Could Bitcoin Transactions Be 100x Faster?

Nicolas T. Courtois[1], Pinar Emirdag[2] and Daniel A. Nagy[3]

[1]University College London, UK; [2]Independent market structure professional, London, UK,
[3]Eötvös Loránd University University, Budapest, Hungary

N.Courtois@cs.ucl.ac.uk, Pinar.Emirdag@alumni.brown.edu, Nagy.Da@gmail.com

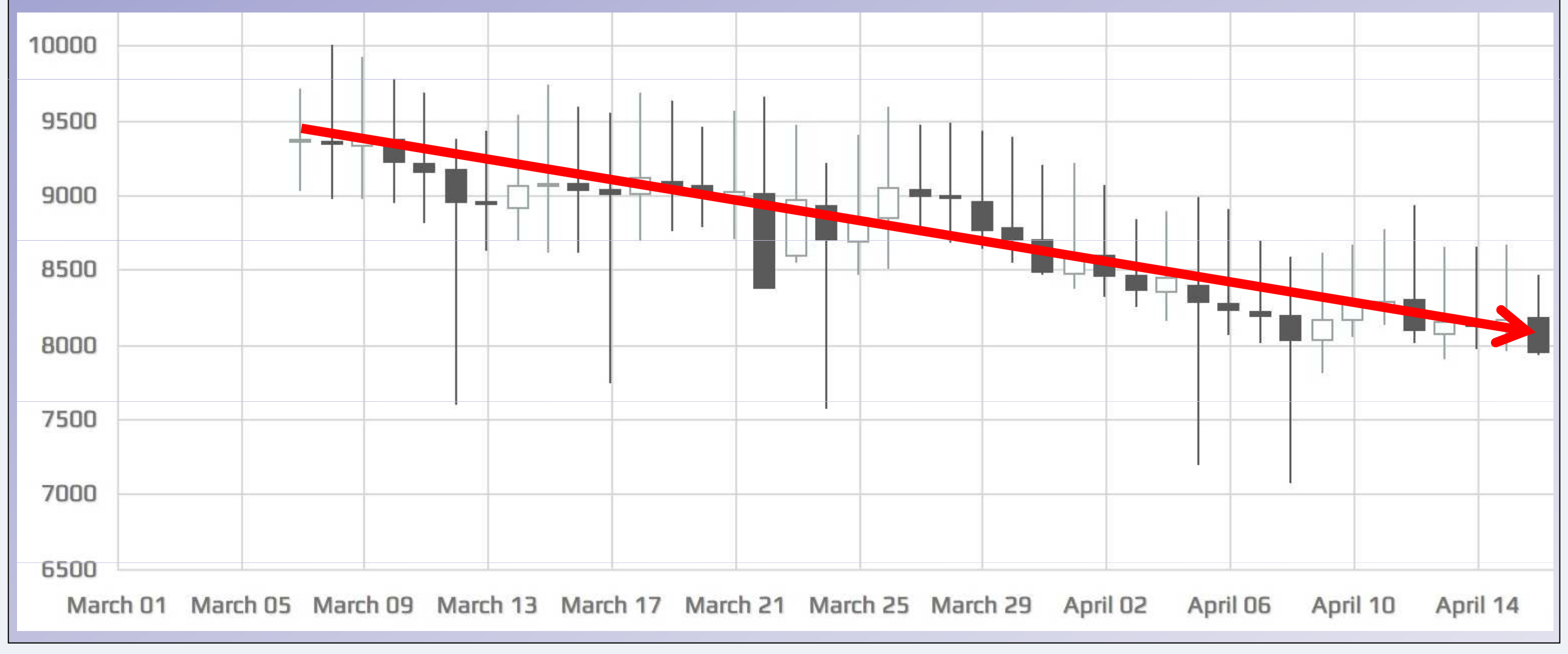
Bitcoin

Bitcoin is decentralized peer to peer currency and payment system. The security of bitcoin greatly depends on a **distributed hashing infrastructure**. Some bitcoin nodes have very substantial computing power and they are policing the network based on their self-interest: the are allowed to produce new coins and uses/sell them. An attacker needs to manipulate network nodes in control of a substantial fraction of the computing power. The current bitcoin is NOT perfect and NOT sufficiently decentralized but it is good enough to be used in practice. Current market cap of bitcoin is about 6 billions of dollars.

Satoshi vs. Reality. The inventor of bitcoin Satoshi Nakamoto [a pseudonym] was a brilliant visionary scientist and engineer.
However he did NOT predict everything (cf. 1,2,3,4 below and 5. on the right).

1. Miners vs. P2P Incentives

Problem 1. In Section 5 of his paper he postulated that each peer-to-peer network node should be mining. In reality he forgot to create monetary incentives for people to run bitcoin nodes and their number (some 5,000) is MUCH LOWER than the number of bitcoin miners (maybe 100,000). Bitcoin peer network is in steady decline and at dangerously low levels!



2. The 51% Attack Risks

Problem 2. 51% attacks assume a **dishonest majority** in terms of hash power contributed. The actual risks from 51% attacks are VERY HEAVILY underestimated in the bitcoin community. For example Satoshi wrote:

"If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules[…] than to undermine the system and the validity of his own wealth.“

All this is **rather mistaken** if we look at current bitcoin. Satoshi failed to see that key problem is the control/abuse and NOT ownership of hash power for the purpose of mining blocks, and this can be **a lot easier**:

- The attacker does not have to be wealthy or powerful.
- Man in the middle attackers just need to hack VERY FEW pool manager servers and can abuse the other people's miners.
- In typical mining scenarios the attacker does NOT control the money from mining: the whole process of mining requires exclusively the public keys and he does NOT have the private keys. The honest option does NOT exist.

3. Longest Chain Rule

Problem 3. Longest Chain Rule: we are the first researchers to criticise it. "One of the fundamental mistakes of bitcoin is that they use 'the Longest Chain Rule, to decide simultaneously which block gets accepted and which transactions get accepted" (from interview of Dr Courtois to FT, 08/2014). Fast transaction are at the mercy of (slow) blocks. Poor network neutrality!

4. Monetary Policy

Problem 4. Monetary policy. Problems are exacerbated by reward halving. As time passes less and less coins are given to miners with sudden jumps. Then either fees must increase, or the hash rate will decrease and bitcoin will become MORE vulnerable to double spending attacks in the future.

Decentralized Markets

In theory bitcoin has nothing to do with stock markets? On second thoughts:

- Markets are decentralized, especially in the United States.
- Units/resources are fungible and in limited (fixed) supply.
- Financial institutions increasingly just do NOT trust each other, and they also want to build co-operative electronic systems which can function in presence of malicious participants.
- Markets are becoming increasingly transparent, at least for audit purposes.
- Bitcoin solves the difficult problem of who owns a given asset at any moment in time in novel very innovative ways similar to solutions initially created to implement NMS (National Market Structure) regulations in the US.

5. Value Transfer and Timestamps

Problem 5. Satoshi simply forgot to implement timestamps in bitcoin. Maybe because 'secure timestamps' are not easy to achieve. However, and accordingly, if two conflict transactions exist in the network, even with honest participants we don't know which transaction was first to be produced.
=> This can be fixed in a variety of ways including third party commercial solutions and specific peer confirmation solutions proposed in our paper.

The 20 Second Solution

Once we have timestamps [+ maybe some collaborating network nodes], we don't need to wait for 10 minutes to confirm transactions.
We can privilege earlier transactions and make sure that as time passes by, more recent transactions have steadily decreasing chances of being accepted. This removes the necessity to wait 10 minutes, especially for smaller transactions.

Security => Speed (Yes!)

In financial markets one can execute trades microseconds. In bitcoin we need to wait for 10 minutes and a large multiple of it for larger transactions. Speed is slow mostly out fear of possible double spending attacks, which imposes certain precautions. Fixing these security problems simply allows to make bitcoin transactions much faster, or rather to accept them much earlier.

Empowering the Peers

We are looking at **conservative** reform proposals which does NOT change the 10 minute timing for creation of new blocks. Our key proposal is to:

- Chain transactions though additional outputs which are immediately spent.
- If the attacker wants to undo one transaction (double spend), he has to SIMULTANEOUSLY forge signatures for numerous other transactions of anonymous peers on the network. Numerous child transactions also prove that the initial transaction was widely diffused in the network. Double spend fails.

Enhancements

1. In the current bitcoin network the median time until a node receives a block is 6.5 seconds [Decker-Wattenhofer]. This is "zero-fee propagation". Peer confirmation is likely to accelerate the development of better networks: initially fees could be paid to diffuse transactions faster.
2. Additional security can be achieved by reusing shares (proofs of computational effort) used in pooled mining. These prove the existence of transactions at any moment T but were lost in the current bitcoin network. Overall we can combine Proof-of-Stake [spending peers] and Proof of Work [shares] to validate transaction timestamps by both methods.

Conclusion and Future Work

This is NOT yet a complete solution. Future solutions should be such that:

- They are permission-less: they can added to selected network nodes.
- Several solutions can co-exist and co-operate (free market approach).

In addition, the recipients of transactions can co-operate to diffuse transactions. The recipient software should make sure the transaction is firmly entrenched in the mempools of several bitcoin nodes, then he checks random nodes for competing transactions. This can also be a business done for a fee.