Proof of Bitcoin Node
A Mechanism for a Bitcoin Full Node Incentives & Bitcoin Mining Rewards Program

Ahmed Zsales, Daniel Ames, Georgem, Chaositech, WoodenBush, Coins101

October 2015

Abstract

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of Bitcoins is carried out collectively by the network using nodes which are the backbone of the system. Node numbers have been steadily falling at a time when transactions and the numbers of users are increasing. To reverse the decline and incentivize the creation of many thousands of nodes, we put forward a series of recommendations from simple communication strategies to creating a second tier block chain network to reward full node operators and Bitcoin miners in order to secure the Bitcoin network for the global user base, in particular mobile users in developing countries with little financial or internet infrastructures.
“If you can keep a node running that accepts incoming connections, you'll really be helping the network a lot. Port 8333 on your firewall needs to be open to receive incoming connections.”

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin v0.1 released
Newsgroups: gmane.comp.encryption.general
Date: 2009-01-08 19:27:40 GMT

1 http://article.gmane.org/gmane.comp.encryption.general/12776/match=
Contents

1. Introduction............................................................................................................................ 4
2. Node count history.................................................................................................................. 6
3. Types and functions of Bitcoin nodes.................................................................................. 9
4. Transactions conducted by nodes .......................................................................................... 16
5. Bitcoin popularity and transaction processing...................................................................... 17
6. Costs of hosting full nodes ................................................................................................... 21
7. Implications of increased block sizes.................................................................................... 26
8. Moore’s Law .......................................................................................................................... 32
9. Bitcoin incentive programs .................................................................................................... 34
10. Incentives: lessons from alternative cryptocurrencies....................................................... 40
11. Bitcoin Full Node Incentives & Recommendations.............................................................. 49
12. Conclusion........................................................................................................................ 55
1. Introduction

Bitcoin is able to operate as a trusted global currency without any central authority or control.

To achieve this, people and businesses connect to each other through a decentralized network, known as a peer-to-peer (P2P) network. Each individual or business that is part of the network runs a program and each program is called a ‘node’.

The Bitcoin network has different types of nodes. The most important type that supports and protects the network is a full Bitcoin node. These full nodes are used by individuals and businesses as their wallet to store, send and receive Bitcoins.

In addition to being a wallet, full nodes contain a complete history of all transactions on the entire Bitcoin network. On its creation, one of the major problems that bitcoin solved was a method for enabling a global decentralized database; and as a P2P network, full nodes continuously synchronise so they all contain a record of who owns what.

The other major problem that bitcoin solved was a method for verifying how to trust the data that goes into full nodes. This is enabled through processing transactions on the bitcoin network by computers performing calculations, called mining, which validates the data that gets sent to full nodes.

This store of data is the Bitcoin ledger system which is simply called the block chain, because the ledger is made up from blocks of data in an ever growing chain.

*The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.*

*The block chain provides...an ordered and timestamped record of transactions. This system is used to protect against double spending and modification of previous transaction records.*

The size of a Bitcoin full node is currently around 45GB. With the current internet infrastructure, especially in developing regions around the world, it is the ever growing size of a full node and the amount of data that each one sends and receives every month that makes running a full node a problem for many people and therefore a potential problem for the health of the network.

---

2 bitcoin.org/en/how-it-works, June 2015
3 bitcoin.org/en/developer-guide#block-chain
Since the introduction of Bitcoin in 2009, the number of full nodes grew to an estimated 10,000 to 14,000. These numbers have been steadily declining and the Bitcoin network currently has an estimated 6,000 full nodes. This reduced level is capable of supporting the current network, but it is the declining trend in the number of full nodes, during a time of exceptional growth in Bitcoin popularity, that is of concern and the focus of this paper.

There have been attempts to give incentives to individuals and businesses to operate full nodes, with limited success. Here we explore factors that impact full nodes, altruistic attempts to increase the number of full nodes, as well as exploring possible longer-term commercial incentive solutions that could be self-sustaining.

Sections 2-9 of this paper provide a review of the background and context to the issues under examination. The remaining sections 10-11 of the paper look at recommendations and potential solutions to increasing the numbers of Bitcoin full nodes and sustaining the increased numbers of nodes, in addition to funding Bitcoin miners, over the life of Bitcoin.

For the most part, this white paper is intentionally written in non-technical language as the issues that require to be addressed cut across everyone who uses Bitcoin.
2. Node count history

A node refers to any computer that is running the Bitcoin client software and participating in the peer-to-peer network by relaying transactions and blocks.

Bitnodes, a project funded by the Bitcoin Foundation, has kept track of full node figures since its launch in 2013. In June 2015, Bitnodes introduced a 12 month full node history chart. During the 12 months to June 2015, the numbers of full nodes declined 21% to around 5,900 with an average node count during the year of 6,700 nodes.

![Node count chart]

A variety of published estimates from Bitnodes since its launch suggests there were more than 387,000 nodes in May 2013, with China accounting for 22% or 85,000 nodes.4

Other estimates from Bitnodes reported by the press indicate that there were 124,000 full nodes in November 20135, with China accounting for 14,100 nodes or 11.3%.

A review of these reported node statistics by the top 10 countries shows a marked change in both the total numbers of nodes and their distribution by country.

---

4 bitnodes.io - Deutschland No 3!, bitcointalk.org, 19 May, 2013
5 Why China is Leading the Global Rise of Bitcoin, Coindesk, 18 November, 2013
“The early December 2013 network snapshots, i.e. with over 100k nodes, are not valid as the crawler at that time took several hours just to complete one full network snapshot and it includes all nodes from addr responses which can be faked or likely stale.”

The fall in the numbers of nodes, in particular the June 2015 numbers for China, has been attributed by some to substantial swings in the price of Bitcoin, which itself was influenced by the Chinese authorities placing heavy restrictions on regulated financial entities preventing them from dealing with any aspect of Bitcoin. Some have even speculated that China’s controls over the internet have managed to block nodes receiving data, except in isolated cases to enable large mining operations and mining pools to continue trading.

This reduction in the number of full nodes is also notable when considered in the context of a continued increase in the number of transactions on the Bitcoin network; from around 40,000 per day in June 2013 to over 100,000 per day in June 2015^6. This rise in the numbers of transactions has seen an increase in the size of the Bitcoin block chain, in addition to price swings, there have been many common reasons given for not running a full node:

- Increased bandwidth demands placed on home computers and internet connections
- Increased competition for mining
- Increased time and cost requirements and the lack of incentives

Node statistics are difficult to quantify and there are many discrepancies in published and reported figures. This can be due to the daily swings in nodes being turned on and off by individual users and businesses for any number of reasons from individuals at home turning off their computers at night, to businesses carrying out maintenance on their equipment.
While the figures for node numbers above 10,000 may be challenged, there is some consensus that node numbers have dropped from between 10,000 to 13,000\(^7\) down to around 6,000 between March 2014 and June 2015, including a noticeable drop of 2,000 nodes between March 2014 and May 2014. This likely coincides with the Chinese government limiting Bitcoin access to the established and regulated financial system during that period.

While 6,000 nodes can adequately handle the Bitcoin network in its current state, the node numbers are showing a declining pattern at a time when the number of users and the overall levels of transactions are showing a substantial increase.

Furthermore, it is not known whether these falling numbers will have a regional impact on the future growth prospects of Bitcoin as mobile Bitcoin users in developing countries, for example, will have a greater reliance on full bitcoin node users in predominantly first world countries to serve them with data from the Bitcoin network.

---

\(^7\) Daniel Cawrey, What Are Bitcoin Nodes and Why Do We Need Them?; Coindesk.com, 9 May 2014
3. Types and functions of Bitcoin nodes

The Bitcoin community website defines a full node as follows:

“A full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes.”  

Every transaction that has ever taken place or will ever take place on the Bitcoin network is stored on full Bitcoin nodes. This is how the Bitcoin network maintains a full ledger of all transactions.

From an everyday user’s perspective, a full node is simply their Bitcoin wallet. However, in recent releases of the Bitcoin client software, the wallet feature can be disabled leave the software to act mainly as a back-up of the Bitcoin ledger.

In order to synchronise the full Bitcoin ledger, the entire ledger, currently more than 70 million transactions, has to be downloaded, checked and ordered. This can take a significant amount of time, between one to three days depending on internet speeds and how long the user’s computer takes to process the ledger into its correct order.

Bitcoin full nodes with the wallet feature enabled are considered the most private and secure way for users to access and use Bitcoin. By downloading all of the historical transaction data that has ever taken place on the Bitcoin network, the security tools inside official Bitcoin clients ensures users always have the correct ledger chain and the software also ensure users are not connecting to a rogue or corrupted ledger chain.

Lightweight bitcoin clients differ in that the block chain is not stored on your computer, so they rely on a server to receive and send transactions. Users of full nodes will also be sending out details of the ledger to other nodes and the various types of lightweight mobile wallets using the network. Having lots of Bitcoin full nodes means that there is always a copy of the entire Bitcoin ledger available, so nodes can come and go and the nature of the network means that multiple copies of the ledger are always available and being maintained.

1.1. Full node users

Bitcoin was launched in 2009. At that time, everyone who used Bitcoin used a full node as that was the only option.

8 Bitcoin.org, Running A Full Node
As Bitcoin has grown in popularity new wallets and wallet services have been independently developed by individuals with technical expertise and also businesses wishing to offer commercial wallet and currency exchange services to Bitcoin users. Some of these commercial businesses even offer faster connections to their own full nodes, with a few calling their nodes ‘super nodes’ allowing mobile wallets they produce to synchronise very quickly.

Bitcoin node users are broadly split into these groups:

- Miners
- Individual users
- Merchants
- Businesses
- Commercial block chain analysts
- Software developers
- Governments, government agencies and regulators

Statistics on Bitcoin users are difficult to obtain due to the P2P decentralized nature of the network. Between November 2009 and June 2015, the Bitcoin client software was downloaded over 5.5m times\(^9\).

One of the main reasons often cited for the decline in the numbers of full nodes was the introduction of specialised Bitcoin transaction processing equipment. This processing equipment is used to ‘mine’ data on the Bitcoin network and in return these miners compete for incentive rewards from the network. These rewards are currently 25 BTC or roughly $6,000 at time of writing, made up from brand new Bitcoins that are ‘minted’ into the network every 10 minutes.

This Bitcoin mining process will continue until 21 million Bitcoins are produced, at which time no new Bitcoins will be created. At this point miners will have to sustain their operations by processing transactions on the Bitcoin network and earning income fees for processing transactions.

In practical terms this means that when people send each other Bitcoins, the miners check the historical records contained in the block chain to ensure that the money the users is spending hasn’t been spent before. As part of this step, the miners also check if the person sending the Bitcoins, without knowing who the senders or receivers are, actually owns the Bitcoins he or she is sending.

Each of these transactions is validated and then inserted into a new block, usually with many other transactions, and then this block becomes part of the historical block chain

---

\(^9\) sourceforge.net/projects/bitcoin/files/stats/map, June 2015
ledger. Full node owners then receive these blocks and they are added to the other blocks in the block chain contained on their full node.

During the first few years of Bitcoins existence, people who wanted to earn rewards from processing Bitcoin transactions could do so using an ordinary home computer running a Bitcoin node.

As can be seen from one of the first Bitcoin wallets, the pickaxe symbols indicate the wallet is mining and receiving rewards for being part of the mining process. As can also be seen, this node is receiving transactions, in this instance the first ever Bitcoin transaction sent by Bitcoin inventor, Satoshi Nakamoto, to one of the first Bitcoin cryptographers and software developers Hal Finney10 who helped to improve the software before it was launched.

As the value of Bitcoin increased and more people wanted to earn these rewards, people began to create specialist mining software and businesses began to invest in ever faster processing equipment, much of which is now contained in industrial buildings and data centres.

Competing with these professional mining operations makes it less attractive for individuals at home to compete for the rewards without having to invest themselves in faster equipment and incurring significant additional electricity and cooling system costs to operate the specialist equipment.

Based on today’s Bitcoin prices, the mining rewards allocated to the above home computer during the week shown, would be worth in the region of $150,000. A home computer mining today would be unlikely to earn $0.50 in the same period of time.

The Bitcoin wallet can still be used for mining, but the emergence of specialist software enabling people to run many of the new specialist mining equipment with just one Bitcoin wallet makes it unlikely for individuals using their home computer to ever see a return on investment.

In a relatively short period of time, Bitcoin mining moved from a network largely made up of enthusiasts using ordinary home computers in 2009/10; to predominantly pooled mining in 2011/2012 using a mixture of equipment including graphics cards and small scale specialist miners; to industrial scale data processing operations and pooled mining resources by 2013/2014.

As this shift to industrialisation and centralisation was taking place (for example, by 2015 five Chinese ‘mining pools’ account for over 60% of the transaction processing power running the Bitcoin network) fewer full nodes were being used.

1.2. Multibit wallets

As the Bitcoin network grows and more transactions take place, the storage requirements of full nodes grows correspondingly. A full node currently has between 40GB to 45GB of data and requires a complete synchronisation with the entire Bitcoin network of historical transactions before it can be used.

The ever growing size of the Bitcoin network and the time it takes to synchronise with the network before a node can be used as a wallet has led to the development of lightweight wallets that allow users to download a very small fraction of the Bitcoin network.

Multibit is an example of a popular lightweight wallet that loads just enough data that relates to a particular users transactions. As such it can be used within minutes of being downloaded.

MultiBit and wallets like it are called "SPV wallets" or ‘simplified payment verification’ wallets. They are capable of processing thousands of blocks per second and due to their speed they are the recommended option for brand new users to avoid them getting frustrated with waiting days for the Bitcoin client to download and synchronise.

For these lightweight wallets to work, they must connect to full Bitcoin nodes from which they obtain basic details about the Bitcoin ledger. In particular they access the index

---

11 8btc_news, Why upgrade to 8MB but not 20MB?, 12 June 2015; redd.it/r/Bitcoin/comments/3a0n4m/why_upgrade_to_8mb_but_not_20mb
header ordering system for each block that the ledger uses, which provides each lightweight wallet with high level details about each of the user’s own transactions.

So while lightweight wallets provide easy access to the Bitcoin network, the more popular they become, the more demands they place on full nodes, while also making it less attractive to run a full node.

1.3. Mobile wallets

The increasing popularity of smartphones continues to have a material impact on general online habits around the world. Having mobile Bitcoin wallets is helping to fuel the growth of Bitcoin, especially as running a full node is becoming increasingly problematic in some regions with low penetration of computers and slow internet speeds.

Smartphones allow individuals to use Bitcoin through a growing selection of Apps, primarily on the Android operating system, but with Apple Apps showing some signs of growth as well.

Mobile wallets share similar features to lightweight wallets. These Apps facilitate the download of a sub-set of transactions rather than downloading the full Bitcoin ledger. Full nodes are therefore essential for supporting the growth of Bitcoin through the popularity of these mobile wallets.

Mobile wallets are also seen as essential to facilitating access to finance and cheap remittances in areas of the world with low internet penetration and limited options for accessing financial systems. Many parts of Africa, Asia and South America could benefit from full nodes in their regions to encourage and support the growth of mobile wallets.

Mobile wallets are very convenient for users, but they are considered less secure than Bitcoin wallets running from full nodes.

This is in part due to the software used to operate mobile wallets being less robust when compared to full Bitcoin node wallets. In addition, these types of wallets need to trust that the information being given to them is correct as they do not hold their own full copy of the Bitcoin ledger to check against.

1.4. Online wallets

There are many online wallet services. Blockchain.info has one of the most popular online wallet services in the world. User statistics from its website show there are 3.5m Bitcoin wallet user accounts on its service.\(^\text{12}\)

---

\(^\text{12}\) block chain.info/charts, June 2015
Another service, Coinbase.com, claims to have over 2.3m user accounts with over 2.9m bitcoin wallets\textsuperscript{13}.

Online wallets enable users to avoid downloading any form of Bitcoin programs onto their computer. This enables them to access their Bitcoin funds anywhere they can get an internet connection.

These online wallets typically use an internal accounting system to keep track of Bitcoins and some allow users to transact with each other or with currency exchange services provided by the service provider.

These wallet services typically do not see transactions conducted on their systems ending up on the Bitcoin block chain.

1.5. Full node distribution methods

There are several ways in which people can obtain the services of a Bitcoin full node client. However, as merchants increase and promote their services, users searching for Bitcoin wallets will be less likely to be directed to places where they can obtain a trustworthy full node client.

Full node clients can be obtained from Bitcoin community orientated places, including the Bitcoin Foundation website or websites supported by the foundation. However, it is often difficult to obtain a Bitcoin wallet as a new Bitcoin user without being first directed to popular commercially driven online wallet services or mobile apps.

1.6. Synchronisation times

With the Bitcoin ledger at around 45GB, prior to Bitcoin version 0.10, the time it took to download a full Bitcoin node was between 2-3 days, depending on the quality of the internet connection being used.

As of version 0.11, a Bitcoin node can download the essential part of the block chain, the header indexing information contained by each block in the block chain, in around 2-6 hours.

This means that a Bitcoin node can be used as a wallet in a relatively short space of time. As the wallet is being used, the rest of the block chain database continues to be downloaded over a longer period of time.

Downloading the block chain is only one aspect of the process to becoming part of the Bitcoin network by running a full node. As the blocks are loaded into the Bitcoin software, the ledger history is being checked and validated. This means that while

\textsuperscript{13} coinbase.com/about, June 2015
internet speeds to download the block chain are an important factor, the speed of the computer being used by the Bitcoin client software is also a factor in how long it takes to fully synchronise a node.

1.7. Miners and full nodes

The process of verifying transactions on the Bitcoin network is carried out by ‘miners’ who process calculations in competition with each other to be the first to find the answer to a mathematical problem which earns them a reward.

At current prices, the rewards open to all miners are approximately $6,000 USD worth of Bitcoins released every 10 minutes, which equates to approximately $320m each year.

Mining is a distributed consensus system that is used to confirm waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system.

To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain.

This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.14

Before the introduction of specialist mining equipment, individuals used Bitcoin full nodes to mine transactions as the Bitcoin client contains all the software required to do so.

However, now that mining equipment is purpose built, miners only require an address that they can send their mining rewards to, which means that they no longer need a Bitcoin client, despite recommendations from the Bitcoin technical community that they operate one for their own financial security.

As mining equipment gets faster and more specialised, the mining process will continue its current path of becoming concentrated into pockets of high end facilities and data centres reducing further the numbers of smaller miners. This is likely lead to further reductions in the numbers of full nodes.

14 bitcoin.org/en/how-it-works, June 2015
4. Transactions conducted by nodes

A Bitcoin full node was set-up on an Amazon cloud environment to see how many transactions a full node would process. This test provided a very robust and professionally managed environment with very little to no downtime and very high bandwidth.

Between 2 June 2015 and 9 June 2015, this test node relayed:¹⁵

- 1,925 BTC, or $443,000 worth of transactions
- The largest transaction relayed was 534 BTC, around $123,000
- The smallest transaction relayed was 0.00050787 BTC, around $0.12
- The average transaction relayed was 15.5 BTC, around $3,600

While extrapolations are difficult to make given the number of variables that could impact the outcome, a simple extrapolation of these results show that one full node could relay between $1.3m to $23m of transactions over a 12 month period.

Applied across the 6,000 nodes currently making up the Bitcoin network, the network could relay over 600m Bitcoins or $138bn in transactions each year, before factoring the demands of an ever growing number of users on the network.

It is worth noting that Bitcoin nodes do not relay every transaction on the Bitcoin network. For example, businesses that handle high volumes of transactions, such as exchanges, typically process transactions using their own internal databases, ledgers and settlement systems. Users wanting to move funds out of these closed systems, such as exchanges, would then come into contact with the Bitcoin network to handle their funds.

---

¹⁵ 52.16.127.223:8333 /Satoshi:0.10.1
5. Bitcoin popularity and transaction processing

As Bitcoin has increased in popularity, the numbers of transactions has been steadily increasing and with the current software architecture it is expected to reach a point where the network is approaching capacity.

Analysis by Tradeblock\textsuperscript{16}, a Bitcoin technology services and advisory company, suggests that the Bitcoin network will reach capacity by summer 2016 when growth in transactions will require an increase in transaction handling as waiting times will exceed 1 block, from the current 0.1 block wait time.

Updates to the network to handle more transactions are technically easy to implement, but as they require the majority of all users to make the update, including miners and businesses, there are many inherent risks in making the upgrade.

Should network capacity be reached, users would have to wait longer and longer for their transactions to be processed, potentially discouraging people from using Bitcoin.

Users can pay fees to the network miners to give their transactions priority over other transactions as miners can choose to process those paying the most to get ahead of the processing queue.

This screen grab from a Bitcoin node in June 2015 gives an indication of the fees and time-scales to process transactions.\textsuperscript{17}

\textsuperscript{17} Theymos; 23 June 2015; reddit.com/r/Bitcoin/comments/3apgkm/what_the_coinwalle...
However, where the Bitcoin network is at capacity, even the payment of fees does not ensure speedy delivery of transactions. This could, for instance, lead to an auctioning system encouraging larger transactions making fees increasingly expensive, but not necessarily prohibitive, for micro-transactions.

As can be seen from this transaction processing chart\(^\text{18}\), most people that want their transactions processed will typically opt for the fastest times.

![Transaction Processing Chart](https://bitcoincore.org/smartfee/fee_graph.html)

As fees increase, it can become very profitable for the miners encouraging them to invest more in mining infrastructure, making the Bitcoin network even more secure than it already is.

However, this could also encourage more industrial mining operations run by relatively few organisations causing some to fear the network becoming centralized and liable to governments interfering through regulations and control orders.

While the fees to get transactions processed faster can still be competitive compared to services such as credit cards or PayPal, it is the impact on processing waiting times that

---

18 [https://bitcoincore.org/smartfee/fee_graph.html](https://bitcoincore.org/smartfee/fee_graph.html)
could be the bigger issue for the future prospects of Bitcoin and its mainstream adoption battle.

A system at capacity where there is no guarantee that a payment will be processed within a few minutes or hours also means that using Bitcoin in a retail store is impractical.

Bitcoin’s ledger system is made from a series of blocks, where each block is made from a number of transactions. Each transaction is a piece of data. Currently, the blocks used in the Bitcoin network have a maximum capacity of 1mb of data.

The Bitcoin network processes blocks every 10 minutes, which means that there is a maximum number of transactions that the network can process every day. At present the Bitcoin network can process 6 blocks per hour and it is therefore limited to around 7 transactions per second due to the 1mb block size limit.19

By contrast PayPal processes around 115 transactions per second, while the Visa credit card network handles over 2,000 transactions per second20. In order for Bitcoin to handle that number of transactions, the blocks in the block chain ledger need to be around 8mb each instead of the current 1mb.

It is possible for the block sizes within the Bitcoin ledger system to be increased to handle enough transactions for the entire world’s population. But making these changes enables the network to potentially introduce more data into Bitcoin network, requiring full nodes to have greater storage for the block chain and extra capacity to handle greater transaction numbers.

1.8. Side chains and lightning networks

In order to process more transactions and introduce new Bitcoin related services, enabling Bitcoin to scale and facilitate many different types of activities, for example contracts, technical proposals have been put forward for side chain21 networks and lightning networks22.

Sidechains are block chains that are interoperable with each other and with Bitcoin, avoiding liquidity shortages, market fluctuations, fragmentation, security breaches and outright fraud associated with alternative crypto-currencies.23

Lightning networks are expected to be tools for enabling micro transactions to happen off the Bitcoin block chain on a variety of channels with only some of the transaction data

---

19 https://en.bitcoin.it/wiki/Scalability
20 https://en.bitcoin.it/wiki/Scalability
22 Poon, J and Dryja, Thaddeus; The Bitcoin Lightning Network, DRAFT v.0.5
23 blockstream.com, June 2015
being required to enter the block chain. Some expect that the majority of micro transactions by volume would be handled by Lighting networks enabling Bitcoin to scale to billions of transactions each day.

While these new innovations have the potential to enable Bitcoin to scale without adding significant data burdens on full nodes, the technology behind these proposals is not yet available.

Bitcoin is likely to reach capacity before these innovations are released, tested and implemented, so it is likely that significant data increases around the Bitcoin network will be seen before Side chains and lightning networks are introduced.

This does, however, raise the prospect that future scalability problems impacting full nodes may not be as pronounced as some might consider. It also raises the prospect that extra transaction layers could reduce the amount of fees going to miners.
6. Costs of hosting full nodes

A Bitcoin node storing a complete copy of the block chain requires a lot of hardware memory space.

System requirements provided by a community supported project, Bitcoin.org, gives the recommended requirements for operating a full node24:

- Desktop or laptop hardware running recent versions of Windows, Mac OS X, or Linux.
- 50 gigabytes of free disk space
- 2 gigabytes of memory (RAM)
- A broadband Internet connection with upload speeds of at least 400 kilobits (50 kilobytes) per second
- An unmetered connection, a connection with high upload limits, or a connection you regularly monitor to ensure it doesn’t exceed its upload limits
  - It is common for full nodes on high-speed connections to use 200GB upload or more a month
  - Download usage is around 20GB a month
  - The first time install requires around 30GB-40GB of data to be downloaded
- 6 hours or more a day that your full node can be left running

Nodes running inside people’s homes or those operated by small businesses can typically have limited upload speeds. While it is becoming increasingly common to have very fast download speeds, a typical node will send five to ten times more data than it downloads. This can depend on how many nodes are available to share the data transfers and how many neighbouring nodes are connected to each other, which can typically be up to 40 nodes.

Because of the large amounts of data that can be streamed out from a node to other nodes in the Bitcoin network, user’s broadband routers can suffer from data overload causing buffering to occur. For an ordinary home user, this may interfere with watching HD movies, for example, and so they may decide not to run a full node.

There is some evidence from the daily variations in the numbers of full nodes that people turn off their full nodes for long periods of time. This can be for any number of reasons such as people turning off their computers overnight; turning them off when they are at work; turning them on and off to watch online streaming video content; turning off computers to go on holiday; or a mixture of all of the above.

Countries in developing regions typically have poor internet infrastructure, but these areas are usually in most need of cheap and efficient financial payment systems. These countries would potentially be well served by lightweight or mobile Bitcoin wallets, but as their user numbers grow, more full nodes in developed nations would potentially be required to support these SPV wallets.

### 1.9. Types of full node hosting

If Bitcoin’s software settings were changed to be able to serve 1% of the 7 billion global populations, allowing for two transactions per person per day, the network could produce around 1.7GB of data every 10 minutes (assuming 250 bytes per transaction and 144 blocks per day). This would generate a block chain growing by more than 7 terabytes (TB) each month. With nodes able to send out 10 times more data than they hold, in order to serve the Bitcoin network, full nodes under this scenario could each generate over 70 TB of data bandwidth on the internet each month.

Even at the current data capacity of around 42GB and monthly transfers of over 150GB to 200GB per month, there is a significant burden on networks, processors and storage hardware. When pushed to handle large amounts of data, average systems would likely require constant maintenance and replacement compared to those systems operating under domestic or light commercial loads.

There are different methods to running a Bitcoin node. Examples currently include:

- Desktop or laptop computer
- Raspberry Pi 2
- Specialised low power Bitcoin hardware, e.g. Bitnodes Hardware B1
- Private server hardware equipment
- Cloud based server equipment

### 1.10. VPS hosting

In terms of speed and constant availability of data serving the network, operating cloud based nodes, typically on systems called virtual private servers (VPS), is a more reliable way to run a full node.

---

25 getaddr.bitnodes.io/hardware
This is compared to operating one within a home or small business environment where computers are turned off regularly, there is less data bandwidth and the hardware is less robust.

However, running cloud based nodes, while the preferred option by some, can be very technical.

Gavin Andresen, the Bitcoin Foundation’s former Chief Scientist, indicated a preference for people running full nodes using VPS type services and expressed that people who do not know how to run a full node should not try:

“Most ordinary folks should NOT be running a full node. We need full nodes that are always on, have more than 8 connections (if you have only 8 then you are part of the problem, not part of the solution), and have a high-bandwidth connection to the Internet.

“So: if you've got an extra virtual machine with enough memory in a data centre, then yes, please, run a full node.”

The shift from running nodes at home to running nodes in professionally managed environments is something that has been considered a likely possibility for many years. The creator of Bitcoin, Satoshi Nakamoto, expressed in 2010 that a move to hosted full nodes was likely to happen:

The current system where every user is a network node is not the intended configuration for large scale. That would be like every Usenet user runs their own NNTP server. The design supports letting users just be users. The more burden it is to run a node, the fewer nodes there will be. Those few nodes will be big server farms. The rest will be client nodes that only do transactions and don't generate.

From the initial set-up to regularly checking that a node is operating as normal, hosting a node generally requires some active participation making this type of hosting unsuitable for the general public.

There are many different cloud based virtual private server hosting solutions that range in costs from $5 / month to $50 / month.

These costs can increase substantially if users require services that run on Microsoft Windows operating system as the cost of the operating system (OS) licence is added to the hosting cost. Free Linux operating systems are one of the most popular options for these VPS services, due to the cost savings on OS savings.

26 reddit.com/r/Bitcoin/comments/1scd4z/im_running_a_full_node_and_so_should_you/cdw3lrh?context=3
27 Nakamoto, S; Re: Scalability and transaction rate; 29 July 2010; satoshi.nakamotoinstitute.org/posts/bitcointalk/287/
Some of these service providers operate a cost structure based on the amount of data bandwidth used each month. Other services have tiers of hardware quality and monthly data allowances.

As the demand for cloud services increases, better deals are being offered with some VPS providers offering many terabytes of data transfer or even unmetered data transfers.

VPS operators typically have terms and conditions that prevent Bitcoin software being operated on their systems. There could be any number of reasons for this precedent from historical problems with P2P file sharing software being used to distribute illegal material, to service providers concerned about their hardware being used for mining and causing excessive overheating.

Although VPS services offer higher bandwidth, greater processing capabilities and always on services, the number of VPS providers is small when compared to the preferred outcomes of having a diversified node network with many thousands of nodes.

1.11. Maintaining full nodes

Operating full nodes comes with a requirement to keep the nodes updated.

The Bitcoin Core wallet is regularly updated to incorporate new features and security releases. While many people do update their wallets, not everyone does it at the same time.

The current version is called Bitcoin Core 0.11.0.28

While updating wallets is relatively straightforward, people can and do run into complications. In particular, those with positive wallet balances need to back-up some of the files that hold the details of the account balance and transaction history.

This process can cause security risks as people have been known to store wallet data files in online storage locations and in unsecured locations, where malware has either deleted their files or thieves have been able to steal their data.

Full nodes running zero wallet balances, i.e. with the wallet feature disabled, would be one way to avoid the complications of maintaining and securing funds stored on full nodes.

Users must also be aware that they need to make some changes to their routers, their ‘port’ settings which need to allow connections to and from TCP port 8333 in order for a node to be able to broadcast data out of their network.

While these are minor technical challenges, to the general public these can be unnerving technical barriers.

### 1.12. Impact of internet bandwidth growth and throttling practices by ISPs

Nodes running inside people’s homes or those operated by small business can typically have limited upload speeds as many broadband connections are asynchronous, offering less upload capacity than download capacity. Whilst it is becoming increasingly common to have high download speeds, a typical node will send five to ten times more data than it downloads.

For the majority of people, running a full node will not impact their ability to send emails or access online services. Sending large emails will not be materially impacted, except for people that regularly send large files.

People that synchronise large amounts of data with cloud storage systems, video messaging, VoIP, or those that use Bittorrent file sharing would notice an impact on their upload speeds.

For heavy users of streaming services such as Netflix, YouTube, Amazon, their streaming habits could impact on their total bandwidth consumption, especially those on metered or capped bandwidth plans.

While Bitcoin wallet software operating full nodes does take lower order priority in terms of processing power when people use their computers, people with slower processors may notice an impact when using applications that require a lot of processing power.

Many predict that hardware and bandwidth limitations will be met by technological advancement. While others fear that Bitcoin will either always operate at the margins of technological capabilities as its popularity grows; or commercial entities will emerge to host full nodes as domestic and small business infrastructure fails to keep up with Bitcoin’s support requirements.
7. Implications of increased block sizes

Since its inception, the size of the Bitcoin ledger system, the block chain, has been steadily growing.

The current size of each block in the Bitcoin ledger is 1mb. This allows for around 2,500 transactions to be stored in each block. As the numbers of transactions keep growing, the size of these current blocks will likely need to increase in order to cope with future growth of the network while maintaining reasonable transaction confirmation times.

Several proposals have been suggested from no increase in block sizes to 20mb block sizes, with one of the more popular suggestions being to increase block sizes to 8mb.

Bitcoin Improvement Proposal 100 (BIP100\textsuperscript{29}) is a suggestion by one of the Bitcoin software engineers to increase the block sizes from a fixed limit of 1mb to a flexible system that can be increased in stages as voted upon by miners who are the ones that have to process the data that goes into the blocks.

There will likely be many more proposals before a collective agreement is reached.

If blocks are increased in size, it is likely that the size of the ledger system could increase from around 42GB to 50GB and then to 100GB in the medium-term. The block chain size would continue to grow ever larger for the life of the Bitcoin network, unless changes are made to limit the amount of historical data that was kept.

In the event that consumer internet services do not keep pace with the growing size of the Bitcoin ledger, then miners, various businesses and professional hosting solutions would be required in order to maintain node numbers. Those with substantial Bitcoin holdings would also want to invest in their hardware and bandwidth to run their own full nodes to protect their economic interests.

\textsuperscript{29} Garzik, J; Making Decentralized Economic Policy, June 2015. gtf.org/garzik/bitcoin/BIP100-blocksizechangeproposal.pdf
While consumer internet connections are an important factor to consider, the internet connections available to miners who process Bitcoin transactions are also a consideration.

Many Bitcoin miners are located in developing regions where electricity is cheap as that is one of their single biggest costs. However, fast internet services can be patchy in some of these areas. These remote industrial scale data processing operations can suffer from an inability to communicate with the Bitcoin network fast enough in order to send and receive the data they are seeking to process.

This can cause many problems for them, in particular wasting time and money processing transactions that are not accepted because they took too long to be communicated back to the network, enabling competing miners to earn the rewards for processing the data first.

When situations like this occur, miners and pool operators spend some of their time looking for ways to work around the network’s recommended processes and this increases the risks of problems occurring for them and the network. This is a situation which actually occurred\(^\text{30}\) on 4 July 2015 when part of the network split because a major mining pool operator tried to cut corners by processing only parts of transaction blocks in order to earn more money. The impact being that a global warning had to be issued that some user’s Bitcoin transactions were at risk under certain circumstances, with lightweight and online wallets being particularly vulnerable.

1.13. Pruning the block chain ledger

The very first Bitcoin white paper recognized that the ledger system would continue to grow in size and potentially become unwieldy for a large decentralized network.

> "Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space."\(^\text{31}\)

The major version update for the Bitcoin client which jumped from v.0.10 and to v.0.11 introduced pruning where a full node owner can remove details from older transactions which could eventually see the size of the ledger database reducing to just 1GB in size compared to around 42GB today.

However, a full ledger history will still be required to be maintained on the network. As a consequence, it is expected that the numbers of full nodes that continue to hold a full ledger history will fall significantly while also seeing an increase in the numbers of full nodes that utilize the pruning feature. Few details on pruning are available for review at this time.

---


\(^{31}\) Nakamoto, S; Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org/bitcoin.pdf
1.14. Centralization implications

Bitcoin is a decentralized network without a central controlling entity. The users of Bitcoin are the core elements of the network, provided they operate nodes or there are sufficient numbers of nodes for the network to be able to survive attempts to control it or shut it down.

Where there are too many barriers to operating full nodes, the diversity of the network could potentially be at risk causing centralization points of attack or failure.

Those with vested economic incentives, such as businesses, would potentially continue to support the network, but as more and more businesses are relied upon, regulations and attempts by authorities to control the network become a danger for the decentralized nature of the Bitcoin network.

While this aspect was anticipated by Satoshi Nakamoto in 2008, it was mainly considered in the context of centralization of mining efforts.\(^{32}\)

The international nature of Bitcoin makes regulatory controls difficult to coordinate for authorities, but not totally impossible over the longer-term. Bittorrent, for example, was seen as an uncontrollable decentralized network, but laws and legal challenges have reduced its use significantly with courts forcing internet service providers (ISPs) to intervene by forcing them to restrict public access to Bittorrent sites and services. The courts have also forced ISPs to help copyrights holders identify customers that have accessed pirated content.

Encouraging the adoption of more full nodes removes some of these centralization risks.

1.15. Wallet and Node Updates

Significant updates to the official Bitcoin client happen on a fairly regular basis. For the most part these updates are highly recommended in order to gain the benefits of the latest technology and security releases, but the updates are typically non-mandatory.

However, there are types of updates that are mandatory across the entire Bitcoin network, these are called hard forks.

There are many risks associated with updating Bitcoin clients and the process can be technologically difficult for the average Bitcoin user and most would need some guidance. An increase in the network’s ability to handle larger blocks would, for example, initially require a hard fork.

Unless people are actively engaged with various Bitcoin community websites or keep up with Bitcoin related media, knowing why and when to update can be missed by many node operators. Some evidence of this risk can be seen from data tracked by Bitnodes which tracks, amongst other things, the various Bitcoin clients that are being used to run nodes.

A hard fork is likely to see a significant drop in the number of full nodes, for example, because many existing nodes do not update and therefore stay on a superseded block chain. But this process could also be used as an opportunity to encourage people to update or to start running full nodes because of the risks of falling node numbers.

1.16. Sybil attacks

People that attempt to introduce software to snoop on transactions moving around the Bitcoin network or trick the network into diverting data are said to carry out Sybil attacks.

There are various types of Sybil attacks. One form is to create lots of fake nodes and attempt to record what people are doing with their Bitcoin transactions and to follow transactions with the intent of uncovering the people behind the transfers.

People may carry out these types of attacks for nefarious reasons; as a surveillance service; or to track down criminals. Another reason is to allow businesses to track where users are moving their funds in order to meet regulatory compliance obligations by having the ability to ban people from their services if individuals have visited or engaged in potentially illegal activities on the internet.

There are an increasing number of consulting businesses that have deployed an extensive network of Bitcoin nodes in order to collect data about transactions, such as regional trading activities and data about miners. This data is sold in its raw formats or

33 Bitnodes, 23 June 2015
analysed as a service. As more businesses adopt Bitcoin payment, the scope for commercial exploitation of transaction analysis will increase.

Tradeblock is one such company that deploys many Bitcoin nodes around the world to offer data mining services, as can be seen from notes on its website:

Note: TradeBlock maintains an extensive bitcoin network data architecture with multiple nodes across geographies to ensure maximum fidelity. As a result, we are able to view and record every transaction message broadcast to the network, including those that are not heavily relayed.

Elliptic is another company seeking to profit from using block chain data. While there are few details on the analysis approach they are using, what they have made clear is that they are seeking to link block chain transactions together in order to create an anti-money laundering reporting service. The intention being to alert their customers to individuals potentially acting unlawfully or to prevent clients from getting indirectly involved with moving funds that have previously been used for illegal activities.

The fewer the number of full nodes serving the network, the more data these commercial services will be able to collect through their own nodes, encouraging them to deploy more nodes on to the network.

Falling node numbers also point to similar Sybil attacks that could be created by governments and public sector bodies around the world. It would be disingenuous to suggest that the Bitcoin network is mainly formed of commercially deployed nodes or networks of government spy nodes. However, over time this could be the case if their numbers continue to increase and independent full nodes significantly decrease.

Sybil attacks where false nodes are used to obtain incentives or to collect data, can slow down the network as legitimate full nodes and lightweight wallets attempt to communicate with these false nodes. With enough false nodes the network can become noticeably slower for users, as well as potentially increasing the overall bandwidth costs for those that host full nodes.

The greater the number of independent full nodes, the harder and more expensive it is to launch Sybil attacks to deploy sufficient numbers of nodes to gain meaningful amounts of useful data. Conversely, as the numbers of nodes decreases, the greater the information gather potential and influence that these fake nodes can have on the Bitcoin network.

Bitcoin mining is built upon the basis that miners have to expend energy, called Proof of Work (PoW), before being rewarded with financial incentives. Mining is an example of financial disincentives being used to prevent Sybil attacks. Amongst the more popular

counter Sybil attack measures, in particular against the creation of false nodes, financial penalties, deposits, proof of work or collateral requirements are effective at preventing large scale attacks for all except very well resourced organisations or governments.
8. Moore’s Law

The prediction that computer processing capabilities and speeds will continue to grow has been largely proven to be true. Moore’s Law says that computers double in capabilities every 18 months; which corresponds to about 60% annual growth rate.

As Bitcoin’s bandwidth requirements and block chain size grow, Moore’s Law predicts that there will be sufficient technological advancements and internet bandwidth capacity for Bitcoin to remain a decentralized system.

The growth in mobile users, mobile hardware technology, storage technology, cellular data transfer technology and the infrastructure to deploy mobile services, means that Bitcoin will likely see faster growth on mobile platforms compared to PC’s.

New improved Bitcoin nodes with better security and features will encourage people to use full nodes. At the same time, the costs and effort to operate full nodes will diminish.

Whilst technologies advance, the current make-up of Bitcoin’s infrastructure may reach capacity constraints before these constraints are met by improving technology.

Many of the problems preventing people from running full Bitcoin nodes are likely to diminish in time, so any efforts or incentives to increase the number of full nodes will likely be temporary measures that will be resolved within the next 5-10 years by software and hardware advancements.

1.17. Nielsen's Law of Internet Bandwidth

Nielsen’s Law is similar to the more established Moore’s Law. Nielsen’s Law of internet bandwidth states that a high-end user's connection speed grows by 50% per year.

While bandwidth capabilities are very much regional in nature, the overall technology developments are encouraging, but problematic for this generic rule. The biggest disparity in bandwidth growth is between developed economies and developing economies.

Developed economies have access to many different forms of data capabilities from mobile telephone towers to optical cables laid in the streets. Businesses active in serving this market are developing capabilities to enable mobile phones to download HD movies in seconds.

By contrast, developing economies often do not have any internet infrastructure, except in small pockets of economic activity such as capital cities where internet access is expensive for the majority of people. For the foreseeable future, developing countries will
rely on developed countries to provide the majority of full nodes from which they can access Bitcoin via lightweight SPV wallets on their mobiles, tablets and computers.
9. Bitcoin incentive programs

The continued success of Bitcoin is still underpinned by the emission of newly minted coins to reward and motivate people. Financial rewards are an integral part of Bitcoin’s DNA. However, there are no rewards built into running full nodes.

This could be as a consequence of the introduction of specialist mining software; pooled mining systems; and a shift from simple computer mining, to graphics card mining, to purpose built ASIC mining equipment that have all eaten away at the need to operate a full Bitcoin node. The combination of these factors may not have been fully appreciated during the early stages of Bitcoin development so incentives were never considered, or the issues were known but they were left for resolution at a later date.

There have been many Bitcoin community discussions about using incentives to encourage more full nodes, including a trial to provide incentives. Funded by the Bitcoin Foundation, Bitnodes has operated a trial incentive program which requires node owners to register basic details about their node in order to receive incentives.

These incentives are paid weekly to random eligible nodes.

In this program, incentives are grouped into bands depending on the number of total nodes in the network. Nodes are assigned into pools that number 100. The weekly incentives are then paid randomly to one node in each pool of nodes, with incentives ranging from $10 to $30.

The incentives program is due to end in December 2015, or when the node count reaches 10,000 whichever comes first. This indicates that a minimum of 10,000 nodes is considered a desirable target for the current size and scale of the Bitcoin network.

People entering this program have reported some technical knowledge barriers required to register a node. There have also been comments that the incentives are more of a token gesture due to the level of the pay-outs and the 1 in 100 odds of winning the weekly incentive lottery.

1.18. Incentives vs. altruism

35 getaddr.bitnodes.io/nodes/incentive 10 June 2015
36 Pink, D; Drive: The surprising truth about what motivates us, Canongate, 2011
This quote from a long-term Bitcoin supporter touches on some of the problems of running a full node and some of the motivations to do so:

“...simply, there is lack of motivation to run full bitcoin node. you need SSD (because on HDD it consumes lot of I/O - at least in my case), open new port on firewall, update it time to time, it consumes lot of CPU/memory resources and bandwidth..and as a result is good feeling - which is obviously not enough anymore.

“PS: and yes, I'm running full node for last 2 years.”37

There are many motivating factors that drive human behaviour. Beyond biological needs, encouraging desired outcomes with financial rewards is one of the most popular ways to achieve desired outcomes. Money doesn’t motivate everyone, but it can be used to motivate people on a mass scale.

In the present context, money as a motivator works particularly well in situations and activities where rewards are tied to formulaic steps that require little to no cognitive skills on the part of participants.

In addition to financial motivations, people respond positively to altruistic contributions where the individual’s participation helps society in some way. However, purely altruistic reasons to be active and engaged produces far less of any particular desired outcome if the financial incentives are not there to remove money as an obstacle to participation.

People are prepared to volunteer their time if it doesn’t cost them any money. Moreover, their motivation and participation rates increase if they can make a small profit. Participation rates increase further still if financial rewards are provided and where people feel that their contributions have significant social purpose, such as disrupting established financial systems that are considered to benefit the few.

There is already some evidence of this behaviour in the Bitcoin system. Before the introduction of expensive specialist mining hardware, thousands of people participated in mining using smaller less expensive mining equipment from graphics cards to USB type devices. These were cheap to purchase, easy to set-up and easy to operate with basic software and easy to understand instructions.

These small mining operations generated very modest profits for the users, but people in their thousands were engaged with the process giving up substantial amounts of their free time to tend to their equipment and engage with like-minded individuals in online forums.

37 Xialla; 23 June 2015; bitcointalk.org/index.php?topic=1093151.msg11695128#msg11695128
As newer faster and more expensive mining hardware was introduced, these small operations became loss making and these enthusiasts shut down their operations and stopped donating their free time to support the diversification of the Bitcoin network. Many also disengaged with the various online forums.

1.18.1. Interpretation of the empirical evidence on financial incentive

In the present context, asking people to operate full nodes as a gesture of goodwill in order to benefit the Bitcoin project will yield many volunteers. However, as their costs increase, the numbers prepared to volunteer would be expected to diminish.

Where incentives are distributed equally to those that participate and those incentives meet the costs or exceed the costs of running a full node, the expected outcome would be the creation of many thousands of nodes.

Incentives should be aimed at providing a reasonable return on costs, with technical mechanisms to discourage the creation of industrial scale Bitcoin node operations which create centralizations risks.

1.19. Historical Bitcoin incentive examples

Bitnodes operates the only incentive program aimed at operating full nodes that we were able to identify that had any substance.

There have been Bitcoin community discussions on whether to allocate some of the Bitcoin mining rewards to give financial incentives to full node operators. Generally these discussions have not progressed as mining is seen as being more critical to the Bitcoin network. In addition, there are fears that Bitcoin incentives programs could be taken advantage of by people who could create many nodes that give the appearance and characteristics of full nodes, but are actually fake nodes.

Many of the incentives schemes that have been considered for incorporation into Bitcoin suffer from these types of Sybil attack threats.

Microsoft Research\(^{38}\) has put forward an incentives proposals that rewards information propagation to avoid loss of incentives to fake nodes created in Sybil attacks. The rewards structures are a combination of mining rewards and a share of transaction fees as mining rewards are slowly phased out. This system requires significant changes to the Bitcoin network and therefore there is no indication that the proposals will be moved forward into production.

Proposals have also been put forward for nodes to be paid from transaction fees. While this is possible, the method for allocating such fees has not been produced. Further,

---

\(^{38}\) Babaioff, M, et al; On Bitcoin and Red Balloons; ACM Conference on Electronic Commerce (EC’12), February 2012
such a scheme may encourage people to create nodes that fail to transmit information about transactions to other nodes in order for the node owner to ensure they get to keep transaction fees and avoid any chance that other nodes may be awarded the fees instead.

One of the main barriers to sharing miners fees are the miners themselves. As the current miners reward mechanisms are phased out, the miners are expected to earn the majority of their income from fees. At present, the fees required to sustain their operations, without the allocation of newly minted coins, are likely to be insufficient.

While there are many global and regional factors that can influence the mining costs for each transaction, it seems unlikely that any further dilution of miner’s revenue would be able to sustain both the mining network and a network of many thousands of full nodes at this time.

1.20. Pay-per-use

An alternative proposal to encourage the creation of more full nodes is to pay people to operate them for supplying block chain data to non-full nodes. Anyone wishing to pull data from full nodes would then have to pay a fee to receive the data.

For example, mobile Bitcoin wallets do not currently download all of the data on the block chain, but to operate they do need to access some data from the block chain. As mobile wallets continue to increase, they pull more and more data from the block chain. At the point that people rely on mobile wallets, they could be charged a fee which would be sent back to the Bitcoin network and then shared amongst all of the full nodes or shared amongst nodes on a regional basis.

While the technology for a pay-per-use data model would be technically difficult to implement, it has received some support\(^3^9\).

1.21. Miners incentives vs. Nodes

The miner’s incentives are clearer as they relate to the issuance of rewards when miners create new blocks and process transactions into those blocks for a fee.

However, over time these rewards to miners are halved every four years until they approach zero. Operating the Bitcoin network is not free and miners incur substantial costs and as these rewards diminish it is expected that fees to process transactions will increase to cover the costs of running the network. This chart\(^4^0\) illustrates how the


\(^{40}\) Kaskaloglu, K; Near Zero Bitcoin Transaction Fees Cannot Last Forever; 2014; http://sdiwc.net/digital-library/near-zero-bitcoin-transaction-fees-cannot-last-forever.html
reduction in rewards should, in theory, be met by a commensurate increase in transaction fees.

In the event that fees fail to generate sufficient income for miners to continue processing the transactions on the Bitcoin network, then some miners may be forced to switch off their equipment if they cannot afford to maintain operations. This will be tested, to some extent, around the summer of 2016 when the rewards issued to miners will drop from the current 25 BTC / block to 12 BTC / block.

This scenario would potentially be mitigated by substantial increases in the price of Bitcoin, but the issues would persist over the longer-term meaning that it would only be a matter of time before the network either raised fees to a point where it would diminish future growth or the network found another mitigating mechanism to reward miners.

Bitcoin is in many ways a self-regulating network and smaller miners would very likely step-in to support the network and protect their financial interests. However, meaningful reductions in miners at a time when Bitcoin is very popular and has full nodes that carry large amounts of historical data creates opportunities for people to attack the system for financial benefit or to undermine its integrity.

These risks have been known for some time and remain in the background as there is no urgency at this point to address them fully.

“In the long run, the policy on transaction fees should be set so that enough many miners have incentive to run clients having a good enough combined hash power to protect the network. But on the other side of the coin, the fees that miners collect should not be any higher than sufficient in order not to discourage users from using Bitcoin as a means of transferring money.”

A Bitcoin full node incentives program could begin by incentivizing full nodes to be sustained and new nodes created, but over time that program could be extended to compensate miners as there is an intrinsic relationship between the two key components of a decentralised, secure and healthy Bitcoin network. This has the potential to balance

---

41 Andresen, G; DevCore Boston 2015 | What Satoshi Didn't Know | Gavin Andresen, Bitcoin Foundation; https://youtu.be/rQ3e1Pzu7iI?t=27m30s
42 http://bitcoinclock.com
against any increases in off network transactions by those seeking to save on increased transaction fees.

With some investigation on the technical feasibility of rewarding full nodes and miners, a model to financially encourage diversification of the miners in order to shift away from centralized models, such as mining pools with, say, greater than 5% of the processing power of Bitcoin, could be researched.
10. **Incentives: lessons from alternative cryptocurrencies**

Alternative crypto currencies are seen as distractions from encouraging the use of Bitcoin.

There are also people that consider altcoins as an active area of innovation around features that people would like to see developed inside Bitcoin, but recognize many of these features will likely never be incorporated into Bitcoin. Side chains\(^{44}\) have been developed in order to introduce mechanisms to enable innovation around Bitcoin without having to significantly change Bitcoin.

While side chains are researched, developed and tested, there are case studies of node incentives from existing altcoin projects.

### 1.22. DASH

Formerly known as Darkcoin, DASH uses a two tier network in order to incentivise people to set-up nodes that operate as servers which conduct transactions for their own network. These second tier of nodes are called *Masternodes*\(^{45}\):

> In addition to traditional Proof of Work (PoW) rewards for mining Dash, users are also rewarded for running and maintaining special servers called masternodes. Thanks to this innovative two tier network, Dash can offer innovative features in a trustless and decentralized way.

> Masternodes primary function is to carry out the anonymization phase of the Darksend protocol and to validate transactions almost instantly. In the future, there will be more services performed by the masternodes network.

> In return for providing this services, one masternode is selected by the network to receive a part of the reward of each mined block.

The approach used by DASH has proved to be hugely popular. Relative to the total market value of DASH, around $13m, they have incentivised the creation of around 3,000 masternodes, in addition to full nodes operated as wallets.

To prevent Sybil attacks, DASH introduced a model that requires node owners to associate 1,000 DASH, with an approximate value of $2,500 at time of writing, with each masternode they wish to operate. This creates a collateral obligation that makes it expensive to attack the network and practically *impossible* to create fake nodes.

---

\(^{44}\) Back, *et al*; Enabling Blockchain Innovations with Pegged Sidechains; 2014; blockstream.com/sidechains.pdf

\(^{45}\) dashpay.io/masternodes2/ June 2015
At current market rates, the total amount used as collateral by all the node owners in the DASH network is between $7m-$8m; attackers would have to spend at least 30%-50% of this value to be able to mount any sort of meaningful Sybil attack. In addition, masternodes owners have to demonstrate that their nodes are operating effectively and efficiently within a node rating system that monitors all the masternodes on the DASH network.

In return for operating a masternode, users are paid a relatively high share of mining rewards, 50% as at June 2015. The allocation of these rewards are assigned on each round by ten randomly selected masternodes who find the last node owner to have been paid and together these masternodes sign a payment to that node owner.

This means that all nodes are paid in turn avoiding any lottery style incentive payments. As a consequence of being allocated an equal share of mining rewards, masternode owners make a healthy profit from operating their nodes.

In the event that masternode owners need their 1,000 DASH funds, they can spend these funds as normal, at which point their masternodes is removed from the list of available nodes and incentive payment are no longer paid.

1.23. Proof of Stake

Originally developed for use in Bitcoin to avoid people sending many unnecessary near zero value transactions to themselves creating a type of ‘block chain spam’, Proof of Stake (PoS) is now a popular type of crypto currency used by many projects hoping to compete with Bitcoin.

These altcoin projects are based on many of the same features of Bitcoin, but instead of miners expending energy through proof of work (PoW) during the mining process to secure their network, the security within a PoS network is related to nodes that are left on all the time.

To encourage people to leave their nodes on, rewards are paid to node owners through a process known as ‘staking’. Many PoS networks allocate a percentage of the total coins in circulation, or they create an annual supply of new coins each year, to reward staking node owners. This staking process is also referred to as interest payments.

Nodes that are left on and staking receive interest type payments that are related to their wallet balance. To further encourage owners to keep their nodes on as much as possible, staking interest payments are typically rewarded over a period of time, from a few days to a week or more. Closing a node during the staking period typically means losing their interest payments for a period of time.
As PoS systems allocate rewards directly to node owners, they remove the requirement for miners altogether and those that have their nodes on with a balance greater than zero have a chance to create new blocks for the network. The chances of creating a new block for the network is relative to the amount of the balance in the wallet. This is cost efficient and environmentally favourable. However, many believe that the process of expending energy mining is what makes attacks against the network difficult, or in the case of Bitcoin, near impossible.

Attackers wishing to create false transactions on the Bitcoin network must expend millions of USD in mining equipment, facilities and on electricity with little prospect of making a profit on their attempts.

PoS systems have been labelled as being centralized features as they need one or two nodes to allocate interest payments, making them potentially less secure than the mining system used by Bitcoin. However, the PoS interest incentives structure has proven to be attractive with many altcoin projects using PoS to drive their network security.

1.24. Spreadcoin: Spread Bitcoin

Spreadcoin (SPR) is a previously semi-abandoned project that has been used to pursue a Bitcoin node incentives program and explore decentralized business models to support a program indefinitely.

SPR has a similar incentivised network of nodes used by the DASH project, operated by its own implementation of second tier nodes coded from scratch. SPR intends to use this second tier node system to process decentralized operations and transactions.

Instead of calling their second independent layer of nodes Masternodes, their nodes are called ServiceNodes to reflect the intention of providing services on top of the SPR block chain.

Unlike DASH, each ServiceNode user is required to host a full Bitcoin node. Without a full bitcoin node operating correctly and serving the Bitcoin network, a ServiceNode is not considered part of the SPR network. This is being developed using a model called Proof of Bitcoin Node (PoBN).

To compensate ServiceNode users financially and to sustain the costs of hosting a Bitcoin node over the long-term, revenue derived from the provision of services on the SPR network is paid to node owners and to SPR miners. This is in addition to sharing an allocation of the mining rewards paid to SPR’s miners.

Instead of attempting to find a mechanism to incentivize Bitcoin nodes directly on the Bitcoin network and therefore find ways to avoid Sybil attacks on the Bitcoin network; the SPR network nodes themselves are incentivised to host full Bitcoin nodes.

To create a ServiceNode and to participate in a share of revenue from decentralized business services operated on the SPR network, ServiceNode owners must provide collateral to prevent Sybil attackers. This means that ServiceNode owners have to stake their own funds to run a node. As with DASH, these collateral funds can be removed at any stage, which would also remove the user’s ServiceNode from the Spreadcoin network.

Once a ServiceNode is created, the operational health of each node is monitored by its neighbouring nodes and where service standards fall below expectation, nodes are removed from the network and replaced by better performing nodes.

SPR has estimated that its decentralized network could operate between 2,000 and 4,000 Bitcoin nodes, with their own static IP addresses being a requirement to encourage decentralization. To prevent the Spreadcoin network being viewed as a potential Sybil attacker, the source code will be open source in order for experts to vet the code for any perceived attempts to attack the Bitcoin network or use data in a way that could undermine confidence in Bitcoin.

The rationale underpinning the ServiceNode concept, which would end up supporting a meaningful number of Bitcoin full nodes, has several components:

- Bitcoin is the market leader which is reaching an escape velocity in terms of adoption and any attempts to compete with Bitcoin will be difficult if not impossible. The network effect that Bitcoin has reached, the level of venture capital investment, the numbers of software engineers focusing on how to advance and profit from Bitcoin make its market advantage almost unassailable.

- The concept of a second project supporting the main Bitcoin project was influenced by the Prisoner's dilemma\(^47\). While the popularity of Bitcoin grows, the falling node count is a risk not only to Bitcoin but the entire crypto currency ecosystem. At this point in Bitcoin’s development, any incentive mechanism is difficult to implement because of the technical challenges to introduce changes to the Bitcoin economy, in addition to the lack of sustainable funding mechanisms. An optimal solution, therefore, would involve taking away the technical challenges from Bitcoin and incorporating a solution through another project, which itself would struggle without Bitcoin being successful.

An incentive scheme that encourages the use of VPS solutions is preferred as professionally hosted nodes can potentially provide a better service to the Bitcoin network. However, the diversity of VPS providers could be a limiting factor that would need to be reviewed in greater detail. Nodes could also be set-up on home PC’s and small hardware units such as Raspberry Pi, but VPS solutions would potentially give high bandwidth scalability options for the Bitcoin network.

1.24.1. Decentralized Platforms For Centralized Crypto Businesses

While Bitcoin is a decentralized network the services being built around it are centralized.

Bitcoin’s growth has created many opportunities for new businesses to build new services or to transfer existing inefficient business models to more effective block chain business models.

Venture capital and private businesses have so far invested between $600m to $1bn in Bitcoin related ventures. Based on expectations of gaining a substantial return on investment, this would value these businesses in the region of $3bn to $15bn in 2015, which is greater than the $3bn to $4bn market value of all the current Bitcoins in circulation.

This investment capital going into Bitcoin related businesses is expected to increase substantially. Much of this investment is expected to be focused on the block chain, block chain data mining and distributed forms of agreements via the block chain, called smart contracts, all of which are exploitable features of the Bitcoin technology.

However, while this is a significant and positive step, the majority of these new businesses face high regulatory burdens which favour larger businesses over smaller businesses. Innovation that is proven to be effective, is more easily adopted by large businesses who can afford regulatory hurdles.

The creation of decentralized Bitcoin services is difficult to achieve as investors and business owners use commercial entities to profit from their work. Spreadcoin is attempting to resolve some of these difficulties by creating a second tier network that deploys decentralized services that can sit alongside Bitcoin. The creators of SPR say their vision is to Decentralize Everything.

One way to look at their concept is to consider a decentralized protocol, Bitcoin, being supported by another decentralized protocol. This approach has the potential to open up new options for investors and business owners.

48 State of Bitcoin Q1 2015: Record Investment Buoys Ecosystem; Coindesk.com
For example, financial services are typically centralized around a small number of cities and regional hubs. Where regulations in these locations are hostile to Bitcoin services, it is difficult for small to medium sized organisations to establish in the first place. Moreover, where regulators decide to make substantial regulatory changes, businesses face the prospect of moving operations, closing down, raising equity or charging customers more.

Having the option to decentralize some Bitcoin related services means that they can be operated anywhere in the world and moving operations would typically involve moving data from one set of servers in one region to another set of servers in another region where regulations are more favourable.

Creating a Bitcoin incentives scheme through commercial or charitable entities would create both regulatory risks and financial pressures that would lead to questions around the independence and integrity of any governance structure used to operate the global programme.

Any successful Bitcoin incentives scheme would potentially run regional regulatory risks and coordination through a decentralized project would diminish many of those risks. An open source decentralized node incentives scheme being used as a vehicle to fund a decentralized open source Bitcoin network could create the conditions for a sustainable programme or series of parallel programs over the long-term.

1.24.2. Funding the bitcoin incentives program: Data Mining As A Service

The need for Spreadcoin's Bitcoin node incentive program is considered to be a short-term requirement to support the Bitcoin network during a period of marginal risks due to falling node numbers. This period is expected to last 3-5 years while the internet infrastructure develops sufficiently to make running full Bitcoin nodes on a mass scale relatively trivial.

However, basic block chain data flowing through full nodes has commercial value. Left to market forces, businesses such as marketing firms would set-up farms of full nodes and use them to identify users and user’s habits. Governments and public sector agencies could also establish farms of nodes for identifying and tracking down users.

By deploying a program to incentivise bitcoin nodes, the SPR network could operate an open source data mining service that could generate valuable block chain data revenues which in turn would be used to pay full node owners. Members of the open source community could also create scripts they would like added to analyse Bitcoin block chain data.

Launching pre-emptive data mining services with a significant presence would make it harder for other services to establish or gain any additional meaningful data. Several
Commercial operations have already launched services in order to profit from the data that can be mined from nodes including anti-money laundering services to restrict Bitcoin users who some might consider pose regulatory risks.

These for-profit organisations seek to extract value from the blockchain without necessarily supporting it. The more profit they derive from their services the greater will be the motivation to create more nodes.

An incentives program governed by the Bitcoin community could lead to the creation of 3,000 to 5,000 over the medium-term. Structured favourably a full node program could prove to be exceptionally popular, mimicking the popularity of small-scale mining which drew thousands of people to Bitcoin before industrial mining took hold.

In the event that pruning features are successfully deployed into Bitcoin, there is the possibility that upwards of 10,000 full nodes could be seen on the Spreadcoin network over the longer-term. This would require low level technical hurdles so that individuals could get involved for fun, community engagement, social purpose and a reasonable profit.

With Bitcoin nodes approach 10,000, these node numbers would yield more valuable data about transactions on the Bitcoin network, in particular details on key international financing channels and pockets of regional financial activities. A successful Spreadcoin incentives program could be used to fund both Bitcoin full nodes and Bitcoin's miners.

This would provide a barrier to entry to anyone wanting to launch a competing private service where the Bitcoin community would not be able to influence what they did on the Bitcoin network.

1.24.3. Commercially Driven Bitcoin Data Mining Examples

Coinalytics.co
Online cryptocurrency data and research provider TradeBlock has raised $2.8m in funding as part of a new investment round led by Andreessen Horowitz that also included SecondMarket CEO Barry Silbert, Devonshire Investors and FinTech Collective.\(^4^9\)

Clearly, businesses are investing in Bitcoin data mining and block chain analysis tools. Data as a service is already a valuable sector with Experian, Equifax, Acxiom and TransUnion having a joint market capitalisation in excess of $50bn and each business has annual revenues significantly greater than the current costs to run the Bitcoin network.

Data generated by the block chain or relayed by full nodes could include auditing and accounting data for businesses using Bitcoin; in depth reviews of smart contracts; logistics processing of orders placed using Bitcoin; consumer transaction trends; smart phone geolocation based transactions trends; and any number of data points from new services yet to be created using Bitcoin.

This approach does not seek to prevent all Bitcoin data mining services from establishing. Data mining and data analytics businesses such as Tradeblock, blockchain.info, Blockstream and those that seek to support Bitcoin through commercial ventures could benefit from data supplied to them and they could help to create data specifications for the types of data that would they would like to purchase. However, those businesses and entities focused on uncovering users IP addresses would be at a disadvantage.

---

Bitcoin’s biggest assets are its full nodes and the block chain. Full node owners and miners should benefit from the data that they help to process, protect, provide and store.

1.24.4. Bitcoin Side Chain

Spreadcoin has indicated an intention of looking at what would be required to become a Bitcoin side chain once the technology to operate a second tier decentralized node network is established and the side chain technology is implemented.

Where a project becomes important enough to the Bitcoin network, it would potentially be advantageous to have its block chain being tied to or protected by the hashing power that protects the Bitcoin network today.

While a potential side chain transition is underway, SPR has indicated a need to build a p2p exchange enabling incentives to be interchanged with Bitcoin.
11. **Bitcoin Full Node Incentives & Recommendations**

Technical people engaged within the various Bitcoin communities are aware of the need to run full nodes and why they are helpful to protect the privacy of users and to secure the network. However, technical experts are significantly outnumbered by the masses of people that would benefit from using Bitcoin and with some guidance could operate a full node correctly.

Simple to understand language is one of the best engagement tools that can be used to encourage thousands of technical and non-technical people around the globe to run full nodes.

Creating incentives to run a full node has many benefits, but there are also many complications.

There are several recommendations that arise from this white paper. Some are easy to implement and some are difficult to implement.

**11.1 Businesses promoting Bitcoin full nodes to some of their customers**

It is apparent that commercial organisations are spending significant amounts of money developing products and services to run on the Bitcoin network. They promote their products and services and many of these businesses have millions of customer accounts.

The amount of time and effort that these business spend on making their customer experiences as easy as possible does not usually result in the creation of full nodes.

These businesses will feature prominently in search results for Bitcoin and sources of Bitcoin information. By spending time and resources on promoting themselves, they drown out information on why, how and where people can access full nodes.

Businesses that rely on Bitcoin, such as online wallet providers, should find ways to promote the running of full nodes to some of their customers or users.

All businesses relying on Bitcoin should have accredited or trusted Bitcoin Foundation logo links to official repositories where people can find and download the latest Bitcoin clients.

**11.2 Bitcoin community promoting the running of full nodes**

Running full nodes can be a self-regulating activity. If individuals believe that the Bitcoin network is under threat because node numbers are falling too far, many will run nodes to
protect their investment. Regular social media postings by Bitcoin developers and prominent contributors on node numbers may trigger people to keep an eye on number numbers.

Official Bitcoin full node promotional activities and awareness should be in different languages to encourage more full nodes around the world.

11.3 Encouraging small businesses and merchants to run full nodes

There are over 100,000 small businesses and merchants that now use or offer Bitcoin. These businesses typically use commercial merchant payment services to operate their Bitcoin acceptance and fulfilment needs.

Some of these small businesses will have faster and more robust technology and internet services which are operational all the time. They may also have staff that can be trained to operate nodes or devote some of their time to understanding what is required and the benefits to their business of spending the time looking at the issues.

These types of small businesses should be encouraged to operate a minimum of one full node in each of their office or retail locations. If they use merchant services, they should be encouraged to run a full node with a zero balance.

Small businesses should also be encouraged to operate three full nodes, possibly in diverse locations, and be given easy to understand instructions on how to use multi-signature features to protect themselves against theft or failure of hardware.

The Bitcoin Foundation should produce short, 30-60 second, infomercials for small businesses to explain the block chain ledger system, what a full node does, why it is essential for the privacy, security and safety of their funds and how small businesses can help by running nodes with zero balances and or use the multi-signature features.

11.4 Encouraging large businesses to operate full nodes

Larger businesses that rely on Bitcoin, such as wallet and merchant services providers, should encourage between 10%-20% of their staff to run full nodes with zero balances on dedicated hardware, such as a Bitnodes B1 device.

11.5 For profit Bitcoin full node incentives program

Building a node incentives program that creates many thousands of nodes is very challenging. For example, commercial enterprises would look to build node farms in order to profit from the incentives, which would potentially lead to centralization concerns.
Businesses wishing to run many thousands of nodes in industrial facilities would find it difficult to build farms due to the amount of bandwidth they would need compared to what would be available from internet service providers.

However, cloud based server farms are a possibility if node management software were developed for commercial exploitation to profit from a node incentives scheme.

Building a second tier network to operate Bitcoin full node incentives to avoid Sybil attacks and centralized node farms is potentially the more viable option.

Building a second tier of nodes that can generate revenue and fund an incentives program, while also removing the risks of Sybil attacks, should be pursued. Preferably in association with Bitnodes and or Bitcoin community representatives to provide a governing structure.

Any separate project seeking to establish an independent node funding scheme would potentially be welcomed, but any funding scheme may be viewed as a potential risk if it proves too popular and causes others to reduce their independent active participation in running full nodes which could lead to problems with diversification of the Bitcoin network.

11.6 Incentives and fees revenue share

Asking Bitcoin miners to share rewards or transaction fees would be difficult to achieve whilst the costs of mining are marginally profitable and any increase in block sizes would potentially see a reduction in the levels of fees paid by users. The issues of sharing rewards would also be compounded if people felt that the rewards were being stolen by Sybil attackers.

Any Spreadcoin derived incentives program should factor the distribution of sufficient funds to enable small profits for each node to discourage node farms from being established, as has already been seen with Bitcoin mining operations.

While the majority of the revenue from mining data held by full nodes should go back to the SPR Bitcoin full node owners, SPR miners and Bitcoin miners, a proportion of the funds should be sent to the Bitcoin Foundation to support educational activities and translations of materials associated with the incentives program.

Another allocation of funds could also be used to pay for the development of various tools that can be used to analyse the data held by full nodes.

This is an overview of the SPR Bitcoin full node incentives model:
Asking Bitcoin businesses and merchants to pay fees to full nodes would have similar problems to asking miners to share rewards or fees. In addition, any extra fees to compensate full nodes might make Bitcoin as expensive as other payment channels.
such as debit cards or credit cards. This can detract from the attractiveness of using Bitcoin.

Any incentives program that benefits Bitcoin full node operators and Bitcoin miners, will take time to implement and while the current Bitcoin node network can manage, an incentives program should commence as soon as possible to take into account development and adoption times.

During this transitioning period a new data mining proposal will be put forward as a Bitcoin Improvement Proposal (BIP) with the view to replacing or working alongside the existing proof of work miner calculations. This will inevitably take a long time to implement as changing, adapting or replacing the current PoW algorithm will meet with resistance. The initial planned process involves miners processing blocks and as a consequence of successfully propagating blocks which are accepted by the network, the miner will then be allocated data to mine on behalf of a blockchain data buyer. A working revenue model will make it easier to demonstrate the value of making significant changes of this nature.

11.7 Helping developing countries to create their own Bitcoin infrastructure

Creating an incentives program could enable the skewing of the amounts paid to developing countries to encourage the creation of a longer-term sustainable Bitcoin infrastructure in regions with poor internet services. However, while incentives could be calculated based on IP addresses or regional node traffic data, it is not clear how fair this would be seen by people in developed countries.

Businesses would potentially find the data that could be relayed by nodes in Africa and developing parts of Asia of significant value. Data relating to financial services would help many different types of businesses make better informed decisions. If so, any weighting of incentives to developing regions could be funded commercially.

A regional Bitcoin development program could, over the longer-term, reduce the burdens of millions of SPV (Special Purpose Vehicle/Entity) users in developing regions leeching data from nodes in developed countries. This approach would also contribute to the decentralized nature of Bitcoin.

It would take some time to build up sufficient revenue streams for any incentives program to have any material impact. However, a program with sufficient community backing could give many thousands of individuals the confidence to invest in setting up full nodes knowing that their investment will be rewarded.
12. Conclusion

Bitcoin full nodes are of fundamental importance for verifying and storing Bitcoin’s decentralized database of transactions. They also enable lightweight wallets to flourish making Bitcoin more popular, so they are vital for the security, diversity and the health of the entire network. As node numbers continue to decline, at a time when Bitcoin is increasing in popularity, more and more pressure will be placed on the Bitcoin network.

Commercial entities wishing to collect data for profit and for regulatory purposes will find establishing many hundreds of nodes on a smaller Bitcoin node network will enable them to collect more valuable data. With sufficient regulatory influences these businesses could also be forced to provide data to governments around the world. These and many other centralization risk factors could contribute to undermining the security and integrity of the Bitcoin network.

Bitcoin’s growth and overall security to date has been facilitated by mining rewards. These mining incentives have created a profit mechanism by which the network is protected as the costs to earn the rewards are significant, making attacks against the network very expensive for all but the richest businesses or governments.

Creating the conditions for increasing the diversification of the Bitcoin node network, while also facilitating a method for rewarding miners as the levels of mining rewards fall and the certainty over transaction fees to support miners remains untested, is something that can be achieved through exploiting the data stored on the Bitcoin block chain and the data that moves around the network.

Data mining and making it available to businesses enabling them to make informed decisions on transactions and smart contracts on global, regional and seasonal transactions, means that the block chain can become Bitcoin’s profit generator. A successful implementation of data mining tools could see users Bitcoin transaction fees subsidized and help give businesses greater understanding of Bitcoin. These factors in turn would increase adoption. This would create a positive feedback loop making full nodes and block chain data more valuable.

Creating an internal knowledge based economy based around the block chain and data flowing between Bitcoin full nodes has the potential to reward desired outcomes of increasing numbers of full nodes, increasing decentralization, encouraging further investment in mining, encouraging greater investment in bandwidth technologies, mobile connectivity and expansion across all regions around the world. Moreover, the creation of Bitcoin data mining tools by the Bitcoin community would create barriers to entry to commercial data mining efforts that aim to focus on uncovering IP addresses and user accounts.
The decentralized database held in full nodes and the data produced by the Bitcoin block chain are among the networks biggest assets. These can be leveraged to fund incentives that support the growth and diversification of the Bitcoin network, for Bitcoin’s entire lifetime. It is an area that should be actively pursued and Spreadcoin’s attempts, in particular, to trial a solution for creating sustainable incentives to support Bitcoin’s infrastructure, with anti-Sybil attack measures, shows promise compared to previous Bitcoin incentives programs and should be examined in greater detail.