Introduction

This protocol spec describes how atomic-swap based, tradeable and mintable NFT can be built on SmartWeave, smart contract protocol where smart contracts can't directly manage native coin (AR). NFTs are full-fledged universal stores of value along with fungible tokens, and having fully working NFT mechanisms (and so working store of value) is essential for ecosystem growth.

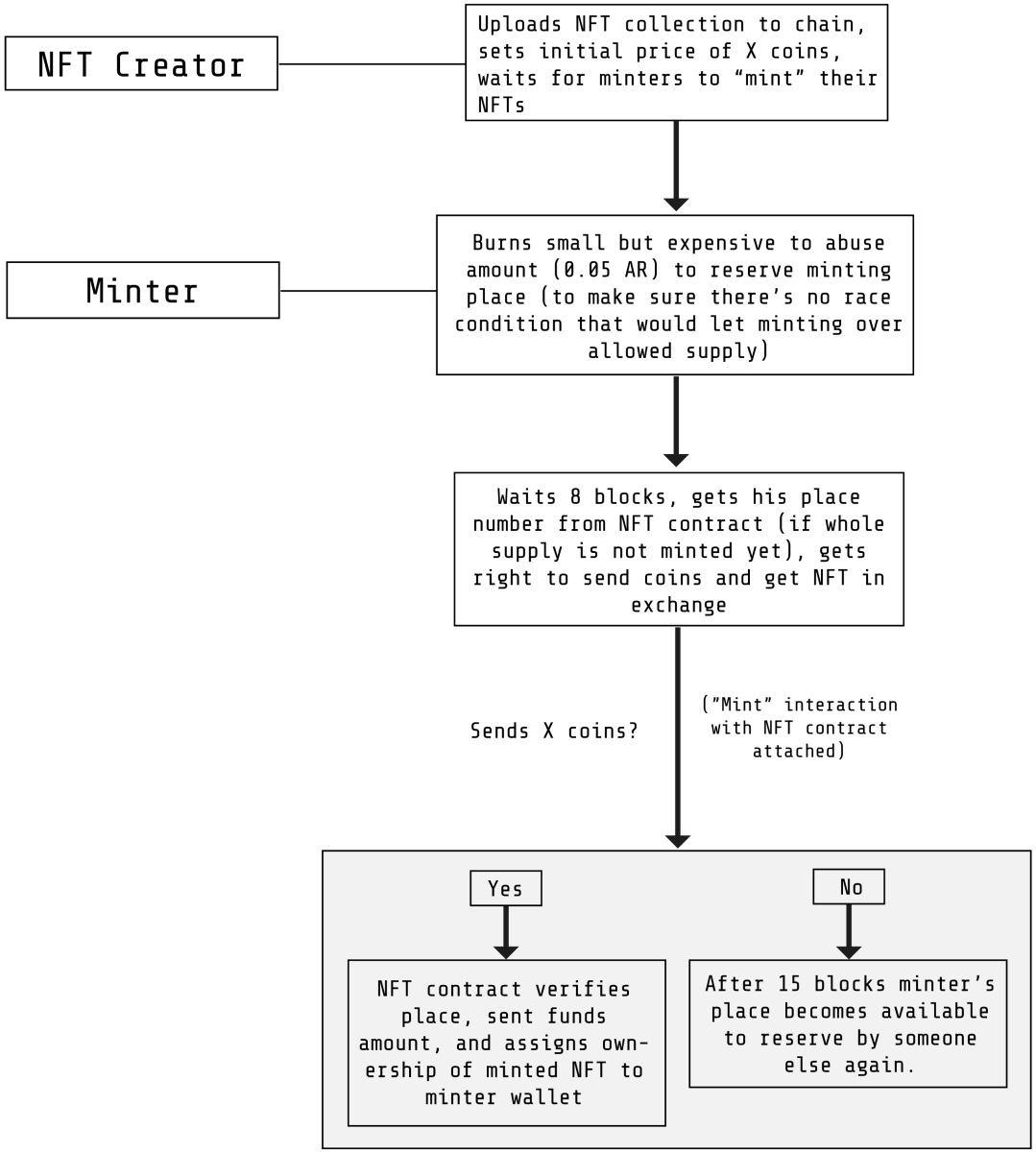
Author: Nik Rykov <nik@hns.is>
Co-authors: JF <jf@arweave.app>

Last update:1/3/2023

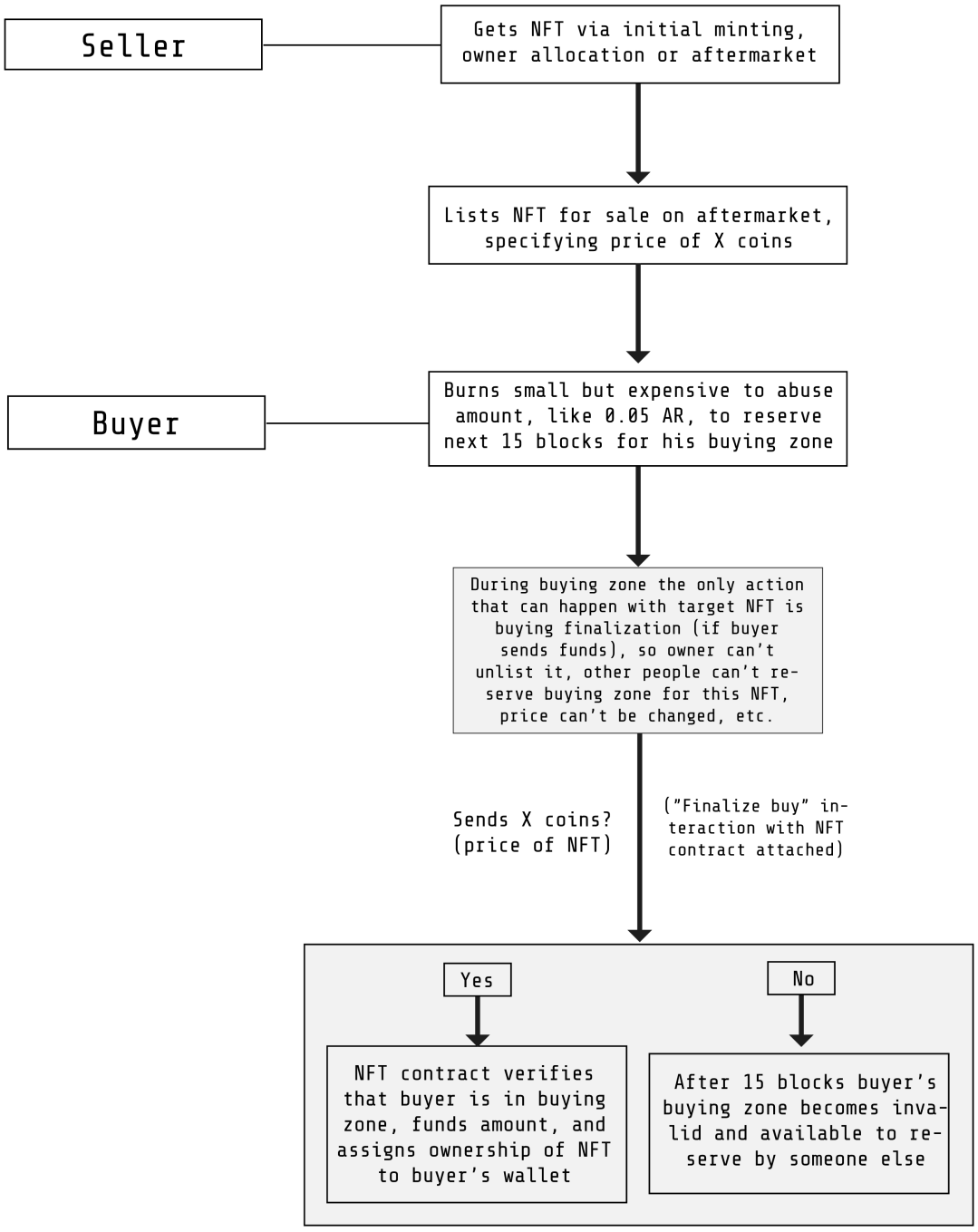
Actors

NFT Creator	Uploads collection, puts it for minting, wants to get AR from initial sale aka “Minting”
Minter	Buys NFT from NFT creator on initial sale with fixed price specified by creator
Seller	Bought NFT from initial sale or aftermarket, lists it, and wants to sell it
Buyer	Wants to buy NFT on aftermarket

Minting


NFT Creator
Uploads NFT collection to chain, sets initial price of X coins, waits for minters to “mint” their NFTs
Minter
Burns small but expensive to abuse amount (0.05 AR) to reserve minting place (to make sure there’s no race condition that would let minting over allowed supply)
Waits 8 blocks, gets his place number from NFT contract (if whole supply is not minted yet), gets right to send coins and get NFT in exchange
Sends X coins?
(”Mint” interaction with NFT contract attached)
Yes
NFT contract verifies place, sent funds amount, and assigns ownership of minted NFT to minter wallet
No
After 15 blocks minter’s place becomes available to reserve by someone else again.

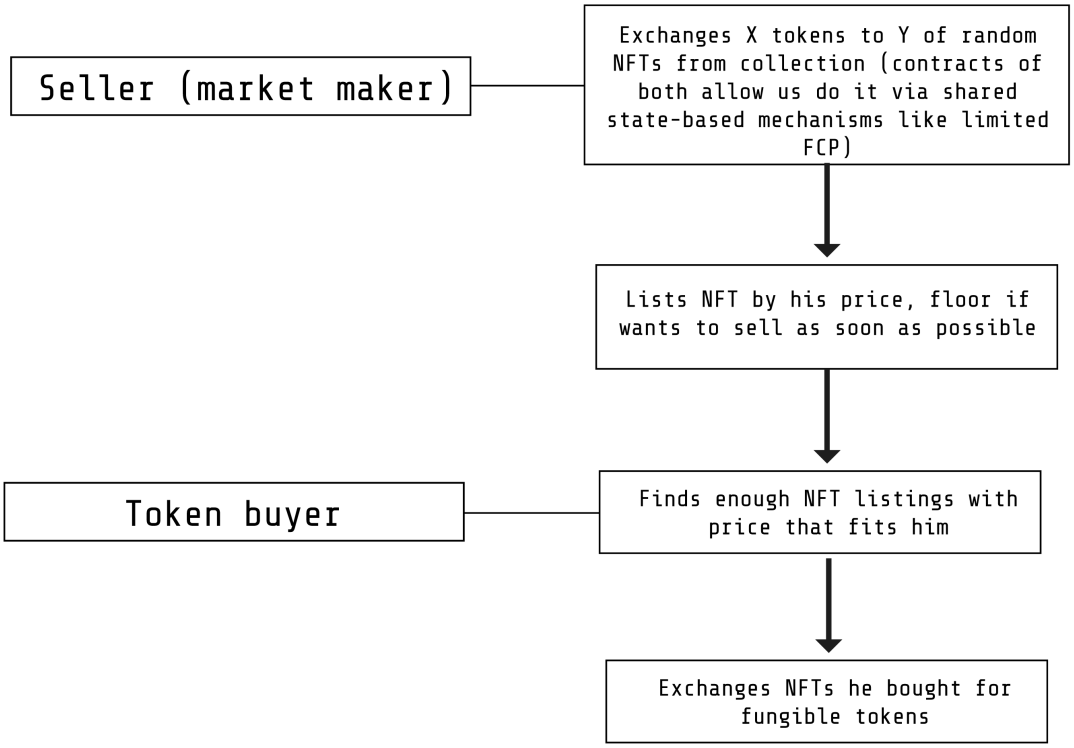
Trading


Seller
Gets NFT via initial minting, owner allocation or aftermarket
Lists NFT for sale on aftermarket, specifying price of X coins
Buyer
Burns small but expensive to abuse amount, like 0.05 AR, to reserve next 15 blocks for his buying zone
During buying zone the only action that can happen with target NFT is buying finalization (if buyer sends funds), so owner can't unlist it, other people can't reserve buying zone for this NFT, price can't be changed, etc.
Sends X coins? (price of NFT)
("Finalize buy" interaction with NFT contract attached)
Yes
No
NFT contract verifies that buyer is in buying zone, funds amount, and assigns ownership of NFT to buyer's wallet
After 15 blocks buyer's buying zone becomes invalid and available to reserve by someone else

Applying to trading of fungible tokens

Working NFT market will also allow us to trade fungible tokens through it as well. We just need to allow 1:1 conversations between any NFT from collection and X amount of fungible token.

Buying fungible tokens with AR through NFTs:



Anchoring and reorg protection

As arweave network is PoW-based and uses Nakamoto consensus, it has probablistic finality and reorg possibility. Anchoring allows us to protect from reorgs.
When sending transaction, you specify anchoring block hash, and if this block is not found in blockchain, your transaction invalidates. This allows us to protect from chain reorgs, explicitly linking transactions to specific fork of chain.
Without anchoring, Tradeable-Mintable-Atomic-NFT protocol would be vulnerable to reorgs (NFT owner could just receive coins for his NFT and make reorg, where he could push unlist or price-change transaction, making buy contract call invalid, but still getting funds).
Specially because of anchoring we left this relatively big margin to finalize sale (15 blocks).
While last 10 blocks is just margin to let buyer send funds, first 5 blocks is time for buyer to get block hash from buying zone, to let buyer send finalization transaction anchored to his buying zone, so that he can be sure that his funds will be returned to him if reorg will happen and buyer will unlist NFT in it, change price for it, or someone will buy it there.