Shift – Introductory White Paper

Phantom: a decentralized storage suite

Version 1.0.1

Isabella Dell - Craig Campbell - Ralf S.

February 1, 2018

Contents

ABSTRACT

Censorship and the suppression of information has been a common problem throughout human history. The advent of blockchain and other decentralized technologies has created a technological revolution that can ensure no content is easily censorable. A combination of storage and presentation layer technologies has the potential to empower end users and operators with the ability to preserve data free from censorship.

Shift proposes a solution to the problem of censorship and defines how a combination of these new technologies solve that problem.

1 INTRODUCTION

This white paper provides an introduction to Phantom, a unified technology suite used as a platform for hosting content in a decentralized system. The scope of this document is to specify the general technical approach Shift is undertaking. This will be done by defining the problems that Shift is attempting to solve with Phantom as well as describing how the different technologies address those issues.

1.1 Definition of the Problem

In the world today, there is no greater potential threat to the freedom of information than the operators of the Internet themselves. Server hosts, governments, and ISPs (Internet service providers) control the Web and can remove access to content through server shutdowns, blacklisting and DNS (Domain Name System) takeovers. The technology available was not mature enough to prevent these authorities and their attacks on the Internet. IPFS (the InterPlanetary File System) (Benet, 2014) and other technologies are in a state of readiness to be leveraged to create a new decentralized Internet to mitigate the threat of censorship.

1.2 Expand on the Problem

1.2.1 Net Neutrality and Internet Service Providers

ISPs act as the single entry point to the Internet for nearly all end users today. These institutions are usually private commercial entities providing connectivity to their customers. ISPs are not going to vanish any time soon – the threat they pose to the freedom of the Internet is clear and present. One example of ISPs manipulating what end users can do was seen in the late 2000s. Comcast implemented a form of traffic shaping targeting BitTorrent users (to Marlene H. Dortch, 2008; Eckersley, 2007), preventing them from accessing the content they chose to access, even if that content is freely available content. This attack on their paying customers should be considered a violation of Net neutrality, the principle that all content and applications should be accessible regardless of source.

Net neutrality was an unwritten concept which governed the Internet since its inception. Freedom of information was seen as a fundamental need to advance technology for all of humanity's benefit. One potential threat to Net neutrality is from the ISP which can block, limit, or slow access to content they may not agree with. ISPs may choose to charge more for premium access to content. While bypassing the ISP is generally not possible, content providers can use new technologies to decentralize their content and spread it in a way that ISPs will not be able to censor easily.

1.2.2 Government Agencies

Governments as a whole have a stake in the Internet for law enforcement, counter terrorism and intelligence gathering operations. Given these powers and responsibilities, they are also granted many authorities over the Internet via judicial systems. For example, in the United States, a website or service can be shut down by the FBI with the proper warrant (Search.usa.gov, 2018), effectively censoring that website. In some circumstances, the agency will repurpose a website to cast a wider net to capture even more evidence. While this style of takeover is usually reserved for severe criminal activity (Silk Road, illicit services), it does represent a direct attack on individual liberties. (Martin, 2013).

Other examples of Government attacks on the Internet can be seen in the political space. In September 2017, the Spanish Government seized the top level domain provider for ".cat" (Morris, 2017), effectively granting them full control of the DNS running under that extension. Furthermore, the Government began to forcibly censor websites supporting the Catalan referendum and ultimately prevented vote submissions from polling locations. Government censorship is a clear and present danger to the Internet today. The new Internet must evolve past these problems to keep information freely available.

1.2.3 Centralized Server Hosting

Server providers and operators, such as Amazon and Microsoft, provide systems to host websites or other applications. Often, these providers are too keen to cooperate with government agencies and their requests for service termination (Raphael, 2009; Chen, 2017). Additionally, they operate as a centralization force in the ecosystem of the Internet. Hundreds of thousands of websites were impacted by an outage at Amazon S3 East in early 2017 (Amazon, 2018). During this outage, many major websites were completely inaccessible, and large portions of the Internet ceased to function.

As the Internet continues to scale, these providers will gather more users requiring hosting and these issues may occur more often. Mitigating this problem is possible with some newer technologies like IPFS, but the infrastructure to bring websites into IPFS and present them to the masses has not been widely available.

1.3 Proposed Solution

In order to solve the problem of web centralization and censorship, there must be a system or software layer available to remove or mitigate against single points of failure. On the Web there are various points of failure – server hosts, DNS (Domain Name Service) providers, and Internet connectivity to the WAN (Wide Area Network). Unfortunately, solving WAN connectivity is out of scope for this document, but server hosting and DNS issues can be mitigated through the use of a suite of software named Phantom being developed by Shift. Phantom is a layered application providing a technology stack built for decentralization.

Phantom provides the solution to many sources of web censorship. As the name suggests, services hosted on Phantom may vanish from one host but remain accessible from another host in the network. Phantom implements an IPFS backbone to create the storage layer of the Shift network. End users can submit their files for long term storage using a blockchain based space leasing system. Website operators can serve their entire website from the Shift storage cluster using Hydra to render resources and keep their content live using Jenga, which dynamically updates resources for discovery, if they are being censored. This technology suite creates a seamless end user experience that cannot be easily censored.

2 STORAGE LAYER

2.1 InterPlanetary File System

The Phantom storage layer consists of a freely available technology called the InterPlanetary File System. IPFS is a peer-to-peer hypermedia distribution protocol (Benet, 2014) which serves as the backbone for many decentralized storage applications. It provides a well documented protocol for implementing a distributed file system suitable for serving web applications and other types of content. IPFS is described as having no central point of failure and is fully peer-to-peer, meaning any user can participate in the system. This file system protocol does not rely on any central authority to govern its operation. IPFS is poised to create a new decentralized Internet infrastructure that is free from censorship.

2.2 Implementation – Shift Storage Cluster

The default state of the IPFS infrastructure is represented as a globally shared network. This can lead to problems when it comes to verifying data integrity, availability, and custom implementation details such as earning token rewards for running a storage node. For this reason, Shift runs a private swarm. The storage nodes use a custom swarm key to ensure that they can only talk to other nodes using the same key. This also prevents Shift nodes being used to host and deliver content that was added outside of the Shift network which should improve reliability and performance.

In order to store data permanently, IPFS implements a concept called pinning. Pinning content means that the content will be available permanently (or until it is unpinned). By default the pinning only applies to a single peer that it is pinned to, but that means if that machine goes offline, the content can be lost. The way around this is by using an IPFS cluster: a subnet (or private net) running the IPFS daemon, containing only Shift peers.

The Shift cluster runs as a wrapper around the IPFS daemon. It allows the end user to connect a group of IPFS nodes together so that content can be stored and replicated within the group. The cluster elects a leader to be in charge of keeping track of which content is available in which locations.

The Shift cluster provides a modular clustering system for use with IPFS. This clustering system works in conjunction with the IPFS daemon in order to accomplish the following tasks:

1. Pin, unpin and repin content to peers
2. Provide an HTTP API for communications
3. Assert and follow cluster consensus
4. Replication factor
5. File storage and retrieval

These functions come together to provide an extensible decentralized storage system that operates completely independently from the public IPFS network. This is vital to allow users to insert and persist content within the system.

2.2.1 File Pinning

During the operation of IPFS, unused files are naturally cleaned up over time. In order to keep files permanently, they must be pinned within the system. Pinning prevents the garbage collection process from removing the item prematurely, ensuring that it will always be available within the cluster.

2.2.2 HTTP API

IPFS offers a suite of internal commands and functions to interact with the network. These same set of functions are mirrored to an HTTP API allowing external software to interact with the system. These functions allow Phantom to communicate with IPFS remotely without needing the end user to join the cluster.

2.2.3 Consensus

The IPFS cluster requires consensus between nodes to ensure that all stored information is kept in sync. This is especially important for pinned content, which must be stored indefinitely. A node is elected as the leader and operates as such until it goes offline or a new leader is elected.

2.2.4 Replication Factor

The Shift hosted cluster is currently configured to replicate each piece of content to redundant nodes to prevent data from being lost. This means each file is backed up in multiple additional locations beyond the primary location. In case one of the backup locations is unavailable, the cluster will automatically replicate the content to additional nodes. This allows the network to scale since the data does not need to be copied to every node.

2.2.5 File storage and Retrieval

Once data is pinned within the system and participating nodes receive the propagated data, the storage nodes retain that data in the cluster. When requests for that data arrive at the storage nodes from the serving nodes, the storage nodes provide that data to the serving node which caches the data to prevent the need to retrieve the same data repeatedly. New service nodes can join and provide the data from the storage nodes.

Files are retrieved from the system by cryptographic hashes. These hashes are generated when the file is inserted into the system and saved for later use. This is especially important for storing files using a blockchain as this hash can provide an identifier to link the file address to the transaction paying for the storage.

2.3 Service Layer

Phantom provides a service layer that functions on top of the storage layer services. These services include HAProxy and Jenga. The primary function of the service layer is to connect Phantom to "Old-World" Internet protocols, such as DNS, and provide traffic management for the storage layer.

2.3.1 HAProxy

Phantom includes HAProxy, which provides discrete addressing and traffic handling for API endpoints for both IPFS and its cluster. In addition to handling the back end traffic, it also handles any front end requests to the system. It leverages SSL to provide encrypted communications between client and server. It also takes care of all incoming requests, to be forwarded to either the daemon or the cluster. With HAProxy acting as a shield, only whitelisted calls will be executed by the target application. All forbidden requests will be rejected.

2.3.2 Jenga

Since no mainstream browser supports IPFS natively yet, there needs to be a way to map an incoming request to a specific server. It could be solved using a Chrome or Firefox browser extension to pick an IPFS node to serve the content in the browser, but this is not ideal, because end-users should not have to install third-party software before they can visit a website hosted by Phantom.

Another possible solution is using an internal load balancer, but this also has issues. The primary issue is that it is centralized. If the load balancer fails, all requests to Phantom would fail. The second issue is found in throughput or performance issues, such as when the system has to scale to handle more traffic. The system would be required to support throughput of the entire Phantom network which is not feasible for a worldwide file storage system.

Jenga solves both of these issues by providing a scalable solution that works without requiring installation of any additional software for the end user viewing the content.

Jenga is a DNS monitoring solution that observes top level DNS entries for changes and records those changes. When changes relevant to the IPFS cluster are detected, Jenga updates all storage nodes in the cluster. By maintaining persistent communications with all nodes, Jenga can create a consensus on healthy DNS state and subsequently evict non conforming nodes from the system. This prevents attackers from joining the cluster and injecting an improper DNS entry, removing the DDoS (Distributed Denial-of-Service) attack vector from the system.

Jenga creates a bridge between the decentralized Web and the classical Internet, which relies solely on DNS records. Jenga creates a dynamic web addressing system and facilitates traffic scaling from one node to many thousands based on the records placed in the system. This functionality is transparent to the end user, requiring no external interaction for the system to operate. At a fundamental level, Jenga enables the system to address some of the central points of failure: DNS censorship and traffic shaping.

In order for Jenga to function, it must maintain contact with all connected peers of the IPFS cluster. If Jenga detects a change in the cluster, it updates DNS with the new information. In the event that a node is misbehaving or is offline, Jenga will take action and remove that peers' allotted CNAME record, thereby evicting it from the cluster. Peers can rejoin the system after errors are corrected and report a healthy status to Jenga.

When the gateway is called upon by an external actor, one of the peers in the cluster is selected to serve the data to the caller. This process is made seamless by the replication of data throughout the cluster.

In order for a new site to join the system, that operator must provide a CNAME record for their domain which is pointed at the gateway. In the event an operator does not want to use the gateway, the operator can create DNS records pointing to their own gateway. The data will still be delivered from the cluster, but the site will lose some of the benefits of the Phantom gateway, mainly the guarantee that all healthy nodes that are available for serving are utilized.

3 BLOCKCHAIN SECURED

Content security is of utmost importance in a decentralized system. Any data that goes in must come out untampered with and the consumer needs to be able to trust its authenticity. Blockchain technology is leveraged by Phantom to ensure immutability and truthfulness within the system, as an unfalsifiable ledger removes many trust related issues.

3.1 Delegated Proof-of-Stake

Shift is described as a decentralized blockchain secured by Delegated Proof-of-Stake. The elected 101 (the number N currently is 101) delegates act as the custodians of the system. These delegates generate the blocks in their allocated slot every 27 seconds (blocktime) and provide a ledger with transaction finality for Shift's web hosting platform. In addition to tracking account balances and registration states, it provides a system of cryptographic linkage between private and public keys.

Every user in the system can have one or more private keys at their disposal, and these keys can be used to provide ownership of tokens within that system. This is especially important when combined with the blockchain which will host Phantom. Users will need to send some tokens from the Shift blockchain to the Phantom sidechain.

3.2 Phantom Sidechain

Building on the existing system offered by Shift, the sidechain will implement new functionality specific to the platform. The functionality expands on the concept of the transaction type found within Shift and, a new group of transaction types will be created for use in the sidechain.

Type 10 - Storage Request
An end user, or system needs to store content within the cluster. In order to do so, the user submits a request to secure storage within the cluster. Upon receipt in the sidechain, and confirmation into the blockchain, the user will be allocated storage within the system. This storage will enable the user to insert files into the system.

Type 11 - Return Storage
At some point, a user may not need to use storage any longer. In this case, the user will submit this type of request to unlock their tokens. After the transaction is confirmed, the user will be refunded their tokens from the system.

Type 12 - Provide Storage
In order for the system to operate correctly, storage must be provided to the system. A user with excess storage can provide it to the network by submitting a request, including amount of storage to add and must have Proof-of-Stake backing the request.

Type 13 - Withdraw Storage
As in Type 11, a user may want to refund their tokens, concluding their business offering storage to the network. This request is submitted to the network, and upon confirmation, the user is refunded the locked tokens associated with the storage commitment.

3.3 External Interactions – Deployment

Phantom is deployed via the Shift mainchain applications interface. In order for an operator to deploy Phantom for their own use, the operator will need to run a copy of the Shift mainchain. Additionally, an operator will need to use the Phantom interface to upload their own files, or work with the provided suite of APIs for inserting new content. Self deployment of Phantom is not necessary for an end user to interface with the system.

4 PRESENTATION LAYER

As with many layered applications, the end user interacts with the top layer, or the presentation layer. In Phantom, the presentation layer consists of Hydra and works in conjunction with the storage and service layers.

4.1 Hydra

A content management system is a web application used to publish documents and site content without the need for technical knowledge. The end user can submit plain text, and the software will render the layout in a consistent way. A website with dynamic content and regular updates is difficult to operate without a CMS. In order to overcome some limitations of IPFS, such as the lack of ability to operate with software written in some common server-side languages and lack of support for many database systems, a custom made CMS was created.

The custom CMS, called Hydra, is a new technology that operates as a CMS built on IPFS. Hydra works in conjunction with Phantom's file manager and is currently capable of handling most common tasks such as adding, modifying and removing content. The basic feature set will serve the needs of most users and the codebase is open source to allow developers to customize and improve the software for their own needs. Hydra was written to be extensible to end users and its codebase is designed in a modular way. For example, a site page and a blog post share the same rendering engine but may have different schemas. Creating a new module is performed programmatically using Node.js by specifying some configuration items. The resulting files can then be served solely via IPFS, and all rendering occurs client side.

The front end and the back end components are separated. This enables developers to use their preferred framework such as Vue, React or Angular. The data files and module structures are rendered into JSON files, which can be used with external systems such as the Wordpress API.

4.2 Phantom UI – File Manager

The Phantom User Interface comes with an intelligent file management interface which enables end users to view and modify content that is managed by the system. The end user tracks their content through the use of a Shift account. Content submission requests are paired to this account and will be available to a user from any system. This allows the network to present the files and changes to those files after being published.

Users are able to manage their stored content in the same fashion as a typical modern operating system. Actions taken by each user propagate to the cluster. The interface provides an advanced code editor complete with syntax highlighting for all commonly used file types.

IPFS creates a unique hash for each data file, which prevents hosting or uploading identical content. This functionality streamlines the upload process, as duplicate files can be identified before being submitted. Additionally, it enables the system to operate efficiently and reduces bandwidth usage for end users and operators alike.

Phantom UI contains a DNS wizard to control the addressing of hosted domain names utilizing the Shift hosted storage cluster. This removes the single point of failure caused by requiring content submitters to host their own systems. Phantom uses Jenga to populate the list of healthy nodes that will serve the content for a requested domain.

4.3 Content Retrieval

Data stored within the system is done at a content level, rather than a locational level. This new approach provides many benefits. The primary benefit is that the location of the data is no longer relevant, allowing many nodes to present the same information and when any of the data is changed, a new hash is produced. The file system is made more intelligent by combining these benefits to create a merkle hash (root) and a relative path to a subfolder or file.

Websites are addressed by URL and content is fetched by hash. A mutable hash is used by the domain resolving system. A mutable hash can be updated by end users using their private key combined with the immutable hash. This feature allows content updates without requiring domain record updates.

5 SECURITY LAYER

Security is paramount in any system. For a decentralized system, security is a fundamental necessity to create stability and build trust in its operation.

5.1 Shift Cluster Security

The cluster plays a very important role within Phantom. Within the cluster, there are multiple authentication mechanisms for hosts. These are in place in order to keep the cluster secure against attacks and other threats not covered in this document.

The first layer of authentication is done at the blockchain level. A user will need to complete the registration process on the blockchain by sending the Type 12 transaction registering their committed storage amount. Once this is done, the user can then register in Phantom as a cluster participant and complete the join process.

At the second layer, users are required to launch the application using the private key used to register with the blockchain and the encrypted join key from the storage cluster. The application will then search the blockchain for the associated storage commitment and confirm the validity. Afterwards, the application will decrypt the issued key from registering with Phantom and allow the user to join the cluster.

5.1.1 Preventing Oversubscription

In order to prevent oversubscription, both the cluster and the blockchain committed storage allowances are monitored closely by the system. When there is a low availability of storage, there will be more incentive to join and serve data, as users wishing to insert data into the cluster will pay a higher premium to use the cluster. Over time, the demand by users ongoing storage needs and supply by operators should equalize.

Operators will offer their storage in set time frames, with renewals or additions being allowed at any time before the contract expires. If an operator ceases operation before the end of their committed time frame, they will lose their stake. This requires operators to maintain high uptimes to maintain the system. There will be an allowance of a set number of hours offline for each cluster operator by the blockchain.

As mentioned above, operators are penalized for acting poorly. The loss of their funds is a large deterrent that should be sufficient for handling operator misbehavior. Users can also act poorly by oversubscribing or flooding the network. These types of misbehaviors could lead to a temporary freeze of the staked funds.

Malicious user actors will be handled by limiting the volume of content they are allowed to submit to the system over a period of time. Users can make a set number of transactions in that time frame before they begin costing substantially more to initiate after the threshold is exceeded for the period.

5.2 Data Privacy

The security of the content entering the system is just as important as securing the system itself. Users will be given the option to encrypt any data prior storage submission. However, it must be noted that any content that is encrypted is only readable with the key to unlock it. Therefore, users must be take caution when encrypting content and protect their private key appropriately.

Within Phantom, users will be able to encrypt content with specific recipients other than themselves in mind. A list of public keys can be provided and used to create encrypted messages that contain the decrypting key that only the recipient's private key can decrypt.

5.3 Illegal Content

In decentralized systems, illegal content always makes a niche for itself. For Phantom, hosting of severely unlawful content content will not be allowed. Users found injecting illegal content into the system risk losing their stake and may have their content removed. The system will only maintain pinned content, and content unpinned will be swept out quickly. This is vital as operators' rights must be protected over the user in this case.

6 CONCLUSION

Phantom is one of the world's first decentralized storage applications backed by a blockchain. It is implemented on top of the Shift blockchain as a sidechain and decentralized application. By leveraging IPFS and clustering, Jenga and Hydra, Phantom provides a censorship resistant platform for web hosting and content delivery.

REFERENCES

Amazon. (2018). *Summary of the amazon s3 service disruption in the northern virginia (us-east-1) region.* Retrieved from `https://aws.amazon.com/message/41926/` (accessed January 31, 2018)

Benet, J. (2014). *Ipfs - content addressed, versioned, p2p file system.* Retrieved from `https://filecoin.io/filecoin.pdf` (accessed January 31, 2018)

Chen, C. (2017). Tired of dmca, riaa now seeks isp cooperation in catching and stopping copyright infringement. *Privacy News Online*. (https://www.privateinternetaccess.com/blog/2017/02/tired-dmca-riaa-now-seeks-isp-cooperation-catching-stopping-copyright-infringement/ (accessed January 31, 2018))

Eckersley, P. (2007). *Comcast is also jamming gnutella (and lotus notes?).* Retrieved from `https://www.eff.org/deeplinks/2007/10/comcast-also-jamming-gnutella-and-lotus-notes` (accessed January 31, 2018)

Martin, J. (2013). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *SAGE journals*. (http://journals.sagepub.com/doi/abs/10.1177/1748895813505234 (accessed January 31, 2018))

Morris, D. (2017). Spanish polish raid .cat admin offices, threatening the internet's cutest domain name. *Fortune*. (http://fortune.com/2017/09/23/spanish-dot-cat-domain-name/ (accessed January 31, 2018))

Raphael, J. (2009). Isps join riaa's fight against piracy: Is your isp one of them? *PCWorld*. (https://www.pcworld.com/article/161978/riaa.html (accessed January 31, 2018))

Search.usa.gov. (2018). *Seize domain names - immigration and customs enforcement (ice) search results.* Retrieved from `https://search.usa.gov/search?affiliate=ice.gov&query=seize+domain+names&commit=Search` (accessed January 31, 2018)

to Marlene H. Dortch, Z. K. A. (2008). *In the matter of formal complaint of free press and public knowledge against comcast corporation for secretly degrading peer-to-peer applications, file no. eb-08-ih-1518.* Retrieved from `https://ecfsapi.fcc.gov/file/6520169715.pdf` (accessed January 31, 2018)