Tao Network, Revision 1.4, August 18, 2016

A Digital Phonorecord Delivery System for Virtual Audio Records

Bryce Weiner

bryce@tao.network

Abstract. The Virtual Audio Record (VAR) is a phonorecord which is fixed by cryptography instead of physical media. In this white paper is presented a novel solution for the distribution, settlement, access, and exchange of VARs, as well as the provision of audio metadata for such content.

Introduction. The Virtual Audio Record (VAR)[i] is a concept developed by the Tao Network Developers in order to implement a system for the transfer of audio content within full compliance of the US Copyright Act (Title 17, Sections 101, 115; 2010), as well as address the challenges presented in the US Copyright Music Marketplace (2014).[ii] The exact cryptographic nature of a VAR allows for unprecedented flexibility in content provisioning and control. The Tao is a network protocol for digital phonorecord delivery utilizing modern cryptographic methods, distributed data storage, and blockchain technology. The result is an ecosystem which creates the experience of a "virtual phonorecord": the experience created by implementation of a VAR where it is able to retain all of the attributes of a phonorecord but without the physical component.

Related Works. The Tao Digital Asset Management Network is made possible by unique applications of an identity schema developed by Bryce Weiner[iii] and the design for a Virtual Audio Record as conceived by the Tao Network Developers.

Definitions

Identity – A unique public and private key pair derived from the ED25519 elliptic curve for public key encryption (PKE).
Content – The media contained within a VAR.
Platform – A third-party application which offers VARs for retail purchase by consumers and/or enables the activation of purchased VARs.
Address – A Base58-encoded string deterministically derived from the public key portion of an Identity.
Entity – A corporation or individual participating in the Tao network.
Record Label Identity – An identity which serves to authenticate the entity which is responsible for management of content within the TAO network. Addresses for Record Label IDs begin with the letter "L."
Media Identity – An identity which serves to validate content. Addresses for Media IDs begin with the letter "M."
Distributor Identity – An identity which serves to authenticate the entity which is responsible for the distribution of content within the TAO network. Addresses for Distributor IDs begin with the letter "D."
Retailer Identity – An identity which serves to authenticate the entity which is responsible for the proper settlement of funds for the retail purchase of content. Addresses for Retailer IDs begin with the letter "R."
Platform Identity – An identity which serves to authenticate the entity which is responsible for the provision and delivery of a VAR. Addresess for Platform IDs begin with the letter "P."
Consumer Identity – An identity which serves to authenticate the consumer (end-user). Addresses for Consumer IDs begin with the letter "C."

Retail Staging Address – An alphanumeric string deterministically generated from the combination of a Media ID and a Retailer ID. Retail Staging Addresses begin with the letter "r."
Activation Staging Address – An alphanumeric string deterministically generated from the Media ID which is used to provision purchased VARs. Activation Staging Addresses begin with the letter "a."

Anti-Fraud Protection

The TAO network is employed as a distributed, peer-to-peer system in order to protect data integrity and prevent fraud. As a result, transactions submitted to the network are processed in 15 second batches, called "blocks." To guarantee a valid transaction, a minimum of 6 blocks are required for a transaction to be considered as valid, requiring up to 90 seconds for any given transaction submitted to the network to be accepted as valid.

TAO Network Governance

The TAO network is to be governed by a not-for-profit entity consisting of those companies which develop the software and produce, record, and distribute content. A steering committee shall be formed which will be responsible for reviewing and approving changes to the protocol and the ecosystem implementation. Membership in the TAO governance organization is mandatory for record labels, platforms, and distributors who wish to participate. Identities for use of the TAO network by those entities are created and managed by the organization.

Entity Activation

Record Label

An entity which provides content for distribution on the TAO network is considered a "record label." All such entities must be members in good standing of the TAO governing organization.

Media

Media activation and management is solely the responsibility of the record label which created the content to be distributed.

Distributor

Distributors must be members in good standing of the TAO governing organization and must prove a solid and successful business approach towards distributing digital content.

Retailer

Retailers are not required to be members in the TAO network governing organization, however they must be registered within the ecosystem in order to activate content for the consumer.

Platform

Entities which provision content purely in digital form directly to consumers are considered "platforms." Platforms must be a member in good standing of the TAO governance organization.

Consumer

Consumers access the TAO network through platforms or specially designed TAO network consumer hardware. Identity provisioning is handled by the method in which an individual first accesses the network for content.

Decentralized Storage and Processing

The Master Record Vault

The Master Record Vault is a collection of physical servers that form the distributed hash table (DHT) storage of encrypted masters. Entities may elect to store their content locally or share

storage space with other producers in the ecosystem. All masters are encrypted by the respective owners and cannot be accessed or consumed without proper authorization. Authorization is provided by smart contracts which validate remittance of payment and authenticity of content.

The Consumer Vault

The Consumer Vault is unique to each consumer and is a DHT cloud store of purchased content. The DHT is created by a network of consumer devices that provide MQA quality output. During network bootstrap, the DHT will be hosted on servers by Tao Digital Labs LLC while consumer hardware is developed and brought to market.

The TAO Blockchain

The TAO blockchain executes the smart contracts required for the validation of payments and is processed on the same consumer hardware which supports the DHT cloud storage. This assures that no single entity gains control of the network and consumers have an active part in the provisioning of the content they purchased.

Assuming…

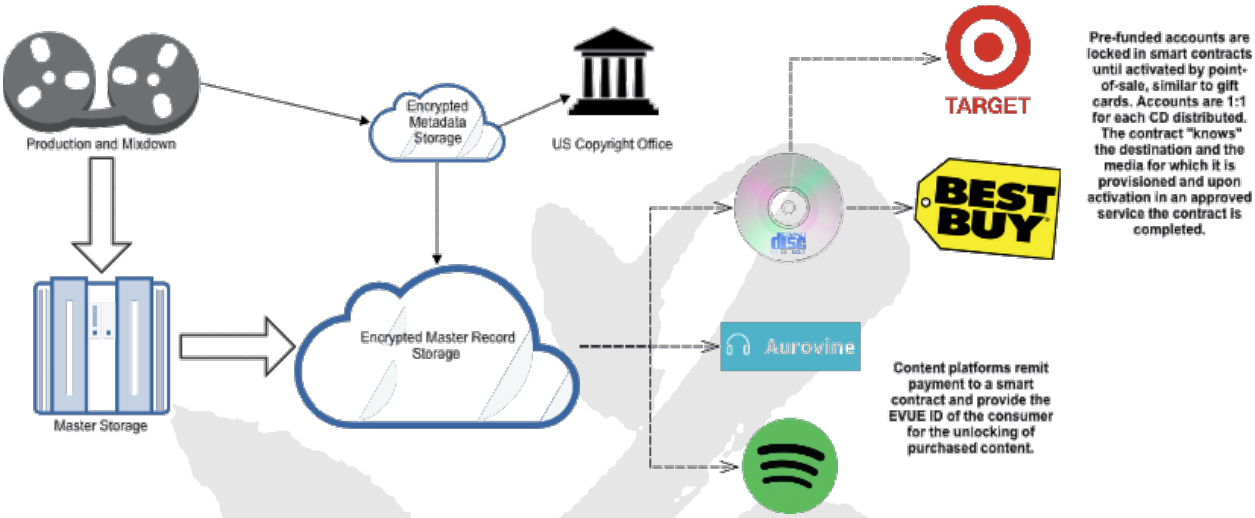
11	**:1 compression ratio**
72.72727273	**MB per VAR**
100,000	**MB capacity per device**
100,000,000	**VAR consumers**
100	**albums per lifetime of a consumer**
15%	**of consumers have VAR enabled hardware**
10,000,000,000	**total album purchases**
727,272,727,273	**MB total data**
1,500,000,000,000	**MB network storage capacity**

Oracle Nodes

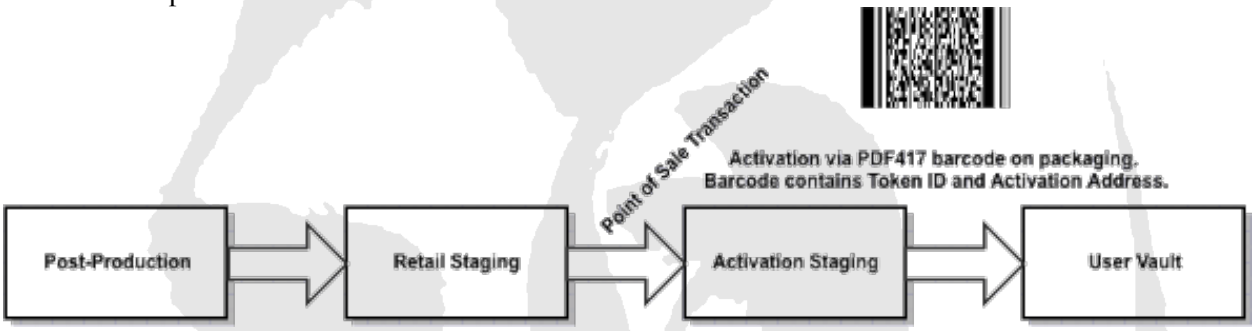
Oracle nodes process transactions for groups of content, fulfilling the role of a publisher within the system. Oracles validate proofs of purchase and release purchased content. Because an Oracle node can only process content for which it has the appropriate keys, each node serves as a trusted entity for the creators of the content which it manages. This allows traditional, large scale music publishers to retain direct control over digital masters as well as provide the infastructure for independent publishers to deliver content.

Point-of-Sale Activation

To enable point of sale activation, a PDF417 barcode is printed on the packaging of the physical media. The barcode contains two components: the Media ID of the content being purchased and an Activation Staging Address (public key). Activation validation verifies the amount remitted is equal to or greater than the MSRP of the content. Upon verification, content is transferred from the Retail Staging Address to the Activation Staging Address by an Oracle node. The private key to transfer the content from the Activation Staging Address to the consumer's Vault is contained inside the sealed packaging. The private key is represented as a QR code as well as an alphanumeric string to aid in importing the value into the platform application.



Assuming the consumer as already activated their Consumer ID in the platform of their choice, the consumer scans the QR code (or enters the alphanumeric string) containing the private key required to transfer the content into their Vault. Content is prepared for consumption within three (3) minutes of activation via point-of-sale.



Fiat-based Platform Activation

Fiat-based platform activation operates similarly to point-of-sale activation, with the exclusion of the printed key components. Activation validation verifies the amount remitted is equal to or greater than the MSRP of the content. Upon verification, content is transferred from the Retail Staging Address to the Activation Staging Address. The private key to transfer the content from the Activation Staging Address to the consumer's Vault is then provided by the platform to the TAO network along with the consumer's Consumer ID as entered into the application. Content is then transferred into the consumer's Vault within 90 seconds.

Cryptocurrency-based Platform Activation

Cryptocurrency-based platform activation requires a module specific for each cryptocurrency blockchain to be supported. While the process does not change, the specific nature of execution of the smart contract does. The planned cryptocurrencies to be supported are currently Bitcoin and Ethereum.

A Consumer ID is still required to provision content to the consumer. Once the transaction is verified on the settlement blockchain of choice, the content is automatically released to the consumer with the Consumer ID provided. Price validation occurs via APIs to reputable, regulated exchanges (Gemini, Coinbase, itBit) for MSRP settlement validation.

Transfer of Content Based on Consumer ID
Transfer of content is accomplished through a special transaction type on the TAO blockchain. This transaction is non-reversible. When content is transferred it is no longer available to the original consumer. All rights and licenses transfer with the content, identical to physical media.

Cross-Platform Provisioning Based on Consumer ID
As a Consumer ID is a mathematical construct, it may be used in several devices or platforms at once, providing the consumer access to their content in a virtually unlimited number of ways.

Provisioning Metadata
Metadata provisioned to the TAO ecosystem remains in the control of the creator or publisher. Auditing agencies such as ASCAP and BMI can be granted special "update" status to maintain proper industry standards, however the data from the VAR signature chain to be included in the metadata is purely in the control of the publishing entity.

References

[i] Bryce Weiner, Virtual Audio Record – A New Phonorecord Format, January 30, 2016

[ii] US Copyright Office, Copyright and the Music Marketplace (accessed 2016-01-30) http://copyright.gov/policy/musiclicensingstudy/copyright-and-the-music-marketplace.pdf

[iii] Bryce Weiner, An approach to depersonalized identity, decentralized personal data sharing, and password management with integrated cryptocurrency wallets utilizing hierarchical deterministic trees and elliptic curve cryptosystems (accessed 2016-01-30) https://github.com/bryceweiner/White-papers/blob/master/Whitepaper%20%232.pdf