaction rate that is orders of magnitude greater than the current limit.

Higher transaction rates can be handled, for instance, by increasing the block generation rate. To be able to handle ten thousand transactions per second, the block generation rate would have to be increased from one block every ten minutes to 25 blocks per second.

Summary

Bitcoins are generating much interest and a growing use in today's society, especially among the younger, more tech-savvy set. They are poised to either become a major currency for international trades, or they are set to collapse. Only time will tell.

However, one thing is clear. Bitcoin mining is for the wealthy who are prepared to take on major risk.

Acknowledgement

It you are interested in exploring bitcoins further, a useful reference is the Bitcoin Wiki at https://en.bitcoin.it/wiki.