TECHNICAL SHEET

The "Crypto Art Gallery" works of art are immersive, interactive and audiovisual digital works.

They are sold in physical form AND as NFT, thus authenticated in the blockchain as unique.

For now, the NFT "Crypto Art Gallery" are only visible on Oculus Rift and HTC Vive headsets and headsets accepted by the STEAM platform. This does not include standalone headsets such as Oculus Quest and others.

1 - SALE

The works " Crypto Art Gallery " are software applications (.exe). They are available in VR and screen broadcast only for PC, provided in case of sale (without screen).

2 - LENDING

The digital works Crypto Art Gallery are .exe applications (running under Windows 10)

They can only be diffused on a computer equipped for VR and powerful, and in screen diffusion. For the protection of pirate copy, we have established a protocol for the delivery of our works on third party computers, used by the organizers of exhibitions and festivals.

The loan of our works is subject to a contract that commits the organizer to be responsible and vigilant on the material and software management before, during and after the use of the Arts Digitales works. The organizer must accept the security protocol set up by the artist who configures each work to be broadcast on a specific computer park provided by the organizer.

Minimum hardware configuration in case of loan:

- PC computer running Windows 10

- RAM memory 16 GB or more

- GTX 1070 graphics card or higher

- Intel i7 7700 K processor or higher

- SSD hard drive with SATA connection (no external USB drive, no mechanical drive)

- Ethernet connection

Protocol for installation/protection of works

- The installation of the digital works and tests, thus programmed, will be done locally by the organizer. We ask the organizer to have the procedure provided in the technical sheet followed by a competent computer technician and administrator of the computers dedicated to the exhibition.

Detailed procedure for the recovery of the non-sensitive data of the processor serial number of each computer dedicated to the exhibition with the application ScanDigitArt, developed by The company HoloVR Prod.

Introduction:

This procedure allows to recover the serial number of the processor which will appear in a text file that the organizer will be able to check and consult at will, in order to judge its non-sensitivity as data, before sending it to us by the means that he judged good, fast and secure. The ScanDigitArt application is guaranteed virus-free by the company HoloVR Prod.

Step 1:

The HoloVR Prod company sends to the organizer, a password so that it downloads the ScanDigitArt application on the site of the HoloVR Prod company on the following link XXXXXXX.com (to come)

Step 2:

The organizer must launch the ScanDigitArt application on each computer one by one from the same USB key.

Step 3:

After the end of the procedure contained in step 2, the USB key contains the serial numbers of the processors of the computers dedicated to the exhibition in the folder "Expo", and file "Numproc.txt", which must be sent by the organizer to Mr. Bernasconi Gérard director of the company HoloVR Prod, in .zip format by the means he deemed good, fast and secure.

Step 4 :

The company HoloVR Prod sends back within 72 hours to the organizer responsible and signatory of this contract, the digital works of art in the form of one or more applications .exe, programmed to operate only on the computers listed.

Step 5:

The organizer may copy the Digital Arts received in Step 4 to the computers selected by the organizer in Step 2. The Digital Arts works will be active from the date decided between the parties until the end date of the exhibition.

Step 6:

The day after the last day of the exhibition, the organizer undertakes to delete the files of the Digital Arts works in the form of one or more .exe applications on each computer used during the exhibition.

USB PORT DISABLING PROCEDURE

Procedure for locking USB storage ports, removable hard drives and USB keys. To prevent unauthorized copies of our digital works, here are some security measures that should be implemented on every computer.

The first is to disable writing to USB devices. To do this, you should follow these instructions:

1.   Press [Windows]+[R]

2.   Type **gpedit.msc** in Run and press **[Enter].**

3.   The **"Local Group Policy Editor"** window appears:

4.   Click on **Administrative Templates**

5.   Double click on **System**

6.   Double click on **Removable Storage Access**

7.   Double click Removable Disks: **Deny Write Access**

8.   Select the Enabled button and click **Apply** and **OK**.

The second is to disable the automatic mounting of new disks that have never been used before. To do this, you must:

1.   Open a command prompt ([Windows]+[R] and type "**cmd**", then **[enter])**

2.   Type the command **diskpart**, then press [enter].

3.   In diskpart, type **automount**, then press [enter].

5.   If automount is disabled, there is nothing to do.

6.   If automount is enabled, run the **automount disable** command (still in diskpart).

The last point is to disable the USB drives completely:

1.   Open a command prompt ([Windows]+[R] and type "**regedit**", then [enter]), then "**Allow**" **YES**

2.   In the "**Registry Editor**" window, follow the path of the following tree

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR

In the left window, click on the **USBSTOR** folder, and in the right window double-click on **"Start".**

3.   In the "Modify 32-bit DWORD value" window, change the **value to 4**.

REACTIVATION OF USB PORTS

After the exposure, you can reactivate everything that has been deactivated by performing the same steps, only replacing all instances of enabled with disabled.

The first step is to re-enable writing to the USB devices. To do this, you need to follow these instructions:

1.   Press [Windows]+[R]

2.   Type **gpedit.msc** in Run and press **[Enter].**

3.   The "**Local Group Policy Editor**" window appears:

4.   Click on **Administrative Templates**

5.   Double click on **System**

6.   Double click on **Removable Storage Access**

7.   Double click Removable Disks: **Deny Write Access**

8.   Select the Disabled button and click **Apply** and **OK**.

The second is to re-enable automatic mounting of new drives. To do this, you must:

1.   Open a command prompt ([Windows]+[R] and type "cmd", then [enter])

2.   Type the command **diskpart**, then press **[enter].**

3.   In diskpart, type **automount**, then press **[enter]**.

5.   If automount is enabled, there is nothing to do.

6.   If automount is disabled, run the **automount enable** command (still in diskpart).

The last one is to completely reactivate the USB drives:

1.   Open a command prompt ([Windows]+[R] and type "**regedit**", then [enter]), then "**Allow**" **YES**

2.   In the "**Registry Editor**" window, follow the path of the following tree

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR

In the left window, click on the **USBSTOR** folder, and in the right window double-click on **"Start".**

3.   In the window "Modify the 32-bit DWORD value" change the **value to 3.**

4 - Questions for the organizer

Important: We ask that you provide us with the following list answering point by point the following questions (we can also do a video conference for this):

1) What is the number of computers you will deploy. One is needed per digital work. It is possible, at your request, to create an interface to have all our collection or certain works on one station and choose them in a "virtual gallery".

2) Are the computers and VR headsets the property of the organizer? Are they rented? Are they lent by third parties (including personal computers and headsets)?

3) How many VR headsets are connected to the PC? (we do not port to Oculus Quest or other standalone headsets), their names and brands.

4) The organizer must provide us with the data sheet of each computer, at least:

- name and frequency of the processor,

- name and reference of the graphics card,

- quantity of RAM memory,

- free space and quality of the hard disk (SSD or mechanical).

- know if these computers are used for other purposes during the exhibition.

4 - As a reminder:

The works of Art resulting from the concept "Crypto Art Gallery" are immersive digital works offered for sale in the form of NFT.

Our artworks are adapted and conditioned by the digital universe:

- The collector or visitor can immerse himself with a Virtual Reality headset and evolve in the universe created around the sculpture, a large set created by the artist. He can walk, fly, teleport, stay at his human size or grow like a giant.

- Each statue can take 10 poses that are randomly triggered when the visitor moves around the sculpture or every hour in screen projection.

- Each day is synchronized with the place where the work is located and we find the day/night cycle. Each day tints the universe of the work with a different random color.

- The ambient sound and the music are also random and composed by the artist in this objective.

- The collector, the gallery owner and the museum will also be able to display the work of art on a giant screen thanks to a virtual random camera system that rotates around the sculpture and towards the artistic points of interest, and whose infinite movement is never the same. The random data changes its movements constantly in real time.

These works are created in immersion in VR creation software. The first collection was created in Open Brush and Unity open source software (a real-time 3D rendering and programming engine).

The works are each available for sale in 1 copy.

In exhibitions, the works can be duplicated after agreement and contract with the organizer, and available for viewing in a "virtual gallery", i.e. several works visible to only one computer.