

# **NFTs for Identity, Naming, Reputation**

Concept research & how they can fit into  
LNP/BP, RGB & Internet2

Dr Maxim Orlovsky

LNP/BP Standards Association,  
CEO Pandora Core AG

# Design goals: #AICUUT

- Antifragile
- Individualistic
- Confidential
- Uncensorable
- Unconfiscatable
- Trustless

**Identity (RGB22)**

# Identity must be

- Unique (globally or under well-defined scope)
- Verifiable by multiple parties  
(confidential identity is not an identity until revealed)
- Not transferrable

# Identity-related roles

- Identity holder:  
subject or object assigned identity
- Identity owner:  
subject created identity and having the right to revoke it

# Identity

**Globally unique verifiable by multiple parties untransferable**

property assigned by some subject (identity owner) to itself or another object or subject (identity holder)

- Identities must be *revocable or replaceable* by the owner
- Owner must have a way of *proving identity ownership* without executing revocation procedure

# Designing identities

- Theorem: to be **decentralizingly-assigned** identities must be **made of entropy**
  - Consequence: decentralized identities are meaningless for humans
- Theorem: to have an **ownership provability** under trustless conditions, identities must commit (**timestamp**) to decentralized ledger
- Theorem: to have a **decentralized revocation, single-use-seal** mechanism is required
- Theorem: to be **untransferable, client-side-validation** is required
- **Conclusion:**  
**Bitcoin + RGB** matches requirements for decentralized #AICUUT identity system

# Identity system: RGB22

- Asymmetric key pair is an identity: globally unique entropy
- This information is a part of RGB identity genesis
- Genesis may also contain arbitrary supplementary data in custom (existing) formats
  - No need to invent new standard for holding identity data
  - But there is a need to enumerate supported standards
- RGB contract should have “revoke” and “replace” procedures



# Confidentiality & identity

- Hierarchical identity derivation: ability to hold multiple identities which can't be publicly linked - but the link can be disclosed by the identity owner if he likes to
- Derivation of new identities is called "identity extension"

**Decentralized naming system (RGB24)**

# Name

Globally unique **meaningful** identity needed by humans according to their protocols (ability to pronounce, visually check and think of)

- Names can be transferred
- Names can't be confidential
- By using homestead principle, timestamps & PoW names can be made #AIT (individual, trustless and assigned in decentralized way)
- By using ledger, names can be made #UU (uncensorable/unconfiscatable)

# Decentralized name resolution

- By global P2P network
- Maintaining DHT table
- And RGB state disclosures

... which is Lightning network operating LNP and RGB (Bifrost)  
(outside of the scope of LN state channels)

# Name system & decentralized name resolution

- It must be timestamped to a single bitcoin UTX0 in a unique way (homesteading + spam prevention). This becomes name genesis.
- Genesis must be published to LN/Bifrost network
- Each party interested in using name keeps track of network announcement for historical reasons
- Name-to-other-id resolution happens with special state extensions signed by the current name owner, which auto invalidates on name transfer. This information is also published to LN/Bifrost network
- Ownership is proven by RGB consignments + signature using the bitcoin key controlling UTX0 assigned ownership right

**Reputation**

# Attribution. Reputation.

- Reputation is a set of attributions (provable claims)
- Attribution is a link between two identities or name and identity
- Name resolution: process of revealing identity link to a certain name
- Attribution can be trustless if identities are anonymous
- Attribution can be final & uncensorable if it is *timestamped*
- Attribution may be confidential if it is made with *client-side-validation*
- Thus, attribution and reputation needs RGB

# Attribution in RGB22 identities 1

- We need to have “provably derived identities” where they are linked in client-validated-part, but not on a blockchain
- Genesis identity will be never disclosed and must result in a tree of identities, each of which may be disclosed individually
- With each level tree branches down to leaves must have a higher probability for the need of identity link
- The tree can be made of public state extension, not requiring bitcoin transactions, committed only when there is a need of establishing the link



## **Attribution in RGB22 identities 2**

- External signatures/attribution/names must be attachable to each individual identity (branch or leaf of the identity tree)
- This should be doable with state extensions, which may be committed upon the need of proving the fact

# **Summary on identities, names & reputation**

# With such system

- Identity is a public key from RGB22 identity creation, revocation or replacement state transition
- Proof of identity ownership is a signature with corresponding private key
- Revocation or replacement of the identity is a state transition
- Claims are proven by RGB declarations (parts of state history)
  - linking identity with "claim" state extensions
  - linking identity state extensions
- Set of claims (for court/arbitration) is an RGB consignment
- Reputation is a disclosure consisting linking multiple RGB contracts & identities

# RGB22: Identity & reputation

## Assigned state

- Revocation/replacement right with current public key and self-signature in DER format
- Commitment right

## Meta

- Identity metadata in some standard format
- Claim statement
- Notarising signatures

## Transitions

- Genesis creating (multiple) ids
- Revoke / replace (multiple) ids
- Committing previous state extensions

## Extensions

- Creation of more identities
- Claim attributing certain fact

# RGB24: Decentralized names

## Assigned state

- Ownership right
- Commitment right

## Meta

- Name
- Naming metadata

## Transitions

- Genesis creating single name
- Transfer of ownership
- Committing previous state extensions

## Extensions

- Name resolution to identities

