Loot NFT: The Proof of Play Protocol

James Duchenne, Suyash Sumaroo and Lance Baker
james@lootnft.io; suyash@lootnft.io; lance@lootnft.io
www.lootnft.io
12 July 2021

1. Introduction

The Bitcoin blockchain is a game where miners compete to be first in finding a specific nonce (number used once only). The winning miner publishes a block of transactions and receives a *coinbase* reward (i.e., bitcoins). As miners expend resources in this process, finding the nonce is their *proof of work*. The system designed by Loot NFT is similar: miners battle against each other to be the last to bid in a time-limited, pay-to-bid auction when the timer expires.

Loot NFT's bid currency is known as the bid unit (BUN). It is a token of limited supply with a fixed value used as a unit of account to calculate an auction's proceeds and to prove a miner's participation level in a gamified auction (i.e., *proof of play*).

Miners use BUNs to bid. During an auction, BUNs are locked in a semi-decentralized memory pool and not released until the end of that auction; this reduces their circulating supply temporarily. When an auction concludes, BUNs recirculate back to the ecosystem for purchase by miners to bid at subsequent auctions.

The winning miner's reward is a non-fungible token (NFT) granting a right of ownership to the NFT and any underlying items embodied by that NFT. In addition, all miners are rewarded with a cryptocurrency (Ticket) that they can use as redemption or purchase currency. Redeeming Tickets remove them from circulation, which in turn requires more bids to create. Tickets are issued based on a miners BUN to Ticket production ratio (Mining Ratio). Miners achieve better Mining Ratios the more NFTs they collect.

The process concludes when a smart contract publishes the NFT in a timestamped chain, linking the prior NFT sold to the next, and so on and so forth. In bitcoin, a block header (an identifier for each block of transactions mined in a chain) consists of a unique alphanumeric number. On Loot NFT, the header for each block of NFT in the chain is the creator's name, the title of the NFT, the winner of the auction, and the unique transaction identifier at the time that NFT was created.

A miner can re-list their NFTs for auction but cannot bid on them. However, it is possible that a miner re-acquires the same NFT subsequently. In that case, a suffix is added to the owners name in the block header. Moreover, re-listed NFTs are tainted by past bid transactions that they carry along with them to future blocks (making them much like identical twins that form different traits as they experience life differently).

NFTs are typically illiquid items. On Loot NFT, they can be made highly liquid as their prices may be disassociated from their intrinsic values, while preserving an unforgeable chain of title since the transactions are recorded on a blockchain. There are multiple practical embodiments of the *proof of play* protocol, such as an application in marketing for known and unknown creators to get attention and price discovery for their works. It allows anyone in the world to access high-valued items irrespective of purchasing power, and mints a cryptocurrency that is issued based on playing fervor and auto-adjusts its circulating supply with use. Fan messages could also be carried together with transactions (i.e., BUNs used to bid), embedding them in an NFT for life.

2. The Problem

Purchasing power disparity locks out most people from participating in auctions of valuable NFTs. On the other hand, NFT creators are in a highly competitive market, which means that lesser known, yet talented creators struggle to break out. Further, the NFT market can be illiquid. Much like the breakthrough innovation behind bitcoin being in the field of game mechanics, the solutions to these problems are rooted in the manner and types of incentives provided to participants at scale.

3. The Solution

Loot NFT provides a possible solution to these issues by combining a *gamified* auction where participants can compete for a low cost and a meeting point for people who want various outcomes from the same process (e.g., whether competing for an item they like, participating to mine Tickets, collecting NFT sets to unlock status and rewards, or supporting a creator).

Loot NFT uses a blockchain infrastructure that follows a path of radical transparency since transactions are public, although their origination is pseudo-anonymous for privacy reasons. Therefore, it may be easier to earn the trust of participants on the platform compared to the traditional, including pay-to-bid, auction environments that are often veiled and susceptible to manipulation.

4. The Specificities of Loot NFT

Loot NFT is an invite-only platform with an arcade-like business model where members bid in gamified auctions. Winners receive an NFT and everyone bidding receives Tickets that are redeemable for limited-edition items or services.

Each auction is time-limited. Members use BUNs (limited supply of 500,000,000 at 0.20 USDC each) to bid, one token at a time. The BUNs are spent and not refundable. A bid in the last 15 seconds resets the timer back to 15 seconds. The last member to bid when the timer expires receives the NFT. BUNs are *trapped* in the auction until the auction ends. Multiple live auctions reduce the circulating supply of BUNs, which in turn ensures there is a winner, although the time taken for an auction to conclude is unknown.

Tickets are also issued to Members that bid in auctions. In this process, members are known as miners. Tickets are issued to miners according to their Mining Ratio. All NFTs are offered in a collectible set of 5. Collecting sets grants miners better Mining Ratios.

Tickets on Loot NFT are redeemable for the following: to invite others (or as a joining fee), to pay for re-listing of NFTs, whitelisting destination cryptocurrency addresses (for e.g., to send member commissions, to send NFTs off the platform, etc.), transferring Tickets or NFTs out of Loot NFT (i.e., off site), voting to vary certain variables on the platform, and for consuming other services. Here, Loot NFT’s membership base can only grow if new members that have been invited own Tickets with which to pay the joining fee, or an existing member pays a new member's invite fee with Tickets.

Loot NFT uses an Ethereum-based permissioned blockchain to initiate, record, and audit transactions. A network of smart contracts creates a second-layer blockchain for each NFT auction. It inherits the underlying blockchain’s integrity. Some parts of this infrastructure are semi-decentralized, such as the memory pool that receives bids in real-time. Bids from each miner’s provenance public address(es) are aggregated first, then added to that of all miners, and that data is hashed in the blockchain at regular intervals such that the prior information cannot be subsequently manipulated. When the auction concludes, each provenance public address initiates a transaction to a smart contract that:

(a) Checks whether all the integrity milestones have been met (checksums)

(b) References an NFT that was previously linked to it as an input and double checks the provenance information to assign it to that reference

(c) Creates a new smart-contract entity for that specific auction out of which Tickets are issued from a *ticketbase.* That smart contract sources data from a user attribute smart contract to calculate a miner's Ticket allocation, checks the previous auction in the chain, and adds the current one to that chain

(d) Forwards the BUNs received to a time-locked wallet called the Oven. The Oven redistributes BUNs back to the ecosystem as fuel for subsequent auctions.

Batching transactions reduces congestion and complexity at the blockchain layer. In addition, since there are no specific times for auctions to conclude, NFTs can be chained in an orderly manner (i.e., remote likelihood of time clashes with auctions ending at the same time). If time clashes occur, the information that is received and processed by the blockchain first will be the next one in the chain. Note, the above is performed in a permissioned environment for the purposes of audibility and provenance only.

When an NFT is sent off site, that NFT is burned (i.e., sent to an unspendable cryptocurrency address), and a new NFT is created on another blockchain in the custody of its owner's nominated cryptocurrency address. The provenance metadata (linking it to the NFT on the permissioned blockchain and block) is permanently anchored in the newly issued NFT, proving provenance and the timestamp at which the handshake between the permissioned blockchain and the public blockchain was made.

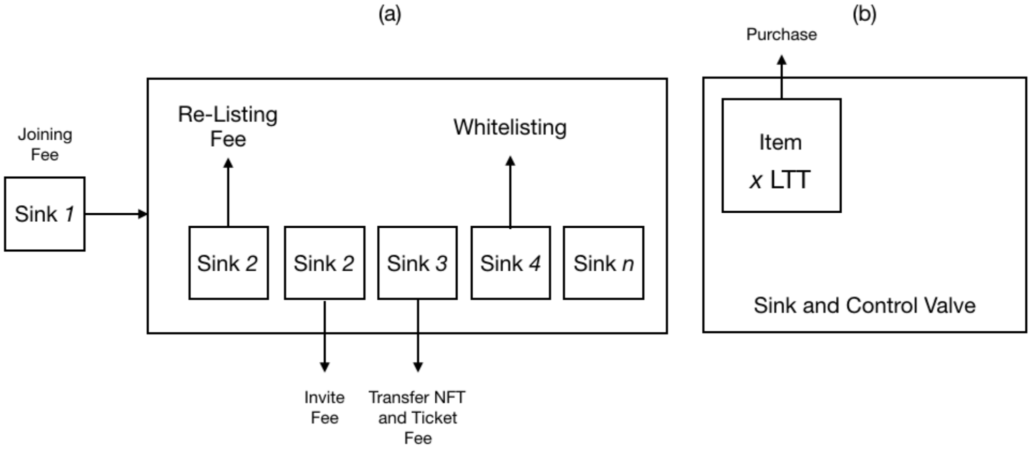
From an educational perspective, Loot NFT provides a visual way for non-blockchain savvy people to experience blockchain dynamics. Bidding is the process of proving participation rather than mining depending on hashing power (or staking wealth). Mining Ratios determine how many Tickets are mined in an entertaining manner (excelling at the game lowers the Mining Ratio instead of buying newer ASIC computers to remain competitive), and once an auction ends, a block is "found" and published.

5. Considerations for Ticket Values on Secondary Markets

Loot NFT does not (and cannot) own Tickets since only miners can produce them.

The consequences of Tickets being a cryptocurrency are significant (e.g., the ability to send them off site, which is a change in custody from Loot NFT to miners). In turn, this can lead to peer-to-peer transfers and trading on secondary markets.

5.1 The Loot NFT sinks



(Reference a) Services offered by Loot NFT (other than bidding) are priced in Tickets; these are known as Ticket sinks.

(Reference b) An exclusive store of limited-edition items not available anywhere else for sale (i.e., master sink and control valve) offers them at a fixed Ticket value irrespective of the variable value of Tickets on the secondary market. (LTT refers to Tickets)

5.2 Theoretical Considerations

(a) If the secondary market value of Tickets increases, this may cause non-members (of Loot NFT) not to shop at the store (i.e., they may find items too expensive). If they really want the item, the best way to get Tickets is to mine them. However, they cannot mine unless they sign up. Signing up requires them to pay a joining fee with Tickets.

(b) If the secondary market value of Tickets is lower than their mining cost, it is more attractive for non-members to shop at the store. This may cause the *velocity* of Tickets burned to increase thereby decreasing the circulating supply of Tickets.

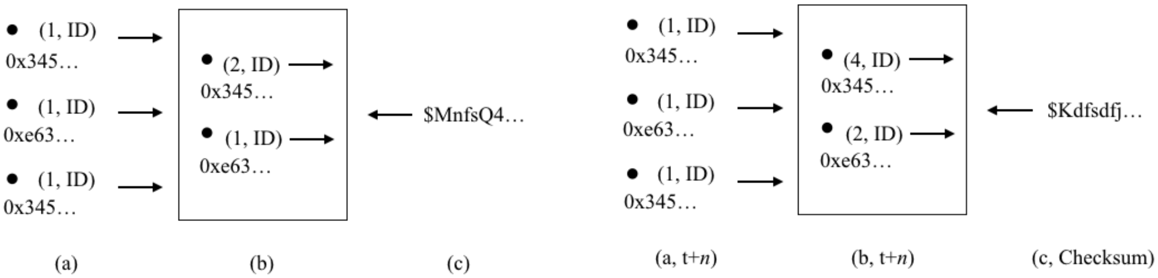
(c) Due to the battle-bidding process, NFTs may attract a higher value than what a person paid for them. In order to re-list NFTs, members need Tickets to pay re-listing fees.

Thus, the store also acts as a control valve for a secondary market value of Tickets. Too high a value increases desirability to join, too low reduces the circulating supply. However, if the desirability to join the platform is independent of the store's attractiveness, or if Tickets are used by third parties as a means of payment (or even in DeFi staking scenarios), this could build up pressure to obtain Tickets. With data mining it may be possible to automate the sinks and control valve to grow a healthy ecosystem.

6. The Technicalities

The architecture is composed of a permissioned blockchain infrastructure, an NFT Minting smart contract, a Mining smart contract, a Block smart contract, and a User Attributes smart contract, in addition to a semi-decentralized memory pool.

Miners have public cryptographic addresses that can receive NFTs, BUNs, and Tickets (reference a). Each bid carries an NFT identifier and is received at the memory pool where it is aggregated (reference b). At specific milestones, the data structure is hashed and persisted in the blockchain (reference c).

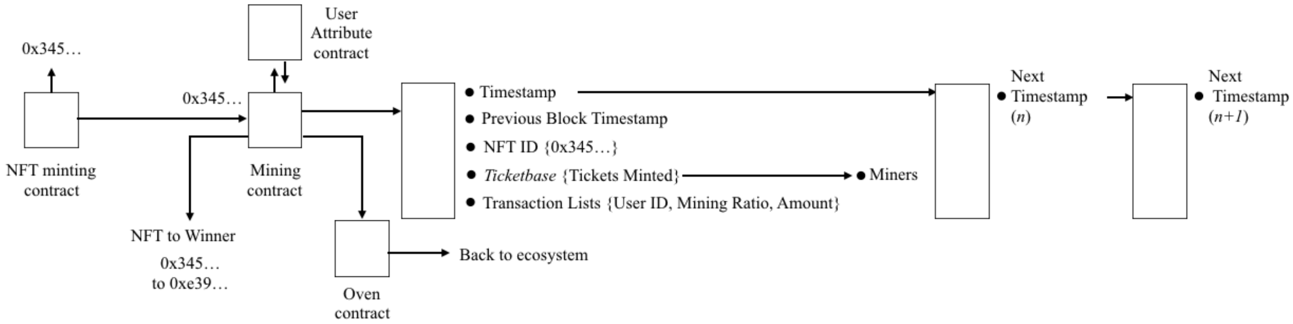


At time t+*n*, new bids enter the memory pool. The previous batch's hash is presented, and if matched, the new data is aggregated to it and a new hash of the sum is obtained. This occurs for each new input at the relevant intervals. If the previous hash has been tampered with, a new hash is created only for the new batch, and the previous batch is referred for inspection against the unaggregated inputs for that time period. At the next time interval, the erroneous batch is hashed again and checked against the old hash, less the incorrect inputs, for inclusion and aggregation. At the end of the auction, provided the checksums have been verified, the total aggregate batch of transactions (for each address) is sent to the blockchain for processing. An explorer can be built for the memory pool.

6.1 Smart Contracts and the Mining of Layered Blocks

When an NFT is minted, its address is registered to the Mining smart contract. Transactions from auctions are then sent to that smart contract with the NFT identifier such that it understands that the transactions relate to an auction that ended for a particular NFT.

At this point, the following occurs in the system:



(a) (i.) BUNs are forwarded to the Oven

(ii.) The NFT is sent to the winner’s public address

(iii.) The Mining Ratio from the User Attributes smart contract is retrieved

(iv.) The miner’s Mining Ratio, NFT address reference, and BUN used in bids by that miner are sent to the Block smart contract

(b) The Block smart contract creates a block record with the NFT’s address, calculates the *ticketbase* out of which Tickets are minted to a miner’s input address(es), and records the identifier and timestamp of the previous block record (note, for the *genesis* block, there would not be a *previous block* since it is the first block); and

(c) The same process is performed for re-listings.

The result is a chain of title (or block) for the NFTs sold using smart contracts. While this system is designed for the purposes of Loot NFT, its applications could be multiple, i.e., land transfers, royalty transactions, genealogy research, and more.