Thesis no:
URI: urn:nbn:se:bth-16294

Scalability of the Bitcoin and Nano protocols: a comparative analysis

Hampus Bowin
Daniel Johansson

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the bachelor degree in Software Engineering. The thesis is equivalent to 10 weeks of full time studies.

Contact Information

Authors:
Hampus Bowin
Email: hampusbowin@gmail.com

Daniel Johansson
Email: daniel.j-@hotmail.com

University advisor:
Dr Andrew Moss
Department of Computer Science

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet: www.bth.se
Phone: +46 455 38 50 00
Fax: +46 455 38 50 57

Abstract

In the past year cryptocurrencies have gained a lot of attention because of the increase in price. This attention has increased the number of people trading and investing in different cryptocurrencies which has lead to an increased number of transactions flowing through the different networks. This has revealed scalability issues in some of them, especially in the most popular cryptocurrency, Bitcoin. Many people are working on solutions to this problem. One proposed solution replaces the blockchain with a DAG structure. In this report the scalability of Bitcoin's protocol will be compared to the scalability of the protocol used in the newer cryptocurrency, Nano. The comparison is conducted in terms of throughput and latency. To perform this comparison, an experiment was conducted where tests were run with an increasing number of nodes and each test sent different number of transactions per second from every node. Our results show that Nano's protocol scales better regarding both throughput and latency, and we argue that the reason for this is that the Bitcoin protocol uses a blockchain as a global data-structure unlike Nano that uses a block-lattice structure where each node has their own local blockchain.

Keywords: Scalability, Cryptocurrency, Bitcoin, Nano

Acknowledgments

We would first like to thank our university advisor Dr. Andrew Moss for his guidance throughout the writing of this thesis. He helped us with everything from writing to technical issues and also provided us with computers which made the experiment possible.

Contents

Abbreviations

Abbreviation	Explanation
tps	transactions per second
DAG	Directed Acyclic Graph
PoW	Proof of Work
CPU	Central Processing Unit
RAM	Random Access Memory
SSD	Solid State Drive
CSV	Comma Separated Values

Glossary

Term	Definition
Latency	Latency is the time it takes for a transaction to be confirmed.
Throughput	Throughput is the number of transactions that are confirmed per second.

1 Introduction

The blockchain structure is one of the core components of Bitcoin, the first commercially successful cryptocurrency, which is a purely peer-to-peer payment solution that does not require financial institutions to operate [1]. The concept blockchain was first introduced in November, 2008, and implemented in January, 2009, as a part of Bitcoin by a person, or group, under the alias Satoshi Nakamoto [2]. It is a distributed ledger in which transfers of resource ownership can be recorded and therefore it removes the problem of having a central point of failure. The data distributed among users is cryptographically authenticated, which makes it difficult to tamper with the stored information.

Bitcoin's blockchain implementation suffers from multiple known scalability issues. One issue is the hard-coded maximum limit of only seven transactions per second (tps) that the Bitcoin network can handle, which is due to the size of the blocks in the blockchain and the time it takes to generate a block. This means that the tps can not increase as the number of attempted concurrent transactions made by users increase. When comparing the throughput of Bitcoin's network to VISA that can manage up to 56,000 tps, there is a huge scalability issue which needs to be solved if Bitcoin wants to compete with VISA as a payment method [3]. Another problem with Bitcoin based blockchains is that confirmation times increase when the number of transactions increase [4].

In one year from January, 2017, the value of one bitcoin increased from approximately $900 to $20,000 [5]. This led to a high degree of media coverage, which made Bitcoin popular among the public and increased its user-base as well as that of other cryptocurrencies. Bitcoin and its blockchain has also made its mark in the technology industry, where many major companies such as Microsoft, IBM etc. have shown their interest in the technology. Recently it has also been revealed that Bitcoin's energy consumption is huge and that is it not sustainable from an environmental perspective [6]. We live in a world where environmental problems are important to solve and for the blockchain to be attractive it cannot be a part of the problem.

Numerous people are working on different solutions to the scalability issues. Some have made forks of Bitcoin and modified the source code, e.g. increasing the size of the blocks. By increasing the block size, more transactions can be included in each block and thus it will be possible to confirm more transactions each second. Other approaches are adding layers on top of Bitcoin. An example is the Lightning Network, which is a network of micropayment channels [7]. The Lightning Network makes it possible for two parties to open a channel where they can continuously update their balances without broadcasting everything to the blockchain. This reduces the load on the main blockchain. There are also some cryptocurrencies, ByteBall, IOTA and Nano to name a few, that have opted for a DAG structure (directed acyclic graph) instead of the traditional blockchain in order to avoid its problems with scalability.

Unlike the blockchain, which is a single chain of blocks, the DAG structure consists of several blockchains. In the DAG each node represents a transaction and each edge represents a reference to another transaction. Apart from the referenced transaction, each transaction also contains a proof of work (PoW) which confirms one or more transactions. Nano was one

of the first cryptocurrencies to use this structure [8] and it was implemented in December, 2014. Nano aims to be a payment solution just as Bitcoin but without the transaction fees, high transaction times and scalability issues. Unlike the Bitcoin protocol, Nano's protocol does not require a lot of computational power and so it can run on low-power hardware.

The purpose of this study is to determine which one of Bitcoin's and Nano's protocol offers better scalability in terms of latency, the time it takes for a transaction to be confirmed, and throughput, the number of transactions that can be confirmed per second. This will be done by doing experiments with nodes inside a private network that send transactions to each other. The technological differences between the two technologies will also be discussed and conclusions will be drawn from both this and the experiment to see the difference in scalability.

It is of value to have a scientific comparison of scalability since there is little research about the scalability of Bitcoin's protocol and none about the scalability of the Nano's protocol.

2 Research Questions

RQ1: Which protocol offer better scalability in terms of latency, Bitcoin's or Nano's?

RQ2: Which protocol offer better scalability in terms of throughput, Bitcoin's or Nano's?

RQ3: What technological differences, that have an impact on the scalability in terms of latency and throughput, are there between the Bitcoin and Nano protocols?

2.1 Motivation

Typically users want transaction times to be fast and do not want them to be affected by other people using the same network. Fast transaction times are directly related to the latency of transactions and throughput the network can handle. This is known to be a problem for blockchains and the DAG structure is said to solve this. By comparing the technological differences of the protocols that affect the scalability, the bottlenecks of each protocol will be examined. By knowing the bottlenecks, the protocols can be improved, modified or even combined to achieve better scalability.

2.2 Goals

The goals with this study is to determine which one of the Bitcoin and Nano protocols that offers better scalability in terms of latency and throughput. Their technological differences and how they affect the scalability will also be discussed to address any potential bottlenecks and issues.

2.3 Expected Outcome

We expect to see that the Nano protocol offer better scalability in terms of both latency and throughput. This is because the Bitcoin protocol uses a single blockchain while Nano's uses a local blockchain for each account, making it possible to send transactions asynchronously.

3 Research Method

3.1 Theoretical Method Design

Literature referenced in this paper was obtained from searching the databases Google Scholar and Microsoft Academic. In the search, terms related to blockchains, DAGs and scalability were used.

The search strategy consisted of three steps. At first, the database was searched using search strings created from the keywords. Those that resulted in more than 2000 literature were excluded. Then the relevant literature was sorted out based on the title, abstract and introduction. Lastly, the remaining literature was read through to further sort out those that were irrelevant.

To decide whether the literature were relevant or not the following criteria were used:

- it had to be a scientific publication written in english or swedish
- it had to be within the school's subscription
- it had to include the keywords used in the search in the title, abstract or introduction.

List of keywords that were included in the literature search and used to form search strings:

- analysis
- bitcoin
- blockchain
- comparison
- directed acyclic graph
- dag
- tangle
- experiment
- measure
- scalability

Search strings created from the keywords are listed in table 1 below together with how many results they resulted in as well as the date the latest search was made.

Search string	Results	Date (last search)
blockchain dag scalability	83	2018-02-08
blockchain scalability experiment	144	2018-02-15
blockchain experiment measure scalability	155	2018-02-20
blockchain comparison dag	166	2018-02-09
blockchain scalability directed acyclic graph	1184	2018-02-09
bitcoin scalability	1479	2018-02-09

Table 1. Search strings used in the literature search.

3.2 Empirical Method Design

In order to answer the research questions an experiment was conducted where both a private Bitcoin, and a private Nano network were set up and tested with an increasing number of nodes in each test which also had different numbers of tps sent from the nodes. These

parameters were selected to study how the networks behave when adding resources to them and when increasing the load of every node in the network.

As the ability of the Bitcoin and Nano protocols to scale is investigated, Bitcoin's protocol was modified to achieve an average block interval of 1 minute instead of 10 minutes, which is the rate at which block are being generated in the real Bitcoin network. By changing this the blocks will be generated at a faster rate compared to the real Bitcoin network and thus the maximum achievable throughput will be higher. In the Nano protocol there are no parameters which limit the number of transactions that can be confirmed per second, and therefore nothing was modified to try and affect it.

To make the comparison as fair as possible, the CPU time required to confirm a transaction was calibrated to be the same for one node in both implementations. This eliminated the difference in CPU time required to confirm a transaction between the networks and so the scalability was only affected by the actual implementation.

The reason Bitcoin's protocol was chosen, was due to the fact that Bitcoin was the first commercially successful cryptocurrency and is an alternative to traditional payment solution. It is also the most popular cryptocurrency which have revealed some issues regarding the scalability. The blockchain structure is said to be one of the reasons it can not scale and therefore Nano was chosen as it is a DAG-based cryptocurrency. Just as Bitcoin, the purpose of Nano is to be an alternative to traditional payment solutions and also to solve the problems that cryptocurrencies using the blockchain suffers from.

3.2.1 Experiment Configuration

Firstly, the source code of Bitcoin Core version 0.16.0 was cloned and the modifications presented in table 2 below were made.

Modification	**Reason**
Block interval	The block interval was set to 1 minute instead of 10 minutes, which is the default. It was done so that the network would be 10 times faster than the real Bitcoin network, in order to test the protocol, and to have more data available for the protocol to use when recalculating the difficulty.
Difficulty adjustment interval	The difficulty adjustment interval was set to 10 blocks, meaning that the difficulty is recalculated every 10 blocks. It was set to 10 blocks because of the value of the block interval in order to make so that the difficulty was recalculated every time nodes were added to the network during the test.
Coinbase maturity	The coinbase maturity was set to zero confirmations instead of 100 confirmations meaning that the block reward is received instantly when generating blocks and not after 100 confirmations. This was done to speed up the setup of the tests.

Modification	Reason
Genesis block	A new genesis block was generated with a difficulty that takes around one minute to generate in order to host a private network and to have the difficulty be the same throughout the test.
Network	The source code was modified so that it would not connect to the main Bitcoin network.

Table 2. The modifications made to the Bitcoin source code and the reasoning behind them.

With this modified, Bitcoin Core was built which generated the executable bitcoind.

Secondly, the source code of Nano node version 10.0 was cloned and built. Then a genesis account and block were created using the node. Afterwards, the source code was modified to use the newly created genesis block after which the node was rebuilt. Also, the Nano node configuration was modified to use one CPU core since bitcoind only uses one.

When that was done the CPU time required to confirm a transaction was calibrated to be the same for both implementations. To do this the CPU time required to confirm a transaction in the modified version of Bitcoin was first off calculated. It was done by starting bitcoind in regtest mode on two nodes after which enough blocks to get the first block-reward were generated on the first node, and an address was generated on the second node. When both nodes were set-up, 50,000 transactions were sent from the first node to the second node and for each 10,000 transactions a new block was generated. With this data the CPU time required to confirm a transaction was calculated by taking the average number of transactions that fit into one block and divide it by the block interval of 1 minute. Lastly the difficulty was modified in the Nano node's source code. Since two types of blocks, send and receive, have to be generated in order to confirm a transaction in Nano the difficulty was modified to take half the CPU time that of the CPU time it took to confirm a transaction in Bitcoin.

3.2.2 Experiment Setup

Four tests were performed for each protocol where the first test sent two tps from every node, and this double for every test up until the fourth and last one which sent 16 tps from every node. It is represented by table 3 below.

	Test 1	Test 2	Test 3	Test 4
Number of tps sent from each node	2	4	8	16

Table 3. The number of tps sent from each node in each test.

Each test started off with two nodes and every 10 minutes the number of nodes in the network were doubled. The tests ran for 40 minutes each, ending at 16 nodes in the network. It is represented by table 4 below.

	0 - 10 minutes	10 - 20 minutes	20 - 30 minutes	30 - 40 minutes
Number of nodes	2	4	8	16

Table 4. The number of nodes in the network at different time intervals during the tests.

Every node was paired up with another node and only sent transactions to that node. It is illustrated in figure 1 below

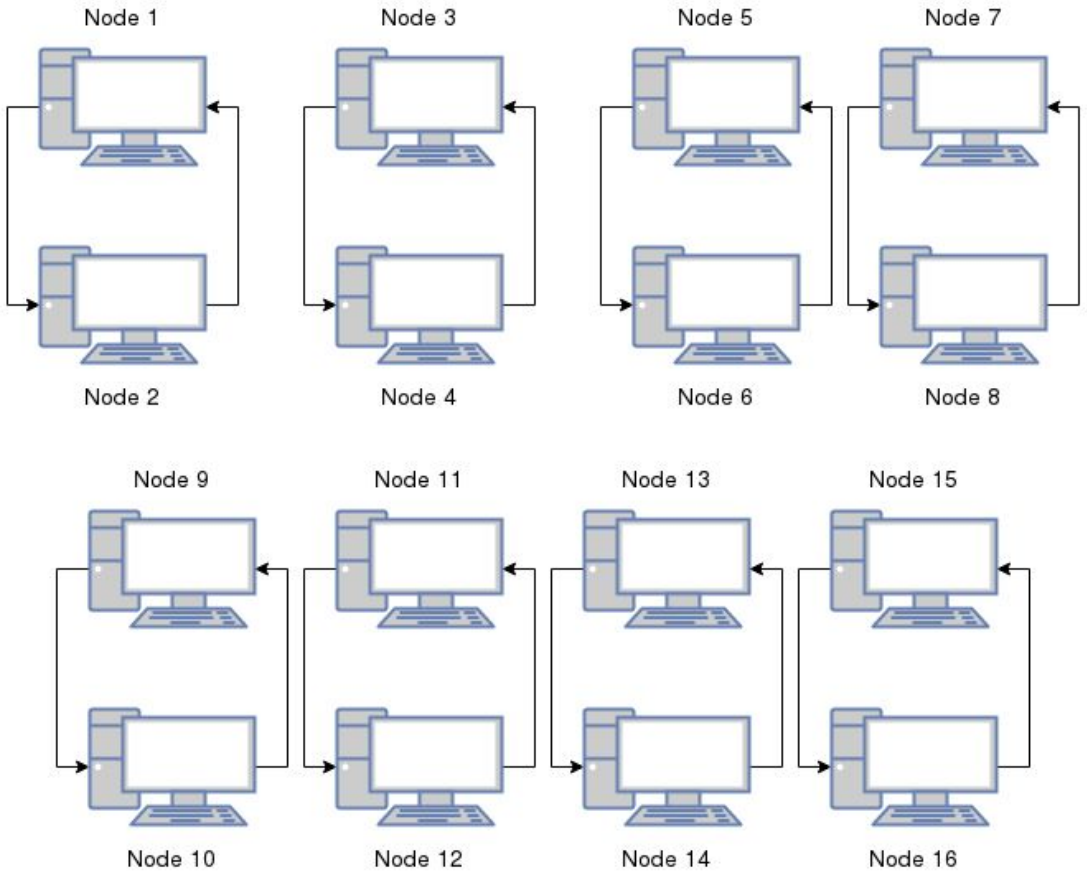


Figure 1. The node setup. Arrows represents the flow of transactions.

Before each test all nodes were started and connected to each other. In the Bitcoin tests an address was generated for every node, followed by generating a block which provided Bitcoins that were sent to each address. In the Nano tests, a wallet and account was generated for every node. One node was set up with the genesis account from which Nano currency was sent to the other accounts that were generated.

Each test was repeated two times to ensure that the data gathered was consistent and correct as well as to avoid any outliers that could adversely affect the result.

3.2.2.1 Parameters

The parameters used in the experiment was nodes and number of tps sent from each node. Each node represented a computer which was a full node. The number of nodes used were 2, 4, 8 and 16. The different number of tps that was sent from each node were 2, 4, 8 and 16.

3.2.2.2 Environment

The nodes used in the experiment were computers running Ubuntu 16.04 LTS with the following specifications:

- CPU
    - Product: Intel Core i7-6700
    - Speed: 3.4 GHz
    - Cores: 4
    - Threads: 8
- RAM
    - Type: DDR4
    - Speed: 2133 MHz
    - Size: 16 GB
- Storage
    - Type: SSD
    - Speed: 3200 Mbit/s

They were running on a local network with a speed of 100 Mbit/s.

3.2.3 Measurements

Measurements were done on the scalability in latency and throughput of the two implementations. It was measured by looking at how the latency and throughput changed when introducing more nodes in the networks and increasing the transactions sent from each node.

3.2.4 Data Collection

To be able to measure the scalability in latency and throughput of the implementations, the time each transaction was sent and the time it was confirmed was collected from the tests. When running the Bitcoin tests, this data were obtained at the end of each test by retrieving the transaction time and block time of all transactions that were sent from every node. In the Nano tests, this data were collected during each test by logging the time of every send and receive transaction together with the block hash for every node. After each test the data from every node pair were processed to retrieve the send and receive time of every transaction. All data were saved into CSV files so that they could be easily imported to Microsoft Excel.

3.2.5 Data Analysis

The CSV files containing data collected from the tests were imported to Microsoft Excel where the data was processed further. When processing the data the parameters in the experiment were taken into consideration. This data were used to calculate the average latency and throughput for every test and for each iteration of nodes in every test. Based on those values, graphs were created and used when analysing the scalability of the Bitcoin and Nano protocols. From the analysis a comparison based on their ability to scale was made.

3.2.6 Limitations and Validity Threats

Possible limitations and validity threats that were found throughout the experiment are presented below.

The fact that there are fees in the Bitcoin protocol that affects the order in which transactions are being confirmed could have affected the latency of transactions. We tried to set the fee to zero as well as to be the same for all transactions, in both the source code and the configuration, without any success. This could have affected the result negatively but as we processed the gathered data we could see that it did not have a big impact on the results.

Preferably, we would have liked to run each test at least five times to make sure our results were consistent and avoid outliers. But as we only had time to run them two times due to the experiment setup taking longer than expected, the results might contain data that is incorrect.

4 Literature Review

4.1 Summary

Based on our findings, the papers do not seem to be in conflict with each other when it comes to scalability issues of the blockchain structure. This gives us a clear view on what to expect from the results. Alos, since there is little research on scalability of cryptocurrencies in general we could only find a few papers with a slight relation to our work. Some of the papers that we found are somewhat related and mostly discuss solutions to the scalability problem of blockchains. This leaves us with an unexplored field to work in.

4.2 Mapping of literature and research questions

This table maps the literature found during the literature study, to the research questions they are related to.

Literature	**Research Question**
Comparative Analysis of Bitcoin and Ethereum	RQ1, RQ2, RQ3
Scalability Analysis of Blockchains Through Blockchain Simulation	RQ1, RQ2, RQ3
Bitcoin: A Peer-to-Peer Electronic Cash System	RQ3
Nano: A Feeless Distributed Cryptocurrency Network	RQ3

Table 5. Column two shows which research question the literature answers.

4.3 Results

Research Question 1, 2 and 3

RQ1: "Which protocol offer better scalability in terms of latency, Bitcoin's or Nano's?"

RQ2: "Which protocol offer better scalability in terms of throughput, Bitcoin's or Nano's?"

RQ3: "What technological differences, that have an impact on the scalability in terms of latency and throughput, are there between the Bitcoin and Nano protocols?"

Marit Rudlang [9] mentions that one of the scalability issues of Bitcoin is the maximum block size of 1 MB, which limits the number of tps the Bitcoin network can process to a maximum of about seven.

Sneha Goswami [4] seem to be in agreement with Rudlang regarding the impact that the block size has on the scalability of Bitcoin's blockchain. When discussing bottlenecks in blockchains she mentions the size of the blocks in Bitcoin's blockchain, which are fixed to a

maximum of 1 MB, and the block interval, which in Bitcoin is 10 minutes. In order to avoid these bottlenecks the size of the blocks in the blockchain can be increased, which would increase the throughput of the network. This would lead to an increase in scalability of the network, due to the increase in number of transactions that it would be able process per second. Decreasing the block interval would also increase the scalability, as higher throughput would be achievable. Goswami also concludes that blockchains suffer from an increase in confirmation times when the number of transactions increase, when analysing the relation between transactions and confirmation times in blockchains.

Research Question 3

RQ3: "What technological differences, that have an impact on the scalability in terms of latency and throughput, are there between the Bitcoin and Nano protocols?"

Satoshi Nakamoto [1] proposes Bitcoin that uses a chain of blocks to record transactions made in the network. When explaining how the network functions he mentions that transactions are broadcasted to every node in the network which puts them into a block. They do this while trying to solve a PoW so that they can broadcast the block to the other nodes in network. Nakamoto also says that the difficulty of the PoW is determined by a moving average which targets a certain number of blocks per hour. This is done to compensate for rising processing power in the network.

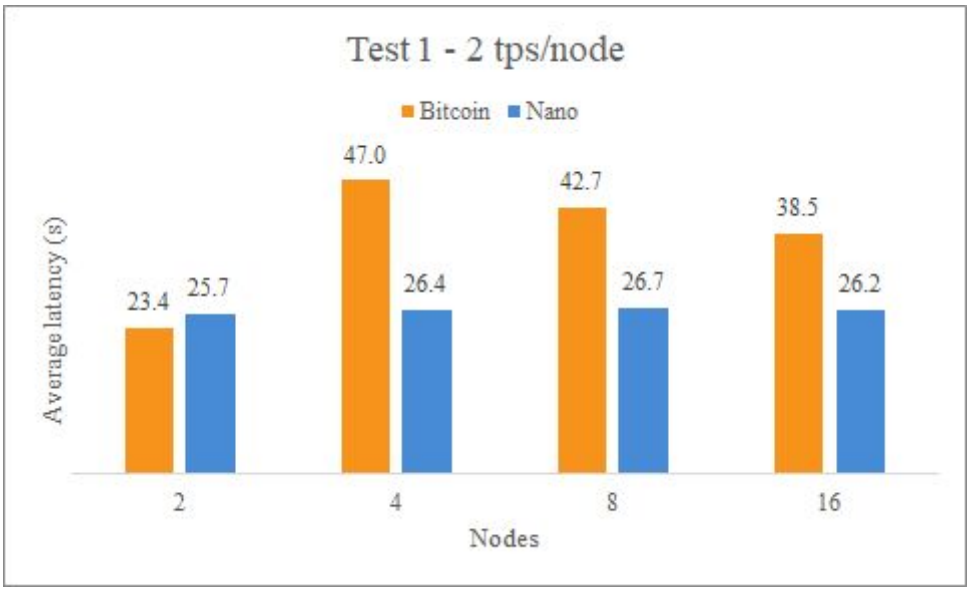
Colin LeMahieu [8] introduces Nano that unlike other cryptocurrencies uses a block-lattice structure in which each account in the network has its own blockchain called account-chain. The account-chain represents the transaction history of the account and can only be updated by the owner of the account. This makes it possible to update an account-chain immediately and asynchronously to the rest of the account-chains in the network. It is also the reason why there are no block intervals in the Nano implementation. LeMahieu claims that the block-lattice structure eliminates the access issues and inefficiencies of a global data-structure, which Bitcoin and other cryptocurrencies use. He also mentions that a PoW, which is used as an anti-spam tool in Nano, has to be computed in order to send a transaction.

5 Results and Analysis

5.1 Research Question 1 - Latency

RQ1: "Which protocol offer better scalability in terms of latency, Bitcoin's or Nano's?"

In graph 1, as well as in annex 1, 2 and 3, the results of how the average latency was affected when increasing the number of nodes in the network are presented and compared between the Bitcoin and the Nano protocol.

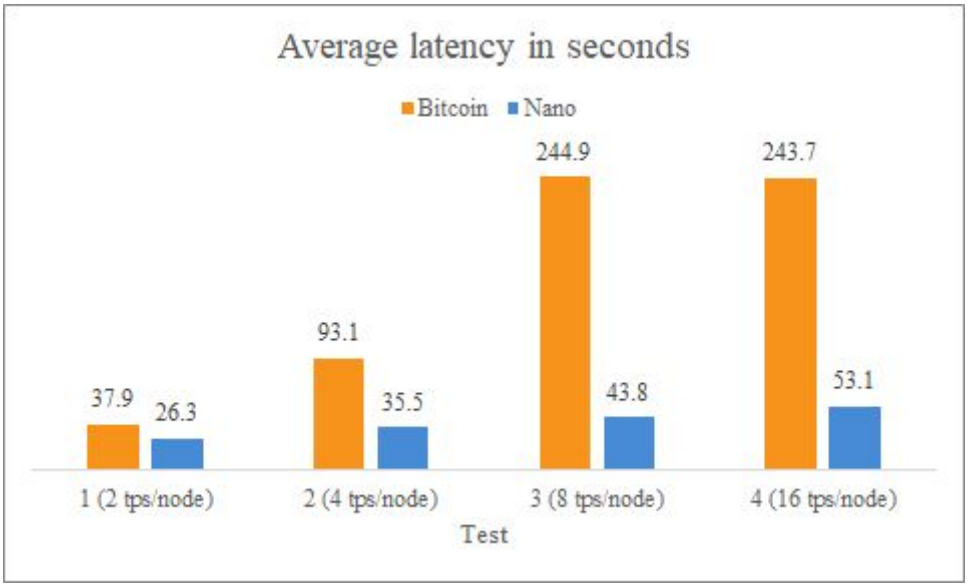


Graph 1. Average latency, in seconds, for both protocols at each iteration of nodes, sending 4 tps from every node.

For Bitcoin, we saw that the average latency increases in all of the tests, except for the first one, which means that Bitcoin is not able to scale when increasing the number of nodes in the network. The reason as to why the average latency decreased in the first test could be that more transactions were confirmed at that point in time due to more blocks being generated.

For Nano, we saw that the average latency did not increase in any of the tests which indicates that it scales linearly. It also suggests that the network can handle an increasing load with the addition of resources without the latency being affected.

In graph 2, the results of how the average throughput was affected when increasing the number of tps that were sent from every node are presented and compared between the Bitcoin and the Nano protocol.



Graph 2. Average latency, in seconds, for both protocols in every test.

For Bitcoin, we saw that the average latency more than doubled up until the last test. It indicates that Bitcoin is not even close to be capable of scaling. The reason it increased is because of the increase in number of tps sent from each node which lead to a large increase in unconfirmed transactions. This is in line with what Sneha Goswami [4] found when analysing the relation between transactions and confirmation times in blockchains, which is presented in the literature review.

There are two possible reasons for the decrease in latency in the last test. The first one could be that a limit was reached where only a certain number of transactions could be sent through the network per second. This can be explained by looking at annex 7 and 8, which are related to the third and fourth test respectively, where we can see that not more than roughly 85,000 transactions were sent in both of the tests. The second reason could be that more transactions were being sent than confirmed, i.e. the apparent reduction in latency is therefore because a number of the blocks were failing to ever confirm, thus reducing the average.

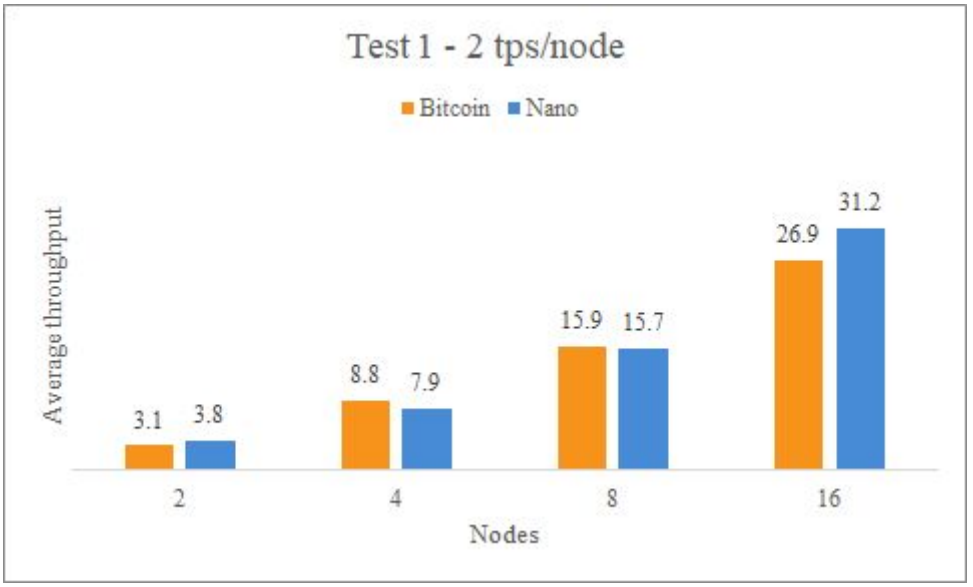
For Nano, there was a slight increase in latency between each test and therefore it does not scale. This is probably caused by the amount of computational power required from each node, which increases when the number of tps sent from each node increases.

To conclude the findings, in Bitcoin's protocol we found that the latency did not scale, neither when adding resources to the network nor when increasing the load of the network. In the case of Nano's protocol, we found that the latency increased slightly when increasing the number of tps that were sent from every node, which indicates that it does not scale when increasing the load of the network. Though, when adding nodes to the network the latency was not affected, which means that it scales when adding resources to the network.

5.2 Research Question 2 - Throughput

RQ2: "Which protocol offer better scalability in terms of throughput, Bitcoin's or Nano's?"

In graph 3, as well as in annex 4, 5 and 6, the results of how the average throughput was affected when increasing the number of nodes in the network are presented and compared between the Bitcoin and the Nano protocol.

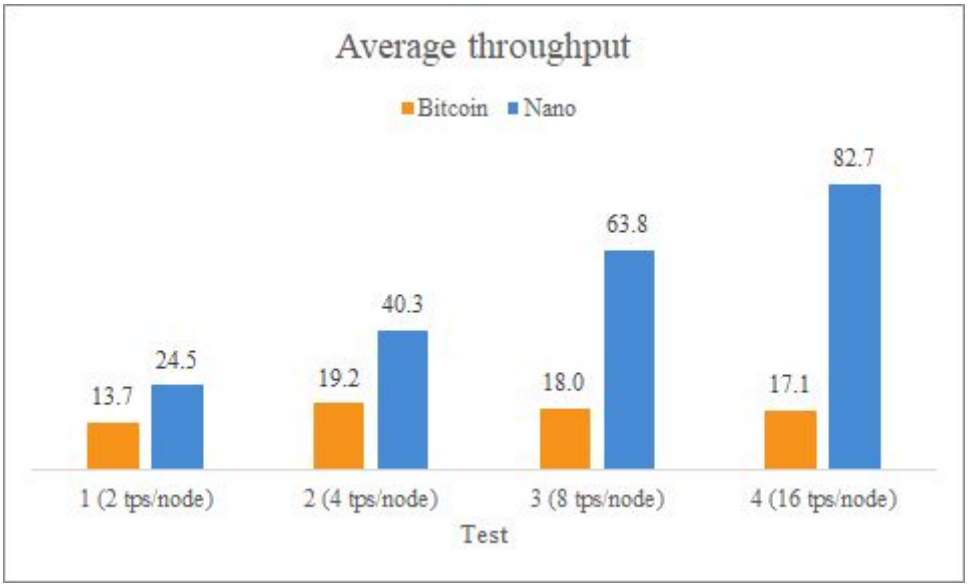


Graph 3. Average throughput (confirmed tps) for both protocols at each iteration of nodes, sending 2 tps from every node.

For Bitcoin, there was an increase in throughput throughout the first and second test, as seen in graph 3 and annex 4, but this was not the case in the third and fourth test, as presented in annex 5 and 6. This suggests that Bitcoin can not scale in throughput when the load of the network increases and resources are added to it.

For Nano, we saw that the throughput increased exponentially with the addition of nodes in all of the tests. However, for every test, where the number of tps sent from each node increases, we saw that the actual throughput moved further away from the expected throughput. For example, when sending 16 tps from each node in the fourth test, as presented in annex 6, the expected throughput at 16 nodes is $16 \cdot 16 = 256$ confirmed tps but it only reaches 174 confirmed tps. This is, again, probably caused by the amount of computational power required from each node, which increases when the number of tps sent from each node increases.

In graph 4, the results of how the average throughput was affected when increasing the number of tps that were sent from every node are presented and compared between the Bitcoin and the Nano protocol.



Graph 4. Average throughput (confirmed tps) for both protocols in every test.

For Bitcoin, we saw that the average throughput did not change much between the tests and the highest average was achieved in the second test with 19.2 confirmed tps. As the throughput is lower in the third and fourth test, even though the tps that were sent from every node was higher, it indicates that Bitcoin can not scale.

For Nano, there was a close to linear increase in average throughput between all of the tests which suggests that Nano is capable of scaling linearly in throughput.

To conclude the findings, we saw that Bitcoin's protocol, just as with the latency, did not have the ability to scale in throughput, neither when adding resources to the network nor increasing the load of the network. In Nano however, there was an exponential increase in throughput when adding resources to the network and a linear increase when increasing the load of the network, suggesting that Nano's protocol scales well in both cases.

5.3 Research Question 3 - Technological differences

RQ3: "What technological differences, that have an impact on the scalability in terms of latency and throughput, are there between the Bitcoin and Nano protocols?"

Based on the results from the experiment we found that the Nano protocol is very much capable of scaling compared to Bitcoin's protocol. The reason they are scaling differently could be that they differ in how transactions are handled, which is presented in the literature review. As said by Satoshi Nakamoto [1], a transaction in the Bitcoin protocol is broadcasted to every node in the network and when the block, in which the transaction has been recorded, has been added to the blockchain, the transactions is confirmed. In the Nano protocol, transactions can be sent and confirmed asynchronously in the network according to Colin LeMahieu [8]. This is possible due to the block-lattice structure used in Nano where each node has its own blockchain, called account-chain, instead of one global data structure like the blockchain in Bitcoin. The account-chain contains the transactions history and can only be updated by the owner of the account.

In the experiment we relaxed the block interval in the Bitcoin protocol by making it 10 times lower than the block interval in the real Bitcoin implementation and thus we expected the limitation in throughput to be 10 times higher, i.e. 70 confirmed tps. What we found was that the throughput was not limited at seven tps which suggests that the block interval affects the scalability. This is conforming with what Sneha Goswami [4] said about the effects of the block interval, which is found in the literature review.

Another thing that we found in the Nano protocol was that the nodes did not manage to send all transactions as the number of tps sent from every node increased. This indicates that the PoW required to send and receive a transaction in Nano's protocol, which was mentioned by Colin LeMahieu [8] and can be found in the literature review, affects the scalability.

7 Conclusion

We have done research on which of the two protocols, Bitcoin and Nano, that offers better scalability in terms of throughput and latency, as well as what technological differences they have which affect these scalability aspects. By conducting an experiment, where tests were performed on private Bitcoin and Nano networks, data was obtained which were analysed and compared to the results from the literature review.

The real Bitcoin network has limitations today because of the block size and block interval. To see if there are other limitations, the block interval was modified to be ten times faster in the experiments conducted. What we found was that the Bitcoin protocol is not able to scale in either throughput or latency, even though relaxing the limitation. We also found that latency has a direct relation to throughput and Bitcoin's protocol has a limitation to how much throughput it can handle. Nano however, was able to scale in throughput but not as well in latency, according to our collected data. Based on these results we answer the research questions in the section below.

RQ1: Which protocol offer better scalability in terms of latency, Bitcoin's or Nano's?
In the Bitcoin protocol we saw that the latency was not able to scale when either adding resources to the network or increasing the load of every node in the network. When increasing the load of every node in Nano's protocol the latency did not scale either, but when adding resources to the network it did. Based on this, the Nano protocol scales better than the Bitcoin protocol when it comes to latency.

RQ2: Which protocol offer better scalability in terms of throughput, Bitcoin's or Nano's?
The throughput was not able to scale in the Bitcoin protocol when either adding resources to the network or increasing the load of every node in the network. In the Nano protocol, however, we saw that the throughput was capable of scaling in both cases. Based on this, the Nano protocol scales better than the Bitcoin protocol when it comes to throughput.

RQ3: What technological differences, that have an impact on the scalability in terms of latency and throughput, are there between the Bitcoin and Nano protocols?
First off, as Nano's protocol scales better in both latency and throughput, the way the protocols handle transactions seem to be the reason as to why this is the case. As found in the literature review, transactions in the Bitcoin protocol are recorded in a block and added to the blockchain, a global data structure, when a node has solved a PoW. Instead of a global data structure, Nano's protocol uses a block-lattice structure where each node has its own blockchain in which transactions are recorded. This makes it possible to send and receive transactions asynchronously in the network Secondly, by relaxing the block interval in Bitcoin's protocol we saw that the throughput was higher than the hard-coded limit in the Bitcoin implementation, indicating that it limits the scalability. We also found that the PoW in Nano's protocol limits the number of tps that can be sent from a node, thus affecting the scalability.

8 Future Work

Since the popularity of cryptocurrencies increases, more research on scalability is required. As a follow-up to this work regarding the Bitcoin protocol, more experiments can be run with different values on the parameters block interval and block size. Regarding the Nano protocol, the experiments can be run with more than 16 nodes, which were used in the conducted experiment, in the network to find out what the capacity is for the throughput and if there is any other bottlenecks regarding the network. There is also the possibility to combine these two protocols based on what we found to create a more scalable protocol.

9 References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. [Online] Available: https://bitcoin.org/bitcoin.pdf

[2] Satoshi Nakamoto, “Bitcoin v0.1 released” , 2009. [Online] Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

[3] Jing Chen, Silvio Micali, “ALGORAND”. [Online] Available: https://arxiv.org/pdf/1607.01341.pdf

[4] Sneha Goswami, “Scalability Analysis of Blockchains Through Blockchain Simulation”, 2017. [Online] Available: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3979&context=theses dissertations

[5] Coinmarketcap, “Bitcoin - BTC”. [Online] Available: https://coinmarketcap.com/currencies/bitcoin/

[6] Alex de Vries, “Bitcoin’s growing energy problem”, 2018. https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6

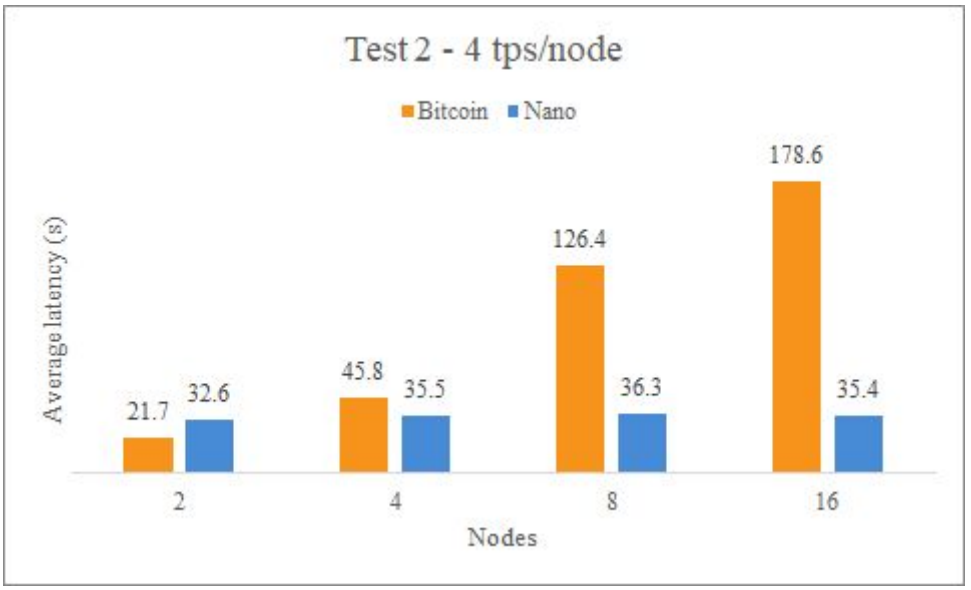
[7] Joseph Poon, Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”, 2016. [Online] Available: https://lightning.network/lightning-network-paper.pdf

[8] Colin LeMahieu, “Nano: A Feeless Distributed Cryptocurrency Network”. [Online] Available: https://nano.org/en/whitepaper

[9] Marit Rudlang , “Comparative Analysis of Bitcoin and Ethereum”, 2017. [Online] Available: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2451325/17050_FULLTEXT.pdf?sequence=1

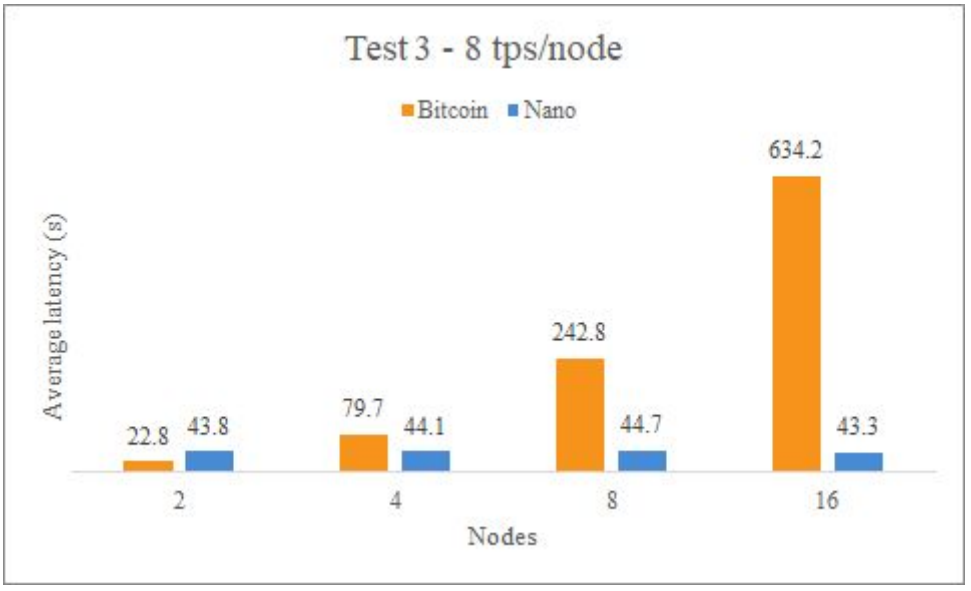
10 Annexes

Annex 1



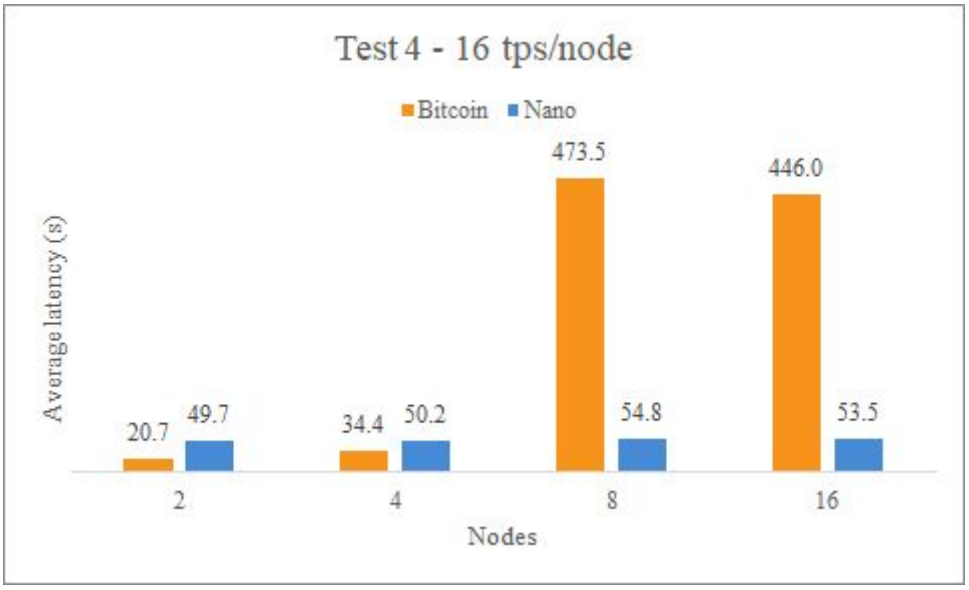
Average latency, in seconds, for both protocols at each iteration of nodes, sending 4 tps from every node.

Annex 2



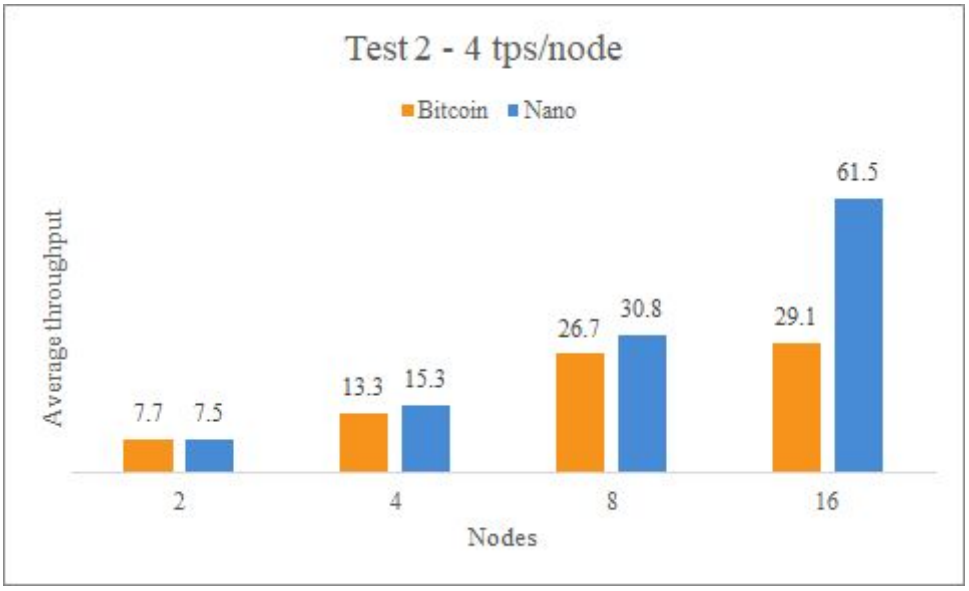
Average latency, in seconds, for both protocols at each iteration of nodes, sending 8 tps from every node.

Annex 3



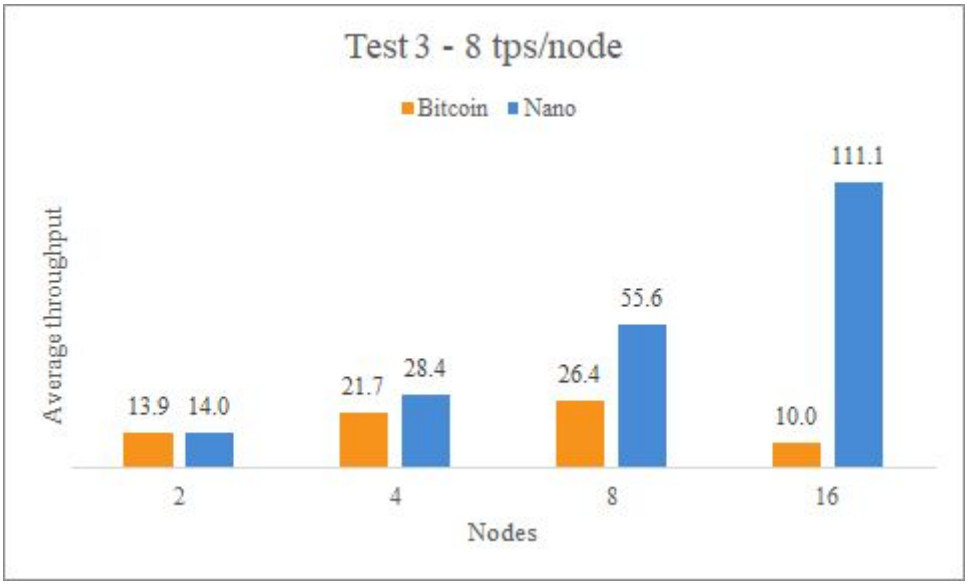
Average latency, in seconds, for both protocols at each iteration of nodes, sending 16 tps from every node.

Annex 4



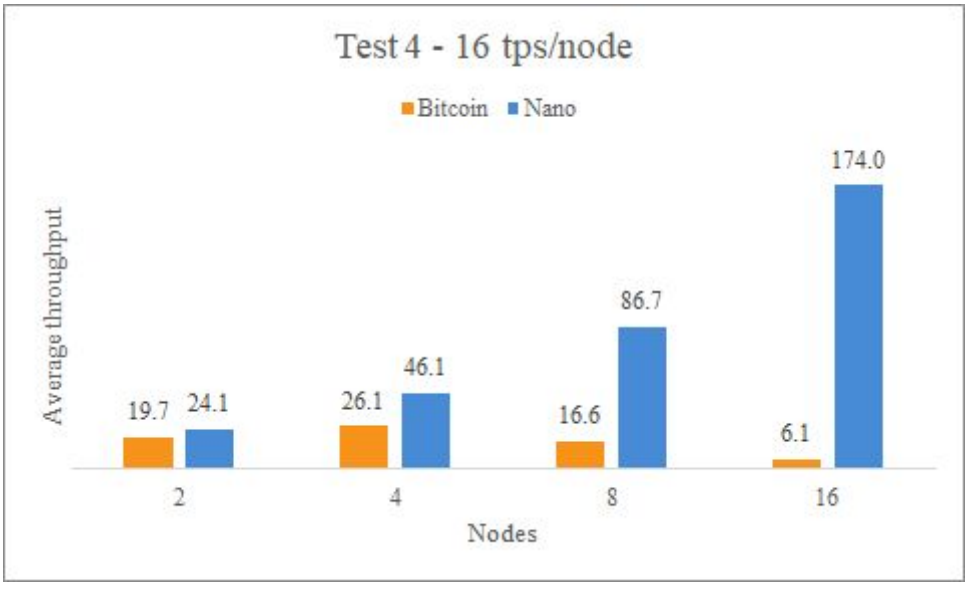
Average throughput (confirmed tps) for both protocols at each iteration of nodes, sending 4 tps from every node.

Annex 5



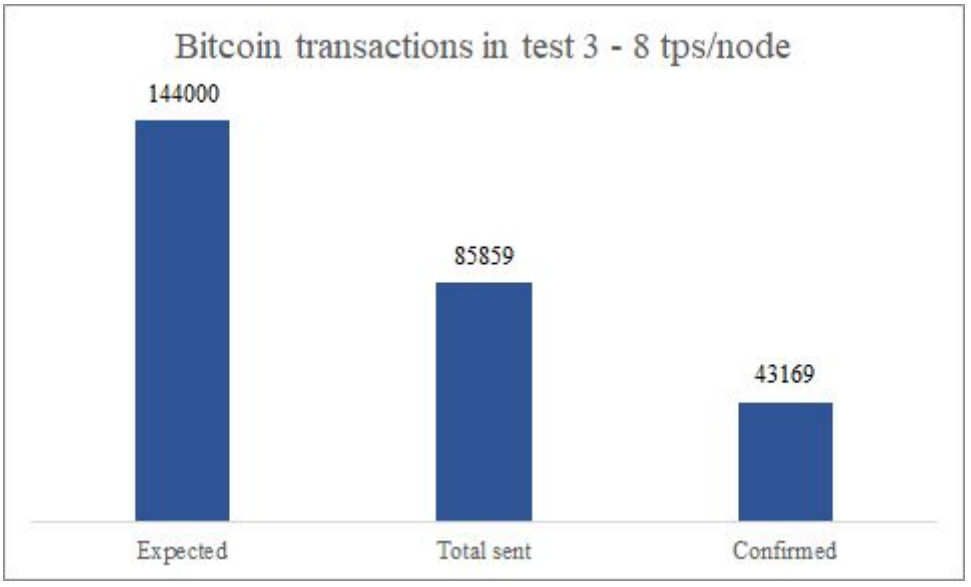
Average throughput (confirmed tps) for both protocols at each iteration of nodes, sending 8 tps from every node.

Annex 6



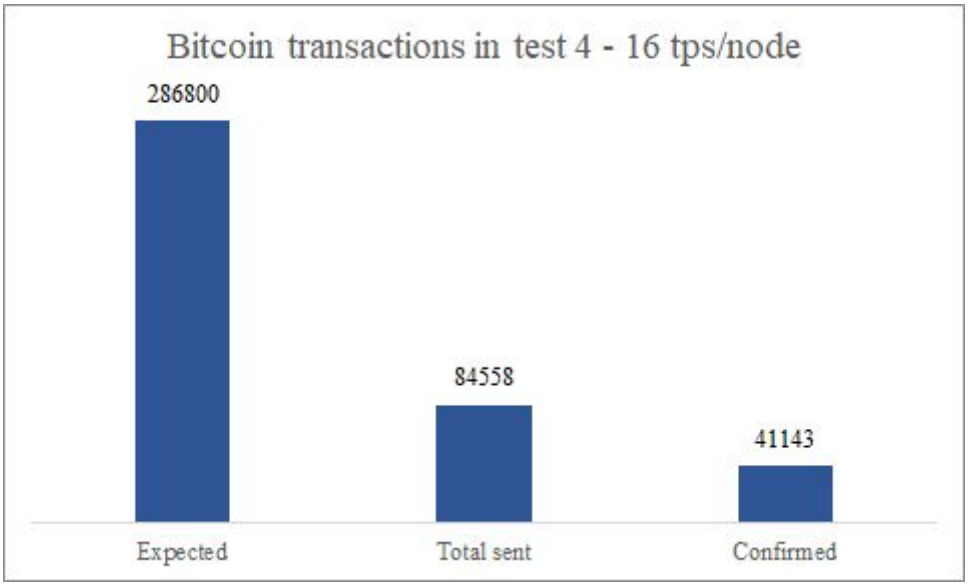
Average throughput (confirmed tps) for both protocols at each iteration of nodes, sending 16 tps from every node.

Annex 7



The number of transactions that were expected to be sent, were sent and were confirmed, sending 8 tps from each node.

Annex 8



The number of transactions that were expected to be sent, were sent and were confirmed, sending 16 tps from each node.