DIGITAL SERVICES DIGITAL NETWORKS

HELIUM
March 2017

Abstract

Decentralization is a defining foundational feature and benefit of blockchains. As blockchains increase in data size the hardware, bandwidth and expertise required to keep nodes optimally dispersed and synchronised increases in complexity and cost. This poses risks to decentralization and therefore the integrity and security of blockchains. To maintain the key characteristics of decentralized blockchains, Blockchain as a Service (BaaS) is a natural progression. High bandwidth BaaS networks operated by third parties without needing trust to hold consumer or Enterprise grade data using Proofs of Service is proposed. The addition of end to end encryption between nodes within common control on public or private blockchain networks preserves privacy. This new approach creates the opportunity to launch Digital Services Digital Networks (DSDN) where anyone can run a blockchain node for anyone else with priority connectivity and performance requirements which are rated and set at market determined price levels similar to managed cloud hosting products.

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.

Satoshi Nakamoto, July 29, 2010, 02:00:38 AM
Bitcoin and Blockchain Inventor

White Paper Preface

As a paper on blockchain technology, it is helpful to use the first and most popular blockchain as a reference point. However, the paper is not focused on a singular blockchain solution, rather the infrastructure, security and ease of use for interacting with any blockchain for ordinary individuals and businesses of all sizes.

Introduction

The invention of the peer-to-peer ledger protocol (Nakamoto, 2009) is the underlying technological success of Bitcoin as electronic cash. The Bitcoin network builds its publicly accessible ledger of information by timestamping transactions hashed into blocks through proof-of-work (Back, 1997), forming a permanent record.

Blocks contain transacted data within defined maximum block sizes. These blocks are linked together through timestamping to prove the date and time data is added to a block. Additional hashed information to aid in the block-to-block linking process is also included to give users a method to trust the ledger they are accessing is accurate and independently verifiable without having to trust anyone who preceded them.

As each block is created and added to a blockchain, however, the overall size of the blockchain increases in size. While most blockchains begin life as very small databases, over time they can grow significantly. Depending on the storage capacity of locally available physical hardware and bandwidth access to the internet, blockchains can reach a size where they become difficult and expensive to manage. This is especially true on home connections where user's various applications compete for bandwidth resources, in particular, movie streaming services and or online gaming.

Managing blockchain nodes can also be complicated for non-technically minded users who simply wish to use the services of a particular blockchain application rather than be actively involved with increasing the decentralized nature of the network they are using.

As the inventor of the blockchain protocol, Nakamoto recognised that as blockchain networks grew in popularity and size there would be a point where the majority of users would just want to benefit from the utility of the services on offer but do so through lightweight clients. To maintain an efficient functioning network, while preserving the decentralized nature of the blockchain in use, he argued that the infrastructure of the protocol being used would eventually migrate to professionally hosted environments (Nakamoto, 2010).

For businesses wishing to operate sensitive transactions on blockchains having data leaks of this nature would potentially create security risks and or potential for regulatory breaches. However, one of the weaknesses of lay users connecting to blockchains with light clients is the need to create connections with full nodes which hold full copies of a blockchain. Expert users can create secure connections between light clients and their own full node but lay users, however, are exposed to public connections allowing data to be intercepted by third parties snooping for personal information.

We propose the creation of professionally hosted blockchain nodes with end-to-end encryption. These fully managed nodes can be controlled by individual users who wish to outsource the operation and maintenance of their own full nodes. These services can be further extended for use by businesses who wish to benefit from secure access to full nodes, for all their employees, without needing to have in-house technical expertise to manage blockchain nodes that facilitate users transacting various blockchain services via local lightweight clients.

As a premium *Blockchain As A Service* (BaaS) product, ordinary users can purchase access to professionally hosted and managed blockchains of their choosing to benefit from secure and encrypted access with high priority bandwidth channels for public, private or semi-private B2B networks.

Motivation

As blockchains grow in size there are risks that decentralization suffers as fewer people are able to manage or can afford to run full nodes. This poses security risks to a blockchain network as well as making them inefficient. Moreover, running full nodes on any blockchain can be a difficult and daunting operation for those that have few IT skills and would arguably be the group mostly likely to benefit from the increased security that fully validating nodes would provide.

There is evidence from the first major blockchain, Bitcoin, that users avoid running full validating nodes, despite the unrivalled security model full nodes offer. One of the most popular online Bitcoin wallet services, Blockchain.info, claims to have 10m wallet users; compared to around 5,500 full Bitcoin nodes on the network.

We propose solutions to help blockchains maintain or increase decentralization by letting users be users and transferring the burden of full node and blockchain management to those who are better equipped to take on the technical challenges and the operational risks. To encourage third parties and to avoid centralization around a few organisations running operations in data centres, we propose a methodology to enable a distributed network of independent contractors to provide third party managed cloud services for users.

The encouragement of third party contractors to operate blockchain services for users also necessities the development of peer-to-peer encryption. This is also seen as beneficial to improving the security model of blockchains as they become more widely adopted. Security enhancements coupled with managed services also enables businesses and other organisations to more easily adopt blockchain technologies through the general trend to outsource tasks to cloud service providers.

By creating a commercial environment for managed cloud services, blockchain networks will be more able to solve a long standing full node incentives problem where people and organisations are given financial encouragement to support networks.

Blockchain As A Service

Blockchain services, recently termed Blockchain as a Service (BaaS), have emerged as various individuals and businesses seek to monetize this new technology. The focus of this paper is to look at the strengths, weaknesses, opportunities and threats of running full nodes on professionally managed environments as third party services.

The option to provide services on multiple chains, such as project specific private chains, is not considered in full within this paper. The option to create project specific chains using Hyperledger, as one option, for tracking supply chains such as for construction projects is, however, a related subject and service being pursued.

Full Nodes

Full nodes will download and hold a complete copy of a chain and all transaction data, not just block-to-block security information contained in block headers. They are typically designed for use on thick clients which are downloaded on various operating systems.

> *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.1*

As part of its protocol rules, a full node operating on a proof of work (PoW) chain will look for the longest chain to validate against. The depth of the longest chain of blocks is used by nodes to check against people trying to double spend value and this is therefore an essential security feature that full nodes perform. Validating the uniqueness of information is the one security feature that can give or attribute value to individual pieces of data.

Examples of the data structure of blocks within a blockchain can look like the table below:

Operation	Data Size
Block Header	80 bytes
Block Version	4 bytes
Previous Block Hash	32 bytes
Merkle Root	32 bytes
Timestamp	4 bytes
Target	4 bytes
Nonce	4 bytes
Transaction Counter	1-9 bytes
Various Transactions	About 95-99% of block size, with transaction signatures making up about 55% - 65%

1 Bitcoin.org, Running A Full Node

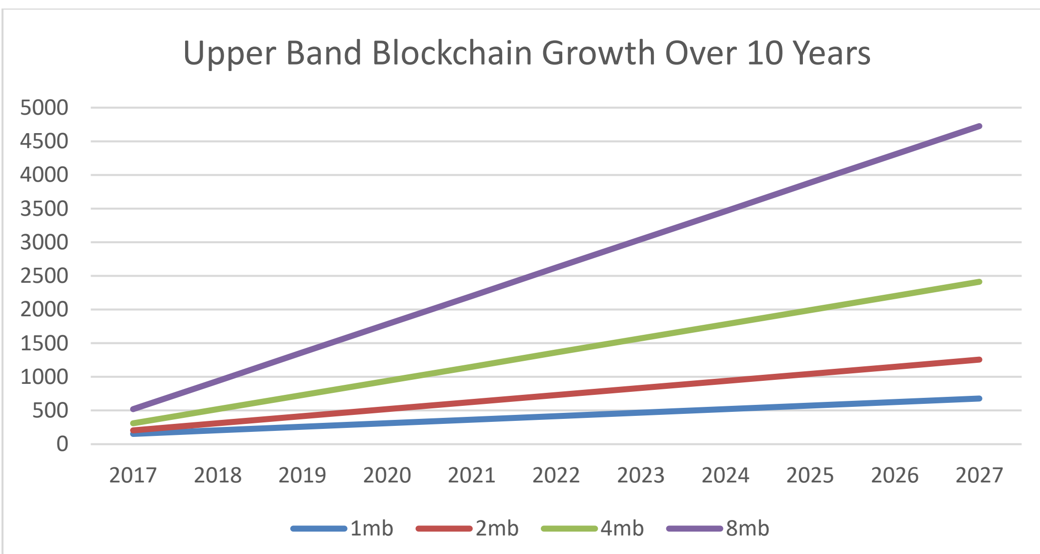
Using Bitcoin as an example, the size of the Bitcoin blockchain at the time of writing is a little over 100GB in size, compared to a few megabytes when it first launched in 2009.

The growth of the Bitcoin blockchain is limited to the maximum size of each block that the protocol permits and the timing that each block is generated and added to the network. With a maximum block size of 1mb and block release times of about 10 minutes, the maximum size the blockchain can is 1mb x 10 minutes x 6 per hour x 24 hrs x 365 days, or around 53GB per year.

If the size of each block is increased, the maximum annual blockchain would be as follows:

Block size (mb)	Block Generation (minutes)	Daily Growth (GB)	Annual Growth (GB)
1	10	0.14	53
2	10	0.29	105
4	10	0.58	210
8	10	1.15	421

As these are maximum block sizes, the actual growth can be anything up to these limits.



Full nodes typically make up the network of any blockchain protocol. Their collective agreement and validation on every block in the blockchain keeps bad actors from stealing funds and introducing dishonest or invalid contracts. The honest operation of a blockchain is best served with an extensive and decentralized number of full nodes.

Bandwidth

Blockchain data sizes of one to two terabytes or greater are well within the physical capabilities of ordinary computer storage hardware. However, while storage hardware is capable of keeping up with the growth of most blockchains, the bandwidth required to upload and download data between decentralized full nodes can be a constraining factor.

An example of the bandwidth used by a home user (moleccc, 2016) with 146 connections (mostly incoming):

month	rx	tx	total	avg. rate
Feb '16	8.87 GiB	22.38 GiB	31.25 GiB	104.62 kbit/s
Mar '16	109.58 GiB	635.21 GiB	744.79 GiB	2.33 Mbit/s
Apr '16	144.85 GiB	1.05 TiB	1.19 TiB	3.95 Mbit/s
May '16	112.24 GiB	1.08 TiB	1.19 TiB	3.80 Mbit/s
Jun '16	95.28 GiB	880.11 GiB	975.38 GiB	3.16 Mbit/s
Jul '16	90.72 GiB	925.71 GiB	0.99 TiB	3.18 Mbit/s
Aug '16	178.99 GiB	1.02 TiB	1.20 TiB	3.84 Mbit/s
Sep '16	133.12 GiB	1.03 TiB	1.16 TiB	3.83 Mbit/s
Oct '16	115.43 GiB	1.18 TiB	1.30 TiB	4.16 Mbit/s
Nov '16	15.69 GiB	213.81 GiB	229.50 GiB	6.46 Mbit/s
estimated	136.41 GiB	1.82 TiB	1.95 TiB	

For people with capped internet plans, large and growing blockchains can exceed their bandwidth allocations, before taking into consideration any HD movie and other streamlining services they may wish to consume. For users in rural locations, countries with poor internet infrastructure and locations where bandwidth throttling is allowed, using blockchains with high bandwidth requirements can be difficult to impossible.

By comparison, based on bandwidth use of 0.7GB per hour for medium quality going up to 3 GB per hour for HD quality files, Netlfix users stream between 33GB to 142GB of HD video each month (Netflix, 2016). Moreover, as very high quality video services increase bandwidth consumption goes up to around 7GB per hour.

While unmetered download plans are an obvious choice for many users, many internet service providers (ISP) have what they call 'fair use' policies. ISP can apply fair use terms and conditions where they deem download and upload usage which exceeds their average customer profiles as falling outside of fair use. In these situations, customer's may have extra charges levied, see their plans cancelled or experience throttled internet access. For those home users that use blockchains and streaming services, their monthly bandwidth consumption could become problematic leading to lower numbers of full nodes as blockchains grow in size.

Advice from Bitcoin.org highlights these and other issues for those looking to run full nodes:

- *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's common for full nodes on high-speed connections to use 200 gigabytes upload or more a month. Download usage is around 20 gigabytes a month, plus around an additional 60 gigabytes the first time you start your node.*

- *6 hours a day that your full node can be left running. (You can do other things with your computer while running a full node.) More hours would be better, and best of all would be if you can run your node continuously.*

Router processing capabilities, computer RAM and computer processing speeds can also be a constraining factor for home users who keep their blockchains operating on a computer that also conducts other activities such as gaming or media editing. As blockchains grow in size the local CPU will be using up more resources as it validates blocks being downloaded into the full node, causing frustration for some users.

Simplified Payment Verification (SPV) Clients

SPV's can be considered as slim down versions of full nodes. They can allow users to perform transactions and many ways to interact with blockchain networks, but they are not as robust as full nodes when it comes to enforcing protocol rules and so users have to place a great deal of trust in others, unlike full node users.

Example (moleccc, 2016) of a full node connecting with other peers and serving SPVs (most typically identified here as bitcoinj (Hearn, 2011)):

```
>$ bitcoin-cli getpeerinfo | grep subver | sort | uniq -c | sort -nr
   21     "subver": "/Satoshi:0.13.0/",
   19     "subver": "/Satoshi:0.12.1/",
    9     "subver": "/bitcoinj:0.13.4/Bitcoin Wallet:4.46/",
    9     "subver": "/bitcoinj:0.13.2/MultiBitHD:0.1.4/",
    9     "subver": "/bitcoinj:0.13.1/Bitsquare:0.3.3/",
    9     "subver": "/bitcoinj:0.12.2/Bitcoin Wallet:2.9.3/",
    9     "subver": "/BitCoinJ:0.11.2/MultiBit:0.5.18/",
    7     "subver": "/Satoshi:0.12.0/",
    7     "subver": "/Satoshi:0.11.2/",
    6     "subver": "/Satoshi:0.11.0/",
    6     "subver": "/BitcoinUnlimited:0.12.1(EB16; AD4)/",
    4     "subver": "/Satoshi:0.9.99/",
    4     "subver": "/Satoshi:0.8.1/",
    3     "subver": "/iguana 0.00/",
    3     "subver": "/bitcoinj:0.14-SNAPSHOT/",
    3     "subver": "/bitcoinj:0.14.3/Bitcoin Wallet:5.03/",
    ………………..etc…….
    1     "subver": "",
```

While the full nodes of a blockchain protocol collectively make up the network, that is they independently validate every block and therefore they collectively enforce the consensus rules that the entire network settles upon, SPV's just rely on the data that is provided to them by full nodes.

SPVs are typically designed to just hold block header information. Because of its much simpler operating parameters, this type of client is designed to hold much less information and therefore requires much less data storage, much less memory, hardly any bandwidth and less processing effort. SPVs are therefore ideal for ordinary users and mobile users, but this convenience typically comes with considerably greater risks than running full nodes.

To overcome some of the security weaknesses within using SPVs, SPV to full node encryption is proposed and at the time of writing a similar proposal had been independently published (Schnelli, 2016).

> *The Bitcoin network does not encrypt communication between peers today. This opens up security issues (eg: traffic manipulation by others) and allows for mass surveillance /*

analysis of bitcoin users. Mostly this is negligible because of the nature of Bitcoins trust model, however for SPV nodes this can have significant privacy impacts [1] and could reduce the censorship-resistance of a peer.

Encrypting peer traffic will make analysis and specific user targeting much more difficult than it currently is. Today it's trivial for a network provider or any other men-in-the-middle to identify a Bitcoin user and its controlled addresses/keys (and link with his Google profile, etc.). Just created and broadcasted transactions will reveal the amount and the payee to the network provider.

This BIP also describes a way that data manipulation (blocking commands by a intercepting TCP/IP node) would be identifiable by the communicating peers.

Analyzing the type of p2p communication would still be possible because of the characteristics (size, sending-interval, etc.) of the encrypted messages.

Encrypting traffic between peers is already possible with VPN, tor, stunnel, curveCP or any other encryption mechanism on a deeper OSI level, however, most mechanism are not practical for SPV or other DHCP/NAT environment and will require significant knowhow in how to setup such a secure channel

While this proposal is based on the Bitcoin protocol, the principle is transferrable to any blockchain. Peer-to-peer encryption of communications is particularly beneficial to organisations which may otherwise put them at risk of data protection laws, regulatory practices and third party snooping of transaction connections including frequency of trade.

Organisations working on private networks have fewer risks, but they are still vulnerable to leaking commercially sensitive information due to hacking, on private networks shared with other organisations or when needing to operate on private networks that are interoperable with public networks.

Decentralized Services Digital Networks (DSDN)

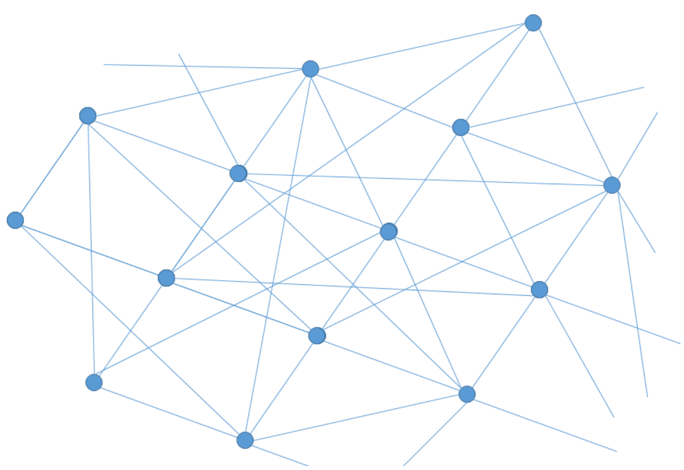
The Schnelli SPV to peer encryption proposal provides a methodology for users to connect to their own full nodes. While this is a significant improvement on the current security model of SPVs, it is potentially only of benefit to those that know how to run and manage full nodes. To facilitate a greater degree of security, for anyone who seeks it, improved security models would entail the provision of a service where users can create and manage a full node without having to be involved in the technical set-up details. This would improve overall security for any blockchain network; increase decentralization as more full nodes would be deployed; and it would be of direct benefit to all users and indirect benefit to the entire network.

The use of encryption opens up the possibility to outsource the operation of full nodes for small, medium or large organisations. The trend to outsource services to cloud hosting providers has been established for several years and it is showing signs of accelerating, with greater competition helping to fuel the growth as services improve and costs come down.

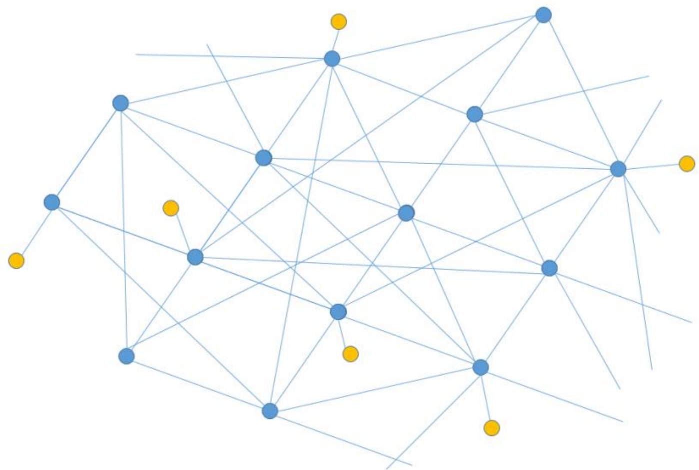
The ease and costs of running a full node on cloud networks, in particular full nodes which are growing significantly or have grown beyond the capabilities of ordinary home or small business connections, makes this option attractive for those who have some technical abilities. For small to medium sized businesses, running full nodes for their organisation will usually entail additional technical support costs, a factor often not recognised by those that do not deal with enterprise software.

This poses the option for a new way to operate Blockchains as a Service, where users can:

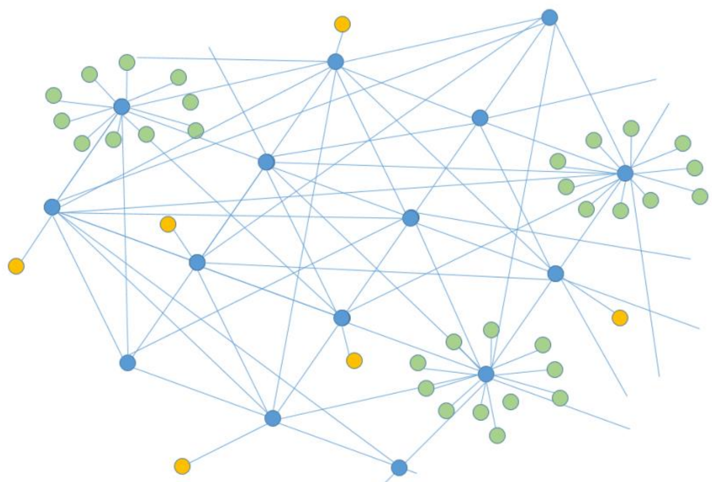
- run full nodes on their own within their own home or local network;
- operate just with SPVs;
- operate with SPVs linked to a full node under their control, within their own home or local network;
- operate with SPVs linked to a full node under their control, with encryption enabled within their own home, local network or remote cloud network; or
- operate SPVs linked to one or many full nodes under their control, with encryption enabled on their local network or remote cloud network.



Decentralized network of full nodes



Decentralized network of full nodes, with SPV clients connecting to full nodes, with encryption where activated



Decentralized network of full nodes, with SPV clients connecting to full nodes, with encryption where activated

Organisations deploying one or many full nodes, with users running one or many clusters of SPVs connecting with secured encryption

Choosing the option best suited to users gives increased choice and flexibility. While opting to host nodes remotely on cloud networks and creating an encrypted connection provides a way to avoid congested home or local networks as blockchains grow in size. This shift to professionally managed cloud networks of full nodes was identified very early on by the inventor of the blockchain (Nakamoto, 2010):

> *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.*

On private blockchains, hosting nodes on cloud services would not cause many organisations any difficulties or concerns, provided the cloud or node hosting environment is professionally managed and has the required security certification. For public blockchains, however, decentralization is one of the defining features of the secure operation of that network, in particular the principle of operating without having to trust anyone on the network. Where nodes become centrally managed, the opportunity for coordinated service denial or Sybil (Jyothi, 2011) coercion increases substantially.

For any full node cloud hosting service, Decentralized Services Digital Networks (DSDN) is an option introduced here to overcome some of the risks with clustering full nodes into pockets of data centres operated by the same companies, while providing the many benefits of running on the cloud.

Multi-Layer Relay Networks

Within a decentralized network, blockchains can be spread around the world and hosted on a variety of networks that range between slow and inefficient to extremely fast and efficient. Where blockchains are reliant, for example, on proof of work to determine the construction of the longest chain of blocks and the consensus that all full nodes settle upon to follow, the propagation speed of newly created blocks around the network is of significant importance. On public networks where different miners (Back, 1997) are rewarded for generating new blocks, there is substantial competition to improve these relay networks and reduce the chances of newly found blocks being refused by the network (orphaned) as these represent loss of income compounded with wasted overhead costs.

Fast relay networks are now commonly used to ensure that newly generated blocks are transferred around public blockchain networks as quickly as possible. The Fast Internet Bitcoin Relay Engine (FIBRE) (Corallo, 2016) has been adopted extensively to transmit information between specific nodes as quickly as possible. These nodes then help to communicate with other full nodes the existence of new blocks so that the entire network is aware of the proposed new longest chain of blocks and can quickly come to a network wide consensus. On a public blockchain there will be many other organisations that produce their own versions of FIBRE in an attempt to be the fastest to have their blocks accepted and competing blocks rejected by a network. Mining pool operator ViaBTC has stated publicly (Yang, 2016) that they host full nodes around the world and that their block relay times are better than what could be achieved with FIBRE:

> *We have also spent much time increasing our block synchronization, we use what I call "Block high-speed network" technology to propagate blocks quickly. We have deployed nodes around the world for this purpose, and we use something similar to Xthin to get propagation times from 15 seconds down to ~1 second, and an additional 0.5 seconds to verify each block. On average when we broadcast an empty block, within ~1.5 seconds we can start mining a full block again.*

Multi-Layer Payment Hubs

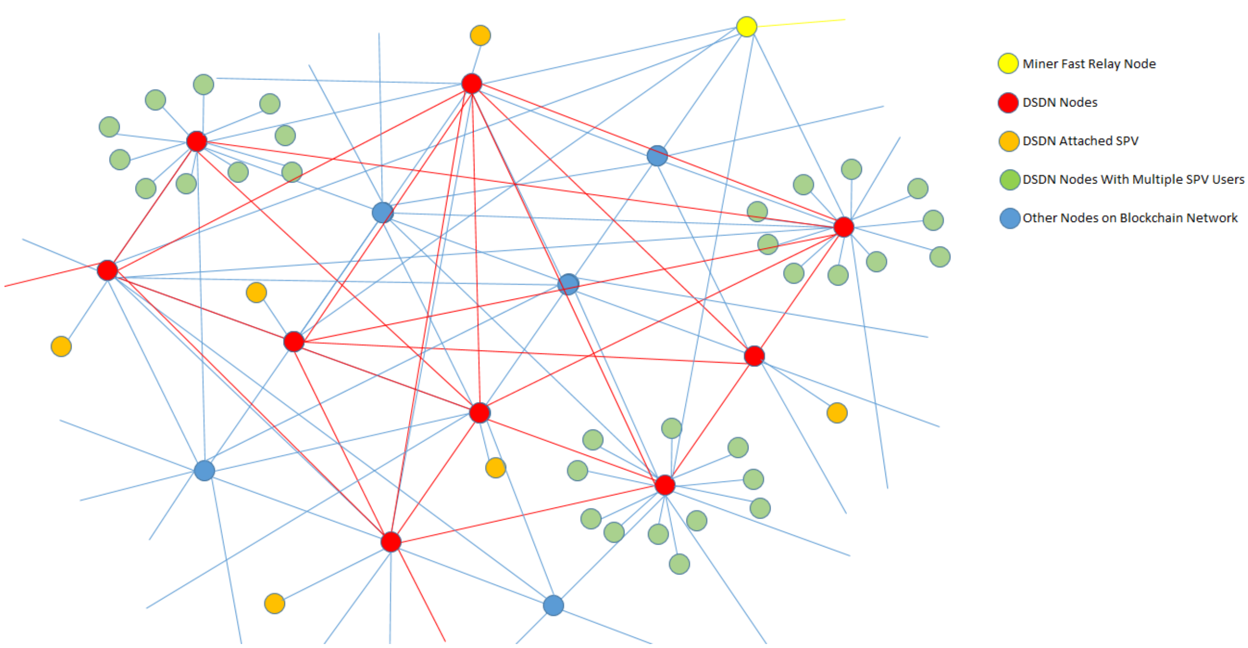
High speed second layer relay networks also facilitate the use of payment hubs. These hubs have the benefit of being on secure DSDN networks with high speed connections which in turn facilitates faster and cheaper payments.

Payment hubs are explored in a separate white paper as they are a by-product benefit of DSDN which introduces increased use of encryption which is necessary to protect counter parties to transactions.

Six Degrees of Separation

DSDN does not propose to compete with miners who implement networks of full nodes running superfast relay code in an attempt for the network to accept their blocks ahead of any other miners. Instead, DSDN is a proposal to be the next hop for propagating blocks around public and semi-private blockchains which use openly competitive PoW to determine the longest chain. By virtue of DSDN being a professionally managed service, miners might want to connect with DSDN nodes to help them get their blocks broadcast faster and accepted by the entire network.

By creating connections with the optimal number of hops between nodes on a particular blockchain, DSDN can improve synchronisation times and block propagation overall, with minimal looping back of connections.



- 6 node connections, 5 relay hops, 6*6*6*6*6=7,776 nodes propagation
- 8 node connections, 4 relay hops, 8*8*8*8=4,096 nodes propagation

Outbound connections between nodes can be optimised by Node Connections^ Hops, in order to self-adjust inbound and outbound connections to the fastest and most efficient configuration between priority DSDN nodes. The self-adjustment rules will ensure that the network will have minimum standards for bandwidth, up time, processing speeds and both inbound and outbound connections to avoid wasted effort. The operation of the rules may require human intervention as there could be hardware and bandwidth cost implications. As such DSDN is intended, by design, to be a remote managed service.

The DSDN network is intended to create two tiers of nodes. The first tier is a priority distribution channel between DSDN nodes. The second tier is connectivity to other non-DSDN nodes on the network. When users initiate a DSDN node instance by launching a DSDN SPV light client, they will launch a full node which connects to DSDN protocol recognised nodes. This design is to give priority to tier one priority connections.

SPV light clients and DSDN full nodes will be monitored by the protocol to ensure an efficient ratio of full nodes are operating. From a network point of view, this will significantly increase the numbers of full validating nodes on a network, while maintaining optimal connectivity hops between nodes within a desired range measured by optimal speed of synchronisation.

Node Connections	Hops	Nodes Relayed
11	6	1,771,561
11	5	161,051
11	4	14,641
11	3	1,331
11	2	121
9	6	531,441
9	5	59,049
9	4	6,561
9	3	729
9	2	81
8	6	262,144
8	5	32,768
8	4	4,096
8	3	512
8	2	64
7	6	117,649
7	5	16,807
7	4	2,401
7	3	343
7	2	49
6	6	46,656
6	5	7,776
6	4	1,296
6	3	216
6	2	36

This introduces an economic barrier to launching a Sybil attack and attempting to isolate specific DSDN nodes as it is greatly increases the resources required to target a DSDN node which is giving priority to its tier 1 connections and then relaying information to other *tier 2* full nodes which help propagate blocks around the network. Within private networks, DSDN is simply an outsourced full node managed cloud service, but with encryption added to every SPV to full node connection by default.

Man-in-the-Middle

One of the principle concerns with launching an encrypted SPV to Full node BaaS arises during the process of creating an initial secure connection. Anyone who is able to intercept the initial connection poses a man-in-the-middle attack risk which can potentially compromise the secure connection, leading to snooping or serving false data. Peer authentication proposals for securing encrypted channels, such as SPV to Full node, have been proposed and are being actively developed (Schnelli, 2016). As DSDN is a commercial managed service, the process to established the initial and ongoing payment mechanism can be used to facilitate an authentication procedure using public / private key pairs.

Digital Services Digital Network

As a commercial managed cloud service providing outsourced blockchain management and secure access, DSDN is concerned with providing the best relay services to assist with the fast, efficient, safe and healthy provisioning of any blockchain protocol.

Managed blockchain services can be provided at different cost levels which an individual service provider can create and propose to potential customers. For example, Standard, Gold, Platinum and Diamond fee structures which can represent the amount of monthly bandwidth required, processor speeds, choice of locations.

Commercial organisations, for example, would benefit from this type of service for a number of reasons:

- Outsource of day to day management of full nodes
- Remove bandwidth constraints on already congested networks
- Clustering SPV's around smaller numbers of full nodes reduces external snooping risks by third parties, on both private and public blockchains
- Removes cost and management of hardware
- Facilitates ease of running multiple blockchains
- Flexibility to increase or decrease requirements
- Deployment of full nodes close to any worldwide location

The development of a market based managed fee structure is essential to encouraging individuals and small organisations to thrive so as to reduce the impact of large cloud services providers on public blockchains. Small operators will also want to offer the best possible connectivity, hardware, bandwidth at particular price points relative to the type of customer.

For example, an ordinary user who just wants a secure connection and a dedicated full node might be prepared to pay $20/month for a managed service; whereas businesses wishing to run full nodes might be prepared to pay $75/month to $250/ month per user depending on the type and level of services and key performance criteria that are required, such as telephone support or one hour disaster recovery options.

The commercial merits for introducing this type of managed service option comes from the reality that people do not run full nodes where there are other options. Using the Bitcoin Blockchain as an example, while it is almost impossible to know who runs Bitcoin full nodes, there is general acceptance that a majority of the 5,000 to 6,000 nodes currently on the network are operated by Bitcoin focused businesses, Bitcoin developers and avid supporters of Bitcoin. This compares to the 10 million Bitcoin wallets that are in use on Blockchain.info, an online Bitcoin wallet service; or the 1m to 5m Bitcoin SPV wallets that have been downloaded from the Android store.

Layer Two Service Node Provision

The specific implementation considered here is to operate on a layer-two protocol which sits above any particular blockchain. While this is not necessary, it does provide an element of *'trustless'* service provision in that those wishing to offer managed hosting of full nodes can be rated by users and by a network according to the networks own protocol rules. Those that perform below network service levels can then be offloaded from the network.

Service providers will be independent contractors or businesses who will be able to advertise themselves and a network they work on. They will be awarded trust marks based on their performance and past history which will attract customers to their services, an approach similar to that used by Uber and many online stores. The economic model will be developed outside of this whitepaper, but options for paying regular fees to be on the network; a share of revenues; or charging based on a franchise approach are potential models that could be considered.

As with any service, users can do all or none of the work. If people and businesses wish to do the work of connecting to the service node network, they save on the service provision costs. However, these self-serving users may still need to pay a contribution to be on the network and have the network give ratings for how well their systems are set-up and running.

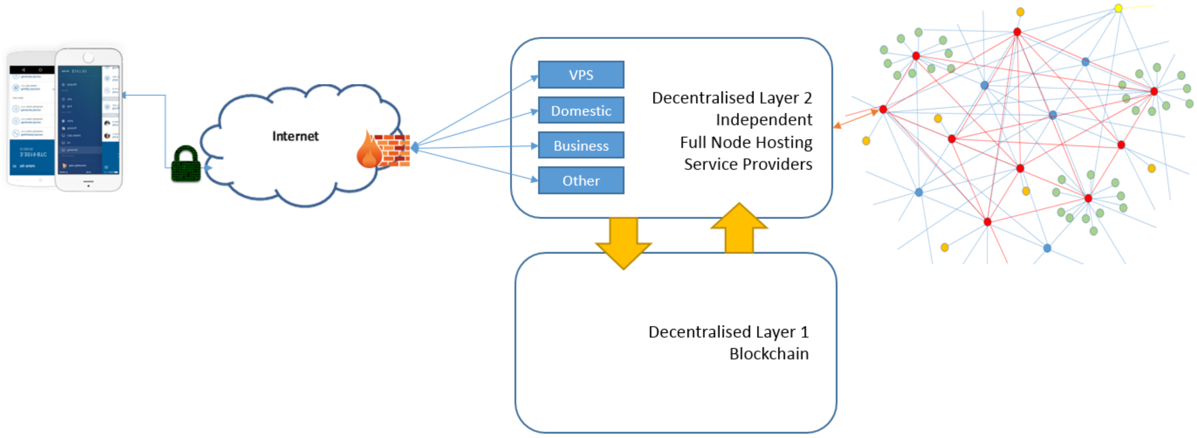
If running on a public blockchain, Bitcoin for example, communication materials could be similar to the following:

> *If you want to run a full Bitcoin node, but you do not know how and or you do not want to do the technical work, then you can:*

- *Go to your smart phone*
- *Launch your full node from an app*
- *Pay a monthly fee to a service provider, who will pay some of that fee to the service node network on your behalf*
- *A service provider will automatically launch the full node for you and enable you to quickly and easily set-up a secure connection between you and your full node*
- *You now have the encrypted security benefits that come with running your own full node, but with the ease of using an app on a smart phone*
- *Please rate your service provider*

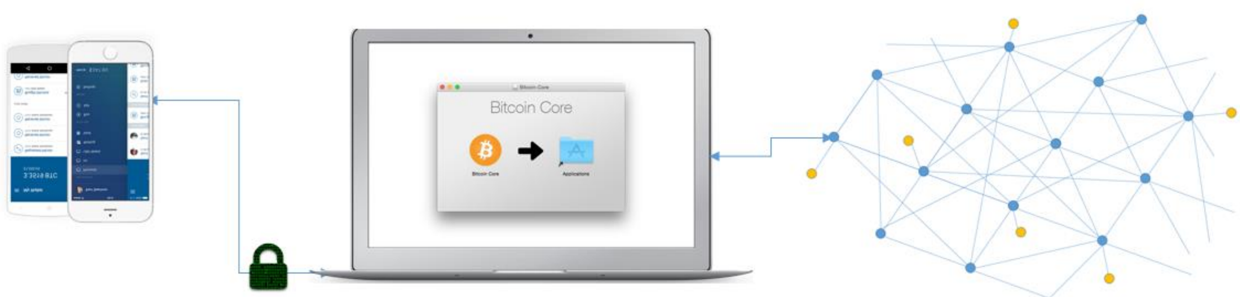
Those wishing to use public blockchains and do not wish to join a service node network would still be able to create their own secure smartphone to full blockchain connectivity, but they would need to maintain that solution themselves. So working within a service node network provides ease of engagement with higher levels of security for an individual, businesses and the blockchain network being used.

DSDN Managed Service Network



The opportunity to earn revenues and the fear of losing that opportunity will encourage responsible service providers and create an element of market driven competition to provide the best possible services at the most economic price points.

Non-DSDN Network with SPV encrypted connection to own Full Node



Much of the SPV encryption technology is specified outside of this white paper and it is known to be technically feasible. The secure connectivity to the layer two DSDN network is new and novel and requires the greater focus to implement.

SWOT

With any technical and commercial solution to complex problems, there will be good and bad points.

Strengths

- Complicated technical challenges of running full nodes on blockchains that are growing in size and complexity are outsourced to those most able to take on the challenges
- Users can focus on just being users, removing barriers to participation
- Increased decentralization through wider adoption of full nodes
- Faster relay networks where increased use of high bandwidth and good quality hardware is used
- Service provider rating system improving quality, service levels and lowering costs
- Service provider collateral requirement to prevent Sybil operators

Weaknesses

- Perception that encouraging professionally hosted options somehow weakens decentralization by providing an attack vector for law enforcement and regulatory oversite
- Managed services have a labour and infrastructure resources cost which will be a barrier
- Vetting of new service providers is not possible and users must rely on evidence of poor service

Opportunities

- Creating an independent contractor network creates jobs around the world
- Competition for managed cloud services will reduce costs, improve deployment technologies and encryption options
- Encouraging greater more diverse adoption of blockchains beyond specific groups
- Greater use of encryption between users operating SPVs and full nodes limiting scope of snooping services

Threats

- Rogue contractors setting up services to steal customer funds
- Government agencies setting up services to snoop on individuals or businesses
- Law enforcement agencies serving notices to contractors to intercept user's transactions
- Too few cloud providers

The DSDN model attempts to move two positions which can be diametrically opposed:

- On a mass scale, people have demonstrated that they do not wish to run full nodes; but it is the safest option; and

- On mass, people have demonstrated that they do want to run SPV's; but it is the least safe option.

By offering an SPV to full node encryption service, these two positions become aligned improving security for both users and any a blockchain network being used.

The Opportunity Landscape

DSDN is a commercial proposition, in particular, for people to run hosted full node services for others who wish to securely run decentralized lightweight clients.

Businesses are increasingly hearing about blockchain technology and how it can allow them to verify, for example, the end-to-end provenance of supply chain interactions or deploy highly secure and live ERP systems for a fraction of the cost of current software tools. Thousands of businesses within individual supply chains can work together without needing to worry about the interoperability of systems with businesses they have no direct communications with and have no insights into the particular IT systems they may be running.

The smartphone market is set to grow from around 2.5bn to 5bn users over the next few decades.

The consumer to business; the business to consumer; and the business to business SPV markets, along with the increasing use of Blockchains within business supply chains are all big open markets for DSDN.

DSDN Summary

- DSDN is an option for individuals and businesses with little or no technical expertise to be able to outsource the operation of either private or public Blockchains with a choice of quality of hardware and bandwidth services.

- Network of full nodes operated by third parties for those wishing to outsource this function and run SPV's locally.

- Third party full node hosting providers operate a Pay-Per-Use full node hosting model based on a full node authenticating with a customer's SPV wallet that the full node is on the network.

- The download and launch of a specific SPV creates a full node on a remotely hosted and professionally managed environment.

- Download and launch of SPV creates an encrypted channel with the professionally hosted and managed full node with username and password controlled by the user on their SPV client, with optional bank grade hardware wallet security.

- Professionally hosted and managed full nodes are operated on best possible connectivity, hardware, bandwidth for the price plan requested by the user. This can range from hosting on VPS or locally on service providers home network.

- Node operators are preferably individuals and not corporate hosting organisations to promote as greater decentralization as is possible when operating a managed hosting service.

- Businesses can still opt to run nodes through centralized cloud hosting options if they have specific security policies, audits and certification that they have to meet.

- Businesses can enable multiple users on a many-SPV-to-one-full node basis to save on costs. Single sign-on authentication and password policies will be premium cost factors which will entail additional effort by the managed hosting provider.

- DSDN can be operated on public, private or public-private networks.

- Easy process to set-up a fully validating node with automated wallet encryption functionality

- Service providers are rated by a layer two protocol and end users

Bibliography

Back, A., 1997. *Hashcash.org.* [Online]
Available at: http://hashcash.org/
[Accessed 4 November 2016].

Corallo, M., 2016. *Fast Internet Bitcoin Relay Engine http://bitcoinfibre.org.* [Online]
Available at: https://github.com/bitcoinfibre/bitcoinfibre
[Accessed 17 November 2016].

Corallo, n.d. [Online].

Hearn, M., 2011. *Bitcoin Wiki.* [Online]
Available at: https://en.bitcoin.it/wiki/Bitcoinj
[Accessed 15 November 2016].

Jyothi, B. S. &. J. D., 2011. SyMon: A practical approach to defend large structured P2P systems against Sybil Attack. *Peer-to-Peer Networking and Applications*, Vol-4, Issue-3 September, p. 289–308.

moleccc, 2016. *Reddit/r/btc.* [Online]
Available at: https://www.reddit.com/r/btc/comments/5b0g4x/remember_that_time/
[Accessed 11 November 2016].

Nakamoto, S., 2009. *bitcoin.org.* [Online]
Available at: https://bitcoin.org/bitcoin.pdf
[Accessed 4 November 2016].

Nakamoto, S., 2010. *Bitcointalk.org.* [Online]
Available at: https://bitcointalk.org/index.php?topic=532.msg6306#msg6306
[Accessed 9 November 2016].

Nakamoto, S., 2010. *Bitcointalk.org.* [Online]
Available at: https://bitcointalk.org/index.php?topic=532.msg6306#msg6306
[Accessed 15 November 2016].

Netflix, 2016. *How can I control how much data Netflix uses?.* [Online]
Available at: https://help.netflix.com/en/node/87
[Accessed 25 November 2016].

Schnelli, J., 2016. *GitHub bip-0150.mediawiki.* [Online]
Available at: https://github.com/bitcoin/bips/blob/master/bip-0150.mediawiki
[Accessed 15 November 2016].

Yang, H., 2016. *r/btc.* [Online]
Available at:
https://www.reddit.com/r/btc/comments/5ddiqw/im_haipo_yang_founder_and_ceo_of_viabtc_ask_me/
[Accessed 17 November 2016].