13 October 2017

Why Bitcoin transactions are more expensive than you think

In this article

- Confronting the Mad Max Problem
- Replacing trust with raw computing power
- Privatising gains, socialising losses?
- Looking for more sustainable alternatives
- One alternative may be Proof of Stake. Miners are not asked to...

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?

Read our 'Riding the Cryptocoaster' report here in full

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

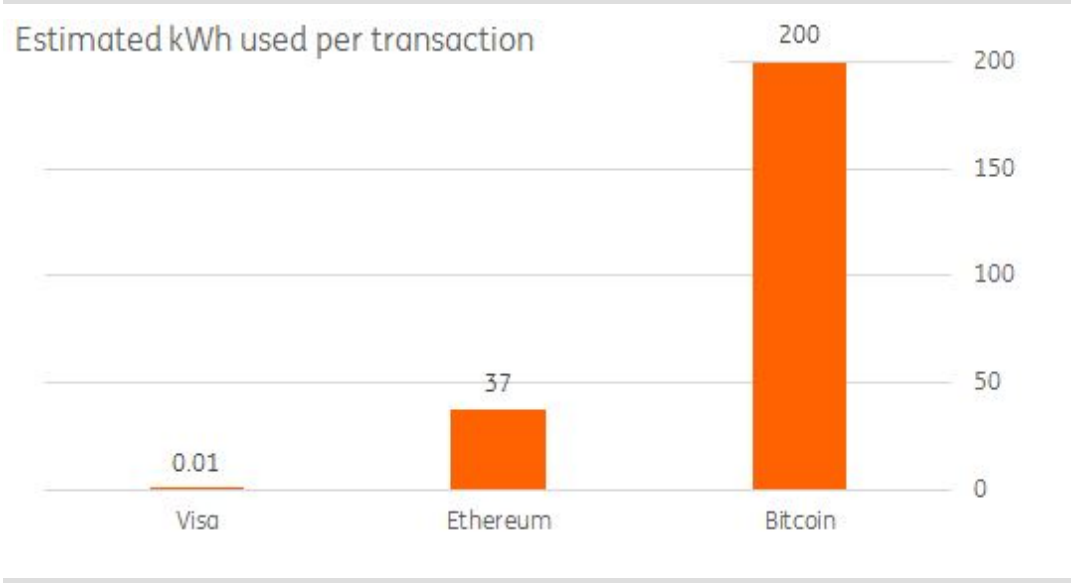
200kWh **Estimated electricity cost per bitcoin transaction**

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.



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.

Teunis Brosens
+31 20 563 6167
teunis.brosens@ing.nl

Disclaimer

This publication has been prepared by ING (being the Wholesale Banking business of ING Bank N.V. and certain subsidiary companies) solely for information purposes. It is not an investment recommendation and it is not investment, legal or tax advice or an offer or solicitation to purchase or sell any financial instrument. Reasonable care has been taken to ensure that this publication is not untrue or misleading when published, but ING does not represent that it is accurate or complete. ING does not accept any liability for any direct, indirect or consequential loss arising from any use of this publication. Unless otherwise stated, any views, forecasts, or estimates are solely those of the author(s), as of this date and are subject to change without notice.

The distribution of this publication may be restricted by law or regulation in different jurisdictions and persons into whose possession this publication comes should inform themselves about, and observe, such restrictions.

The producing legal entity ING Bank N.V. is authorised by the Dutch Central Bank and supervised by the European Central Bank (ECB), the Dutch Central Bank and the Dutch Authority for the Financial Markets (AFM). ING Bank N.V. is incorporated in the Netherlands (Trade Register no. 33031431 Amsterdam). In the United Kingdom this information is approved and/or communicated by ING Bank N.V., London Branch. ING Bank N.V., London Branch is subject to limited regulation by the Financial Conduct Authority (FCA). ING Bank N.V., London branch is registered in England (Registration number BR000341) at 8-10 Moorgate, London EC2 6DA.

For US Investors: Any person wishing to discuss this report or effect transactions in any security discussed herein should contact ING Financial Markets LLC, which is a member of the NYSE, FINRA and SIPC and part of ING, and which has accepted responsibility for the distribution of this report in the United States under applicable requirements.