Mastering Bitcoin Ch.10

Mining and Consensus

Kun-jung Wu

Department of Economics
National Taiwan University

R06323008@ntu.edu.tw

May 7, 2018

Overview

Introduction

Mining

Mining secures the bitcoin system and enables the emergence of network-wide consensus without a central authority.

Key Points

- Proof-of-Work
- Bitcoin Creation and Transaction Fees
- Block Creation Speed
- Mining Difficulty
- Hash Rate

Introduction

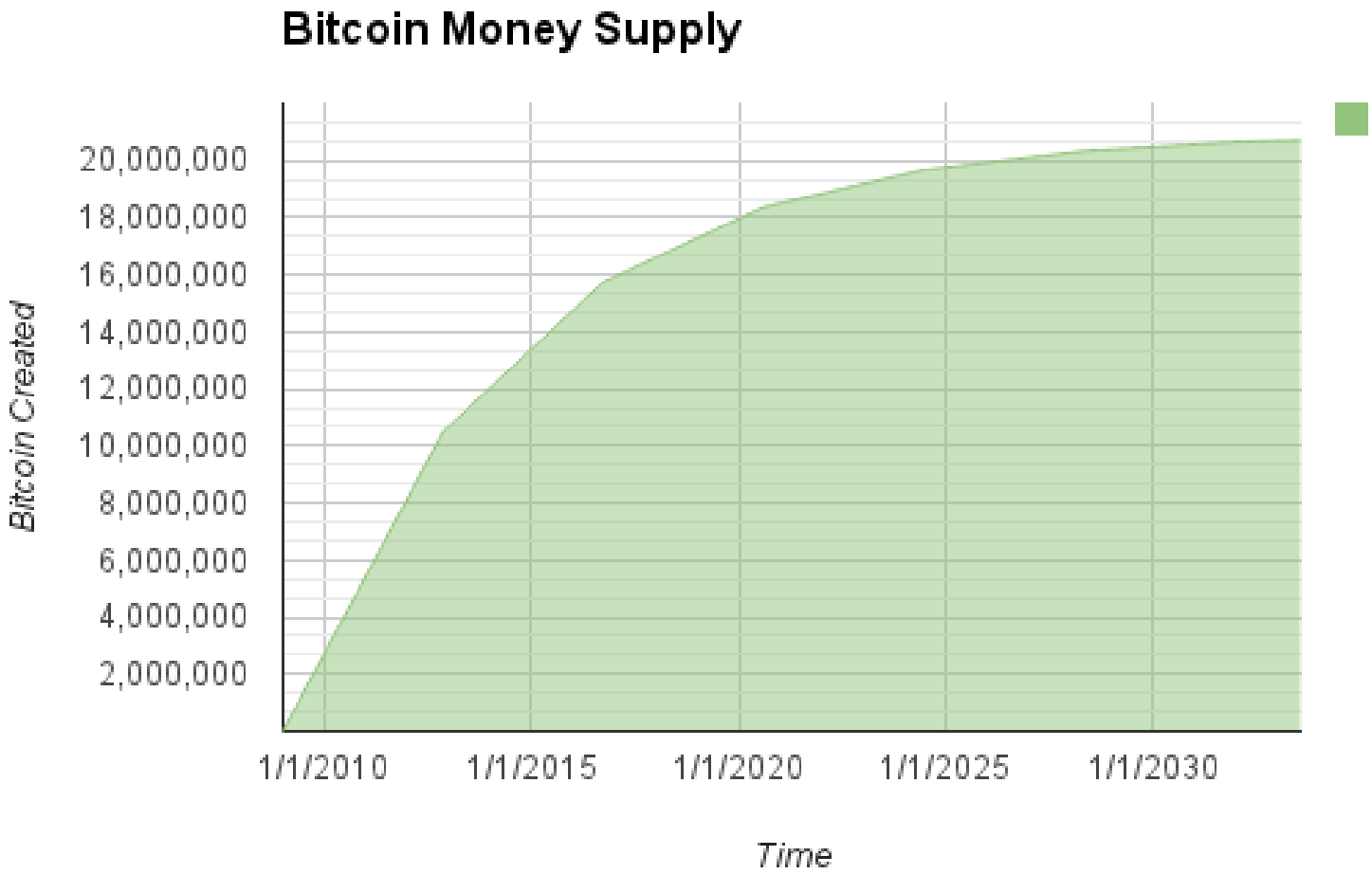
Bitcoin Economics and Currency Creation

- Each block generated on average every 10 minutes
- Every 210,000 blocks, approx. every four years, decreases 50%.
- First Four years creates 50 bitcoin.
- Total of 21 million bitcoin ever created in 2140.
- impose to zero after 64 halving.

Deflationary Money

- In a period of rapid deflation, people tend to hoard money instead of spending it.
- Inflation causes a slow but inevitable debasement of currency, resulting in a form of hidden taxation that punishes savers in order to bail out debtors.

Introduction



Decentralized Consensus

Emergent Consensus is an emergent artifact of the asynchronous interaction of thousands of independent nodes.

Four Independent Processes of every nodes

- Independent verification of each transaction, by every full node.
- Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a Proof-of-Work algorithm
- Independent verification of the new blocks by every node and assembly into a chain.
- Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work

Decentralized Consensus

Independent Verification of Transactions

- Before forwarding transactions to its neighbors, every bitcoin node that receives a transaction will first verify the transaction.
- Only valid transaction can be propagated.
- By independently verifying each transaction as it is received and before propagating it, every node builds a pool of valid (but unconfirmed) transactions known as the transaction pool, memory pool, or mempool.

Decentralized Consensus

Mining Nodes

- is listening for new blocks, propagated on the network.
- The competition among miners effectively ends with the propagation of a new block that acts as an announcement of a winner.
- owever, the end of one round of a competition is also the beginning of the next round.

Aggregating Transactions into Blocks

- Mining nodes keep track of new block and update the mempool.
- Mining nodes constructs candidate block every new round, collecting some transactions from the mempool.

Decentralized Consensus


```
{
    "hash" : "000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
    "confirmations" : 35561,
    "size" : 218629,
    "height" : 277316,
    "version" : 2,
    "merkleroot" : "c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e",
    "tx" : [
        "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
        "b268b45c59b39d759614757718b9918caf0ba9d97c56f3b91956ff877c503fbe",

        ... 417 more transactions ...

      ],
    "time" : 1388185914,
    "nonce" : 924591752,
    "bits" : "1903a30c",
    "difficulty" : 1180923195.25802612,
    "chainwork" : "0000000000000000000000000000000000000000000000934695e92aaf53afa1a",
    "previousblockhash" : "000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569"
}
```

Decentralized Consensus

Coinbase Transaction

- is the first and special transaction in any block
- Block reward plus transaction fee
- Output to miner's address

Coinsbase Transaction's vin

```
{
    "hex" : "010000000100000000000000000000000000000000 ......
    "txid" : "d5ada064c6417ca25c4308bd158c34b77e1c0eca ......
    "version" : 1,
    "locktime" : 0,
    "vin" : [
        {
            "coinbase" : "03443b0403858402062f503253482f",
            (ScriptSig in normal transaction)
            "sequence" : 4294967295
        }
    ],
```

Coinbase Data

- Coinbase transactions do not have an unlocking script
- ScriptSig is replaced by coinbase date, miner can write anything.
- See what Satoshi wrote in the genesis block.

Table 2. The structure of a coinbase transaction input

Size	Field	Description
32 bytes	Transaction Hash	All bits are zero: Not a transaction hash reference
4 bytes	Output Index	All bits are ones: 0xFFFFFFFF
1–9 bytes (VarInt)	Coinbase Data Size	Length of the coinbase data, from 2 to 100 bytes
Variable	Coinbase Data	Arbitrary data used for extra nonce and mining tags. In v2 blocks; must begin with block height
4 bytes	Sequence Number	Set to 0xFFFFFFFF

Constructing the Block Header

Table 3. The structure of the block header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Target	The Proof-of-Work algorithm target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Decentralized Consensus

Voting the mainchain

By selecting the specific parent block, indicated by the Previous Block Hash field in the candidate block header, Miner is committing his mining power to extending the chain that ends in that specific block. In essence, this is how miner "votes" with his mining power for the longest-difficulty valid chain.

Mining the Block

Proof-of-Work Algorithm

the process of hashing the block header repeatedly, changing one parameter, until the resulting hash matches a specific target.

- A hash algorithm takes an arbitrary-length data input and produces a fixed-length deterministic result
- can be easily calculated and verified by anyone implementing the same hash algorithm
- Nonce is used to vary the output of a cryptographic function
- Target is the specific challenge level a valid hash is below than.

Target Representation

The formula to calculate the difficulty target from this representation is:

- target = coefficient * $2^{(8*(\text{exponent}-3))}$

Using that formula, and the difficulty bits value 0x1903a30c, we get:

- target = 0x03a30c * $2^{0x08*(0x19-0x03)}$
- => target = 0x03a30c * $2^{(0x08*0x16)}$
- => target = 0x03a30c * 2^{0xB0}

which in decimal is:

- => target = 238,348 * 2^{176}
- => target = 22,829,202,948,393,929,850,749,706,076,701,368,331,072,452,018,388,575,715,328

switching back to hexadecimal:

- => target = 0x0000000000000003A30C000000000000000000000000000000000000000000

Mining the Block

Retargeting to Adjust Difficulty

Coinsbase Transaction's vin

```
New Target = Old Target * (Actual Time of Last 2016 Blocks / 20160)
```

- Independent of number of transactions
- Preventing takeover attack
- Nonce is used to vary the output of a cryptographic function
- Target is the specific challenge level a valid hash is below than.

Mining the Block

Successfully Mining the block

- the first miner solved the PoW propagates its block to all the peers on the network.
- As mining nodes receive and validate the block, they abandon their efforts to find a block at the same height and immediately start computing the next block in the chain, using Jings block as the "parent." By building on top of Jings newly discovered block, the other miners are essentially "voting" with their mining power and endorsing Jings block and the chain it extends.

The End