Whitepaper

Read our whitepaper below

Zora: Universal Media Protocol

Introduction

Digital tooling and internet communication networks have given people the unprecedented ability to create and share media. But today, creators have unprecedented dependency on internet media platforms. Media is created on, uploaded to, hosted by, and shared within platforms. Platforms control creator identity and host their own social graph, restricting the ability of creators to connect with their audience. And by controlling data and graph, platforms have gained unilateral pricing power over creative media. Each platform has its own opaque methods of establishing the value of media, and creators must learn to play by these rules to make a sustainable business. This is the lesson of Web 2.0: when the process of sharing content with others is owned entirely by private platforms, the cost of this mediation falls heavily on creators.

To combat platform entrenchment, an ecosystem approach that addresses the publishing and sharing of media online is called for. Prospective solutions must seek to unbundle the platform monopoly over media data and social graph, enabling creators and audiences to engage and transact on digital media directly. Information wants to be free, but it also wants to be expensive. In an ideal ecosystem, audiences would enjoy the universal accessibility of media, and creators would enjoy more pricing power and stable returns on media which appreciates in value.

Archived copy · cryp2nova.com

In this paper, we propose Zora Protocol, a universal market protocol for media ownership. Zora provides a cryptographically-enforced registry of media independent of any platform. Media is openly accessible to audiences, curators, and third parties who wish to build on the token. Artificial scarcity on media copies need not be imposed, because the single market embedded in the token enables liquidity and value to accrue to the uniquely registered article. An embedded, permanent market facilitates ongoing price discovery and enables creators, curators, and buyers to flexibly negotiate terms of direct exchange. Creators can set a perpetual ownership stake in their work, and are rewarded whenever ownership changes hands.

Each minute, creators generate unthinkable amounts of information and value. Today that value is priced, captured, and owned by digital media platforms. By enabling platformless media, Zora Protocol welcomes an age where that value returns where it belongs: creators and their communities.

Zora Protocol Overview

Zora is a protocol designed for the Ethereum blockchain that establishes universal, perpetual markets for media in the form of ERC-721↗. Each piece of media is embedded with a market, consisting of a transparent pool of bids. As a result, a universal buy-side liquidity pool develops for the piece of media that an owner can access and act upon at any time. Each market is unique to the piece of media, and its bids can be inspected by anyone. In addition to bids, the media owner may choose to set an ask price for their media, which is a suggested bid that can be executed by a willing buyer. Whenever a bid is accepted, or an ask fulfilled, the piece of media is transferred to the buyer, and the funds from that bid are split amongst its shareholders. There can be up to three shareholders for a piece of media: the owner, the previous owner, and the original creator.

The Zora protocol introduces integrity checks to ensure that media and its metadata is provably unique. These integrity checks can be performed by any system at any time. This integrity safeguard allows for the URI of media and metadata to be updated arbitrarily, ensuring robustness when hosting media off-chain.

Archived copy · cryp2nova.com

Bids

This protocol uses Bids to represent buy-side liquidity for a piece of media. An important distinction of a bid is that it specifies an ERC-20↗ currency to be bid with. This mechanism allows for a market of many currencies to exist for the media. As a result, an owner of a piece of media may choose to accept a bid in a stable currency, a yield-generating currency, or even a community currency that enables access to a DAO. By allowing any valid ERC-20 currency to be used as a bid, the protocol allows for many representations of value to exist in parallel.

In some situations, an individual selling some media may believe that the media will become very valuable in the future, but does not have the means to propagate the media enough to attract bidders. In this circumstance, the owner may choose to accept less capital upfront from a bidder in exchange for a large sell-on fee. A sell-on fee is most commonly used by sports clubs, but it has been adopted into this protocol. This clause can be included by the bidder, whereby the seller, against a lower immediate transfer fee, retains the right to a certain percentage of a potential future transfer fee of the media to a third buyer. If a bid with a sell-on fee is accepted, the piece of media adds the seller as a previous owner to the list of shareholders for the next sale of the piece.

When a bid is accepted, the value of the bid is transferred to the media's shareholders, and the ownership of the media itself is transferred to the accepted bidder. The split of the bid can be unique to each piece of media. For example, assume a creator mints a piece of media specifying the creator share to be 5%. Upon each sale, 5% of the bid's value is transferred to the owner, and 95% of the bid's value is transferred between the owner and previous owner, depending on any sell-on fee defined by the previous sale of the piece.

We define a bid in the protocol as a Solidity struct as follows:

Archived copy · cryp2nova.com

```
struct Bid {
    // Amount of the currency being bid
    uint256 amount;
    // Address to the ERC20 token being used to bid
    address currency;
    // Address of the bidder
    address bidder;
    // Address of the recipient
    address recipient;
    // % of the next sale to award the previous owner
    Decimal.D256 sellOnFee;
}
```

Bid Validity

When splitting a bid between shareholders, this protocol will not round or estimate the share amounts; it requires the bid amount be perfectly divisible into its shares. For example, suppose a piece of media is to have a bid split evenly to the creator, owner, and previous owner of the piece. If a bid were placed with an amount of 2, how would the bids be split? Note that floating point arithmetic does not exist in Solidity, so an approximation of 0.33 per shareholder is impossible.

Thus we must introduce the concept of a bid's validity. We define a bid to be valid if it can be split such that the shareholders amounts are not rounded off or estimated. Fortunately, we find that any bid is valid if it is divisible by the least common denominator of the shareholders when the shareholder percentages are represented as a set of ratios. To convert a shareholder percentage into a ratio, we simply represent it as a fraction with integer numerator and denominator. For example, the percentages 5%, 5.5%, and 5.55% would be represented as $^{5}/_{100}$, $^{55}/_{1000}$, and $^{555}/_{10000}$, respectively.

In order to find the least common denominator for the set of shares, we represent the set of shares as fractions with a common integer denominator and multiply that denominator by the greatest common denominator of the numerators in the set. For example, suppose we have the following set of shares: 1.5%, 15%, 83.5%.

We represent the shares as fractions with a common denominator as follows:

Archived copy · cryp2nova.com

$$S = \{\frac{n}{d} | \frac{15}{1000}, \frac{150}{1000}, \frac{835}{1000}\}$$

S = {dn|100015, 1000150, 1000835}

We can use this representation to find the least common denominator:

$$\begin{aligned} LCD(S) &= d \div GCD(\{n\}) \\ &= 1000 \div GCD(\{15, 150, 835\}) \\ &= 1000 \div 5 \\ &= 200 \end{aligned}$$

LCD(S) = d ÷ GCD({n}) = 1000 ÷ GCD({15, 150, 835}) = 1000 ÷ 5 = 200

Therefore, given the least common denominator of 200, any valid bid must be divisible by 200. Note that at first read, this value may seem high, but recall that the majority of ERC-20 tokens in Ethereum have 18 decimals. Therefore, a bid for the above set of shares must be divisible by 5 * 10-15 units, which we assume to be an acceptable amount for this protocol.

Asks

At any time, an owner of a piece of media may accept a valid bid. However, bids only represent the buy-side of a media market. Without a sell-side, liquidity will fragment into multiple different pools. This protocol therefore uses an ask mechanism that allows for bidders to automatically execute a trade if the ask is fulfilled.

Similar to a bid, the ask must specify a valid ERC-20 currency that is being asked for. An ask will only ever be fulfilled if a bid meets all of the criteria specified. When a bid is accepted or an ask fulfilled, the ask is removed. We represent an ask as the following struct in Solidity:

```
struct Ask {
    // Amount of the currency being asked
    uint256 amount;
    // Address to the ERC20 token being asked
    address currency;
    // % of the next sale to award the seller
    Decimal.D256 sellOnFee;
}
```


Archived copy · cryp2nova.com

Media Uniqueness & Integrity

The primary objective of this article is to establish the market value of any piece of media. It is therefore paramount that no two pieces of media are identical, or else the value of the media risks fragmentation. We introduce a method to ensure the uniqueness of all content published to the protocol. In addition to ensuring uniqueness across all media, this also allows for any entity to validate the integrity of the media represented on-chain.

This protocol recognizes that storing any form of media on the Ethereum blockchain is prohibitively expensive and unnecessarily complicated. As a result, the protocol will make no assumptions about where media content and metadata should be stored. In compliance with the ERC-721 standard, the representation of media on the Zora protocol will simply be two URI pointers: one to the metadata, and one to the content itself. In some circumstances, such as a domain name change, the media URIs may no longer be valid and will need to be changed.

The protocol provides the current owner the ability to update the URIs for a piece of media. In order to ensure the integrity of the metadata and content, the protocol requires two sha256 checksums be included when minting new media. Although the URIs may be updated, the checksums representing the data they point to may not. As a result, any party is able to validate the media and metadata for integrity. It is up to the market participants to check the integrity of the content and metadata often, and it is expected that a failing integrity check on a piece of media will result in the devaluation of that media and removal of buy-side liquidity by bidders on the piece.

3rd Party Support

Interacting with this protocol requires each participant maintain an Ethereum balance such that they can submit transactions to the Ethereum blockchain. In order to avoid this requirement, some platforms or service providers may want to submit transactions on a user's behalf, in order to avoid having users maintain their own Ethereum wallets.

Archived copy · cryp2nova.com

This protocol implements support for EIP-712↗ with a variation of signed permits found in EIP-2612↗. By allowing users to sign an approval for their media to be transferred and sold by a third party, complex interactions can be composed without requiring the user to maintain an Ethereum balance. In addition, these 3rd parties are able to perform actions requiring approval with only a single transaction, whereas most ERC-721 contracts would require an approval transaction to occur prior to any other transaction.

By adding support for 3rd parties to transact on a user's behalf, a new media ecosystem is able to develop using this protocol as a primitive.

Conclusion

This protocol aims to serve as a means for discovering and capturing the true value of created media. Platformless media tokens with embedded markets, or cryptomedia, are the key primitive in facilitating this value capture. By unifying the liquidity for a piece of media and ensuring it is truly unique, collectors can fairly evaluate and bid on media. By providing perpetual equity to creators, creators are able to constantly realize the value of their work. Finally, by providing new offer mechanisms and 3rd party support, new and existing platforms are able to develop revenue strategies compatible with an ecosystem that is sustainable and fair to creators.

Ours truly,

Zora

CRYP2NOVA

Previous
Smart Contracts

Next
ZDK

Last updated 5 years ago

Was this helpful?

Archived copy · cryp2nova.com