

# TruMint: A Trusted Minter

By William Barlow, Ephraim Olson, Isaiah Olson, and James David Williams  
Version 1.1 – June 13, 2022  
info@trumint.xyz

The benefits of transacting on blockchains—instant settlement, immutability of records, automation through smart contracts, etc. —are almost exclusively available for transactions of digital assets. Realizing these benefits with real world assets (“**RWAs**”) within current legal frameworks requires a trusted third party (a “**Trusted Minter**”) to mint non-fungible tokens (“**NFTs**”) that always represent legal ownership to the RWA described in the NFT. Without Trusted Minters, buyers of RWA-linked NFTs must verify sellers’ ownership of the RWAs before transacting, eliminating many of the efficiencies of public blockchains in the process. With a Trusted Minter in place, a buyer of an RWA-linked NFT need only confirm that the NFT was minted by a Trusted Minter to confirm seller’s ownership of the RWA. Trusted Minters will serve as the link between RWAs and digital assets stored on public blockchains.

## Introduction

The ability to transact RWAs on-chain using RWA-linked NFTs has been much discussed, yet progress towards making this possible has been frustratingly slow. RWAs are fundamentally different from digital assets because of the potential for off-chain alteration. RWAs can be lost, stolen, seized, damaged, or destroyed. Importantly, the government of the jurisdiction where the RWA exists has the ultimate power to determine and enforce ownership. This necessitates the use of a method that will be recognized by the relevant government for transfers of RWAs on blockchains. As a result, facilitating transactions of RWAs on blockchain requires more legal innovation than technical development. Unlike transfers of digital assets, transfers of RWA-linked NFTs require verification that the transfer of the NFT will be legally recognized as a transfer of the RWA. In migrating ownership of and security interests in RWAs onto public blockchains, our goal is to minimize both the cost of this verification and the need for trust in multiple third-parties. Central to our model are Trusted Minters, who deploy a combination of legal agreements, smart contracts, digital infrastructure, and security protocols in a “lockbox-and-key” model to ensure that any transfer of an NFT minted by a Trusted Minter also transfers legally enforceable ownership of the RWA.

## Existing Methods to Transfer Ownership of RWAs and Early Attempts to Transfer Ownership Using Blockchains

Ownership of RWAs is presently transferred by recording a legal document with a governmental authority or executing a legal document signed by the transferor. However, these transfers may be rendered ineffective if the purported transferor does not hold title or if title is encumbered. In large transactions, buyers of RWAs and lenders using RWAs as collateral conduct due diligence to ensure that the relevant parties own the assets being sold or collateralized (“**Title Diligence**”).

Title Diligence may take the form of title searches, inspecting prior legal agreements, and searching lien databases. Even these measures are often insufficient to satisfy buyers and lenders. For example, in the United States mortgage lenders normally require buyers to purchase title insurance at a cost of up to one percent of a home's value to insure against defects to title. In other transactions, buyers require strict indemnification by sellers in case of title defect and hold back a portion of the purchase price to address such claims. In short, Title Diligence and title insurance are expensive and time consuming, but the immutability of blockchains promises to drastically reduce these costs.

There have been early attempts to bring the benefits of transacting using blockchains to RWAs. This has been accomplished as follows: a new legal entity (e.g. a limited liability company) is created; ownership of the RWA is transferred to that legal entity; an NFT is minted; legal documents are drafted such that ownership of the NFT represents ownership of the legal entity owning the RWA; and then the NFT is transferred in an on-chain transaction.

If implemented correctly, this process does transfer beneficial ownership of the RWA. However, it does not reduce the cost of, need for, or burden of Title Diligence or title insurance. A buyer must still confirm that the seller held marketable title to the RWA when the RWA was contributed to the newly-created legal entity, that the contribution was made properly, and that the relevant legal documents correctly transfer ownership of the RWA when the NFT transfers. Unfortunately, this model creates an even more burdensome process than existing methods that do not use blockchains. This model also requires the creation of a new legal entity for each RWA whose ownership is recorded on a blockchain and the payment of ongoing fees to maintain the legal entity in order to keep a record of ownership of the RWA on a blockchain. This is not a long term solution. A more developed legal framework is required.

There have also been early efforts to collateralize loans backed by RWAs using DeFi protocols. This has been achieved by minting tokens linked to fractional interests in a protocol which then invests in RWA-collateralized loans managed by the operator of the protocol. This model increases liquidity for investors relative to equivalent off-chain transactions, but this increased liquidity comes at great cost. First, current models generally require a back-door to allow protocol operators to convert contributions into fiat currency in order to purchase the RWA-backed loans. Second, there is no easy way to verify what assets these protocols have invested in. These two issues leave investors vulnerable to fraud. Even if operators of these protocols act in the best interests of investors, there is no way for different protocols to exchange RWAs on blockchains, greatly reducing the potential liquidity of these assets. Once again, a more developed legal framework for holding RWA-backed loans is required to give these protocols greater transparency, security, and liquidity.

## A New Model to Transfer RWAs Using Public Blockchains

As stated previously, our goal in migrating RWA transfer and collateralization onto public blockchains is to minimize the cost of verification and scope of trust required to transact. Our proposed method relies on a third-party called a "Trusted Minter." The job of a Trusted Minter is

to upload ownership of an RWA into an NFT and then ensure that the NFT and ownership of the RWA can never be unlinked. This can be accomplished via a “lockbox-and-key” method.

In the “lockbox-and-key” method, the Trusted Minter will work with the current owner of the RWA to put ownership of the RWA into a form of legal cold storage (the “**Lockbox**”), which does not allow ownership of the RWA to be transferred without the simultaneous transfer of a designated NFT. The Trusted Minter then mints the designated NFT (the “**Key**”) which contains an accurate description of the RWA. Ownership of the RWA can then only be retrieved from the Lockbox by a process that returns the Key to the Trusted Minter, who will be legally obligated to return ownership of the RWA to the Key holder and burn the corresponding Key. Strict security protocols will be needed to prevent the unauthorized transfer of the Key and to address instances where the Key holder loses access to the wallet holding the Key.

With this method, ownership of the RWA can be transferred on blockchains by transferring the Key. Of course, market participants will have to closely vet any Trusted Minter to ensure that its “lockbox-and-key” method is both secure and legally enforceable. Once this vetting process is complete, however, market participants can transact with any counterparty and only need to verify that the NFT held by the counterparty was minted by a Trusted Minter.

## Costs and Advantages of the New Model

The primary cost of adopting this new model will be incurred when a Trusted Minter creates the Lockbox and Key. The Trusted Minter will need to take the necessary legal steps to create the Lockbox, conduct Title Diligence before minting the Key, and mint a Key that accurately describes the RWA. Once this upload cost has been incurred, however, the subsequent cost to confirm that ownership of the RWA remains unchanged at the time that the Key is transacted will be greatly reduced and may ultimately be eliminated.

The impact of these savings may be most profound in DeFi. Implementing the Trusted Minter “lockbox-and-key” model will allow DeFi protocols to exchange RWAs between each other on public blockchains, increasing the liquidity of these different protocols. Furthermore, this model will vastly increase the transparency of DeFi protocols, allowing investors to confirm at any time the assets that back the protocols’ tokens. This model also allows for the possibility of DeFi protocols that both invest in RWAs and do not require a back-door for protocol operators to convert and withdraw the protocol’s assets into fiat since the investments in RWAs can be done entirely through the purchase and sale of Keys.

## Link Between Digital Assets and RWAs

Trusted Minters act as a link that facilitates transactions involving RWAs on public blockchains. Trusted Minters will allow ownership of RWAs to remain indefinitely on public blockchains and for unlimited transactions of RWAs on those same blockchains. For some, the requirement to place any trust in a third party is anathema. However, trustless transactions of RWAs on blockchain are impossible given the inherent constraints of existing legal systems. Our proposed solution

minimizes the scope of the trust required and the cost of verification and in the process brings the benefits of public blockchains to whole new asset classes.

## Conclusions

We have proposed a new model for transferring and collateralizing RWAs on public blockchains using a “lockbox-and-key” model that relies on Trusted Minters. Trusted Minters will place ownership of RWAs in a legal “Lockbox” with a NFT that acts as the “Key.” Ownership of the RWA cannot be retrieved by anyone but the holder of the Key, the holder of the Key may retrieve the RWA at any time, and the Key will be burned upon retrieval of ownership of the RWA. The advent of this new model will allow RWAs to fully realize the benefits of transacting on blockchains. It will also improve the transparency of DeFi protocols investing in RWAs, allow DeFi protocols to invest in RWAs without a back door, and facilitate transactions of RWAs on public blockchains between DeFi protocols.