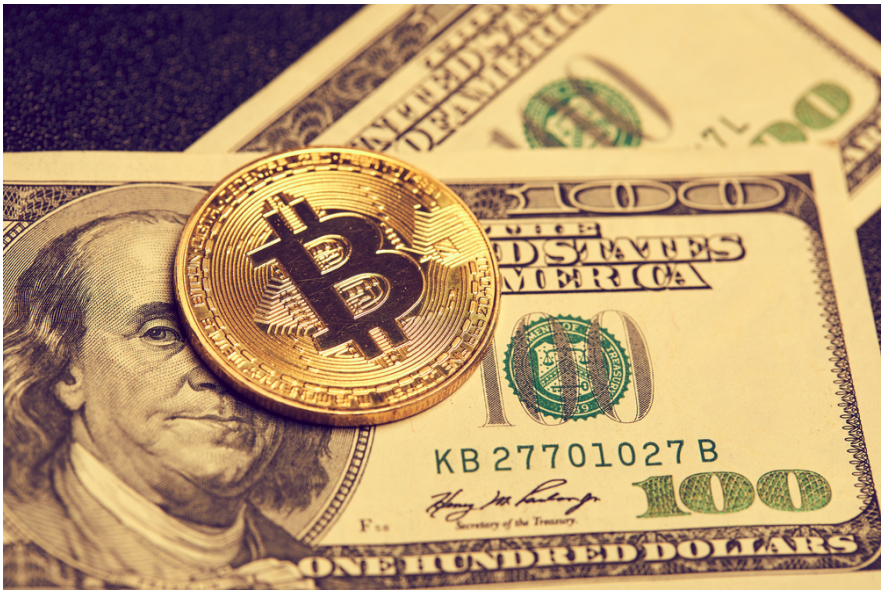
Opinion | 13 October 2017

Why Bitcoin transactions are more expensive than you think

Bitcoins are sometimes marketed as a low-cost alternative to traditional payments but they're not as cheap as you'd think. What's going on?



Confronting the Mad Max Problem

A core element of cryptocurrency is the lack of a central authority. Nodes on the network verify transactions which are rewarded with transaction fees and in the case of bitcoins, newly minted bitcoins go with each verified block of transaction. From the verifying nodes' perspective, these new bitcoins are mined. Hence they are referred to as "miners".

As explained in our report, one of the central issues of cryptocurrencies is trust. How can the rest of the cryptocurrency network trust the verification work done by miners? I'd like to call this the Mad Max problem. In a Mad Max world, with no law enforcement, your base assumption has to be that nobody can be trusted. How to do transactions take place in such a world without anyone getting robbed?

Replacing trust with raw computing power

For example, malevolent miners could verify blocks of fraudulent transactions in which bitcoin is

taken from victims and sent to their own wallets, or where the same bitcoin is spent several times. How do network nodes know that the blocks presented by miners are truly valid?

> *Bitcoin is a Mad Max world, with no law enforcement, where nobody can be trusted*

The innovative concept applied by bitcoin is proof-of-work (POW) system. By making sure that verifying transactions is a costly business, the integrity of the network can be preserved as long as benevolent nodes control a majority of computing power. Together, they will dominate the verification (mining) process. Read Satoshi Nakamoto's original white paper for a more detailed explanation here.

To make the verification (mining) costly, the verification algorithm requires a lot of processing power and thus electricity. In fact, the website Digiconomist has constructed a Bitcoin Energy Consumption Index, estimating bitcoin energy consumption. And the results are sobering. At the time of writing, verifying one transaction on the bitcoin blockchain consumes about 200kWh.

Current Bitcoin Energy Consumption Index

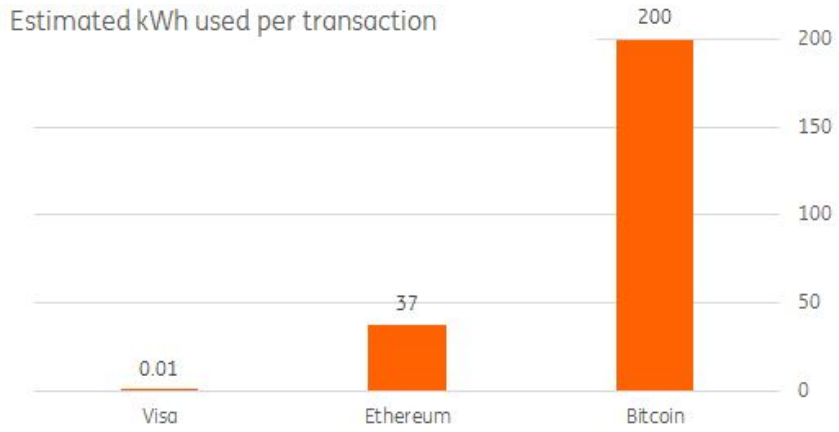
200kWh Estimated electricity cost per bitcoin transaction

Privatising gains, socialising losses?

This number needs some context. 200kWh is enough to run over 200 washing cycles. In fact, it's enough to run my entire home over four weeks, which consumes about 45 kWh per week costing €39 of electricity (at current Dutch consumer prices).

Let's put this another way. To process your bitcoin transaction, which might not cost you anything, 200kWh of electricity is used. Powering the entire Bitcoin blockchain currently, costs over 2200MW which is more than what the biggest Dutch energy plant, the Eemshavencentrale requires.

This might make you wonder why you're not charged €39 for the electricity used? The answer is simply the block reward. The miner whose block is selected to be added to the chain currently receives BTC12. At current BTC prices, the block reward clearly and vastly outweighs electricity costs. Mining is a no-brainer for individual miners, but the benefit to society at large is much less obvious.



Source: Digiconomist, ING

Looking for more sustainable alternatives

Bitcoin's energy costs stand in stark contrast to payment systems that have the luxury of working with trusted counterparties. E.g. Visa takes about 0.01kWh (10Wh) per transaction which is 20000 times less energy.

But blockchain technology could be used in a setting with trusted nodes as well, for example between banks. And this would abolish the need for expensive proof of work.

But operating in a setting without trusted authorities was one of the core goals of the original bitcoin project. At the same time, the cryptocurrency community is aware of the sheer energy consumption issue. Therefore, it is looking for alternatives solutions to the Mad Max problem.

One alternative may be Proof of Stake. Miners are not asked to show they put in work (computing power) in validating but to commit valuable resources beforehand, indicating they have a stake in the proper outcome. For example, miners may have to put an amount of cryptocurrency in escrow which is only released if no fraud is detected, otherwise forfeited.

That sounds like a smart idea. However, it implies that only those wealthy enough to be able to put resources in escrow can join the mining process. This creates a plutocracy, which sits uncomfortably with cryptocurrency's anarchistic and libertarian roots.

My conclusion is that finding a sustainable and fair solution to the Mad Max Problem is one of the biggest challenges for the cryptocurrency community today.