Fees in Bitcoin

Understanding fees, the why, and how to practice your right to choose.

October 31, 2008: The Whitepaper is published

- Fees were mentioned three times:
  - The incentive can also be funded with transaction **fees**.
  - If the output value of a transaction is less than its input value, the difference is a transaction **fee** that is added to the incentive value of the block containing the transaction.
  - Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction **fees** and be completely inflation free.
- No mention of fee estimation, block size limitations or any sort of fee market.

November 10, 2008: “it cannot be made to work”

James A. Donald wrote:

> Furthermore, it cannot be made to work, as in the proposed system the work of tracking who owns what coins is paid for by seigniorage, which requires inflation.

If you're having trouble with the inflation issue, it's easy to tweak it for transaction fees instead. It's as simple as this: let the output value from any transaction be 1 cent less than the input value. Either the client software automatically writes transactions for 1 cent more than the intended payment value, or it could come out of the payee's side. The incentive value when a node finds a proof-of-work for a block could be the total of the fees in the block.

Satoshi Nakamoto

Source: https://satoshi.nakamotoinstitute.org/emails/cryptography/9/

February 10, 2010: What's with this odd generation?

Theymos wrote:

> `I thought BitCoin only generated in 50 coin increments, but I got 50.44 here.`

The average transaction, and anything up to 500 times bigger than average, is free.

It's only when you're sending a really huge transaction that the transaction fee ever comes into play, and even then it only works out to something like 0.002% of the amount. It's not money sucked out of the system, it just goes to other nodes. If you're sad about paying the fee, you could always turn the tables and run a node yourself and maybe someday rake in a 0.44 fee yourself.

Source: https://bitcointalk.org/index.php?topic=48

September 7, 2010: at least some free transactions.

> I propose that tx fee be required for every transaction after X datetime (where X is a few months in the future).
>
> ---
>
> That will probably happen spontaneously if someone make a client (or add the option to the current one) that allows the user to charge transaction fees for the blocks it generates.

Another option is to reduce the number of free transactions allowed per block before transaction fees are required. Nodes only take so many KB of free transactions per block before they start requiring at least 0.01 transaction fee.

The threshold should probably be lower than it currently is.

I don't think the threshold should ever be 0. We should always allow at least some free transactions.

https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/213/#5

Continued: UTXO Consolidation

If you bought your bitcoins, they'll be denominated in larger transactions and won't be anywhere near the fee limit, unless you bought them in several hundred separate transactions. Even if you do reach the fee level, you only have to pay it once to bundle your little transactions together.

https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/213/#10

Miners and relays

Miners are those who trade their energy usage for bitcoin.

- If a miner expects that they can earn more money than the cost of their energy bill, then this is a good business idea.
- Today, a miner might base their suitability on the block rewards, but in the future, they will need to consider the transaction fees more.

Relays are the nodes we run.

- They transmit transactions around like a gossip network. Helping each other get their transactions to miners.
- They validate blocks, keep copies of the blockchain and distribute trust.

Bitcoin fees 101: In a nutshell

- Miners choose which transactions they wish to mine and how many free transactions they wish to include.
- Users choose whether to pay a fee and how much to pay.
- Each transaction takes up space in a single block, some more than others.
- A fee market developed, creating a “price” to mine transactions measured in sats/vbyte.
- Fee estimation services and tools help us determine an appropriate fee to use.
- CPFP and RBF became well understood, and later supported strategies for re-prioritising your transactions.
- Most of the relay network ignores fees under 1sat/vbyte today

Transactions, coins, and size

I hereby declare that the following coins:

- xy3abzg9304dksmksdmksdm... (of size 1 BTC)
- nfue93jm39ifm94f48gn844... (of size 0.5 BTC)
- 9fj39iiz920k9afgb8331zz... (of size 3 BTC)

be redistributed into the following addresses:

- bc1qxyzabc...: 4 BTC
- bc1p93fnks...: 0.4 BTC

And here are my signatures:

- 8a0uynm3n89ang73n8pla1334...
- j983jg3hg5s44sd5225ddf2nv...
- 980m5qvz3qzngm05nqz3cbygf...

Any remainder may be claimed by whoever mines this transaction. (0.1BTC)

Quick history about addresses

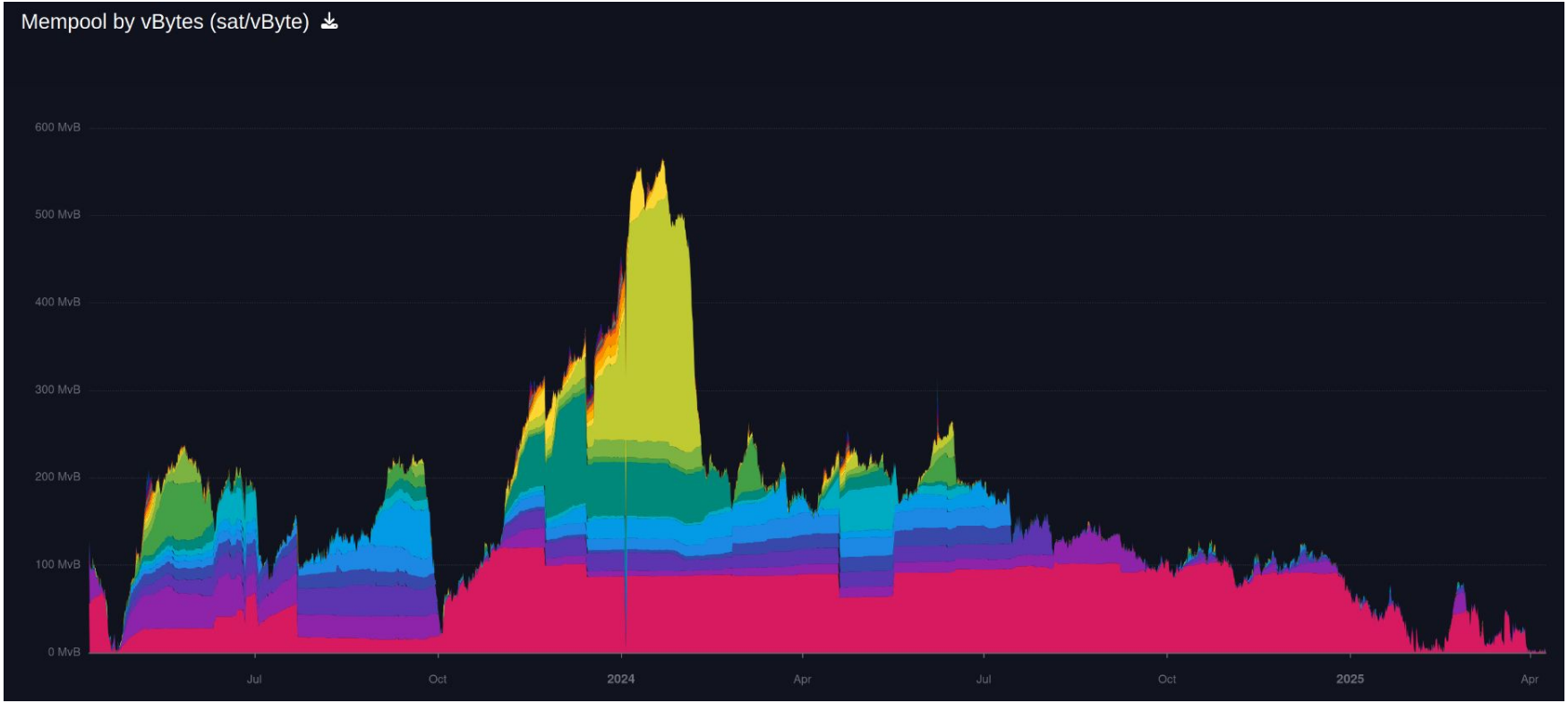
1. P2PK: Pay to public key
   a. 4104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac
   b. Was really pay to “locking script”.
   c. P2MS was a term used for a locking script that used a quorum public keys.
2. P2PKH: Technically first ever address. (hash + prefix is the address)
   a. 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
   b. 76a91455ae51684c43435da751ac8d2173b2652eb6410588ac
   c. Hashes reduce the size of the sending transaction. Saves on fees!
3. P2SH:
   a. 3CK4fEwbMP7heJarmU4eqA3sMbVJyEnU3V
   b. Huge savings for multi-sig and more complex wallets.

Segwit: More savings!

Segregated witness (signatures).

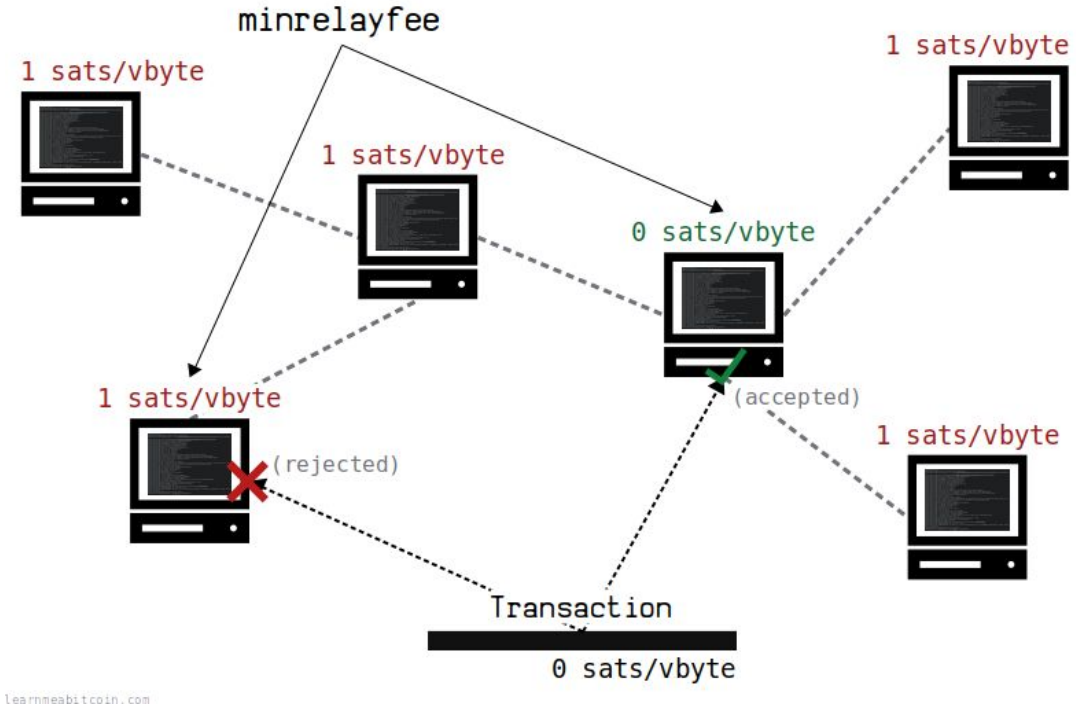
- bc1qryhgpmfv03qjhhp2dj8nw8g4ewg08jzmgy3cyx
- Designed to technically increase the size of blocks without kicking old software off the network.
- Fees went from sats/byte to sats/vbyte
- Signatures were given a “discount”
- Transaction size was now a formula:
  - `(Transaction data) + (Witness data * 1 / 4)`
- Blocks could be UPTO ~4MB now (1 vMB)
- Reduced the receiver’s future transaction size
- (also taproot): bc1p

Congestion


Mempool by vBytes (sat/vByte)
600 MvB
500 MvB
400 MvB
300 MvB
200 MvB
100 MvB
0 MvB
Jul
Oct
2024
Apr
Jul
Oct
2025
Apr

Congestion

Spam caused our 1 sat/vbyte policy.



Custodian fees 😈

- Many participants use exchanges to buy Bitcoin
- Exchanges often charge a “service fee” for withdrawals
- Some also (*ahem* Coinbase) charge a “miners fee”
- Exchanges batch transactions to create more efficient transactions (reduce overheads)
- Still, they OVERCHARGE their users, making a profit here too

Why is Bitcoin so expensive?! I paid £3.00 for a £5.00 transaction.

Dunno, I paid 45p. Wait... Coinbase only paid £2.00 for it and that included other people's transactions too. 😂

Merchants and fees

- Merchants often can’t afford to learn new technology until it becomes necessary.
- Some stepped forward and pioneered accepting bitcoin, but congestion made it uneconomical.
- Payment processors are familiar, but they charge fees.
- Payment processors offer features such as reporting tools and currency conversion.
- Merchants want consistency in order to ensure their profits cover their fees.

Lightning ⚡: The solution?

- Lightning wallets can be cheaper, **especially** during congestion.
- Lightning wallets are fast, but can be less user friendly than on-chain.
  - Liquidity, Channels, Channel Reserve, Swap fees, etc.
- Fees are proportionate to amount, there are no “coins” here.
- Fees are only LESS unpredictable.
- Very useful for micropayments.
  - Streaming, zaps, paywalls, etc.
- Channels are expensive to create.
- Bitcoin doesn’t scale to 8 Billion channels. (yet?)

Useful tips

1. Consider the cost of withdrawal as part of the cost of purchase.
2. Use exchanges that let you withdraw over Lightning.
3. Use fee estimators before making expensive transactions.
    a. https://mempool.space/, many wallets also provide a fee to confirmation time estimate.
4. Consider lowballing the fee if you can afford to (time).
5. Wallets often have the ability to let you set your own custom fee.
6. Don’t spend from exchanges, only withdraw.
7. Transactions don’t need to confirm to be spent*

Useful tips

1. Fees are influenced by the receiver:
    a. if sending to yourself, you could wait months, or years for the transaction to settle. It doesn't matter.
    b. If sending to a merchant, they need to know you have little to no time to defraud them. They will influence you to pay a higher fee for their sake.
2. Have a lightning wallet handy.
3. Pay on-chain if its cheaper and available.

Preparations help

- GET YOUR COINS OFF EXCHANGES
- Study Bitcoin (more)
- Practice!

- Consolidate small coins during low fee moments
- Label your transactions (coin selection/coin control)
- Keep cold and hot funds
- Have a lightning wallet handy

Thank you.