xNFT Protocol

An automatic transaction protocol related to non-fungible token (NFT)

March 2021

Abstract

As one of the latest innovative technologies in the field of cryptoeconomics, “non-fungible token” (NFT; also called “non-divisible token”) has recently been used in cryptogames, virtual space, figure cards, cryptoartworks, and other similar forms. NFT has unique attributes that allow people to easily issue or have “digital products” that are verifiable but not replaceable nor can be counterfeited completely. However, most of the existing NFT transactions are realized in the form of, for example, conventional fixed-price transactions and auctions, resulting in overall low liquidity. According to statistical data, the annual turnover ratio of NFT in the market is only 8% as a whole. This means that only 8% of all pending order NFTs can be sold once a year. Therefore, conventional transaction mechanisms and bad liquidity have seriously affected user involvement in NFT.

To address this concern, a new automatic transaction protocol, called “xNFT Protocol,” is introduced in this paper. In addition to the existing common fixed-price transaction and auction, xNFT Protocol also provides a special transaction form, “Public Blind Box,” that automatically determines the fair price of NFT and draws the price of the blind box with an algorithm without manual pricing. This new development is expected to greatly enrich selling attractiveness, randomness, and mystery for user involvement in NFT transactions and improve liquidity.

1. Overview

With unique, scarce, and indivisible attributes, the non-fungible token (NFT) can be used to represent artworks or digital assets with unique intrinsic values. However, its unique characteristic is that it cannot be interchanged because different NFTs have different values. Hence, realizing free transaction and overall liquidity of NFT is difficult, which seriously restricts the development of the industry.

Although NFT is featured with consumption, financial, and investment attributes, from the view of industrial infrastructure, NFT should be designed with a new fast transaction mechanism, price discovery mechanism, derivative transaction mechanism, and mortgage loan mechanism, with both fast transaction and price discovery mechanisms (including valuation and pricing) as crucial because both features make the financialization of NFT assets possible. In addition, the price discovery mechanism can provide an acceptable fair price to greatly improve the transaction and liquidity of NFT.

With the apparent issues faced by the NFT industry, a new automatic transaction agreement of NFT, called the xNFT Protocol, has been developed that includes conventional transaction mechanism (e.g., fixed-price transaction and auction), unique lottery transaction mechanism (i.e., “transaction with blind box”), and price discovery mechanism. These features are further discussed in the sections below.

2. Conventional transaction mechanism

2.1 Fixed-price transaction

The fixed-price transaction is the most common form of transaction in the NFT market, where sellers can sell their NFTs on the blockchain through the smart contract of “xNFT Protocol” in the form of pending order and designate the required token type and quantity for NFT. After paying the required token type and quantity, the buyer may now complete the transaction through the smart contract of xNFT Protocol. For example, Bob sells NFTs through the smart contract of xNFT Protocol in the form of a pending order. He designates the token

type as USDT and the quantity as 1000 and mandates these NFTs to the smart contract. Alice, the buyer, takes an interest. Once Alice pays 1000 USDTs to the smart contract, the smart contract will immediately transfer these USDTs to Bob's account and the mandated NFTs to Alice's account.

Extension 1: Agreement of royalties

To motivate and encourage creators to produce more excellent cryptoartworks, these creators, who are required to pay royalties by a certain ratio, will be directly paid with remunerations from the paid royalties by related ratio when making the fixed-price transaction through the smart contract of xNFT Protocol.

Extension 2: Agreement of designated counterparty

Sellers who opt to sell NFTs with fixed-price through the smart contract of xNFT Protocol can designate one or more addresses in a whitelist and only allow involvement of these addresses in this fixed-price transaction.

2.2 Auction

Another form of transaction considered one of the most primitive is the auction. It is also the mechanism of realizing high-efficient resource configuration under the condition of incomplete information. According to the well-known "revenue equivalence theorem," regardless of the type of auction (English auction, Dutch auction, the first-price sealed auction, or the second-price sealed auction), the expected auction price is the same, while the winner's expected revenue is also the same and can reach the Pareto optimality when the independent private valuation, symmetric information of bidders, no-budget restriction, and risk neural condition are accommodated. Various types of auctions are done through the smart contract of xNFT Protocol, which some are discussed here.

2.2.1 Dutch auction

Dutch auction (also "price-descending auction") is a form of auction through the smart contract of xNFT Protocol. Under this type, the seller usually sets a high base price and then decreases the price by a prior descending benchmark until a bidder accepts the price. Although

the auction can be greatly accelerated, the transaction is not highly competitive because bidders always wait for a lower price.

2.2.2 English auction

In the English auction (also “price-ascending auction”), the seller usually sets a base price and then increases the price by a prior ascending benchmark. The bidder with the highest bid will be the winner. English auction is simpler and more competitive and, therefore, can maximize the value of any object without definite value. However, this form of auction provides risks to bidders because he/she may be induced by the bidding atmosphere and offer a price higher than the estimated one, which is called the “Winner’s Curse”.

2.2.3 Sealed auction

Another type of auction is the sealed auction, where all bids will be submitted in the form of encryption (sealed form). All bidders offer the price simultaneously and cannot see others’ bids. The bidder with the highest bid will be the winner. Sealed auction has two forms: the first-price sealed auction and the second-price sealed auction.

2.2.3.1 The first-price sealed auction

Under the mode of the first-price sealed auction, the winner shall pay by the highest bid.

2.2.3.2 The second-price sealed auction

Under this form of sealed auction, the bidder with the highest bid will get the auction items but will pay with the second highest bid price.

2.2.3.3 Encryption algorithm

The smart contract of xNFT Protocol uses a unique encryption algorithm for sealed auctions to realize fair and auditable auctions on the blockchain with transparent data. The algorithm encrypts all bids through “salt value + bid timestamp + bid address” and ensures that all bids cannot be changed. The encrypted information is irreversible. Moreover, all bids are verified to ensure that the sequence and the “salt value” are visible to NFT sellers to ensure their right of knowledge during the auction.

The “salt value” is published on the blockchain through xNFT Protocol after the auction. Consequently, all users can verify and audit the sealed bids.

3. Lottery transaction mechanism

The lottery transaction mechanism (also “transaction with blind box”) is an innovative form of transaction through the xNFT Protocol. Before the transaction, the seller injects multiple NFTs into the smart contract of the blind box and indicates the draw price to the buyer. Since the buyers cannot predict the NFT to be drawn in advance, this process is known to provide mystery and surprise to the participants. As the fastest form of transaction, it is designed to improve overall transaction and liquidity in the NFT market and promote sustainable development of the NFT ecosystem. The blind box has private and public options.

3.1 Private blind box

The private blind box allows any seller to create his own blind box through the smart contract of xNFT Protocol, provide all NFTs for a draw, and independently set the draw price of the blind box. The seller randomly draws one NFT after offering the price. The smart contract will transfer tokens of related quantity and type to the seller’s account and the NFTs to the buyer’s account to complete the transaction.

The probability of a draw is equal for each NFT in the private blind box.

3.2 Public blind box

The public blind box is open and allows any seller to provide NFT for the draw through the smart contract of xNFT Protocol. If the triggering conditions are accommodated, the smart contract will automatically enable the blind box for drawing; otherwise, the blind box will be disabled. The Oracle of xNFT Protocol automatically calculates the fair price of each NFT to be drawn and sets the draw price of the blind box with the predefined algorithm. When the buyer randomly draws one NFT, the smart contract will transfer the NFT to the buyer’s account, calculate the bonus or loss of the transaction, and distribute revenue to or compensate the seller.

Please refer to the “Price discovery mechanism” section for the operating principle of Oracle.

3.2.1 Definitions

3.2.1.1 Probability of draw

The probability of draw for each NFT in the public blind box is not equal but inversely proportional to the Oracle calculated fair price, i.e., the higher the NFT is, the lower the probability of draw will be and vice versa. The probability of drawing for the NFT with price P_{out} is:

$$PROB_{out} = (1 / P_{out}) / \Sigma(1 / P_n)$$

3.2.1.2 Fair price

The smart contract of xNFT Protocol collects historical transaction prices of each NFT in the public blind box and recent transaction prices of similar NFT using Oracle, calculates the fair price of the NFT, and then updates regularly.

3.2.1.3 Draw price of the public blind box

Draw price of the public blind box = $\sum P_i t_i * Y$,

where P_i is the Oracle price of the ith NFT in the public blind box; t_i is the probability of drawing for the ith NFT in the public blind box; and Y is the premium rate.

The premium rate Y indicates the transaction profitability of the public blind box and is related to the coefficient of the standard deviation of a fair price for all NFTs in the public blind box. That is to say, the more high-value NFTs are injected into the public blind box, the higher the premium rate Y will be.

The premium rate is set to encourage more sellers to inject high-value NFTs into the public blind box.

3.2.2 Creation of public blind box

Since the protocol of the public blind box is open, any user can create and initialize a new protocol.

3.2.2.1 Initialization of public blind box

After initialization of the public blind box, the creator shall provide NFTs with quantities

not less than the minimum M as the “base” of the public blind box for “market making”, similar to the market maker of Uniswap.

xNFT Protocol initializes the initial data of each NFT in the public blind box with a mapping structure:

NFT → P (Price) = Oracle price

NFT → VOL (Value of Liquidity Weight) = 0

NFT → BONUS (Drawable Liquidity Bonus) = 0

NFT → LOCK (Locked Liquidity Bonus) = 0

3.2.2.2 Initialization of reserves pool

The initial capital of the reserves pool

$V_o = \Sigma max((P_n - P_o),0)$,

where $P_1...P_n$ is the Oracle price of NFT at the base; n is the quantity of NFTs at the base; and P_o is the initial draw price of the blind box.

If the capital scale of the reserves pool is larger than the initial capital, the creator of the blind box can draw capital from the reserves pool. The total capital cannot be E times higher than the initial capital, and the single capital cannot be higher than “current capital scale − initial capital”, where E is the initial capital yield of reserves.

3.2.2.3 Initialization of timestamp

During the initialization of the public blind box, the height of initialization block is $T = T_{now}$, where T_{now} is the current block height.

3.2.3 Price fluctuation

If NFT Oracle detects any change in the fair price of NFT, then it is necessary to feed a price to the public blind box again and transfer those NFTs with changed price and changed fair price.

3.2.3.1 Fluctuated draw price of the blind box

When NFT Oracle feeds the fair price of NFT to the public blind box, the draw price of

the blind box will also change and can be expressed as below:

$P_{new} = (P_{old} + \Sigma(C_{new} - C_{old})) / n * Y,$

where P_{old} is the draw price of the blind box before price fluctuation; C_{new} is the changed Oracle price of NFT; C_{old} is the Oracle price of NFT before price fluctuation; Y is the premium rate of the blind box; and *n* is the quantity of NFTs in the blind box.

3.2.3.2 Update of liquidity weight

If the draw price of the public blind box is changed, then the liquidity weight will be updated:

$VOL_{new} = \max((C_{old} - P_{old}),0) * \triangle T * m + VOL_{old},$

where C_{old} is the Oracle price of NFT before price fluctuation; P_{old} is the draw price of the blind box before price fluctuation; $\triangle T = T_{now} - T$ is the difference value between current block height T_{now} and the block height *T* recorded by the public blind box; *m* is the time of generating a block height for current chain (unit: second); and VOL_{old} is the liquidity weight recorded by the public blind box.

3.2.3.3 Update of NFT price

The smart contract sets the NFT with changed price.

$NFT \rightarrow P = C_{new},$

where C_{new} is the Oracle price of the changed NFT.

3.2.3.4 Update of timestamp

If the draw price of the public blind box is changed, then the block height will be updated:

$T = T_{now},$

where T_{now} is the current block height.

3.2.4 Injection of NFT

After the initialization of the blind box, any user can provide NFT to the contract of the public blind box for buyers to draw, which is called as “injection”. The seller who injects high-value NFT to the contract of the public blind box can obtain a liquidity bonus regularly.

3.2.4.1 Fluctuated draw price of the public blind box

After NFT injection, the draw price of the public blind box becomes:

$P_{new} = (P_{old} * n + P_{in} * Y) / (n + 1)$,

where P_{old} is the draw price of the public blind box before injection; P_{in} is the Oracle price of injected NFT; Y is the premium rate of the public blind box; and *n* is the quantity of NFTs in the public blind box before injection.

3.2.4.2 Update of liquidity weight

Any injection to the public blind box will change the liquidity weight:

$VOL_{new} = \max((P_{in} - P_{old}),0) * \triangle T * m + VOL_{old}$,

where P_{in} is the Oracle price of the injected NFT; P_{old} is the draw price of the public blind box before injection; $\triangle T = T_{now} - T$ is the difference value between current block height T_{now} and the block height *T* recorded by the public blind box; *m* is the time of generating a block height for current chain (unit: second); and VOL_{old} is the liquidity weight recorded by the public blind box.

3.2.4.3 Data initialization for newly injected NFT

The data of the newly injected NFT is initialized with the mapping structure:

NFT → P (price) = Oracle price

NFT → VOL (Value of Liquidity Weight) = 0

NFT → BONUS (Drawable Liquidity Bonus) = 0

NFT → LOCK (Locked Liquidity Bonus) = 0

3.2.4.4 Update of timestamp

The block height will be updated if injection occurs to the public blind box:

$T = T_{now}$,

where T_{now} is the current block height.

3.2.5 Withdrawal of NFT

An NFT that has been injected into the contract of the public blind box but not drawn can be canceled by the seller at any time, which is called as “withdrawal”. The NFT withdrawn from the contract of the blind box may loss the locked liquidity bonus, which will be injected into the reserves pool.

3.2.5.1 Fluctuated draw price of the blind box

After NFT withdrawal, the draw price of the blind box becomes:

$P_{new} = (P_{old} * n - P_{out} * Y) / (n - 1)$,

where P_{old} is the draw price of the blind box before withdrawal; P_{in} is the Oracle price of the withdrawn NFT; Y is the premium rate of the public blind box; and n is the quantity of NFTs in the public blind box before the withdrawal.

3.2.5.2 Update of liquidity weight

If any withdrawal occurs to the blind box, the liquidity weight will be updated:

$VOL_{new} = \max((P_{out} - P_{old}),0) * \triangle T * m + VOL_{old}$,

where P_{out} is the Oracle price of the withdrawn NFT; P_{old} is the draw price of the blind box before withdrawal; $\triangle T = T_{now} - T$ is the difference value between current block height T_{now} and the block height *T* recorded by the blind box; *m* is the time of generating a block height for current chain (unit: second); and VOL_{old} is the liquidity weight recorded by the blind box.

3.2.5.3 Bonus disposal for withdrawn NFT

Balance of the reserves pool

$V_{new} = LOCK_{out} + V_{old}$,

where $LOCK_{out}$ is the locked liquidity bonus of the withdrawn NFT, and V_{old} is the previous balance of the reserves pool.

$BONUS_{out}$ is transferred to the original address of the withdrawn NFT.

3.2.5.4 Data cleaning for withdrawn NFT

The data of the related mapping structure is set to 0 for the withdrawn NFT:

NFT → P (Price) = 0

NFT → VOL (Value of Liquidity Weight) = 0

NFT → BONUS (Drawable Liquidity Bonus) = 0

NFT → LOCK (Locked Liquidity Bonus) = 0

3.2.5.5 Update of timestamp

Any withdrawal to the blind box will update the block height:

$T = T_{now}$,

where T_{now} is the current block height.

3.2.6 Draw of NFT

The buyer can obtain a random NFT from the public blind box after paying tokens of related type and quantity to the contract based on the draw price of the public blind box. This is called “draw”.

3.2.6.1 Fluctuated draw price of the blind box

After the draw of NFT, the price of the public blind box becomes:

$P_{new} = (P_{old} * n - P_{out} * Y) / (n - 1)$,

where P_{old} is the draw price of the blind box before the draw; P_{out} is the Oracle price of the NFT; Y is the premium rate of the public blind box; and n is the quantity of NFTs in the blind

box before the draw.

3.2.6.2 Update of liquidity weight

If any draw occurs to the blind box, then the liquidity weight will be updated:

$VOL_{new} = \max((P_{out} - P_{old}),0) * \triangle T * m + VOL_{old}$,

where P_{out} is the Oracle price of the NFT; P_{old} is the draw price of the public blind box before the draw; $\triangle T = T_{now} - T$ is the difference value between current block height T_{now} and the block height *T* recorded by the blind box; *m* is the time of generating a block height for current chain (unit: second); and VOL_{old} is the liquidity weight recorded by the blind box.

3.2.6.3 Fluctuation of the reserves pool

If $P_{out} \leq P_{old}$, the $(P_{old} - P_{out})$ part will be injected into the reserves pool.

The bonus of reserves is $PROV = \max((P_{old} - P_{out}),0) * U$, where P_{old} is the draw price of the blind box before the draw; P_{out} is the Oracle price of the NFT; and U is the ratio of reserves.

The balance of reserves pool is $V_{new} = PROV + V_{old}$, where PROV is the bonus of reserves, and V_{old} is the previous balance of reserves pool.

3.2.6.4 Update of liquidity bonus

The liquidity bonus is $LIQ = \max((P_{old} - P_{out}),0) * (1 - U)$, where P_{old} is the draw price of the blind box draw; P_{out} is the Oracle price of the NFT; and U is ratio of reserves.

If LIQ is larger than 0, then the drawable liquidity bonus (BONUS), locked liquidity bonus (LOCK), and liquidity weight (VOL) will be updated.

The drawable liquidity bonus is $BONUS_{new} = VOL_i / \Sigma VOL_n * LIQ * (1 - W) + BONUS_{old}$, where VOL_i is the related liquidity weight of NFT; ΣVOL_n is the total liquidity weight of NFTs in the pool of public blind box; LIQ is the liquidity bonus; W is the lock ratio of liquidity bonus; and $BONUS_{old}$ is the

drawable liquidity bonus recorded by the blind box.

The locked part is $LOCK_{new} = VOL_i / \Sigma VOL_n * LIQ * W + LOCK_{old}$, where VOL_i is the liquidity weight of related NFT; ΣVOL_n is the total liquidity weight of NFTs in the pool of public blind box; LIQ is the liquidity bonus; W is the lock ratio of liquidity bonus; and $LOCK_{old}$ is the locked liquidity bonus recorded by the blind box.

The liquidity weight is $VOL_{new} = 0$. For all NFTs, the liquidity weight is reset to 0.

3.2.6.5 Bonus disposal

If a buyer draws NFT from the contract of the public blind box, then the NFT injector will obtain NFT market bonus, locked liquidity bonus, and drawable liquidity bonus.

The NFT market bonus is $SELL_{out} = P_{out} * Y * \max(P_{out} /(P_{out} + P_{old}),1 / Y)$, where P_{out} is the Oracle price of the NFT; P_{old} is the draw price of the public blind box before draw; and Y is the premium rate of the public blind box.

If $SELL_{out} > P_{old}$, then the $(SELL_{out} - P_{old})$ part shall be paid from the reserves pool.

If $(SELL_{out} - P_{old}) \leq V_{old}$, then the balance of reserves pool is $V_{new} = V_{old} - (SELL_{out} - P_{old})$, where V_{old} is the previous balance of the reserves pool; $SELL_{out}$ is the NFT market bonus; and P_{old} is the draw price of the blind box before the draw.

If $(SELL_{out} - P_{old}) > V_{old}$, then the balance of reserves pool is $V_{new} = V_{old} - (SELL_{out} - P_{old})$ and the $((SELL_{out} - P_{old}) - V_{old})$ part will be paid from the “Insurance benefits pool” through Swap displacement. All bonuses of the reserves pool are returned to the “Insurance benefits pool” through Swap displacement until the balance of reserves pool V is recovered to a positive number.

$SELL_{out}$, $BONUS_{out}$, and $LOCK_{out}$ are transferred to the original address of purchased NFT.

3.2.6.6 Data cleaning for purchased NFT

The data of the related mapping structure is set to 0 for the NFT:

NFT → P (Price) = 0

NFT → VOL (Value of Liquidity Weight) = 0

NFT → BONUS (Drawable Liquidity Bonus) = 0

NFT → LOCK (Locked Liquidity Bonus) = 0

3.2.6.7 Update of timestamp

Any draw to the public blind box changes the block height:

$T = T_{now}$,

where T_{now} is the current block height.

3.2.7 Draw of bonus

The seller can draw the drawable liquidity bonus of injected NFTs from the public blind box at any time.

3.2.7.1 Update of liquidity bonus

The seller can draw partial $BONUS_{new} = BONUS_{old} - TAKE$, where $BONUS_{old}$ is the drawable liquidity bonus recorded by the public blind box; and TAKE is the bonus of this draw.

3.2.8 Deconstruction of blind box

If the quantity of NFTs in the contract of the public blind box is lower than the minimum and the rest of the NFTs are withdrawn, then $BONUS_{out}$ and $LOCK_{out}$ will be transferred to the original address of the NFT.

4. Price discovery mechanism

As previously stated, realizing the price in a centralized transaction market or decentralized AMM is difficult because NFTs have unique characteristics compared with other fungible

tokens. In addition, the market price is easily controlled by the holder. Therefore, how to reach a balance between the historical price data and market expectation and control more price bubbles have to be resolved for NFT valuation and pricing.

From the view of capital efficiency, the low-cost auction mode leads to high capital efficiency. Similarly, if the capital efficiency is higher, the cost for price control will be lower. Therefore, reaching a balance between capital efficiency and cost for price control and designing a feasible and practical model have to be resolved for NFT valuation and pricing.

The core of xNFT Protocol's Oracle is to discover the true price of NFT based on some practical data and rules.

From the view of on-chain and off-chain dimensions, practical data include on-chain holding conditions and transactions and off-chain auction details and attentions.

Practical data from the perspective of objective and subjective dimensions include information of current similar NFTs and qualification and endorsement of the NFT issuer.

Moreover, the price discovery mechanism shall also be evaluated from the dimension of capital efficiency. The capital efficiency is $E = P / C$, where P is the discovered price of the product and C is the total expenses of pricing participants. For the current sales mode, the selling at a fixed price is $E = 1$, an auction is $E \leq 1$, and a division may be $E \geq 1$. Some pure off-chain modes are also used for evaluation and pricing, for example, AI, machine learning, and equivalent Oracle (i.e., initial Oracle model), which may increase the capital efficiency to ∞.

The various common scenarios of NFT Oracle algorithm are listed below:

4.1 Oracle scenario 1: Recent transactions

If there is an on-chain transaction for an NFT in a recent unit period (e.g., 7 days), then the available on-chain data include the following:

P_{new} is the recent transaction price after weighted calculation by time and turnover (calculated by USD);

Fee is the service charge of transaction platform (calculated by USD);

Gas is the on-chain transfer Gas (calculated by USD);

F_{buy} is holding frequency of the buyer's address;

F_{sell} is holding frequency of the seller's address;

F_{nft} is holding frequency of the NFT; xNFT Protocol Oracle will create a mapping structure for each address holding the NFT to store the accumulated holding frequency;

O_{all} is the number of holding addresses for this NFT; and

W_{chain} is the weight of the chain, W_{eth} = 100%.

Then, the Oracle price of the NFT is:

$P_o = (P_{new} - Fee) * (2 - F_{buy} / F_{nft} - F_{sell} / F_{nft}) * 50\% * (O_{all} - 1) / O_{all} * W_{chain} + Fee + G$ as.

4.2 Oracle scenario 2: Fragment transaction

If there is an on-chain transaction for ERC20 Token (i.e., fragment) split from an NFT in a recent unit period (e.g., 7 days), then the available on-chain data include the following:

P_{new} is the recent transaction price after weighted calculation by time and turnover (calculated by USD);

A_{total} is the total amount of circulation;

A_{buy} is the quantity of the buyer's holding address;

A_{sell} is the quantity of the seller's holding address;

A_{flu} is the flux;

A_{sum} is the number of transactions in a recent unit period;

O_{all} is the quantity of holding addresses for this ERC20; and

W_{chain} is the weight of the chain, W_{eth} = 100%.

Then, the Oracle price of the NFT is:

$P_o = P_{new} * A_{total} * (2 - A_{buy} / A_{flu} - A_{sell} / A_{flu}) * 50\% * \min(A_{sum} / A_{flu} * 5,1) * (O_{all} - 1) / O_{all} * W_{chain}$.

4.3 Oracle scenario 3: Off-chain transaction

If there is related NFT transaction data off the chain, then the prediction can be made with the off-chain data.

W_{plat} is the weight of an off-chain transaction platform, $W_{opensea}$ = 100%.

Fixed-price transaction and Dutch auction:

L_{new} is the duration of the fixed-price transaction and Dutch auction (unit: minute). The longer the duration is, the stronger the validity of the transaction price will be.

The weight of transaction validity in Scenario 1 is updated to:

$W_{onoff} = (W_{onchain} + (1 - \min(0.2 * 24 * 60 / L_{new}, 1)) * W_{plat} * 20\%) / 120\%$.

Then, the Oracle price of the NFT is:

$P_o = * (P_{new} - Fee) * W_{onoff} + Fee + Gas$.

English auction:

A_{bid} is the number of addresses for the offer. The more the number of addresses for the offer is, the stronger the validity of the transaction price will be.

The weight of transaction validity in Scenario 1 is updated to:

$W_{onoff} = (W_{onchain} + (1 - 1 / A_{bid}) * W_{plat} * 20\%) / 120\%$.

Then, the Oracle price of the NFT is:

$P_o = (P_{new} - Fee) * W_{onoff} + Fee + Gas$.

4.4 Oracle scenario 4: Transaction of other works of the same author

If there is no on-chain transaction for an artwork NFT in a recent unit period (e.g., seven days), then the available transaction data of other NFTs of the same author on the chain include the following:

P_{old} is the recent transaction price after weighted calculation by time and turnover (calculated by USD);

P_{avg} is the latest average price of all NFTs of the same author in recent unit period (calculated by USD);

L_{nft} is the duration after the appearance of the NFT;

P_{pre} is the latest transaction price of NFT created in a unit period before the appearance of

the NFT;

P_{next} is the latest transaction price of NFT created in a unit period after the appearance of the NFT; and

W_{avg} = 10%, W_{pre} = 20%, W_{next} = 20%.

Then, the Oracle price of the NFT is:

$P_o = (P_{old} + P_{avg} * 10\% + P_{pre} * 20\% + P_{next} * 20\%) / (1 + W_{avg} + W_{pre} + W_{next})$.

If P_{avg}, P_{pre}, or P_{next} is 0, then the related W_{avg}, W_{pre}, or W_{next} is also 0.

4.5 Oracle scenario 5: Transaction of similar products

If there is no on-chain transaction for an NFT in a recent unit period (e.g., seven days), then the available data of other similar NFTs on the chain include the following:

P_{new} is the recent transaction price of the NFT (calculated by USD);

Fee is the service charge of transaction platform (calculated by USD);

Gas is the on-chain transfer Gas (calculated by USD);

F_{buy} is holding frequency of the buyer's address;

F_{sell} is holding frequency of the seller's address;

F_{nft} is holding frequency of the NFT; xNFT Protocol Oracle will create mapping structure for each address holding the NFT to store the accumulated holding frequency;

O_{all} is the number of holding addresses for this NFT; and

W_{chain} is the weight of chain, W_{eth} = 100%.

Then, the Oracle price of the NFT is:

$P_o = (P_{new} - Fee) * (2 - F_{buy} / F_{nft} - F_{sell} / F_{nft}) * 50\% * (O_{all} - 1) / O_{all} * W_{chain} + Fee + G$ as.

5. Token economics

5.1 Dual-token mechanism

xNFT Protocol uses the dual-token mechanism, where:

XNFT (xNFT Token) is the governance token issued for 100 million in total and will not be increased further. Thirty percent of XNFTs are used for output of mining, 22% are used for financing, 12% for team motivation, 4% for airdrops, 4% are used for legal consultancy services, 10% for R&D, 8% are used for marketing, 10% of XNFTs are used for ecological and operational cooperation. (Notes: ***The institutional investors of xNFT Protocol will get other NFTs developed by the xNFT Protocol team as per a certain scale in the future.)***

XNP (xNFT Point) is the point for mining, of which the total number is infinite. Through market making or transaction in xNFT Protocol, both the seller and buyer can get XNP that cannot be transferred but can be exchanged into XNFT through the Swap pool.

5.2 Output of mining

To motivate and increase user involvement in the NFT transaction, users of xNFT Protocol who participate in the fixed-price transaction, auction, and transaction with the blind box can output XNP through mining, where:

- Both parties of the fixed-price transaction output XNP as per the transaction amount through mining;
- The seller/winner of the auction and other bidders output XNP as per the transaction amount and bidding price through mining;
- Both parties of the transaction with private blind box output XNP as per the transaction amount through mining; and
- The seller of transaction with public blind box outputs XNP as per Oracle price of NFTs injected into the public blind box and injection duration, while the buyer outputs XNP as per the transaction through mining.

5.3 Multichain deployment

xNFT Protocol supports multiple chains, and therefore, any public chain may be deployed with XNP output through mining. However, the Swap contract between XNP and XNFT will be deployed on one public chain only, as well as the case of XNFT. This public chain is called the “designated main chain” of the xNFT Protocol.

The XNP output from other public chains can be swapped into XNFT only after being swapped into XNP on the designated main chain through cross-chain.

5.4 Waterdrop type injection mechanism

Eighty-five percent output of XNFT per minute will be uniformly dropped into the one-way Swap pool between XNP and XNFT. The real-time swap rate between XNP and XNFT is calculated based on CPMM.

For example, 10 million XNPs and 999 XNFTs are in the Swap pool now. If user Alice sold one million XNPs through the contract of Swap pool, then she could get:

$999 - (10000000 * 999 / 11000000) = 90.82$ XNFTs.

5.5 Insurance benefits pool

Fifteen percent output of XNFT per minute will be injected into the insurance benefits pool. If the balance of reserves is not enough to pay a market bonus to the seller during the draw of the public blind box, then the payment will be made from the insurance benefits pool through Swap. See “Bonus disposal” section.

6. Transaction fees, buyback-and-burn, and governance mechanism

6.1 Transaction fees & buyback-and-burn

The minimum initial values of transaction fees of xNFT Protocol are the following:

- Fixed-price transaction 0.1%;
- Auction 0.3%;
- Transaction with private blind box 2%; and
- Transaction with public blind box 1%.

The transaction fees of xNFT Protocol are mainly used for deployment of the smart contract, cross-chain, invocation of other contracts, Oracle, etc.

After deducting necessary expenses, 80% of the profits of the xNFT Protocol will be used for XNFT buyback-and-burn once per quarter.

6.2 Governance

XNFT holders can vote for community governance of xNFT Protocol. Examples are the following:

- Which NFT contract will be included in the whitelist of the public blind box;
- New methods of enabling the transaction with blind box; and
- Adjustment for the ratio of transaction fees, algorithm, and key parameters.

7. Disclaimer

This paper briefly represents the overall description for **related tokens** (including **XNFT**, **XNP,** or other possible tokens in the future) by xNFT Protocol and can only be used for information disclosure without signature, confirmation, approval, or reply of anybody.

This document does not constitute any forms of investment recommendation and invitation for buy and sale, or any forms of contract or commitment, but the disclaimer and risk warning are legally effective. No user is entitled to make any claim to xNFT Protocol or a related party based on this document.

Any user shall collect the related tokens for the purpose of using their functions and obtaining the service of xNFT Protocol only and not for the purpose of speculation, money laundering, financing for terrorism, or any other illegal activities.

Any user shall get and hold related tokens for himself only, instead of for other's agency.

For users who obtain related tokens: individual user must be an adult citizen in the country of residence and nationality and have the complete capacity of civil right and civil conduct; if a user is an institution, it must be a corporation that is legally established and effectively survives in accordance with related laws and regulations of a country or region and has not been in the process of bankruptcy, liquidation, or takeover.

xNFT Protocol or related party is entitled to refuse any individual for getting related tokens

independently.

In any case, the related token does not represent the following matters or rights:

- Stock rights, right to vote, and right to share profits or other equities of xNFT Protocol and the related party;
- Right to make decisions or right to participate in making decisions in the business operations, management, or transaction of xNFT Protocol and the related party;
- Creditor's rights or right to claim against xNFT Protocol and the related party;
- Right of requiring xNFT Protocol and the related party for buyback or redemption;
- Right of being securities or being registered as securities;
- Share option, subscription right, warrants, and purchase option for any securities, products, or assets;
- Negotiable bill or related voucher; and
- Assets for investment or speculation.

8. Risk warning

The following risks may be possible if you use and hold related tokens. xNFT Protocol aims to remove these risks as much as possible: however, complete elimination of the risks is not guaranteed. You shall be acquainted with and willing to undertake the following risks before getting related tokens:

- Related tokens may become stolen, missing, or cannot be withdrawn or have lost the right of control if the private key of the wallet for storing these tokens is stolen, exposed, or lost.
- The digital cryptotoken system cannot realize existing functions or is invalid as a whole because of the major breakthrough of cryptology and decryption technology.
- Related tokens may not be used permanently or temporarily because of collapse, failure, stagnation, or other faults of ETH or other blockchains for deploying the smart contract of these tokens.

- Related tokens may have changes in quantity or other unexpected changes because of code vulnerability in the smart contract of these tokens.
- There may be no transaction market or transaction price for reference for related tokens because no third party is undoubtedly willing to buy these tokens.
- Any loss may occur if the holder of related tokens fail to understand or misunderstands or forgets the technical background of these tokens or is involved in other forms of negligence.
- Some functions of the related tokens may no longer work normally because of bankruptcy, liquidation, dissolution, insolvency, takeover, or other events of xNFT Protocol or the related party.
- This document shall take effect immediately after being published and can be published again after being modified and updated by xNFT Protocol from time to time.
- xNFT Protocol and related party reserve all rights, including the right of interpretation for all and any part of this document.