Archon Cloud Lightpaper

Kevin Truong, Eric Wang, Samuel Suh

Version 0.4.5
Updated as of January 25, 2019

Disclaimer: This lightpaper is meant to give a simplified technical overview of the Archon Cloud with an emphasis on the decentralized storage solution. This paper will be updated throughout the coming months to include additional detail, and a full whitepaper will be posted to www.archon.cloud when finalized. Constructive feedback or questions are welcome via email to sam@archon.cloud.

Abstract

This lightpaper describes the Archon Cloud, a collection of technological improvements to decentralized file storage systems designed to achieve the performance and reliability of centralized solutions. Archon Cloud consists of an erasure encoded file format, a decentralized file storage architecture, and a parallelized file transfer protocol, with innovations and optimizations to each. We further describe ArchonJS, a javascript library implemented on websites by adding a single line of javascript code, which allows users to browse files from the decentralized Archon Cloud with no need for key management or downloading plugins or extensions.

Why We Built Archon

The original Internet was a way to share information to any intended recipient. Archon provides a new internet architecture that gives uploaders direct control of their files, where files are available, fast, and not centrally controlled. Browsing the internet today does not require making transactions for every image asset, nor does it require key management or browser plugins. Decentralized file storage should work the same way. Archon is built with reliability, speed, and decentralization as the pillars of a new Internet.

Archon is built for reliability; it’s scalable and available.

Archon’s infrastructure couples innovations in data encoding with improvements to file delivery architecture to enable fast reliable file storage that can scale to hold the entire internet. The storage capacity of Archon’s network grows with the number of miners in the network, and files are designed to remain available even if nodes holding file shards leave the network, go offline, or get attacked.

Archon is built for speed.

In a world where it’s normal to navigate away after a two second delay in loading the page, existing decentralized file solutions leave much room for improvement. Files from Archon Cloud load in real time, and decode at speeds benchmarked to GZIP compression, which is the file compression format used today in over 70% of web pages. Our file delivery speeds will become even faster once we implement Fast File Delivery (see Whitepaper).

Archon is built for a decentralized world.

Archon does not utilize a distributed hash table (DHT) to connect to a network of peers, which is more susceptible to eclipse attacks and sybil attacks. Instead, it utilizes a cryptographic domain name server (DNS) that runs independently on a blockchain, protecting against attacks on the miners holding file shards. This storage architecture is blockchain agnostic, and can be implemented across multiple blockchain protocols to provide decentralized storage for multiple blockchain protocols simultaneously. This also makes Archon stronger and more reliable, increasing storage capacity and security, which scales with the size of the mining network.

Storage Technology Landscape

Decentralized cloud storage is an attractive solution to the world’s rapidly growing data needs.
As applications consume ever increasing amounts of data, cost-effective, provisionable and expandable storage solutions offering reliability and speed will dominate. We’ve seen this before in the migration from in-house storage to cloud storage. But if decentralized solutions want to stand a chance to gain mainstream adoption, solving its current problems of scalability, speed and reliability are a prerequisite. Blockchain technology has gained much attention and some decentralized storage projects have already made progress and launched initial public products. However, unlike centralized systems, which are

largely isolated from the outside world, blockchain nodes publicly expose much more information. Consequently, storage solutions need significant design changes to their system architecture to remain secure; they cannot protect solely against accidental failures, but must also protect against malicious storage network attacks. As the next generation of decentralized file storage emerges, it is important to keep in mind that offering cheaper storage is not enough; nor is offering an incentive layer to offset storage costs. In order to gain widespread adoption, decentralized storage must not sacrifice the speed, reliability, and flexibility we have grown accustomed to in order to achieve decentralization.

Archon Cloud is designed to fix the problems that are limiting other decentralized storage projects to bring a competitive decentralized storage solution to the mainstream.

How Archon Works

Archon Downloads

An end-user will experience faster file downloads, and fewer 404 errors without changing any behavior. It just works. Developers will be able to add a single line of javascript code to import the ArchonJS library to enable the site to access files held in the decentralized Archon Cloud via an Archon URL that can be embedded into websites, shared on social media, or archived long term like a typical URL.

In the background, several things enable this seamless user download experience, which happens so quickly users will not notice. When a URL is entered:

1. The DNS cryptographically finds which miners are storing the relevant shards of the encoded file being stored.
2. The user connects with the storage miners holding the shards.
3. The miners send relevant shard(s) to the user until enough shards are downloaded.
4. The shards are decoded back into the original file.

Archon Uploads

An uploader's experience will be as follows:

1. Get an account (this can be any wallet on a supported chain).
2. Add tokens. Tokens are used to store files and cover bandwidth allocation.
3. The uploader chooses the file to upload, with optional additional encryption.
4. Press the Upload button.

In the background, the following will occur:

1. The file is encoded.
2. The file is sharded.
3. A blockchain transaction is sent (including the payment for storing).
4. Miners are cryptographically determined by the DNS.
5. The shards are transmitted to the relevant miners.

Downloader Accounts Not Required, Miner Accounts Required

Creating an account is required for Miners and those who wish to earn rewards on the blockchain. A downloader is not required to create an account. An account holder (such as a dapp) can generate temporary public/private key pairs for the end user during an instantiated session. This allows seamless integration of the Archon Cloud for even casual web surfing of files held in the Archon Cloud. To the end user, it's the same as browsing today's internet, but with faster file downloads and fewer 404 errors from missing files.

Miners are required to have an account, stake tokens, and prove their storage capacity. To create a new account, a miner will gossip his intent to create an account on the network by (1) communicating account information to Archon's network, as well as (2) providing a passed Proof of Space. The more disk space reserved for mining, the more files the miner will receive, in turn earning more mining rewards. Additional Proofs of Space can be submitted at a later date to increase disk space allocated for mining.

ArchonJS

ArchonJS is a javascript library that enables access to Archon Cloud's storage with a single line of javascript imported into a website by the website owner. With this, the end user's web browsing experience is the same as that of today. Images and videos can be rendered on a browser without additional plugins, extensions, or native applications. Files stored in Archon Cloud can be accessed via an Archon URL and can be displayed in real time so the end user is not aware that the files are being held in a decentralized system. ArchonJS locates the shards via the Archon DNS, downloads the shards from the decentralized mining network, and decodes the shards into the original image automatically, completing these steps with minimal additional overhead.

File Processing and Networking

The core of Archon's technology is the Archon Format, which is a file format based on Archon's patent-pending erasure encoding algorithm. Erasure encoded files have the ability to lose large portions of data and still be decoded back into the original file. Archon's format allows for files to be sharded at greater scale and better utilizes larger decentralized networks of nodes. Archon files can be rapidly decoded back to the original file even if sharded extensively, increasing the number of tolerable byzantine faults by orders of magnitude better than previous technologies. If a node holding portions of a file's data goes offline, is attacked, becomes an attacker, or colludes to send incorrect data, the original file can still be reconstructed as long as the minimum threshold number of the shards are downloadable (using any subset of shards whose cardinality meets the threshold). Erasure codes have been well studied and are used extensively in distributed systems and communication channels (such as mobile data).

Additional Information

Thank you for taking the time to learn more about a few aspects of our project. If you have questions, comments, or would like additional details, please reach out to sam@archon.cloud or visit us at www.archon.cloud where we will post the latest information.

Additional sections to be found in the full Whitepaper not covered herein:

- Fast File Delivery
- Blockchain Smart Contracts
- Token Economics
- Mining
- Archon Private Storage
- File Security Concerns
- Archon Cloud DNS and URLs
- Proof of Space