Bitcoin Verification Latency

The Achilles Heel for Time Sensitive Transactions

Ken Griffith & Ian Grigg
Dinero Ltd

Abstract. Bitcoin has a high latency for verifying transactions, by design. Averaging around 8 minutes, such high latency does not resonate with the needs of financial traders for speed, and it opens the door for time-based arbitrage weaknesses such as market timing attacks. Although perhaps tractable in some markets such as peer to peer payments, the *Achilles heel* of latency makes Bitcoin unsuitable for direct trading of financial assets, and ventures seeking to exploit the market for financial assets will need to overcome this burden.

Bitcoin has a high latency for verifying transactions. This is by design.

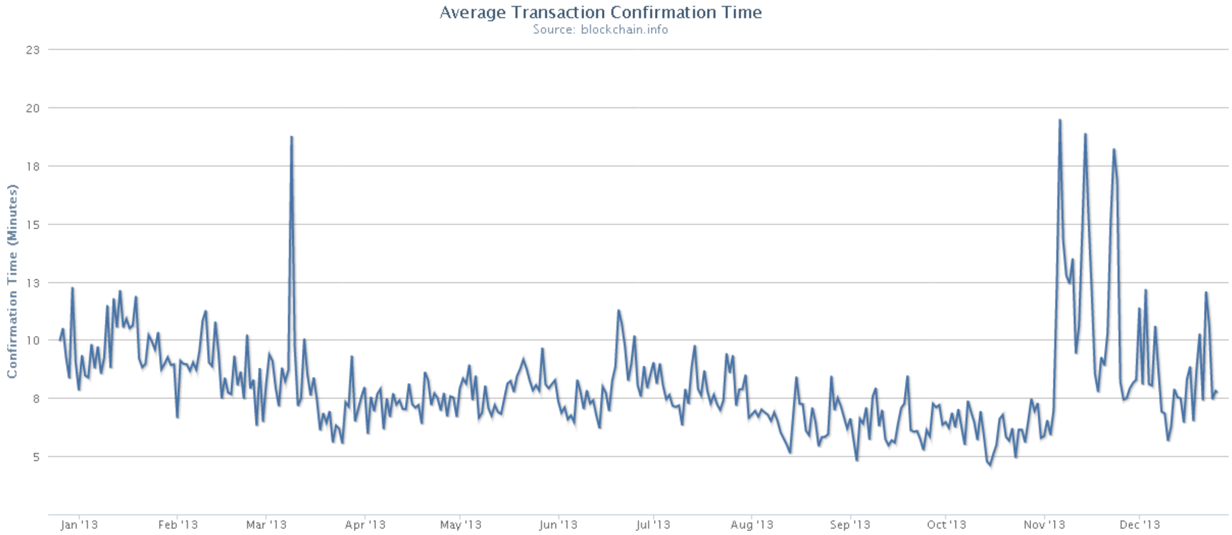
Whenever a Bitcoin transaction is received, it is necessary to get confirmation from other nodes on the network that the transaction was indeed valid. This requires performing the hashing calculations that serve as the proof-of-work that is the heart of the Bitcoin system.

The Bitcoin rules automatically adjust the difficulty of the hashing algorithm in order to produce new blocks at a rate of 1 new block every ten minutes.

Since block creation is the way that transactions are verified, this means that the average transaction confirmation time should be about half the time it takes to create a new block - which is 10 minutes. Therefore average confirmation time should be about 5 minutes.

The chart below shows the average transaction confirmation time in minutes for the year 2013. Confirmation has averaged about 8 minutes, but spikes as high as 19 minutes have not been uncommon. As expected, five minutes is the floor for average verification time.

Chart 1 - Bitcoin Average Confirmation Time for 2013



When we compare the 5 minute confirmation time for Bitcoin to the 70ms settlement time of professional trading platforms like Ricardo it becomes obvious that Bitcoin is an extremely inefficient settlement mechanism. Ricardo is over 4000 times faster for reliable settlement of trades.

The Arbitrage Problem

Arbitrage is inherent to trading. Arbitrage is simply buying low and selling high, or more specifically, finding and exploiting a price discrepancy for the same goods in different markets, or exploiting discrepancy in price in the same market at different times.

With the advent of algorithm driven exchange trading (“algos”), there is a race between algorithms to find and exploit arbitrage opportunities before anyone else does. On the comex and Nasdaq algos are in fierce competition to shave off a few milliseconds on trades.

The uncertainty that surrounds Bitcoin transaction confirmation makes it unsuitable as a platform for exchange trading which require immediate confirmation.

Bitcoin’s Vulnerability to Market Timing Attacks

For time-sensitive applications such as currency exchange and stock trading as well as gambling, latency on the order of minutes exposes the exchange to market timing attacks.

Market timing attacks were broadly used in the 2003 Mutual Fund Scandal [1] in the USA. A trader

[1] http://en.wikipedia.org/wiki/2003_mutual_fund_scandal

using a market timing attack places trades into a high latency market, waits to see which way the market has moved, and then cancels losing trades based on that information. [2]

One type of market timing attack requires the attacker to make a pair of opposite trades or bets. As soon as enough time has elapsed to see which is the winning trade, the attacker attempts to cancel the losing trade. If the attacker is unsuccessful in canceling the losing trade, his opposite trades cancel each other out, eliminating risk of loss to the attacker.

With Bitcoin there are three known double-spending attacks that can be used by an attacker to effectively reverse a payment with a reasonably high chance of success: these are the Race Attack [3], the Finney Attack and the Vector76 Attack [4] [5] which is a combination of the first two.

Market timing will enable attackers to take advantage of Bitcoin's high confirmation latency to monetize Bitcoin double spending attacks, enabling an attacker to place bets (on a Bitcoin gambling site) or paired opposite trades (on a currency exchange) and use a double spend to reverse the losing bet.

This type of attack was successfully performed multiple times against BetCoin Dice in September 2013. [6]

Unless the latency problem can be solved, Bitcoin's vulnerability to market timing attacks makes it unsuitable for use in direct exchange trading.

However, the latency problem is a function of Bitcoin's very soul - the proof of work. If latency could be reduced to near zero, the problem is no longer very difficult to solve - and we haven't proved much work.

The confirmation latency of Bitcoin is half the time it takes to generate a new block. Since this is regulated by design of the Bitcoin software to be one block every ten minutes - it is impossible to reduce the latency without increasing the block generation rate.

Therefore latency is a design feature of Bitcoin that probably cannot be reduced without breaking the entire platform.

[2] Grigg, Nesfield, Mutual Funds & Financial Flaws, U.S. Senate Committee on Governmental Affairs, Subcommittee on Financial Management,the Budget, and International Security, Oversight Hearing on Mutual Funds:Hidden Fees, Misgovernance and Other Practices that Harm Investors, Jan 17, 2004, http://iang.org/papers/mutual_funds.html

[3] Karame, Androulaki & Capkun, Two Bitcoins for the Price of One, http://eprint.iacr.org/2012/248.pdf

[4] Initial Description of Vector76 Attack, https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391

[5] Gavin Andresson, [Bitcoin Development] From the forums: one-confirmation attack, 18 Aug 2011, http://sourceforge.net/mailarchive/message.php?msg_id=27963970

[6] GHash.IO and double-spending against BetCoin Dice, https://bitcointalk.org/index.php?topic=327767.0

ColoredCoins & MasterCoin

There are two Bitcoin-related startups that seek to extend the Bitcoin protocol to enable user-created currencies or digital instruments backed by real world assets.

Both Mastercoin and ColoredCoins plan to use the Bitcoin blockchain to store data concerning balances and trades for user-created alt-currencies.   Both ColoredCoins and Mastercoin use the memo field of ultra low value Bitcoins (ie. 0.00000001 Btc) to store meta-data to represent real world assets such as a gram of gold, redeemable from the backer of that alt-currency. This enables them to use the blockchain as a public ledger of accounts for things that are not Bitcoins.

Both the Mastercoin and ColoredCoins protocols intend to enable blockchain-based bid/offer trades, using Bitcoin itself as the exchange mechanism.

For the reasons elaborated above, Bitcoin's high confirmation latency exposes the network to market timing attacks. Both ColoredCoins and Mastercoin may find they have played into this vulnerability by using Bitcoin itself as a platform for executing trades.

An Algorithm for Market Timing Attack on Mastercoin/ColoredCoin

As cited above, a market timing attack has already been successfully demonstrated against BetCoin Dice. However, there are very few high value trades or bets that currently can be executed with raw Bitcoin, because most exchanges and casinos that accept Bitcoin for payment park it in cold storage and then maintain their own order/bet books in-house with instant-clearing. This is the only sensible way to handle the latency problem.

However, both Mastercoin and ColoredCoins are planning to create high value trading systems that work directly on the Bitcoin blockchain - making them perfect targets for market timing attacks. Bitcoin hackers will be eternally grateful to the creators of this opportunity.

Here is what the attacker needs in order to perpetrate successful high value market timing attacks:

1. Wait for Mastercoin, ColoredCoins or another entity to create a market in reasonably high value digital assets that are traded directly on the Bitcoin blockchain.

2. Acquire an identical pair of high powered mining rigs in order to have enough hashing power to get a substantial head start on the unlucky counterparty to the trade(s) you plan to reverse.

3. Mark your targets - analyze the issuers of the open buy/sell orders in the market to identify, as much as possible, the weak traders in terms of hashing power and connections to other nodes.

Use Vector76 methodology to make direct connections to your marks, as well as the highest powered mining rigs on the network.

4. Write an algorithm to do the following:

   a. Place a pair of opposite trades or bets on the market in question with the intent of matching trades with previously identified weak targets.

   b. Immediately pass a double spend on both trades to your mining rigs, to create two alternate blocks, where you spend the value of each trade to another bitcoin account that you control. Keep these blocks and double spends secret, but hash as far ahead as possible with other valid transactions while waiting for the market signal.

   c. Wait a few minutes for enough market data to determine which trade was the winning bet, and which was the losing bet. The longer you can wait the more the market can potentially move. However, the longer you wait, the lower your chance becomes to successfully reverse one of your trades.

   d. Deploy your double-spend block to reverse the losing trade by having your mining rig preferentially post that block to several hundred other miners. Discard the double-spend block for the winning trade.

   e. If your double-spend to yourself is successfully chosen as part of the longer-blockchain, you win! You have canceled the losing trade.

The clever thing about a market timing attack is that if you fail to reverse the losing trade, the two trades cancel each other out - meaning there is no risk of loss to the attacker. This makes market-timing a perfect way for a mindless algorithm to attempt thousands of low-risk attacks per day even with low chances of successfully reversing a transaction - provided that a sufficiently large Bitcoin market exists on which to use it.

Why Bitcoin Market Timing Attacks Are Presently Uncommon

While the Bitcoin network depends on the majority of nodes being “honest”, the dependability of the participants in the network is far more likely to be determined by pragmatic cost-benefit analysis than by some strong moral commitment to the ideals of the Bitcoin community.

The financial incentive for Bitcoin miners is to deploy their mining hardware in the most profitable manner. The reason that market timing attacks are presently uncommon is partly because they require the assistance of mining equipment in order to have a high chance of success, and there are not a lot of opportunities in the Bitcoin Network to conduct two-way market trades with raw Bitcoin.

Currently the blockchain reward for mining a new block is 25 bitcoins. At current prices the value of the reward falls in the ballpark of $25,000.

As long as the block reward is high and the available opportunities for two-way trading on the Bitcoin Network are few, the most profitable use of mining rigs is to focus on mining new blocks.

However, this situation is likely to change in the future for several reasons.

Why Bitcoin Market Timing Attacks Will Eventually Become Worthwhile

The Bitcoin block reward is cut in half every 210,000 blocks (roughly four years). Once the block reward approaches zero the rewards of mining will be paid entirely by voluntary transaction fees. This will shift the cost of the Bitcoin transaction processing from dilution (everyone shares the cost) to the user making the transaction. It is unlikely that users will voluntarily pay the $50 per transaction that miners are currently being paid, so the reward per block will eventually fall to a small fraction of their present level.

At the same time that Bitcoin mining will be decreasing in profitability, Bitcoin-embedded markets such as Mastercoin and ColoredCoins will be creating trading markets that use the blockchain as the settlement mechanism. As the value of these markets increases, a point will be reached where it becomes more profitable to use a mining rig to perform timing attacks on trades than it is to mine new blocks.

A massive increase in the value of Bitcoins may delay the day when it becomes more profitable to perform market timing attacks than it does to mine Bitcoin - but with enough reward-halving iterations that day will inevitably arrive.

Conclusion

Though Bitcoin’s decentralized transaction register makes it reliable and robust as a way of storing and transmitting value, the latency inherent to the Bitcoin verification mechanism makes it a poor choice of platform for real time exchange settled transactions.

Companies or organizations that attempt to use the Bitcoin Blockchain as a trading platform are likely to eventually find themselves and their customers broadly targeted by market timing attacks.