藝術品資訊透過區塊鏈驗證真偽

一 . 前言：

許多藝術畫廊和拍賣行依賴於作品的原出處出處來確保藝術品的真實性。Provenance 基本上是交易清單，顯示藝術品如何從一個所有者轉換到另一個所有者，追溯到原始所有者 – 藝術家。畫廊票據，展覽記錄，拍賣記錄，運輸標籤或經銷商郵票通常用於追溯藝術品的來源，並證明一件藝術品是原創作品。遺憾的是，偽造文件十分常見，儘管採取了所有預防措施,假冒的藝術品仍時常作為原作出售。

與 Provenance 非常相似，區塊鍊是一個帳本，是使用密碼學鏈接在一起的列表。 但與 Provenance 不同，由於區塊鍊是分散式技術，因此這種記錄幾乎不可能被竄改。每當在區塊鏈上註冊所有權變更時，大型的去中心化網路」通過解決複雜的數學算法來驗證和記錄交易數據。

二. 項目介紹：

1. 項目簡介:

透過區塊鏈的不可篡改的特性來實現鏈上藝術品資訊紀錄真偽驗證。

2.問題分析:

目前藝術品很難真正防偽，第三方單位存在公正性與公信力問題，藝術品相關資訊有可能會被竄改，或者是資料遺失等問題。

3.結果方案

透過區塊鏈信任轉移，將藝術品的 metadata 存在區塊鏈上，並且透過分散式帳本技術，只要透過這層網路都可以隨時驗證。

三. 技術介紹:

1.Ethereum Network:

Ethereum 是一種像比特幣一樣的加密貨幣，Ethereum 是一個執行智能合約的分散式平臺。這些智能合約執行在 Ethereum 虛擬機器上，這是一個由所有執行 Ethereum nodes 的裝置組成的分散式去中心化網路。

2.Dapp:

智能合約可在每個 Ethereum node 上執行並進行驗證，所以計算結果被認為是可信任的。以太坊還開發出了 web3.js 讓開發者可以使用網頁技術撰寫智能合約的操作介面。這樣的網頁操作介面又稱為分散式應用程式(DAPP)。要使用 DAPP，必須在支援 DAPP 的瀏覽器中才能使用(如 Mist 或 Parity)。

四. 技術實現：

1.Trust Server:

私鑰簽名處理，將資料寫到區塊鏈上，並且透過公鑰來驗證寫上去的人的唯一性

運作細節如下：
利用 transaction 的方式把要儲存到 Ethereum 的 Data 上鏈，並存在特定的區塊上。

每個 transaction 存在以下的格式：

Nonce: A number that keeps track of the amount of transactions an account has made. The nonce is used to protect users from replay attacks where an attacker attempts to steal from a user by using a single authentic transaction over and over.
GasPrice: The amount a user is willing to pay the miners per unit of computation (for more on gas read this explainer).
GasLimit: The maximum amount of computation you expect the transaction to require.
To: The address of the receiving wallet of contract.
Value: The amount of ETH you are sending. The value is often 0 when interacting with smart contracts.
Data: When interacting with smart contracts, this field is used to send instructions about how the contract should be updated. When sending money to another user's wallet, this field is completely ignored.

一般在簡單的 Ethereum transcation 中常忽略"Data"的欄位，因此我們可以安全地將任意 data 放在該字段中，而不會影響 transaction。
在完成交易後，將會有一段 transaction hash 回傳，記錄於後台資料庫用以配對實際上傳的藝術品編號，可用 web3.js 或 web3.py 來取得 transaction hash 的 raw transaction 轉換成 UTF-8 的格式可還原成可讀資訊或著也可以用 Ethereum 原生瀏覽器 etherescan 來做轉換，例如:

https://ropsten.etherscan.io/tx/0x99e76995ad0ae0e4d42c6373b47ca14474f300de8d2235344ff07c813070b4e0

Input Data:

Raw:

0x7b226964656e746966696361746696f6e223a7b226172745f6964223a3634312c22617269223a2268747470733a2f2f70726f6a6563742e6f72672e74772f6461722f6172742f363431222c226170706c6963616e745f6964223a39302c226170706c6963616e74223a

22e7a9bae7b8bde887bae781a3e795b6e4bba3e69687e58c96e5afa6e9a997e5a0b46
32d6c6162222c22656d61696c223a22736f6d656f6e6540736f6d6577686572652e63
6f6d222c2270686f6e65223a222b38383632313233343536373822 2c22747970655f6
f665f6f626a656374223a22e6b2b9e795ab222c226d6174657269616c73223a22e5a39
3e5858be58a9b222c22746563686e6971756573223a22e6b2b9e795ab222c226d656
1737572656d656e7473223a22e9ab983a20313030636d2c20e5afac3a20313030636d
222c22696e736372697074696f6e735f616e645f6d61726b696e6773223a22222c2264
697374696e6775697368696e675f6665617475726573223a22222c227469746c65223
a22e6978be8bd89e6989fe5bda2e5af86e7a2bce28094e795b6e4bba3e8979de8a193e
98f88e7b590e4baa4e6b581e58d80e5a18ae79a84e583b9e580bce59b9ee69c94e5afa
6e9a997222c227375626a656374223a22e7a59ee8a9b1e5adb8e79fa5e8ad98e696b0
e9a19ee59e8b222c22646174655f6f725f706572696f64223a22e4b889e69c88203230
3139222c226d616b6572223a22e589b5e4bd9ce88085e5908de7a8b1222c226272696
566223a22e69cace4bd9ce59381e782bae8b387e6ba90e8ad98e588a5e7a2bce7b3bb
e7b5b1e4b98be5afa6e9a997e8a888e795abefbc8ce9808fe9818e415249e58fafe4bba
5e5819ae588b0e4bd9ce59381e59ca8e58d80e5a18ae98f88e4b88ae79a84e8b387e69
699e6b0b8e4b985e5ad98e58f96efbc8ce4b99fe58fafe4bba5e8ae93e4b88de5908ce
8a792e889b2e9808fe9818e415249e4be86e5819ae8979de69687e7a094e7a9b6e3808
1e4bd9ce59381e5b195e8a6bde7ad89e5a49ae58583e68789e794a8efbc8ce4b8a6e4b
d9ce782bae5be8ce7ba8ce98a9ce68ea5e8999be693ace8b2a8e5b9a3e4baa4e69893
e7b3bbe7b5b1e4b98be59fbae7a48ee38082222c226174746163686d656e7473223a5b
7b2275726c223a2268747470733a2f2f686f73742e636f6d2f6174746163686d656e747
32f303030312e6169222c2268617368223a22623735313835306231613537313638613
536393363643932346236623039366530386636323138323734343466373064383838
346635643032343064323731326531306531313665393139326166336339316137656
335373634376533393334303537333430623463663430386435613536353932663838
323734656563353366302 27d5d7d2c226f776e657273686970223a7b226f776e65722
23a22e589b5e4bd9ce88085222c22656d61696c223a226f776e657240736f6d657768
6572652e636f6d222c2270686f6e65223a222b38383632313233343536373822 2c22
7072696365223a224e2f41222c226174746163686d656e7473223a5b5d7d7d

UTF–8:

0x{"identification":{"art_id":641,"ari":"https://project.org.tw/dar/art/641","applicant_id":90,"applicant":"空總臺灣當代文化實驗場 c-lab","email":"someone@somewhere.com","phone":"+886212345678","type_of_object":"油畫","materials":"壓克力","techniques":"油畫","measurements":"高: 100cm, 寬: 100cm","inscriptions_and_markings":"","distinguishing_features":"","title":"旋轉星形密碼—當代藝術鏈結交流區塊的價值回朔實驗","subject":"神話學知識新類型","date_or_period":"三月 2019”,"maker":"創作者名稱","brief":"本作品為資源識別碼系統之實驗計畫，透過 ARI 可以做到作品在區塊鏈上的資料永久存取，也可以讓不同角色透過 ARI 來做藝文研究、作品展覽等多元應用，並作為後續銜接虛擬貨幣交易系統之基礎。","attachments":[{"url":"https://host.com/attachments/0001.ai","hash":"b751850b1a57168a5693cd924b6b096e08f621827444f70d884f5d0240d2712e10e116e9192af3c91a7ec57647e3934057340b4cf408d5a56592f8274eec53f0"}]},"ownership":{"owner":"創作者","email":"owner@somewhere.com","phone":"+886212345678","price":"N/A","attachments":[]}}

以上資訊以永久存放在 Ethereum 網路中，並可以用 txhash:0x99e76995ad0ae0e4d42c6373b47ca14474f300de8d2235344ff07c813070b4e0
得到我們當初寫入之藝術品的相關資訊。