NFT Formalised

Martha N. Kamkuemah

Stellenbosch University (SUN), and the
African Institute for Mathematical Sciences (AIMS) SA

Image source:

BAYC NFT collection. As of yesterday, “9,998 NFTs minted, 5,533 unique owners, with total market cap of $573,762,741”.

What are the functional and epistemic properties of ownership?

Ownership

- Set *Agent* of owners and potential owners; set *Asset* of assets; a temporal subset $Asset_{\exists}$ of assets currently in existence; and time $\mathbb{T}$.

Ownership

- Set *Agent* of owners and potential owners; set *Asset* of assets; a temporal subset $Asset_{\exists}$ of assets currently in existence; and time $\mathbb{T}$.

Definition

The Boolean-valued function

$$Owns : Agent \times Asset \times \mathbb{T} \rightarrow \mathbb{B}$$

is interpreted: $Owns(a, \alpha, t)$ holds iff agent a owns asset α at time t.

Ownership

- Set *Agent* of owners and potential owners; set *Asset* of assets; a temporal subset $Asset_{\exists}$ of assets currently in existence; and time $\mathbb{T}$.

Definition

The Boolean-valued function

$$Owns : Agent \times Asset \times \mathbb{T} \rightarrow \mathbb{B}$$

is interpreted: $Owns(a, \alpha, t)$ holds iff agent a owns asset α at time t.

- Time variable of *Owns* implicit; use temporal operator $\Box$ (for 'now and in future') to express temporal invariants.

Ownership Properties

1. Each existing asset has an owner at any time:

$$\Box\,(\forall\,\alpha : \mathit{Asset}_{\exists}\ \cdot\ \exists\, a : \mathit{Agent}\ \cdot\ \mathit{Owns}(a, \alpha))\ . \tag{1}$$

Ownership Properties

1. Each existing asset has an owner at any time:

$$\Box(\forall\, \alpha : \mathit{Asset}_{\exists} \;\cdot\; \exists\, a : \mathit{Agent} \;\cdot\; \mathit{Owns}(a, \alpha))\,. \tag{1}$$

2. At any time, each existing asset has at most one (hence exactly one) owner:

$$\Box(\forall\, \alpha : \mathit{Asset}_{\exists} \;\cdot\; \forall\, a, a' : \mathit{Agent} \;\cdot\; \left(\begin{array}{l} \mathit{Owns}(a, \alpha) \wedge \\ \mathit{Owns}(a', \alpha) \end{array}\right) \Rightarrow\; a = a')\,. \tag{2}$$

An agent may own many assets, or none.

Ownership Properties

1. Each existing asset has an owner at any time:

$$\Box\,(\forall\,\alpha : \mathit{Asset}_{\exists}\ \cdot\ \exists\, a : \mathit{Agent}\ \cdot\ \mathit{Owns}(a, \alpha))\,. \tag{1}$$

2. At any time, each existing asset has at most one (hence exactly one) owner:

$$\Box\,(\forall\,\alpha : \mathit{Asset}_{\exists}\ \cdot\ \forall\, a, a' : \mathit{Agent}\ \cdot\ \left(\begin{array}{l}\mathit{Owns}(a, \alpha)\ \wedge\\ \mathit{Owns}(a', \alpha)\end{array}\right) \Rightarrow\ a = a')\,. \tag{2}$$

   An agent may own many assets, or none.

3. A non-existing asset does not have an owner, since until it comes into existence it is not assumed to have an identity:

$$\Box\,(\forall\,\alpha : \mathit{Asset} \setminus \mathit{Asset}_{\exists}\ \cdot\ \neg\,\exists\, a : \mathit{Agent}\ \cdot\ \mathit{Owns}(a, \alpha)) \tag{3}$$

Epistemic Logic

- Ownership is ‘publicly certified’, i.e.,

Epistemic Logic

- Ownership is ‘publicly certified’, i.e.,
  - Certified, all are aware of ownership, and

Epistemic Logic

- Ownership is 'publicly certified', i.e.,
  - Certified, all are aware of ownership, and
  - Publicly certified, all are aware that others are aware of what is certified.

Epistemic Logic

- Ownership is 'publicly certified', i.e.,
  - Certified, all are aware of ownership, and
  - Publicly certified, all are aware that others are aware of what is certified.

- $K_i\ \alpha$ reads "agent i knows predicate α ."

Epistemic Logic

- Ownership is 'publicly certified', i.e.,
  - Certified, all are aware of ownership, and
  - Publicly certified, all are aware that others are aware of what is certified.

- $K_i\ \alpha$ reads "agent i knows predicate α ."

- Only truths can be known: if $\vdash K_i\ \alpha$ then $\vdash \alpha$.

Epistemic Logic

- Ownership is 'publicly certified', i.e.,
  - Certified, all are aware of ownership, and
  - Publicly certified, all are aware that others are aware of what is certified.
- $K_i\ \alpha$ reads "agent i knows predicate α ."
- Only truths can be known: if $\vdash K_i\ \alpha$ then $\vdash \alpha$.
- Semantics: Kripke possible worlds.

NFT Specified

Definition

(Public certifiability) Fact ϕ is *publicly certified* amongst a set A of agents:

$$PC(A, \phi) \quad := \quad \forall\, x, y : A \cdot K_x K_y\, \phi\,.$$

Token function τ

$$\tau : \{(a, \alpha, t) : Agent \times Asset \times \mathbb{T} \mid Owns(a, \alpha, t)\} \rightarrowtail \mathbb{B}^*$$

to bitstrings.

NFT Specified

Definition

(Specification $\mathcal{N}$) A non-fungible token, or NFT, is a publicly certified statement that agent *a* owns asset α at time *t*:

$$PC(Agent, \tau(Owns(a, \alpha, t))),$$

where the *Owns* relation satisfies (1) to (3). That is referred to as property $\mathcal{N}$.

Thank You!

NFT formalised