Crosslink Protocol

Abstract
The Crosslink Protocol is a method with accompanying infrastructure for creating on-chain titles for off-chain assets. These *microtitles* are implemented as *non-fungible tokens (NFT)*, which confers permanence, portability, and authenticity. The protocol employs a clever public/private key signature scheme that forms an incontrovertible link between an item, and its title. Using the Solana blockchain–a decentralized public ledger–the protocol can be accessed to mint and transfer items permissionlessly, and to verify an item's provenance without trusted third parties.

Background
Proof of ownership and authenticity are two enormous problems today, neither of which have been adequately solved. Deceptively good counterfeit products are regularly passed off as legitimate, which defrauds customers, and can be incredibly dangerous. Manufacturers often receive defective counterfeit goods as warranty claims, which, if not correctly identified, can also lead to significant financial losses. Finally, for legitimate claims, proving ownership via a receipt or other impermanent piece of paper is comically out of date, and the concept of "title" is not easily demonstrated, or transferred. Witness just two of the types of sprawling intermediaries that have embedded themselves into daily life to support these needs: motor vehicle departments, and property title companies. These are difficult challenges, certainly, but with the use of the Solana blockchain, the technology exists to neatly address them in a cost efficient manner.

Description
A *microtitle* is a blockchain-secured certificate of authenticity, and proof of ownership rolled into one. In its essence, a microtitle bonds physical property (*off-chain assets*) to a unique, *non-fungible token (NFT).* The NFT is created on a blockchain, and the metadata is hosted in distributed file services to serve as a public, and permanent record. Possession of the NFT confers ownership, and the metadata provides the link to the property via encoding of basic information about the item, and a public key. Up to this point, there is nothing novel about our implementation of titles using a blockchain. Indeed, solving this problem is merely an act of assembly, with all of the necessary components already refined and in common use. The most important and perhaps non-obvious aspect that makes the microtitle solution unique is in the bonding or *crosslinking* of off-chain assets to the NFT, using a public/private key pair. With the NFT containing the public key, it is used to confirm a signature that is permanently affixed to the item, which enables parties to verify authenticity.

Crosslink Protocol: How it Works
The following describes the Crosslink Protocol that forms the essential and incontrovertible link between a physical good, and its title:

1. At the time of production, the title creator or manufacturer (mint authority) creates a public/private key pair, not unlike those used in PGP. This is called the *bonding key pair,* which is unique to each item that will be created.
2. The mint authority also creates an NFT. Basic info is encoded into the NFT metadata, such as a link to an image, a serial number, model number, and critically, the public key of the bonding key pair.
3. Next, the manufacturer creates the item—a new product, artwork, whatever.
4. The creator then uses the private key of the key pair to sign a message. This signed message is then permanently affixed to or inscribed on the item, either in the form of a 2D barcode, or an RFID tag. To prevent tampering, this message should not removable.

5. The item is delivered to its owner, in addition to the microtitle (NFT). Now, when a user decides to sell or transfer the item, they also transfer the title to the new owner. Should the new owner need to return the item to the creator, they can quickly and easily prove rightful ownership by presenting the microtitle/NFT. Using the NFT is essential because it confirms:
    i. *Origin:* That only the manufacturer could have created the item. The manufacturer controls the private key(s) to the item, so items that are presented with a valid public/private key, but with a public key that's not found in the manufacturer's records could be determined as credibly fraudulent. Titles would only be accepted that have a mint authority that matches the manufacturer's.
    ii. *Uniqueness:* That the item is truly one-of-one, and that multiple counterfeit products cannot be passed off, potentially using a single, legitimate serial number, for example.
    iii. *Ownership:* physical property is subject to theft. However, with adequate protections in place, digital property is much more difficult to steal. In the event of theft, an owner could easily verify their ownership of the stolen property by presenting the digital title. The incontrovertible link between the inscribed signature on the item, and the NFT's public key provides confirmation that whomever holds the NFT, is also the rightful owner.

Solana Blockchain

The choice of Solana as the hosting blockchain is an important one. While still in its beta phase, and just now two years old, Solana provides functionality that other blockchains simply cannot replicate, and are essential for the implementation of microtitles:

- *Speed*: with block times of less than one second, Solana facilities settlement of property, or even just basic interactivity that is required for businesses, and people to rely on.
- *Bandwidth*: Solana blockchain, with unrivaled transaction rate of greater that 50,000 tx/sec, and it's ability to scale horizontally, ensures that the protocol can support the transaction volume that is inherent in bringing millions of off-chain items on-chain.
- *Decentralization and censorship resistance*: in order to honor individuals' property rights, it is essential that the public ledger used has adequate security and permanence. Solana blockchain currently has nearly 1000 mainnet validators, which is a number that is rapidly growing. These validators maintain the shared state of the ledger, with just a single validator required to declare fraud and punish dishonest ones. Also significant is Solana's Nakamoto coefficient—the number of unique validators that comprise a controlling stake of greater than 33%, that are able to halt or adversely interfere with the network--is currently 19. This number is substantially better than most other networks. Suffice it say that the Solana network is sufficiently robust to geographic failures, censorship, or other malicious interference.
- *Cost*: in a world where millions or billions of physical objects receive a microtitle, the ability to produce these digital titles at low cost and significant scale is essential. On blockchains where transaction fees are both high, and highly variable (Ethereum, for example), it is an unpredictable and oppressive platform to try to build a product like microtitles. Solana's consistently low fees, and a verbal commitment to "reduce fees at the rate of Moore's Law" provides an attractive climate to grow our ecosystem.
- *Technology Stack*: Solana Labs' choice to employ general purpose computing hardware, development tools, even computing language (Rust), ensures that the Solana ecosystem will have a life-cycle that endures longer than if it were built on proprietary tooling. Other blockchains often have their own languages and dialects, which rewards experts, and is uninviting to new developers. Ultimately, we wanted to build on a platform that is *extensible* and *open*, and that had high quality tooling to support our workflow.

Applications
A non-comprehensive list of applications for microtitles follows:

- Companion, collectible NFT and title for luxury watches with embedded RFID chip
- Counterfeit prevention of commercial and industrial goods, such as circuit breakers, programmable logic controllers, and various high-tech equipment
- State or jurisdiction recognizing microtitles to reduce cost, and increase efficiency of their operations
- Public event tickets such as concerts, or sports

Security
A red-shirt exercise raised the possibility that an attacker could counterfeit off-chain assets using the Crosslink Protocol, if any of the private keys for those items had been compromised. This is a legitimate concern, but may be handily addressed using a [minimum] two-of-two multi-signature scheme. For instance, in addition to the bonding signature that links the item to the NFT, the manufacturer could retain a private key that represents the mint authority for the off-chain asset. The signatures would be combined, and with both public keys for the mint authority (manufacturer), and the item's bonding key pair, verifying the on-item message has been signed by *both* key pairs confirms that the item is legitimate, to a high degree. Alternative signing schemes could be employed, which will provide statistically better protection against the threat of compromised bonding keys.

Enforcement
The extent to which *microtitles* can be used and applied is essentially limitless; their effectiveness would only be constrained to the environment, and jurisdictions that recognize them. As it relates to physical goods and property in meatspace, it requires corporate, social, or legal enforcement. For immediate use, one could imagine a manufacturer with valuable products that are often counterfeited. Within their warranty or service departments, they could quickly adopt microtitles and declare that returns will only be honored on products that have an active and valid microtitle. One could also imagine a much more streamlined and hassle-free transfer of ownership for automobiles, for instance, if motor vehicle departments were to recognize microtitles. Finally, the burden of proving ownership to police departments, insurance companies, whomever, would be greatly reduced by using microtitles, thereby increasing market efficiency and reducing costs for all parties.

Conclusion
NFTs are currently a great source of entertainment, combining artistic expression, and a dash of financial speculation. Despite the fun dimension to NFTs, their invention is significant, and may yet be used to solve thorny, real-world problems. Ownership and title transfer for off-chain assets using a blockchain is not in itself a novel idea. The authors would never claim so much. Frankly, the Crosslink Protocol stands on the shoulders of giants, in that it takes advantage of 1) decades of public/private key cryptography, 2) developments in labeling and electronic tagging for physical goods, and 3) the miraculous speed, and reliability of the Solana blockchain. Crosslink Protocol relies on the clever application of public/private keys and a signature verification process to provide an *incontrovertible link* between an item and its microtitle. The rest is, as Anatoly says, "just engineering."

Appendix

Crosslink Protocol Schematic