Could Bitcoin Transactions Be 100x Faster?

Nicolas T. Courtois[1], Pinar Emirdag[2] and Daniel A. Nagy[3]
[1]*Computer Science, University College London, London, U.K.*
[2]*Independent Market Structure Professional, London, U.K.*
[3]*Computer Science, Eötvös Lóránd University, Budapest, Hungary*

Keywords: Electronic Payment, Crypto Currencies, Bitcoin, Double-spending Attacks, Decentralized Markets, Equities Trading, High Frequency Trading, Timestamps, Proof of Stake, Security Engineering.

Abstract: Bitcoin is a crypto currency, a distributed peer-to-peer financial system. Well actually it is an electronic system which manages the provisional ownership of a strictly fixed supply of abstract fungible units which really works as a distributed property register or a digital notary service. This is not so different than managing the ownership of shares in traditional financial markets. Modern financial institutions increasingly just do NOT trust each other, they build co-operative robust and decentralized and increasingly transparent, electronic systems which are and able to both serve the diverse objectives of participants (e.g. traders) and uphold certain security policies. Is Bitcoin actually so brilliant to be called the Internet of money as it is sometimes claimed? Not quite. Consider just the question of speed. Super low latency transactions **are a norm** in the financial industry, and even ordinary people have access to super fast bank transfers and real-time credit card transactions. Bitcoin remains rather the horse carriage of money. In this paper we look at the question of fast transaction acceptance in bitcoin and other crypto currencies. We claim that bitcoin needs to change in order to be able to satisfy the most basic needs of modern users.

1 INTRODUCTION

Bitcoin (Satoshi08). is a digital currency, payment and final clearing/settlement system and technology, a distributed property register and digital notary service, all in one. Current bitcoin suffers from a number of obvious and well known technical problems: slow transactions acceptance, large storage at network nodes, poor anonymity, high volatility, cyber attacks, to name just a few. Bitcoins cultivates a certain type of cryptographer's dream (CourtoisBahack14) in which participants do not trust each other, yet the payment system works due to cryptography rather than through some trusted financial institutions. In this paper we look at the question of fast transaction acceptance in bitcoin and other crypto currencies. Currently people have to wait for at least 10 minutes and more for larger transactions in order to avoid being a victim of double spending attack. We look at some essential questions. Does a decentralized network without central authority imply and mandate slow transactions? Could bitcoin transactions be 100 times faster? Is there a fundamental technical impossibility? Could bitcoin be somewhat fixed at a minimum cost?

1.1 Bitcoin vs. Traded Markets

A refreshing comparison is the comparison to traditional financial markets such as stock markets. There is a number of similarities with bitcoin. Trading is becoming increasingly 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, although this has been very difficult to achieve in today's markets. Bitcoin is as virtual as most of assets in financial markets. Ownership requires some type of proof of ownership (certificate) which problems are somewhat solved in both worlds. Overall we see that bitcoin technology and the traditional financial sector have many similarities. Yet super low latency transactions **are a norm** in the financial industry. In bitcoin they are considered problematic and difficult to achieve, cf. (Courtois14). We should note however that traditional stock markets exchange primarily "promises" rather than property itself. In both cases these things could be transferred very quickly. In stock markets final clearing and settlement process takes typically up to 3

T. Courtois N., Emirdag P. and A. Nagy D..
Could Bitcoin Transactions Be 100x Faster?.
DOI: 10.5220/0005102804260431
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 426-431
ISBN: 978-989-758-045-1

days. Final property transfer on the bitcoin ledger is done automatically and takes a multiple of 10 minutes. In addition current bitcoin network could also circulate bitcoin transactions in microseconds with non-standard software and networks (cf. also Section 4.3). However no bitcoin transaction is considered as valid as long as it was not officially approved by the blockchain which takes about 10 minutes or longer. Moreover transactions do not have timestamps nor they are recorded. We don't even know how old they are. There is a question of inherent instability of bitcoin, both imaginary/perceived and actual risk of any given transaction not being approved later due to some attacks (Courtois14; CourtoisBahack14; DeckerWattenhofer14). There is also a question of lack of network neutrality (Courtois14), of the ambient medium in which financial transactions are done. In traditional financial markets all the activities in the electronic systems are assumed legitimate and principals are trusted. In bitcoin principals are really allowed to be malicious. There is no easy way to exclude some malicious parties from participating in the P2P network.

1.2 Key Objective: Speed

All this makes that bitcoin transactions are slow or are assumed to be so by careful users who wait for a number of confirmations. The only judge is the state of the blockchain in the future.

In modern finance, property irreversibly changes hands in a matter of microseconds or is promised to be so later on, and cheating is excluded. Bitcoin requires users to wait for 10 minutes and longer for larger transactions, and new ways of cheating and for-profit blockchain manipulation are invented every day (Courtois14; CourtoisBahack14; DeckerWattenhofer14). Bitcoin needs to change. In this paper we look at how such a change could be engineered by exploiting the strengths of the current bitcoin network.

2 DECENTRALIZED MARKETS

Before bitcoin came along we have a long history of electronic financial transactions. A long history of practical electronic systems which have been designed, built, sold and massively used in the financial sector. Defenses against market manipulation and other attacks have evolved considerably. What lessons can be learned for bitcoin?

2.1 Speed and Decentralization

In financial services latency has different regimes. In trading of equities (stocks), which is the most “electronic” markets, the latency for matching orders is the micro seconds (10^{-6}). However for example for bonds it will be much slower especially if they are traded over the counter (OTC). In everyday payment world credit card payment is certainly a faster option than wire transfer, however not the cheapest for merchants. Bitcoin potentially disrupts both markets: it can be preferred to credit cards and overseas wire transfers due to lower fees, and it could sometimes be faster than bank transfers. We cannot ignore that there are strong limits to acceptability of current bitcoin: one cannot wait 10 minutes at a coffee shop.

Decentralized finance is not new with bitcoin. Decentralized systems and markets have been around for some time. This are just THE modern way to build things: more robust, less prone to fraud and abuse, etc. Various electronic market systems differ by attributes based on their participants, instruments traded, maturity levels, regulatory regimes and technology adoption. Dealer markets in over the counter (OTC) derivatives and US equities markets are major examples of modern truly decentralized(!) markets. The most common point for all these markets is that there are many “market places”. More precisely price formation happens at a number of different decentralized “nodes”. Nodes in this context could be broker dealers, dealers, exchanges or other matching platforms[1]. Essentially these are various intermediaries which aim to bring buyers and sellers together. In the case of OTC markets direct communication between these markets is very limited, and latency is not as relevant. Importantly in case of US equities, due to the regulatory regime these nodes must be aware of each other, aiming to match the best price at very low latencies. Timestamps for these markets are in the range of single digit microseconds. A simplified version of how these markets work is as follows:

1. Trader A wants to buy X shares of YY.
2. He sends his order to a market “node” P.
3. These orders are represented as “quotes” on the market P.
4. Market P checks for best prices not only on that market but also on all other markets.
5. The order is executed on Market P if the best price is there if not it is **routed** to a market where the best price is found.

[1] Nodes is not a terminology from stock markets, it is used to show similarities with the bitcoin network.

This connected but decentralized market structure is a result of Regulation NMS (National Market Structure) (Nanex13) which was mandated by the US Congress and implemented after 2005. Following (Maese14) the bitcoin network is actually reminiscent of a network which was initially created to implement NMS regulations. No further details are given however we read that bitcoin technology is “brilliant” and maybe a ”kind of value transfer network that you could dream about creating” for the stock markets ”if existing businesses had the luxury of a fresh start”, cf. (Maese14).

In the US there are over 50 liquidity pools (again called “nodes”). Under regulation NMS, there are 14 nodes which are Self Regulatory Organizations (SROs), or the “lit exchanges” which “publish” their data feeds. All nodes including these exchanges themselves have to check the best prices on the 14 official exchange nodes.

In order to complete the whole picture, these quotes are aggregated at the Consolidated Quote System (CQS) cf. (Nanex13). Actually the markets check CQS for best prices which is called National Bid or Offer (NBBO). Once a match happens on one of these nodes, the information about it is “reported on” the Consolidated Trade System (CTS) where all trades are aggregated. Everything is reported immediately with the timestamp of the executing node in UTC time. The combination of CQS (quotes) and CTS (executed trades) is sometimes called the SIP.

2.2 Timestamps

At microsecond levels accuracy issues around hardware, software and application timestamps become relevant. Some of the recent controversies (Lewis14; Nanex13) in equities markets stem from intricacies in inner workings of this system.

The nodes provide direct market data feeds which consists of the quotes at those specific nodes. Some traders (actually machines) have access to these direct data feeds. Other traders access quote data through CQS. Direct data feeds allow to obtain the information faster, a few milliseconds before the SIP data. At one moment the public data feed (CQS) had a delay of 22 milliseconds versus the direct (paid) feeds which was claimed contrary to the NMS regulations, cf. (Nanex13). Direct data feeds cost considerably more, in tens of thousands of $ per month in direct and indirect costs including the necessity to build special equipment, employing network engineers, large telco fees. 2.5 million subscribers pay the exchanges about $500 million each year to obtain such low latency data cf. (Nanex13).

In these markets, timestamps are very important: the first buyer gets the share at one price, another gets it later at another price. The order of the execution of transactions is crucial. Timestamps are generated by 14 trusted nodes or exchanges which are expected to be honest. Their public version, the SIP timestamps have lower precision and could be less accurate, cf. (Nanex13). An interesting question is whether it is possible to manipulate these timestamps for profit. We are not aware of such scenarios.

This question will come back in bitcoin. No one is trusted in bitcoin and in Section 4.1 we argue that bitcoin needs some “peers” to certify timestamps of other network peers. In bitcoin the order of processing the transactions matters less, except in situations of double spending. Unhappily transactions have NO timestamps in bitcoin, the founders of bitcoin simply forgot to implement any(!), cf. (Courtois14). Thus it becomes difficult to distinguish between various situations and take reasonable well-informed decisions which is a crucial question, cf. Section 4.

2.3 Validation

In these decentralized US equity markets there is a process of “policing” and checking for the good behavior which is very different from checks which need to be done by bitcoin miners. for the correctness of the final bitcoin blockchain. There is a price time priority for matching quotes. This means that quotes match at first come first serve basis at the best price. Now at a certain moment there is (or there can be) a demonstration of the sequence of actions described above to regulators and clients and verification that trades were executed at the best price on the 14 exchanges.

2.4 Secure Property Transfer

There isn’t just one way to build decentralized financial systems. Timely decision making is crucial/ Bitcoin system is somewhat fundamentally simpler than equities trading. There is no matching of orders, there is no double-entry bookkeeping. Yet it is all about a some form of having a property register owned by many participants with some degree of network neutrality (fairness in execution). Bitcoin blockchain is a major innovation which could in fact also be used to implement a similar concept of **“Value Transfer Networks”** for the stock markets cf. (Maese14).

We see that the US equities markets are decentralized and that “nodes” have obligation of some form of “market neutrality”: best effort to find the best price for customers on 14 nodes. In bitcoin we have the problem of “network neutrality”. It has a more limited scope. A “fair execution” is only a problem when two conflicting transactions are emitted. However handling such cases is crucial if we want to accept transactions faster. This problem is currently NOT solved in a satisfactory way, see Section 4. One crucial problem is that timestamp information is missing for bitcoin transactions, cf. (Courtois14). Another problem is that information propagates only on the basis of best effort. There is no US Congress regulation which would somewhat “force” the events in the network to reach many other network nodes. We will study these questions in Section 4 and Section 4.3.

3 SLOW TRANSACTIONS

In the US equities market the decentralization does not make transactions slow. In bitcoin it does. According to the initial design (Satoshi08) the initial bitcoin system is decentralized, asynchronous and can work in very poor network conditions, cf. Section 4 in (Courtois14). The key underlying principle which allows to achieve this objective is **the Longest Chain Rule**:

1. At any moment of the history of bitcoin, miners are trying to extend one existing block, and sometimes two solutions will be found.

   We call this (rare) situation a fork.
2. Different nodes in the network have received one of the versions first and different miners are trying to extend one or the other branch. Both branches are legitimate and the winning branch will be decided later by consensus.
3. The **Longest Chain Rule** of (Satoshi08) says that if at any later moment one chain becomes longer, all participants should switch to it.

With this rule, it is possible to argue that due to the probabilistic nature of the mining process, sooner or later one branch will automatically win over the other. Bitcoin is quite stable in practice. Forks are relatively rare. However forks could become more frequent in poor network conditions or due to certain attacks, cf. (CourtoisBahack14).

It is remarkable that in bitcoin literature this rule is taken for granted without any criticism. Following (Courtois14) claims this rule is highly problematic and it leads to very serious problems. One problem is that this consensus mechanism in bitcoin has two distinct purposes:

1. It is needed in order to decide **which blocks** obtain a monetary reward and resolves the fork situations in a simple and convincing way.
2. It is also used to decide **which transactions** are accepted and are part of official history, while some other transactions are rejected (and will not even be recorded, some attacks could go on without being noticed, cf. (DeckerWattenhofer14)).

In principle there is NO REASON why the same mechanism should be used to solve both problems. On the contrary. This violates one of the most fundamental principles of security engineering: the principle of *Least Common Mechanism* [Saltzer and Schroeder 1975]. One single solution rarely serves well two distinct problems equally well without any problems.

We need to observe that the transactions are generated at every second. Blocks are generated every 10 minutes. In bitcoin the **receiver of money is kept in the state of incertitude for far too long** and this **for no apparent reason**. It is a source of instability which makes people wait for their transactions to be approved for far too long time, especially for larger transactions.

Could transactions be accepted earlier? Could we for example make that even in the case of a fork miners are very likely to include exactly the same transactions in both versions?

4 THE 20 SECOND SOLUTION

The following solution was already proposed by several authors. One version was proposed by user joe in 2011 (joe14), and another version in May 2014 (Courtois14). There is a core proposal on which these sources agree, and it is also clear this is not yet a mature solution, more work is needed. The main goal of this proposal is to allow fast transactions. An important notion is the notion of **zero-confirmation transactions** cf. (Chen14), which occur in the current bitcoin software system. The question is really a question of how to fix bitcoin and add additional security and allow people to accept transactions faster. It was sometimes claimed that zero-confirmation transactions could just be accepted and that the risk decreases with time (Chen14). We should not however ignore double spending attacks (Courtois14) and risks increase as attackers discover new more “subversive” attack scenarios (Courtois14) and also for larger transactions. The core proposal is as follows:

1. If two double-spend transactions are received within 20 seconds of each other by some network node, we consider that their ordering/priority is unknown. Peer nodes may accept[2] blocks with ei-

[2] A variant where both would be rejected by default was

ther transaction, and build on top of the longest chain (current solution).

2. If two double-spend transactions are received more than 20 seconds apart by any network node, he considers that their ordering is known. He should reject all blocks which include the later, non-original transaction2 and accept the clearly earlier transaction1.

An inherent problem with this sort of solution is that different network nodes have a different view. This leads to all sorts of problems. The solutions proposed in Section 7 of the more recent paper (Courtois14) differ fundamentally in that they propose to use **timestamps** in order to make these decisions **more objective**. Current bitcoin software already somewhat privileges earlier transactions but there are no timestamps.

4.1 Improved Solutions

Additional techniques are used to ensure that timestamps are not being tampered with. Two solutions for this problem are proposed in (Courtois14). One solution implements a certain type of proof of stake through cooperation of additional network nodes. They are asked to validate the existence of transactions at certain moment by spending **one** of their (smaller) inputs instantly. An additional solution is to reuse shares used in pooled mining which already are ready proofs of existence of transactions, cf. Section 7.2 in (Courtois14).

4.2 The Issue of Forks

It is not obvious that the basic solution described in 4 works well in practice. A possible problem with such solutions was already explicitly suggested in (joe14). The author recommends to:

> ”Reject all blocks that include the later [...] transaction2[...]
>
> stop rejecting blocks containing double-spend transactions [i.e. transaction2] if the block receives 6 confirmations”

This in order to avoid “permanent block forks”. This is in fact problematic: it means that the attacker may have eventually succeeded in his double spending attack and the network accepts it. We can only hope that getting these 6 confirmations is sufficiently costly for the attack not to be profitable anymore.

4.3 Super Peers vs. Speed

Timestamping does not necessarily imply centralized “super-peers” which could be bribed, cf. Section 7 in (Courtois14). It should rather be ordinary peer network nodes not known in advance to the attacker. Recently these were alarming news about the number of nodes declining month after month and falling below reasonable levels, less than 8,000 recently, cf. (Cawrey14). Bitcoin is going to disappear if we do not create monetary incentives for ordinary people to run bitcoin network nodes.

In addition and however we could have a “super-network”. It is NOT correct to believe that miners have no other choice than to rely on the current bitcoin network where the median time until a node receives a block is 6.5 seconds cf. (DeckerWattenhofer13). Miners could actually - because they work for profit - PAY a tiny little bit of money to have access to a much faster and more accurate data about all transactions, super-fast latency data based on a set of some 1000 randomly chosen full network nodes which are connected to a faster ‘backbone’ network. Then it is easy to imagine and easy that miners have access to all transactions within miliseconds rather than seconds. Such network could be run by business providers or as a cooperative and should also provide double-spending alerts automatically.

5 OTHER SOLUTIONS

5.1 Participation of the Recipient

There is a simple solution to double spending attacks which requires only small changes to the current bitcoin wallet software. A mechanism of optional “fast transfers” which mandates sending the raw transaction over to the recipient in addition to submitting it to the network. Then the client software on the money recipient side should make sure the transaction is firmly entrenched in the mempools of several bitcoin nodes after which he checks some random nodes if no other competing transaction was also submitted to the network. Software could show that if the transaction was accepted and display an estimated proportion of peers which already know this transaction. This proportion will grow with time and will allow the recipient to do his risk management. There could also be a business helping the recipient to diffuse their transaction for a small fee and actively scanning the network for double spends.

proposed in Section 7 of (Courtois14).

5.2 Reactive Solutions

Reactive solutions are about dealing with consequences of double spending events. Depending on the product sold, it could be possible to simply cancel the service.

5.3 Scripting Solutions

There is a number of scripting solutions to double spending known in the bitcoin community based on so called contracts coded via the bitcoin scripts and enforced by miners (Hearn14).

6 CONCLUSION

In this paper we look at bitcoin network as a decentralized property transfer network solution and explore a number of similarities with modern stock markets. Interestingly stock markets are addicted to speed, however bitcoin is very slow. In this position paper we argue that bitcoin transactions should be very fast, or bitcoin is not better than credit cards or traditional banks. Blockchain and the *Longest Chain Rule* do not yet solve this problem. We propose to use timestamps and to accept earlier transactions also in the case another transaction is emitted later. We contend that the solutions needs to empower ordinary peer-to-peer network nodes and allow them to generate some income. Our main proposal is to achieve non-zero level of security against double spending at a higher speed than the speed of the main blockchain through distributed consensus and reusing elements which already exist in the current bitcoin network.

In future works we are going to develop more detailed solutions: an extended version of this paper will be published by the authors and certain solutions are already discussed in Section 7 of (Courtois14).

REFERENCES

Daniel Cawrey: *What Are Bitcoin Nodes and Why Do We Need Them?,* 9 May 2014, http://www.coindesk.com/bitcoin-nodes-need/

Caleb Chen: *The Mathematically Secure Way To Accept Zero Confirmation Transactions,* In Cryptocoin news, 13 Feb. 2014, http://www.cryptocoinsnews.com/news/the-mathematically-secure-way-to-accept- zero-confirmation-transactions/2014/02/13,

Nicolas Courtois, Marek Grajek, Rahul Naik: *The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining,* at http://arxiv.org/abs/1310.7935, 31 Oct 2013.

Nicolas T. Courtois, Lear Bahack: *On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency,* 28 January 2014, at http://arxiv.org/abs/1402.1718.

Nicolas T. Courtois: *On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies,* 20 May 2014, http://arxiv.org/abs/1405.0534.

jav, joe *at al*. A discussion thread: *Best practice for fast transaction acceptance - how high is the risk?,* February-July 2011, https://bitcointalk.org/index.php?topic=3441.msg48484#msg48484

Christian Decker, Roger Wattenhofer: *Information propagation in the bitcoin network,* 13-th IEEE Conf. on Peer-to-Peer Computing, 2013.

Christian Decker, Roger Wattenhofer: *Bitcoin Transaction Malleability and MtGox,* http://arxiv.org/pdf/1403.6676.pdf

Mike Hearn: *Contracts,* A list of known methods to form agreements with people via the bitcoin blockchain. https://en.bitcoin.it/wiki/Contracts, July 2014.

Michael Lewis: *Flash Boys, a Well Street Revolt,* Book, March 2014.

Vivian A. Maese: *Divining the Regulatory Future of Illegitimate Cryptocurrencies,* In Wall Street Lawyer, Vol. 18 Issue 5, May 2014.

Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System,* At http://bitcoin.org/bitcoin.pdf, 2008.

Nanex Research: *Nanex 30-Sep-2013 HFT Front Running, All The Time,* public research report, http://www.nanex.net/aqck2/4442.html)