Crystalline

Sina Kamali, Taha Fakharian, Mohammad Saadati, Alireza Arbabi,
Shayan Shabihi, Pouriya Tajmehrabi, Ali Ebrahimi

July 2022

1 Introduction

File-sharing is crucial in several modern networking technologies with files potentially holding various amounts of valuable and vulnerable data. Thus secure and flexible storage solutions are becoming more important by the day. In this work, we represent Crystalline, a blockchain system for sharing files of importance with distinguishing features from the currently existing similar systems.

Crystalline is a transaction-based, dedicated file-sharing system based on a multi-purpose blockchain-based framework. Users are encouraged to upload files to the network, and miners and network nodes are responsible for recording files and coin transactions on it in a publicly viewable manner. The network then takes care of the immutability of the uploaded data by using a decentralized consensuses algorithm.

The coins mined on Crystalline are called Crystals. Crystals serve various use cases and are a core distinguishing on-chain-supported feature of Crystalline. Crystals are awarded to miners and potentially nodes, for the sake of their effort in making the whole network a safer place.

The proposed blockchain incorporated within Crystalline is a multi-purpose chaining system, simultaneously recording files and transactions. Transactions could be made for either fee payments or any other arbitrary coin transactions between pre-specified sender(s) and receiver(s). The proposed blockchain supports various on-chain moderating policies, as well as provides lots of room for the development of off-chain networks.

The nodes agree on the state of the system given a consensus mechanism proposed by a Proof-Of-Activity algorithm. PoA systems are good at maintaining a balance between mining energy consumption and wealth distribution between the miners [2]. Using this strategy, Crystalline becomes a balanced, geometrical rewarding, upload activity valuing network. This protocol also keeps the network more secure from nothing-at-stake attacks, one of the known vulnerabilities of PoS systems that could even potentially lead to double-spending attacks [3].

We will discuss the noted features of Crystalline in full in this document.

2 Related Works

Most decentralized file storage networks can be separated into two categories. The first category is non-coin-based networks. The main incentive behind using these networks is that they are free and do not require the authority to manage uploaded files. A daily-used example of these networks is the BitTorrent network [1]. Another example of this kind of network is Storj [2]. Storj is a decentralized cloud storage network framework that helps build non-coin-based decentralized file storage networks.

The second category, which is the primary topic of this paper, is coin-based file storage networks. Current networks in this second category are far fewer than in the first category. The primary approach of these networks is to make an incentive for nodes to store data by increasing their chance to mine a block relative to the amount of data they have stored and thus, utilize a Proof-Of-Storage(or Proof-Of-Space) consensus. Some examples of this category include FileCoin [3] and Sia [4].

Although this consensus seems reasonable for a file storage network, it's similar to the Proof-of-Work approach, which has some disadvantages. We provide a new and different approach, in which the main goal isn't about uploading large-sized files but prioritizing files of importance instead, and unlike other services, uploading files has a fee. By utilizing a Proof-of-Activity consensus protocol, we encourage the nodes to pay fees for uploading files and to stay active in the network.

3 Main Mechanism

Crystalline is a file-sharing network with base functionalities very much like that of Bitcoin. All nodes in the Crystalline network are symmetric and function the same, thus there is no hierarchy present between the nodes.

In the following sections, we'll discuss what we mean by activity, how the staking system works, and the transaction system in the network.

3.1 Activity

In Crystalline, a user's activity is influenced by their previously uploaded files' sizes and their upload intervals. The following sections describe the specifics of how this mechanism is implemented in Crystalline.

3.1.1 Impact of Time

Crystalline weighs the upload intervals as a factor of activity in the network. In this definition, $t \geq 0$ denotes the time passed from a user's uploaded file, T is an arbitrary interval and r is referred to as the intensity factor. Then, by definition, $timeFactor(t)$ denotes the activity based on the time passed from

the uploaded file. The exact definition is as follows:

$$timeFactor(t) = (\frac{T}{t})^r, t > 0$$

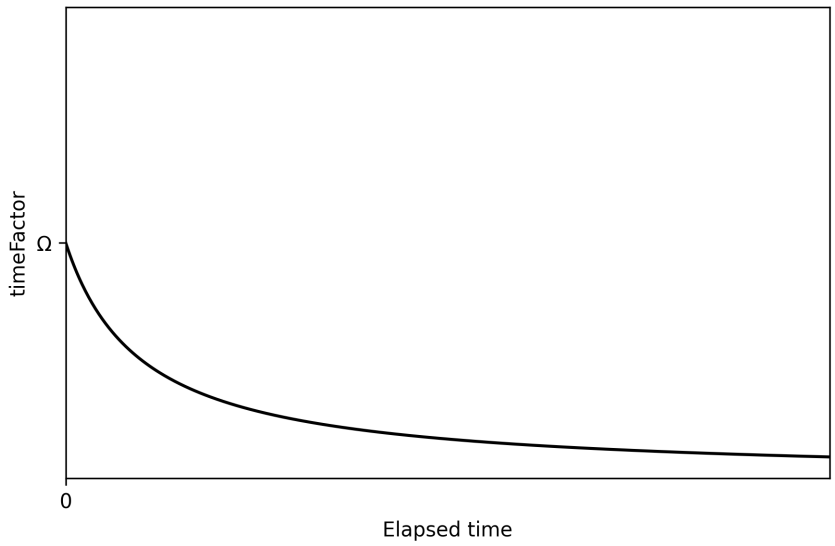

Figure 1: Arbitrarily parameterized $timeFactor(t)$ function

3.1.2 Impact of size

Crystalline weighs the size of the uploaded files as a factor of activity too. Let s denote the respective file size, β be an arbitrarily large positive number as being the maximal size-based fee assigned, and T be referred to as defined in the previous section. Then, by definition, $sizeFactor(s)$ denotes the activity based on the size of the uploaded file. The exact definition is as follows:

$$sizeFactor(s) = \frac{-T}{(s + \frac{T}{\beta})} + \beta$$

The mechanism ensures equal sharing of the network's capacity among different parties and helps keep the capacity for files of critical necessity.

Based on these two factors, we can define the activity of a single file and then, calculate the activity of a user based on their uploaded files.

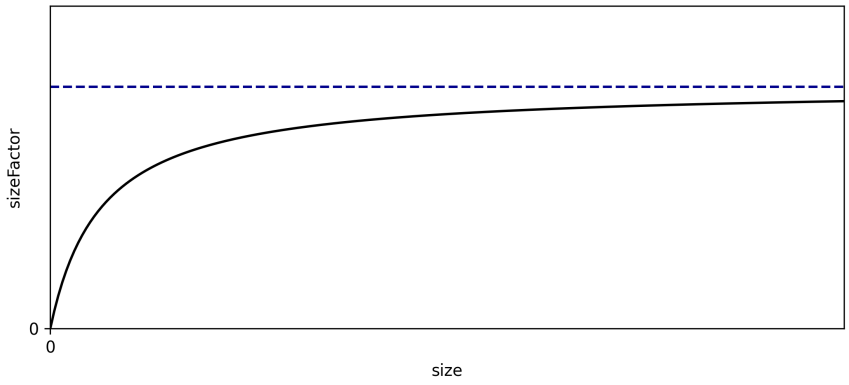

Figure 2: Arbitrarily parameterized $sizeFactor(s)$ function

Definition. 1. *$activity(file)$ is the activity of a single previously uploaded file and is calculated as follows:*

$$activity(file) = timeFactor(timestamp - file.timestamp) * sizeFactor(file.size)$$

The schematic of $activity(file)$ looks like below:

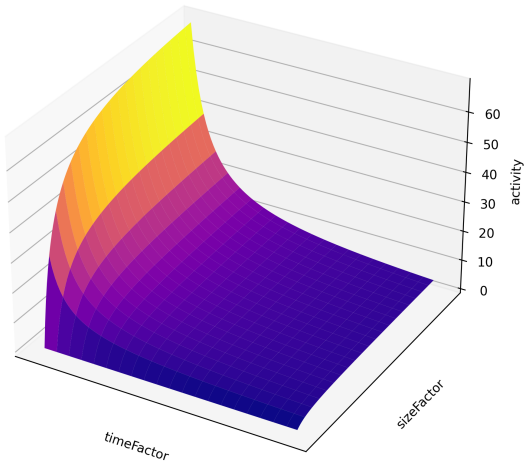

Figure 3: $activity(file)$ diagram

Definition. 2. *$activity(user)$ is the activity of a user and is calculated as follows:*

$$activity(user) = 1 + \sum_{file}^{user.prevFiles} activity(file)$$

3.2 Staking System

In Crystalline, users are able to stake their coins on the network. Staking coins does not accomplish anything of significance on this network, it merely provides the means for users to pay the upload fees without losing their money.

Staked coins cannot be spent or used in any way and cannot be un-staked for a certain amount of time. After which, a user can turn all their staked coins into coins that can be traded with ease.

3.3 Transaction

A user can make two types of transactions on the Crystalline network:

1. A transaction in which some amount of coin is exchanged between two parties.

2. A file upload transaction in which a transaction is made to pay the uploading fees.

Crystalline transactions are much like Bitcoin's $UTXO$s [1]. They can be made, spent, and even paid for in the same way as $UTXO$s.

4 Consensus

Crystalline introduces a newly-defined Proof-Of-Activity consensus and uses it as the main consensus. The main components of the consensus are explained in the following sections:

4.1 Mining System and Mining Formula

Similar to other blockchain networks, mining is done by creating a block whose hash satisfies a mining equation. Since Crystalline uses a PoA protocol, the activity of the miner is used in the mining equation.

Definition. 3. *The mining equation:*

$$hash(BlockHeader) \leq MiddleOf96BytesHexNumber * D * activity(user)$$

The mining rate in the network will be held at a constant rate by using a Difficulty Factor. The D parameter is responsible for controlling the period in which we want each block to be mined (similar to the method used in $Bitcoin$ []). For example, a block is mined every 10 minutes.

Definition. 4. *D is denoted for the difficulty factor:*

$$D = \frac{avg(TimeElapsedToMineBlock)}{ConstantDeterminedTime}$$

5 Reward System

As Crystalline uses a hybrid consensus algorithm based on proof of work (PoW) and proof of stake (PoS) for its blockchain, wealth distribution could be a major problem if not handled fairly. On one hand, the PoS rewarding should have a normal distribution among the miners instead of leaning towards a student-t distribution with a relatively high ν, and on the other, usage of a constant rewarding function makes the system quite simpler, while makes it much harder to implement such a fairly distributed rewarding between miners with sparsely distributed stakes.

To overcome the challenges linked to the described unfair distribution of mining rewards between miners of higher and lower stakes which makes the rich richer over time, we use geometric rewarding [4] for the base PoS rewarding function. The following section discusses geometric rewards further.

5.1 Reward System Specifications

Crystalline aims to have miners be more active by getting them better rewarded. Choosing a geometric rewarding mechanism ensures that the distribution of wealth within the network won't be spiky and unfair, as it will flatten out throughout large quantity block mining.

This rewarding system geometrically configures the current level's reward based on the number of blocks mined so far, a value that resets after a fixed period of mined blocks to give this rewarding function a non-linearity. The reward associated with block number n is denoted with $Reward(n)$ which is calculated as follows:

$$Reward(n) = (1 + R_i^{\frac{n}{T}}) - (1 + R_i^{\frac{n}{T}-1})$$

Here, $i = \frac{n}{T}$, and R_i denotes the constant ceiling for the rewarded funds in each period T. More info regarding this rewarding system and some plots are available in [4].

6 Upload Fees

To mitigate the mentioned attacks, there should be some measures to keep users from abusing the activity system in RPoA; Therefore, users have to pay fees to use the uploading system. The first type of upload fee is an entrance fee to grant users permanent access to upload files on the network. Users are also charged a dynamic uploading fee per file upload. All types of mandatory fees are staked on the protocol. These staked values can be recovered after a certain amount of time, thus, incentivizing the users to keep the network alive until they receive their assets. In RPoA, users can also provide extra fees in their file uploads to make miners mine their files faster.

6.1 Entrance Fee

Definition. 5. *$Fee_{entrance}$ generate the entrance fee of the network:*

$$Fee_{entrance}(timestamp) = \gamma * \alpha * \sqrt{LatestBlockAtTime(timestamp).height}$$

Where timestamp is the user registration time, α is the max base upload fee, and γ is just a constant. By using this entrance mechanism, we prevent adversaries from evading the activity factor of the upload fee. Keep in mind that by using the block height of the time of registration, entering the network becomes more challenging as time progresses, which incentivizes the users to keep the same account and thus its activity and stakes for as long as possible.

6.2 Upload Fee

Definition. 6. *Fee_{upload} is the function that generates the base amount of the upload fee:*

$$Fee_{upload}(user, file) = baseFee(file.size).activity(user)$$

Based on the above function, the upload fee is calculated based on the base fee, and the user's previously gained activity gained based on their past uploads. Here, *$baseFee$* denotes the base upload fee, *activity* denotes the user's activity explained in the main mechanism, and *user* and *$file$* are input to the function.

Definition. 7. *$baseFee(size)$ is the upload fee based on the current file size:*

$$baseFee(size) = \alpha \frac{size}{BlockMaxFileSize}$$

Where α is the max base upload fee, *size* is the size of the file to be uploaded and $BlockMaxFileSize$ is the defined file size capacity of a block.

Using activity to calculate upload fees, Crystalline has an integrated functionality to penalize consecutive uploads by a single user during a short time interval. This attacking vector is very similar to DDoS attacks, and if allowed, renders the network into a state where effectively, only the attacking parties could upload to the network. This results in more activity for the adversaries, transferring total control over the network to them.