# Upfiring

## Whitepaper

June 2nd, 2017

Draft Version 0.9.0.

**Trademarks**

Upfiring, Upfire tokens (UFR), and all associated logos are registered trademarks of Upfiring. All other trademarks or registered trademarks are the property of their respective owners.

**Disclaimer**

The information provided in this document is provided "as is" without warranty of any kind. Upfiring disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Upfiring be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Upfiring or its suppliers have been advised of the possibility of such damages.

This is a preliminary draft. The ideas and specifications proposed in this draft may be considered highly conceptual, and are subject to significant revision or change based on further discussions with partners, advisors and the Upfiring community.

**Document Lifetime**

Upfiring may occasionally update online documentation as the company and app change over time, and in between releases of the related software. Consequently, if this document was not obtained recently, it may not contain the most up-to-date information. Please refer to www.upfiring.com for the most current information.

**Product information** — Documentation, release notes, software updates, and information about Upfiring products, licensing, and service, will be able to be found at the Upfiring website:

http://www.upfiring.com

**Technical support** — Available as soon as the app launches.

**Your comments**

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:

tyler@upfiring.com

If you have issues, comments, or questions about specific information or procedures, please include the title and, if available, the part number, the revision, the page numbers, and any other details that will help us locate the subject that you are addressing.

# Table of Contents

# 1 Introduction

## 1.1 Abstract

Upfiring is a peer-to-peer (P2P) distributed file-transferring platform designed at its core to enhance the way files are shared between users. By decentralizing the file-sharing process, Upfiring completely removes the middleman and allows users to directly exchange information via the blockchain network. Upfiring utilizes the Ethereum ecosystem as its primary platform for transaction-processing [11]. By encrypting communications on the blockchain and allowing nodes to communicate directly, Upfiring can function as a fully-decentralized exchange for files and value transactions - allowing users to download or seed their own files at will. Distributed networks are able to collaborate in a trustless manner without a single point of failure [1]. In addition, smart contracts regulate all transactions by overseeing the encryption of files, verifying proof-of-ownership, and guaranteeing a seamless transfer of value. The use of smart contracts allows for the objective management of transactions without requiring authoritative supervision. The emergence of these technologies have reflected a much greater attitude shift towards the use of the internet – the growing preference for decentralized, trustless applications over centralized, third-party-controlled services.

This paper seeks to provide an overview of the Upfiring protocol and explain its underlying technology and functionality in detail. We will break down the application's key components, compare it to existing non-blockchain P2P file-sharing applications, and explain how Upfiring's unique approach to decentralized, contract-driven incentivization seeks to transform the blockchain file-sharing space.

# 2 Upfiring P2P Network

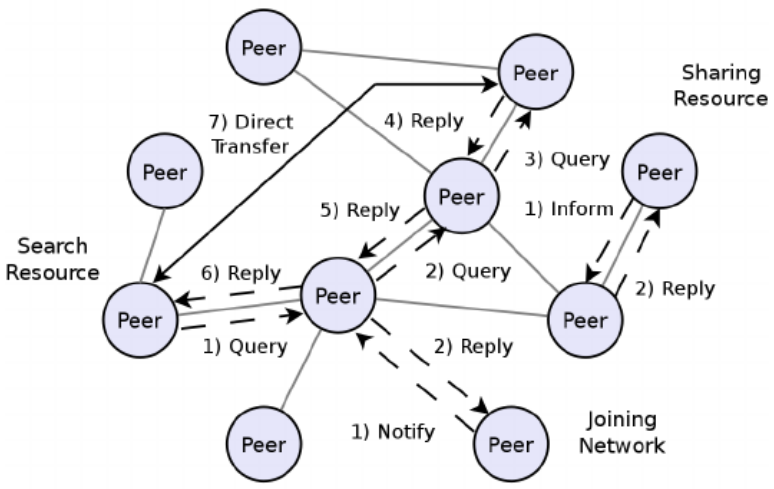
**Upfiring emphasizes connecting and communicating as a means of creating value.**

Intellectualist John Quiggin once emphasized that the largest breakthroughs happen when people can freely share and communicate within communities:

> [ "Throughout the history of the Internet, most of the innovation has come as a by-product of efforts to facilitate communication within social groups of various kinds (academics, bloggers, peer-to-peer file sharing), rather than as the result of profit-oriented investment. Rather than taking the lead, the business and government sectors have adopted innovations developed in Internet communities, and realised significant productivity gains as a result."]

## 2.1 A New Way to Envision File-Sharing

What if you could bring everyday file-sharing to the worldwide free market and allow users to freely exchange files on a decentralized marketplace? This was the idea that set Upfiring into action in early 2016. The file-sharing industry has long been a victim of shutdowns, government interference, and strict regulations stemming from centralization.




*[10] Depicts a fully decentralized P2P architecture*

By removing the central server and allowing nodes in the network to communicate directly without outside interference, Upfiring aims to revolutionize the way the world thinks about file-sharing. Disrupting this market is a multibillion-dollar venture. In the long-term, Upfiring aims to become the leading file-sharing platform for users around the world. The

network utilizes redundancy and breaks files into fragments that are distributed across the network, further strengthening security [1].

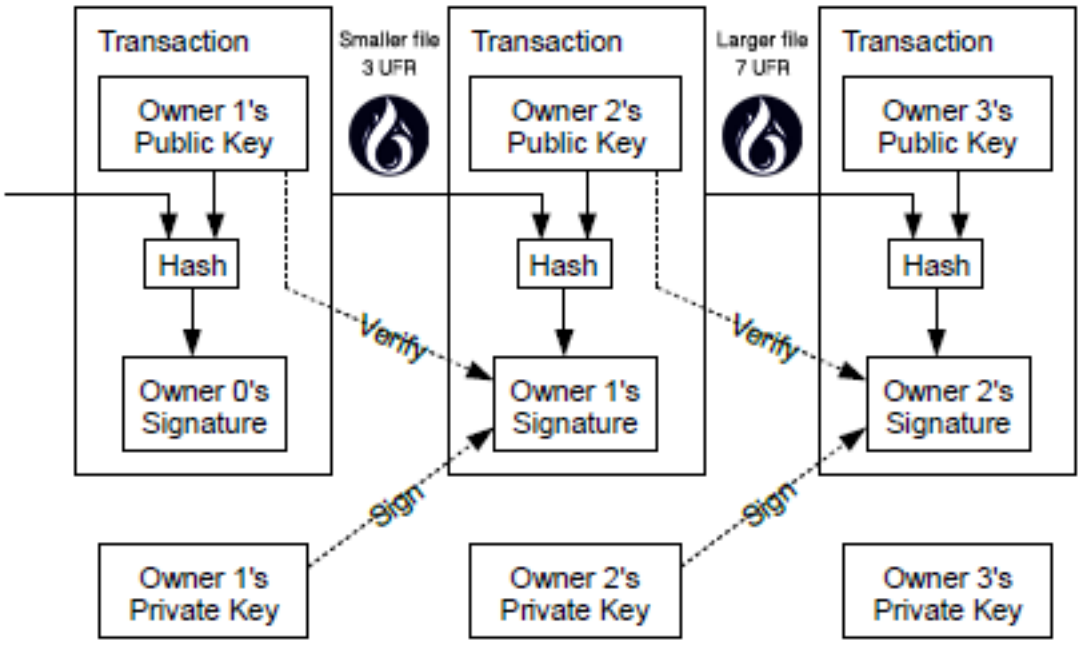
## 2.2 Upfire Tokens – A Brief Overview

Upfire (UFR) tokens are the core of Upfiring's incentivization protocol. Users can "spend" UFR in exchange for files being offered by other users on the network. To accumulate UFR, users can share files with the network (seeding) and be rewarded with UFR each time their file is downloaded. UFR can also be acquired on numerous cryptocurrency exchanges on the web, and will be directly exchangeable for Ethereum.

## 2.3 Uses Cases

Early versions of Upfiring will support the sharing of "safe" file types (.doc, .pdf, .wav), .torrent extensions, and magnet links. We plan to expand support for other types over time. Some use case examples include university students sharing large documents with one another without the file-size limitations of services like Dropbox, artists sharing their own music, writers sharing their work, and programmers releasing applications/browser extensions. In each of these cases, users will proactively accumulate UFR tokens as a reward for using the network. Because the community is in full control of the platform, the possibilities for growth are endless.

## 2.4 Incentivization of file-sharing and seeding protocols




Perhaps one of the greatest solutions that Upfiring offers to the current state of file-sharing is the incentive to seed files. Traditional torrent and file-sharing programs offer no incentive to seed files after a download is completed, often resulting in long download times for users or the complete inability to download files altogether [2]. By tokenizing this aspect of the file-sharing protocol, users can download huge amounts of information from the network at very little cost, while providing passive rewards to those who choose to seed and share their files with the network.

## 2.5 Decentralization as core-component of file-sharing

It is our strong belief that file-sharing should be decentralized and utilize blockchain technology for maximum security. Traditional file-sharing protocols are vulnerable to breaches of security and shutdowns that will be non-issues for Upfiring users [4]. Because the network will be decentralized and run on the Ethereum blockchain, there is no central point of failure - making the network extremely resilient and reliable [11].

# 3 The Application

## 3.1 Features

Upfiring will employ several technologies to create a successful peer-to-peer system:

1. Distributed Hash Tables (DHTs) - used to keep track of metadata within peer-to-peer systems
   - *Kademlia DHT* - allows for high-speed lookups - queries on average $\log_2(n)$ nodes, with optimization of the number of controlled messages sent to other nodes and a high level of security. Currently used in some of the largest P2P applications (BitTorrent).
   - *S/Kademlia DHT* - creates PKI key pairs for nodes and allows for signed messages between them. This adds an extra layer of security to Kademlia DHT.
2. Block Exchanges - allows for peers to trustlessly distribute pieces of files to each other. This technology can track the availability of file pieces and order them efficiently.
3. Node Identities - Nodes will be identified by a node_id, which will be cryptographically hashed to create a public-key through S/Kademlia's protocol. Nodes first exchange public keys on initial contact.
4. Network - Upfiring uses a hash checksum to check the integrity of messages, and can provide reliability through uTP (LEDBAT) or SCTP
5. Smart Contracts - UFR as a distributed ledger - upon successful completion of the proof-of-transfer protocol, UFR tokens are sent from the downloaders UFR wallet to the seeders wallet across the blockchain.

## 3.2 Proof-of-storage and Proof-of-transfer

Proof-of-storage (also known as proof-of-space) protocols are periodically run to check for changes on the network and to authenticate seeded files. Proof-of-transfer protocols consist of several smaller methods that run during each step of the file-transferring process to ensure that transactions are completed in their entirety [6]. Both proof-of-storage and proof-of-transfer results are published to the blockchain and all transactions will be verifiable, ensuring that UFR tokens are transferred appropriately [8].

## 3.3 Roadmap

| Date | Release |
|---|---|
| June 2016 | Idea, planning, inception, concept development |
| December 2017 | Concept validation |
| April 2017 | Upfiring project revealed |
| May 2017 | Initial website launch |
| June 2017 | Whitepaper released |
| October 2017 | UFR Contribution Period v.1.0. |
| Q4 2017 | Upfiring Testnet/Alpha Launch |
| Q1 2018 | Upfiring Beta Launch |
| Q2 2018 | Upfiring Official Launch |

# 4 The Upfiring Foundation

## 4.1 Upfiring Tokens (UFR) – Smart tokens

Upfire tokens are for sole use on the Upfire network. Users should not buy Upfire tokens with the expectation of profit.

Upfire tokens (UFR) are ERC20-standardized and EIP-228-standardized tokens used to power movement on network. Users can earn UFR tokens by seeding files and renting their disk space to the network for any period of time.

## 4.2 UFR ICO Crowdsale Objectives

The purpose of the UFR ICO crowdsale is to distribute UFR tokens to the market. We seek to obtain the necessary funding to drive the continuous development of the application as well as maintain standard business functions. By contributing to the crowdsale, contributors are procuring coins that can be used on our network and should not be doing so with an expectation of profit. Coin value may change at any time based on naturally assessed market value and has no intrinsic worth besides its use on the Upfiring network.

### 4.2.1 Crowdsale V.1.0 Statistics

- Hard Cap: 40,000 ETH
- In case of reaching the hard cap, the contribution period closes immediately.
- Recommended gas limit is 200000
- Maximum allowed gas price is 50 (Gwei 50000000000 wei)
- Can send Ether directly to the smart contract - allow up to 7 days from the time the contribution period ends to receive UFR tokens to your Ethereum address. Please be sure to send Ether from a wallet and not Coinbase or an exchange

## 4.3 Additional Statistics – UFR tokens

- The total number of UFR tokens will be set at a maximum of 1,000,000,000 UFR (1 billion)
- ICO: October 3rd (12:00 PM EST) to October 31st (11:59 AM EST)
- Exchange Rate: 15,000 UFR: 1 ETH
- 600,000,000 Contribution Period v.1.0.
- *60,000,000 In-App Purchasing of Tokens
- *150,000,000 Reserved for Potential Contribution Period v.2.0.
- 190,000,000 Founders (vested over the course of 2 years)

- One additional contribution period may be hosted. This will only occur after the deployment of key application milestones and in the event that additional funding is necessary to complete the project

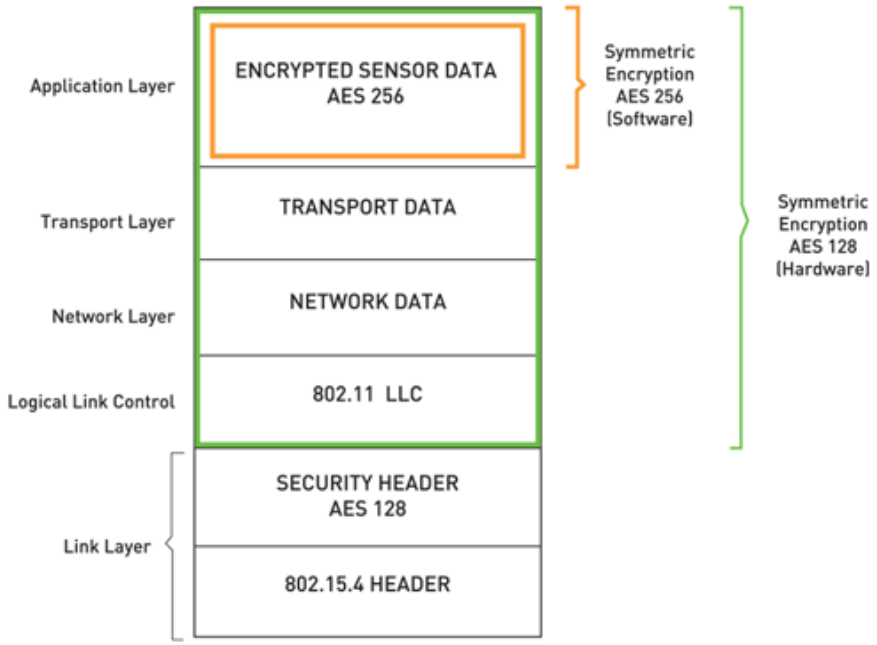
*Released over the next 5 years

# 5 Examples and Illustrations

A main focus of Upfiring will be ease of use for the end-user. Many blockchain applications are incredibly complicated to set up and get running – we want Upfiring to work right out of the box for everyone, on any device.

## 5.1 Upfiring vs. Traditional P2P File-Sharing Services

Upfiring will share and support many of the common features of modern-day P2P file-sharing applications, including seeding, searching, downloading, ratings, and peer evaluation. However, Upfiring offers several inherent features that make the application more powerful than that of major competitors. Through tokenized exchanges, peer and file-ratings, extensive spam filters, and encryption, file-transfers will be both easier to carry out and far safer for the average user. Rather than paying a subscription fee or "purchasing" files, UFR tokens are simply sent to the network as gas to power file-transfers, which then initiates the movement of the files amongst nodes. Upon completion of the transfer, the seeder is then credited with the majority of these tokens.



## 5.2 Network Reputation & Rating System

As a decentralized application, a rating system is necessary to establish trust between clients and hosts. The rating system for both files and users will also improve the quality of transactions on the network. After receiving a file, users will be able to submit an optional, public trust rating and feedback for the user and the file that will be visible to all other users. This will help keep the network free of any unwanted or untrustworthy activity. As a second-layer of defense, algorithms to detect and test potentially malicious files will be employed to mark these types of files with the appropriate warning.

## 5.3 Security

Encryption wraps the file securely throughout the entire transfer process across the network, keeping its contents safe until it is reassembled and unlocked at its final destination node. As such, all aspects of the file will be completely unreadable (including contents like the file name and description) to anyone not directly involved the transaction between the seeder and downloader [5]. This protocol protects the integrity and anonymity of the Upfiring network as a whole and allows for movement to be completely decentralized and unregulated by any third-parties.

## 5.4 Integration & Compatibility

The Upfiring Desktop Application will be available for Windows, MacOS and Linux operating systems with full functionality. The Android and iOS applications will allow access to files, but have reduced functionality in comparison. As Ethereum development continues, we may extend two-way compatibility to a private sidechain of the blockchain [9].

# 6 Algorithms and Transactional Data

## 6.1 File Smart Contracts

Two types of contracts will be distributed across the network - a contract to facilitate the movement of files between peers, and another to manage the exchange of UFR. Each file employs a Merkle root hash by breaking down the file into segments (of constant size) and forming a Merkle tree. File smart contracts store file size information that can be used to determine the UFR price, among other variables, between the seeder and their client. Transaction smart contracts will explicitly specify payout parameters and facilitate the exchange of UFR tokens. As development progresses, we plan to support customizable community-driven smart contracts to allow users to create and adjust parameters themselves, and provide their own *Post*, *Get*, *Put*, and *Delete* methods [10].

## 6.2 Proof-of-Storage and Signatures

Upfiring utilizes a storage-proof transaction system in conjunction with file contracts. The proof data, along with the contract's ID are obtained in order to validate and confirm proof-of-storage [7]. Transactions feature a variety of inputs that must be included in the file's signature before any action can take place on the network. The cryptographic signature includes an input ID, precise time data, and parameters to indicate which parts of the transaction have been signed thus far [3].

## 6.3 Storage Algorithm

Storage can be proven by breaking down a piece of the original file (obtaining a random piece of the file each time) and obtaining its hash list from the Merkle tree. This proof is then submitted to the blockchain and marked as valid or invalid. The algorithm used to validate storage is:

$$CHF\ (contract\ ID\ ||\ CHF\ (FB\ )$$

*where CHF is the cryptographic hashing function and FB is the first block prior to the start of the challenge algorithm.*

# 7 Summary

Upfiring is an innovative upgrade to modern-day P2P file-sharing technologies and seeks to revolutionize the industry. We firmly believe that file-sharing should be decentralized and incentivized, and that the adoption of a blockchain and cryptocurrency for these purposes provides a huge potential for future growth. Incentivizing the file-sharing process will allow our network to grow at an exponential pace and ensure a competitive decentralized marketplace is established. The use of smart contracts will allow transactions to be verified and recorded on the public blockchain so that any disputes can be solved easily within the Upfiring community. We believe Upfiring will be the pioneer of incentivized blockchain file-sharing and are enthusiastic about establishing this platform in a trustless environment.

# 8 References

[1] J. H. Howard, M. L. Kazar, S. G. Menees, D. A. Nichols, M. Satyanarayanan, R. N. Sidebotham, and M. J. West. Scale and performance in a distributed file system. *ACM Transactions on Computer Systems (TOCS)*, 6(1):51–81, 1988.

[2] B. Cohen. Incentives build robustness in bittorrent. In *Workshop on Economics of Peer-to-Peer systems*, volume 6, pages 68–72, 2003.

[3] D. Mazieres and F. Kaashoek. Self-certifying file system. 2000.

[4] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. 2014.

[5] I. Baumgart and S. Mies. S/kademlia: A practicable approach towards secure key-based routing. In *Parallel and Distributed Systems, 2007 International Conference* on, volume 2, pages 1–8. IEEE, 2007.

[6] Ari Juels and Burton S Kaliski Jr. Pors: Proofs of retrievability for large files. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 580–610. Acm, 2007.

[7] R.C. Merkle, Protocols for public key cryptosystems, In *Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society*, pages 100-142, April 1980.

[8] Hovav Shacham and Brent Waters. Compact proofs of retrievability. *In International Conference on the Theory and Application of Cryptology and Information Security*, pages 75–115. Springer, 2008.

[9] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Peolstra, Jorge Timon, Pieter Wuille, *Enabling Blockchain Innovations with Pegged Sidechains*.

[10] Janne, Author & Supervisor, Julkunen & Ylianttila, Mika. Feasibility of Convergent P2P and Web Service Architecture, 2017.

[11] Vitalik Buterin. Ethereum <https://ethereum.org/>, April 2014. URL https://ethereum.org/.

# 9 Resources

**Connect with us**

Facebook | @Upfiring

Twitter | @UpfiringHQ

**Address**

Email: support@upfiring.com

Website: https://www.upfiring.com

This document defines the White Paper to be used for Upfiring projects.