A Tale on Decentralizing an App: the Case of Copyright Management

A. Vitaletti and M. Zecchini
The purpose of Blockchains

Nothing

All
The purpose of Blockchains in Copyright Management

Allow right holders to autonomously and transparently delegate a CMO
The Role of Collective Management Organization (CMO)

- Creators/Right Owners
- CMO
- Right Users (e.g. who listen the music)

Rights: €
License: €
From a Centralised to a Decentralised Approach

Creators/Right Owners → Rights → CMO
The Interested Party Information (IPI)

<table>
<thead>
<tr>
<th>Heading</th>
<th>Short description</th>
<th>Cardinality</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>base_no</code></td>
<td>Interested Party (IP) base number, unique identifier of a right holder</td>
<td></td>
<td>I-001068130-6 identifying the rights holder</td>
</tr>
<tr>
<td><code>name_no</code></td>
<td>IP name number, additional identifier of a rights holder</td>
<td></td>
<td>00334284961 identifying a pseudonym of the rights holder</td>
</tr>
<tr>
<td><code>name</code></td>
<td>IP name</td>
<td></td>
<td>Rossi Mario</td>
</tr>
<tr>
<td><code>cmo</code></td>
<td>Collecting Society</td>
<td>~200</td>
<td>SIAE, SUISA</td>
</tr>
<tr>
<td><code>cc</code></td>
<td>Creation class</td>
<td>16</td>
<td>Musical Work, Dramatic work</td>
</tr>
<tr>
<td><code>ro</code></td>
<td>Role</td>
<td>34</td>
<td>Musical creator, Book publisher</td>
</tr>
<tr>
<td><code>ri</code></td>
<td>Right</td>
<td>26</td>
<td>Performing right, Re-transmission right,</td>
</tr>
<tr>
<td><code>valid_from</code></td>
<td>The date from which the right management is given to the collecting society</td>
<td></td>
<td>01.01.2017</td>
</tr>
<tr>
<td><code>valid_to</code></td>
<td>The date until which the right management is given to the collecting society</td>
<td></td>
<td>31.12.2017</td>
</tr>
<tr>
<td><code>share</code></td>
<td>The percentage of right the CMO is in charged to collect</td>
<td></td>
<td>100%, 75%, ...</td>
</tr>
<tr>
<td><code>terr</code></td>
<td>The territory in which the CMO is in charge of the right management</td>
<td>220</td>
<td>Italy, France, Europe, North America, World</td>
</tr>
</tbody>
</table>

Agreement: \( \langle \text{name}_\text{no}, \text{cmo}, \text{cc}, \text{ro}, \text{ri}, \text{share}, \text{terr}, \text{valid}_\text{from}, \text{valid}_\text{to} \rangle \)
On the Identity... assumption

The identity of the right holder (i.e. name_no) is centralised and handled by the CMO.
Why

- Scalable
- Cost Effective

What is the best we can achieve with platform(s)?

The solution has been developed with ASA (Algorand Standard Assets)

Stateful smart contracts, have been announced and released in the final stage of the project and open new possibilities.
Token generation is centralised: CMOs verifies off-chain that ASAs are well-formed (no duplicates) and, ultimately, issues the new ASA representing the artistic right.
Dispute resolution

First in chain wins!
MAR 24, 2021

SIAE, Italy’s largest collective management organisation, represents authors' rights as digital assets managed on the Algorand blockchain

By: Società Italiana degliAutori ed Editori (SIAE)

*SIAE launches more than 4 million NFTs on Algorand for 95,000+ creators*

Rome, 24th March 2021- Società Italiana degli Autori ed Editori (SIAE), the Italian major copyright collecting agency founded in 1882, and Algorand, a leading blockchain platform accelerating the convergence of decentralized and traditional finance, announce the first major milestone of a project to create a blockchain-based open platform that allows transparent and efficient management of authors' rights.
Optimistic Solution

Token generation is decentralised
By Design: basic

- $A = <cc, ro, ri, terr>$
- constraints: local storage can host 16 local variables, each 128 bytes long and structured as key/value

$16 \times 128 \times 8$

vs

$16 \times 34 \times 26 \times 200$
By Design: Advanced

in-chain

```
{sc}

LocalStorage RH_{pk}
```

\[
\begin{align*}
\text{key}_1 : & \text{root}_1, \text{root}_2, \text{root}_3 \\
\text{key}_2 : & \text{root}_4, \text{root}_5, \text{root}_6
\end{align*}
\]

\[
\text{root}_1 \quad \rightarrow \quad \text{H}_{11121321} \quad \text{H}_{2223313233}
\]

\[
\text{H}_{1112} \quad \rightarrow \quad \text{H}_{1321}
\]

\[
\text{H}_{13} \quad \rightarrow \quad \text{H}_{21} \quad \Rightarrow \quad \text{A}_{21}
\]

off-chain

```
{Matrix}
```

\[
\begin{align*}
\text{A}_{11} & \quad \text{A}_{12} & \quad \text{A}_{13} \\
\text{A}_{21} & \quad \text{A}_{22} & \quad \text{A}_{23} \\
\text{A}_{31} & \quad \text{A}_{32} & \quad \text{A}_{33}
\end{align*}
\]
<table>
<thead>
<tr>
<th>Reference Solution</th>
<th>Optimistic Solution</th>
<th>BitMatrix Solution</th>
<th>MerkleTree Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ easy to implement</td>
<td>+ easy to implement</td>
<td>+ easy to implement</td>
<td>- moderate to implement</td>
</tr>
<tr>
<td>- no on-chain lookup to the state of the system (single transaction)</td>
<td>+ efficient on-chain lookup to the state of the system (single transaction)</td>
<td>+ efficient on-chain lookup to the state of the system (constant number of transactions)</td>
<td></td>
</tr>
<tr>
<td>- no double-spending prevention by design</td>
<td>+ double-spending prevention by design</td>
<td>+ double-spending prevention by design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- limited storage space (~16k elements)</td>
<td>+ larger storage space (~1.5M elements)</td>
<td>- Not unbounded storage space</td>
</tr>
</tbody>
</table>
Are there other competitive platforms in terms of costs/latency allowing to verify snarks in smart contracts?