Art of Proof - A Protocol for Autonomous Bitcoin-Native Artwork

Abstract

We propose a system for digital artwork ownership using Nostr keypairs and the Bitcoin Lightning Network. Each artwork is bound to a private/public keypair (`nsec` / `npub`) and stored in a Vault. The `npub` acts as the artwork's public identity, enabling direct Lightning payments. When purchased, the artwork is removed from the Vault, and the buyer receives both the physical artwork and the `nsec` . Ownership is final, as the Vault destroys the artwork's digital presence upon sale.

---

1. Introduction

Digital art lacks scarcity because files can be copied infinitely. Attempts to solve this through centralized registries or NFTs introduce trust in third parties. We propose a system where each artwork is uniquely bound to a cryptographic identity, autonomously capable of receiving payments, and permanently transferable through key ownership.

---

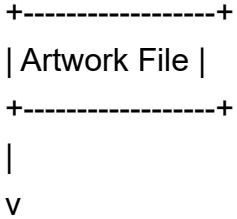
2. Artwork Identity

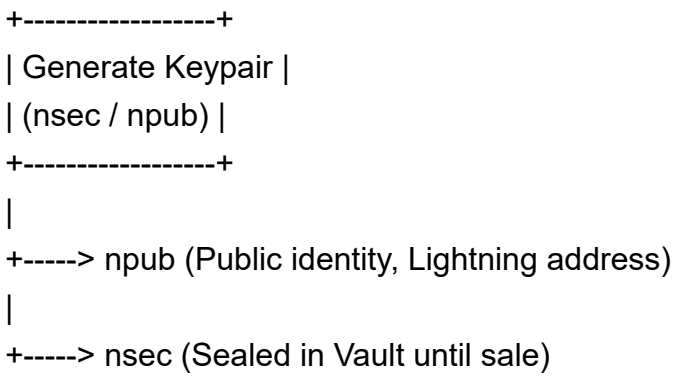
Each artwork is generated with a Nostr keypair:

- The public key (`npub`) serves as its public identity.
- The private key (`nsec`) is stored in the Vault until sale.

The `npub` is mapped to a Lightning address, making the artwork capable of receiving Bitcoin payments directly.

Diagram 1: Artwork Identity





---

3. The Vault

The Vault is an open-source repository where artworks are stored until purchase. It has three functions:

1. Store artworks and their associated `npub`.
2. Seal the `nsec` until ownership transfer.
3. Destroy the artwork's digital presence upon sale.

Destruction ensures uniqueness and prevents duplication.

Diagram 2: Vault Lifecycle

Store Artwork Store npub

- Image/Media + Lightning Address
- Metadata + Public Key
- nsec (sealed)

---

4. Purchase and Transfer

When a buyer purchases an artwork:

1. Payment is made in Bitcoin.

2. The physical artwork and its `nsec` are delivered to the buyer.
3. The Vault deletes the artwork's record, preventing future replication.

Diagram 3: Purchase & Transfer

Buyer ----(BTC Payment)---> Vault
|
v
+------------------+
| Deliver nsec + |
| Physical Artwork |
+------------------+
|
v
Buyer owns Artwork
|
v
Vault destroys digital record

---

5. Autonomy of Artworks

Each artwork can be interacted with directly on the network via its `npub`. Users may:

- Send Lightning payments ("zaps") to support the artwork.
- Discover its existence through Nostr events.

Diagram 4: Autonomous Artwork

```
User ----Zap (BTC)---> npub (Artwork Identity)
```

|
Artwork responds via
Nostr / Lightning presence

Artworks thus function as autonomous agents, alive on the network while under Vault custody and sovereign once transferred.

---

6. Open Source and Forkability

The system is fully open-source. Anyone may fork the Vault, host artworks, or build alternate galleries. Provenance is enforced not by a central authority but by control of the `nsec`.

---

7. Conclusion

We have proposed a protocol that enforces digital scarcity for art without intermediaries. By binding each artwork to a Nostr keypair and enabling direct Bitcoin payments, ownership becomes absolute and final upon transfer of the `nsec`. The Vault enforces uniqueness through destruction, while open-source distribution ensures resilience and extensibility.