Analogous Analogues:
Digital Twins & Hardware Tracking in GLAM Collections

Dian Ross, PhD Candidate

Dr. Edmond Cretu
Electrical and Computer Engineering
Dr. Victoria Lemieux, School of Information, Blockchain@UBC Cluster Lead
University of British Columbia, CANADA

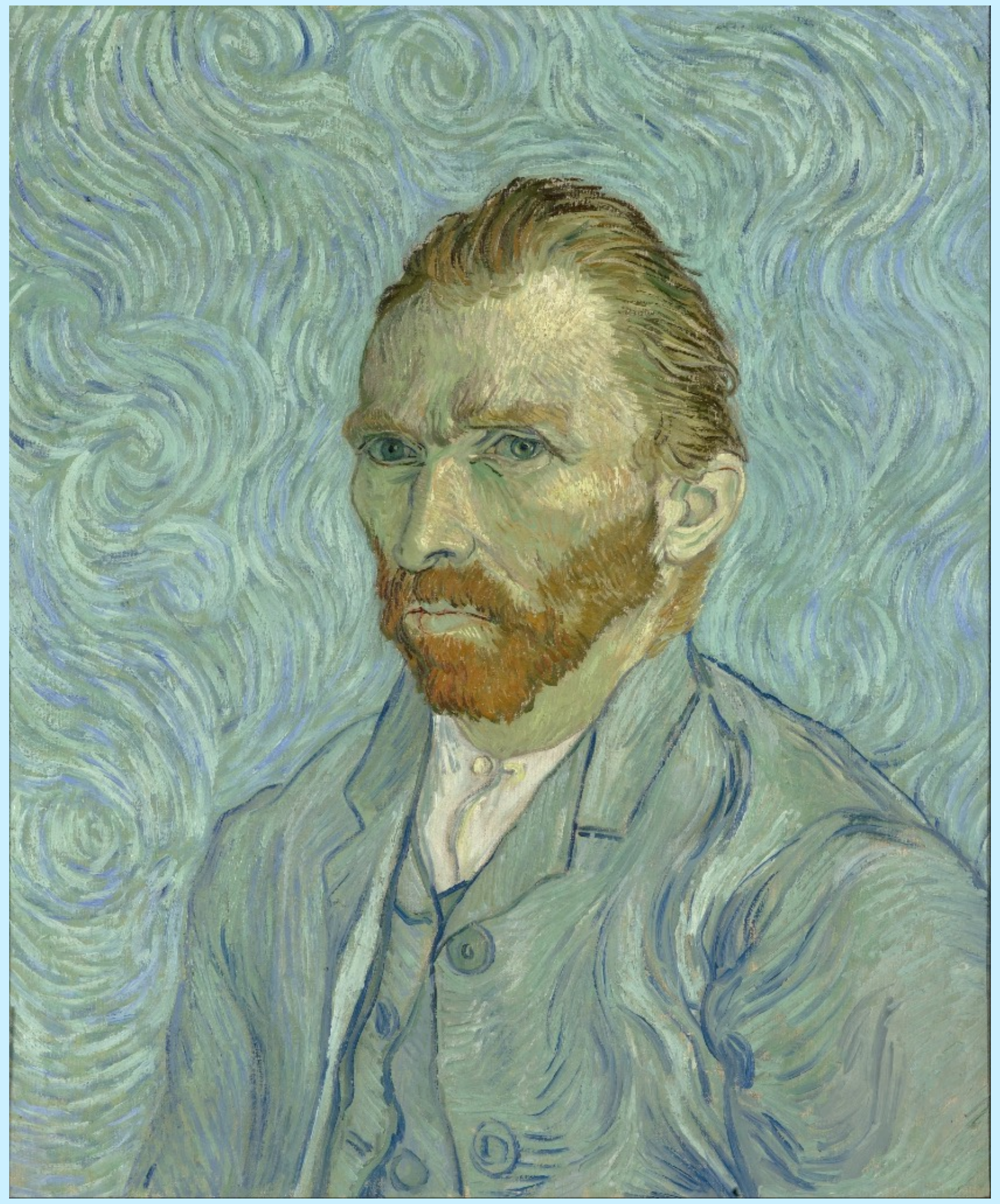
IEEE Big Data
6th Computational Archival Science Workshop

December 17th, 2023

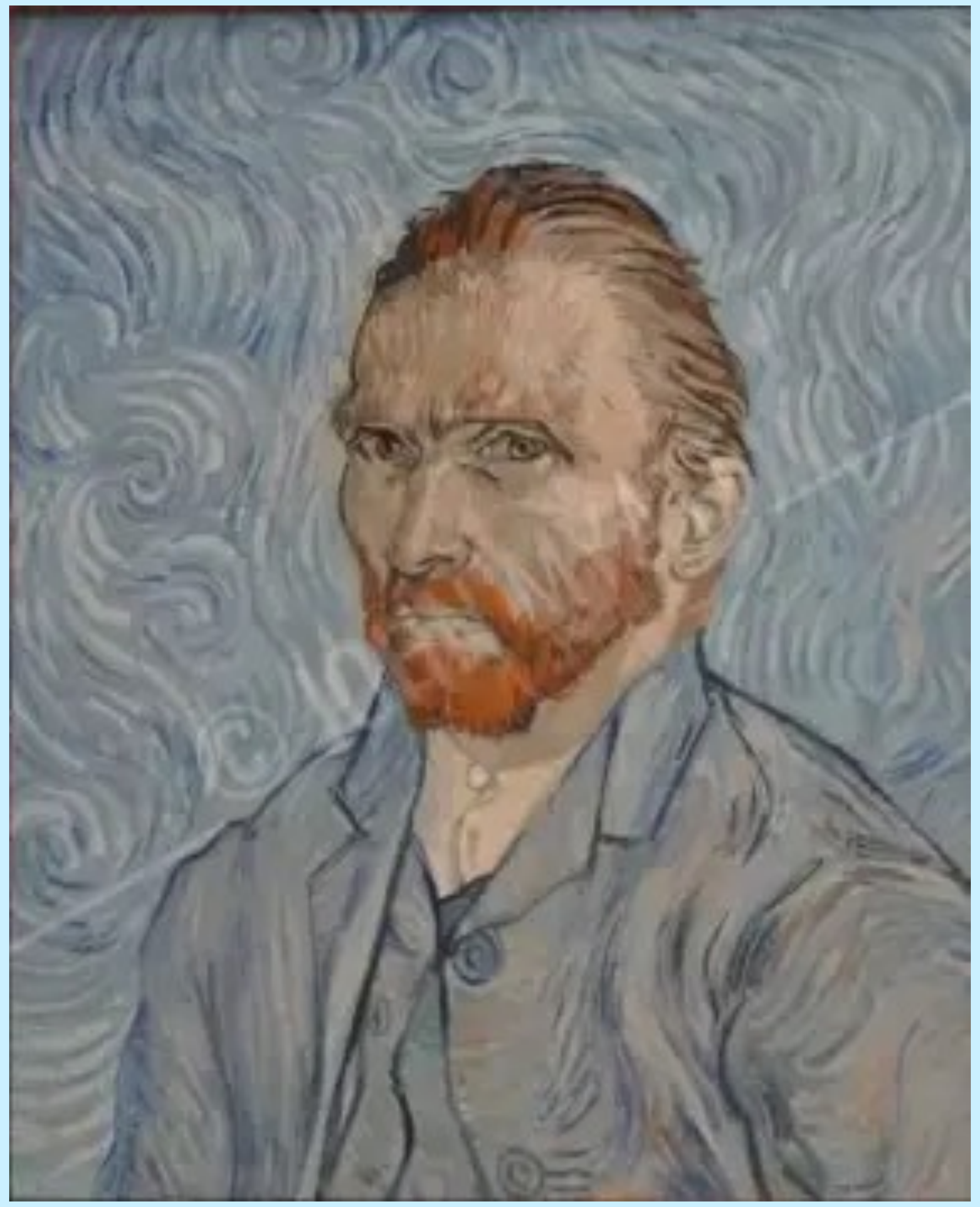
Blockchain
@UBC

Problem: Provenance Tracking

- Throughout history always been fakes and misattributions
- Rise of art as a commodity in the 1980's, more lucrative
  - Increases of 500-1000%
  - Industry notoriously opaque
- Attribution usually web of records
  - Often paper records, stored in disparate places
  - Include:
    - Exhibitions, sales, expert opinions
    - Scientific tests (x-ray, spectroscopy, carbon dating, etc)
- Broken chain due to Nazi seizures still being redressed today
- Minimal or informal records of sale (honour system)
- Often more straightforward to fake records to mediocre fake paintings
  - John Drewe who infiltrated V&A, Tate, and ICA archives to plant records of John Myatt's fakes
- Up to 20% of artwork in galleries, museums no longer attributed to same artist 100 years later
- 52,000 stolen artworks listed by Interpol

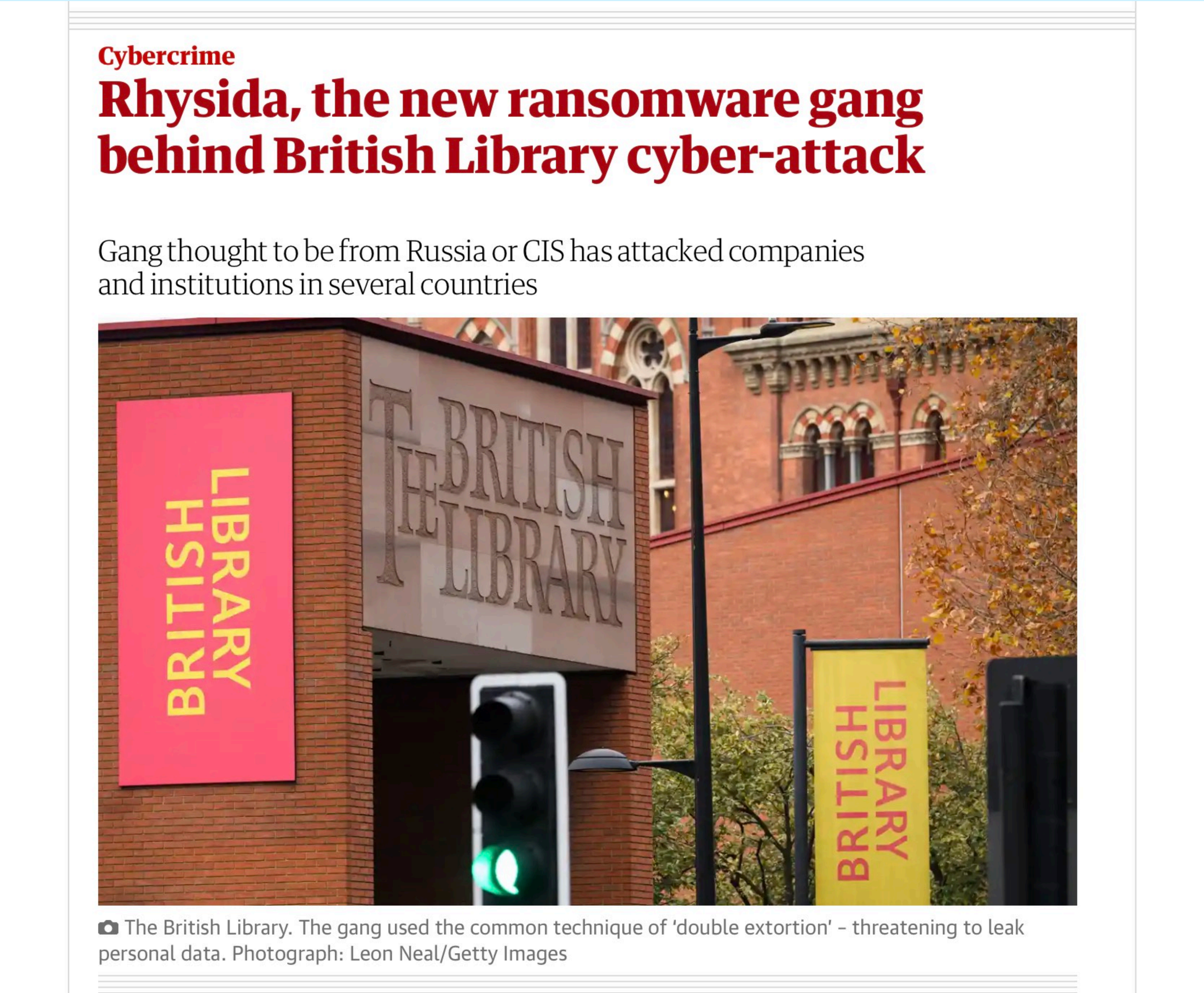


Van Gogh Self Portrait
(1889), Musée d'Orsay



'Genuine Fake' (2021)
John Myatt
(list: $35k USD)

Attacks on GLAMs

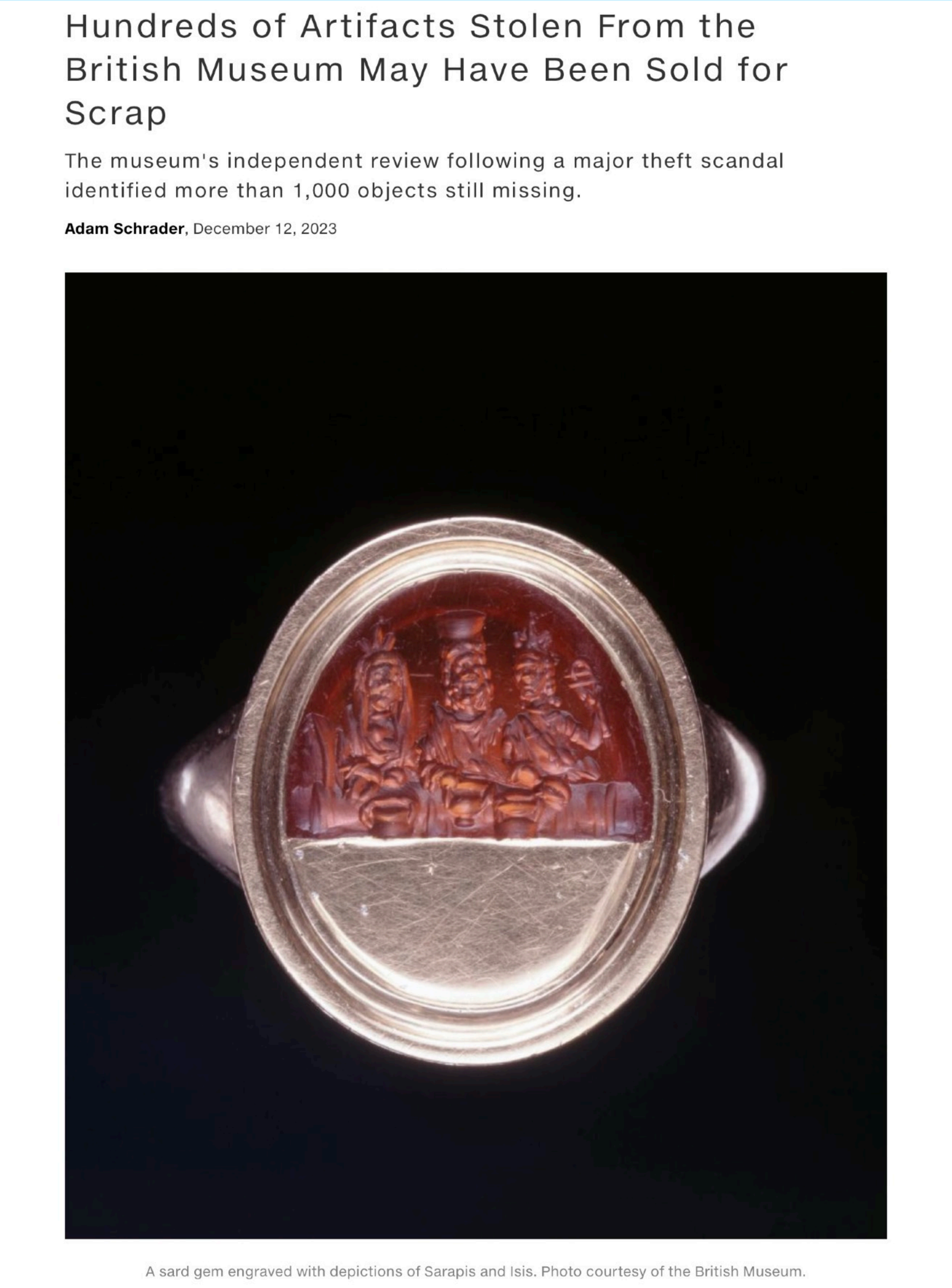


Cybercrime

Rhysida, the new ransomware gang behind British Library cyber-attack

Gang thought to be from Russia or CIS has attacked companies and institutions in several countries

The British Library. The gang used the common technique of 'double extortion' – threatening to leak personal data. Photograph: Leon Neal/Getty Images



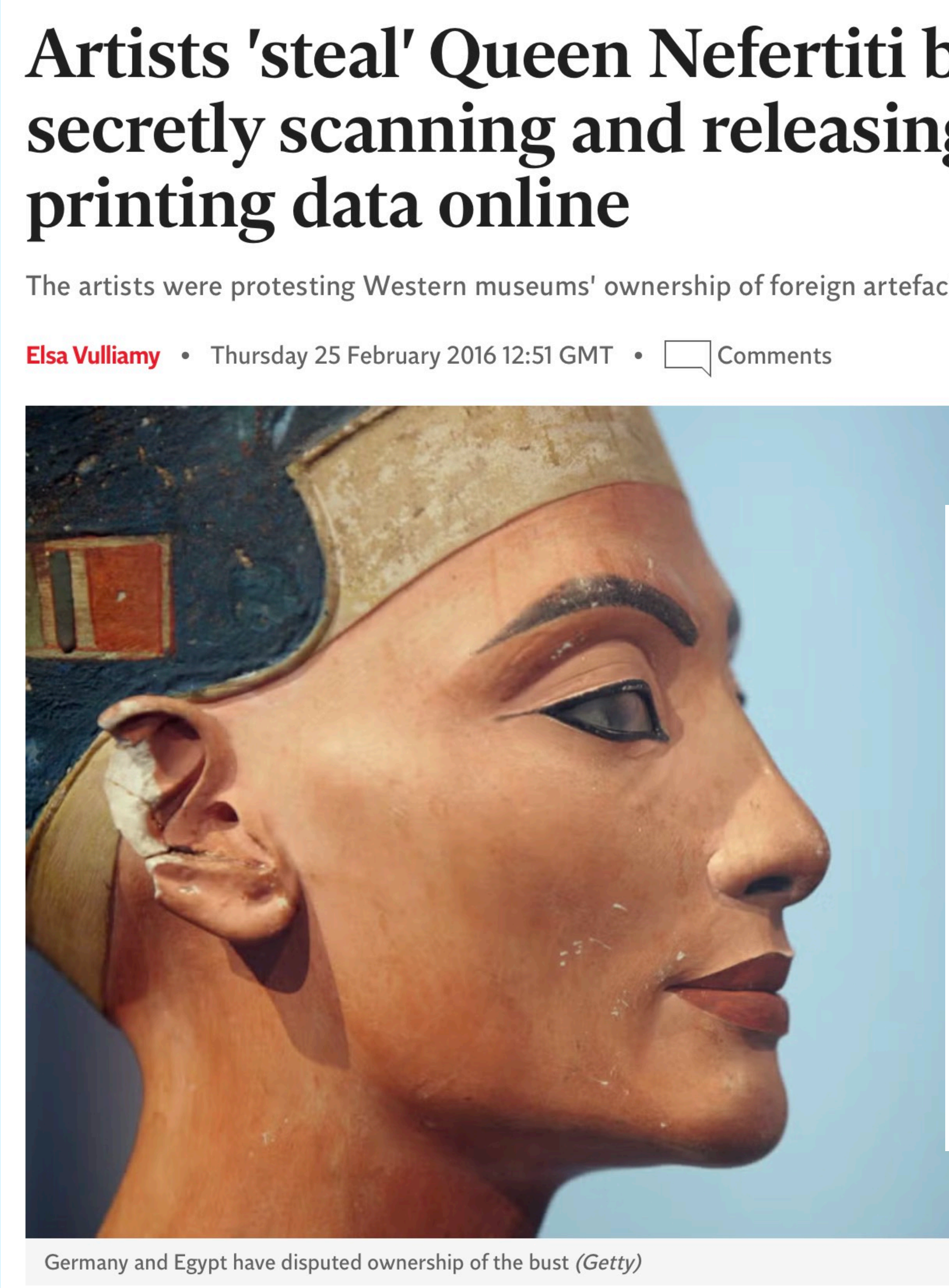
Hundreds of Artifacts Stolen From the British Museum May Have Been Sold for Scrap

The museum's independent review following a major theft scandal identified more than 1,000 objects still missing.

Adam Schrader, December 12, 2023

A sard gem engraved with depictions of Sarapis and Isis. Photo courtesy of the British Museum.

Calls for Repatriation

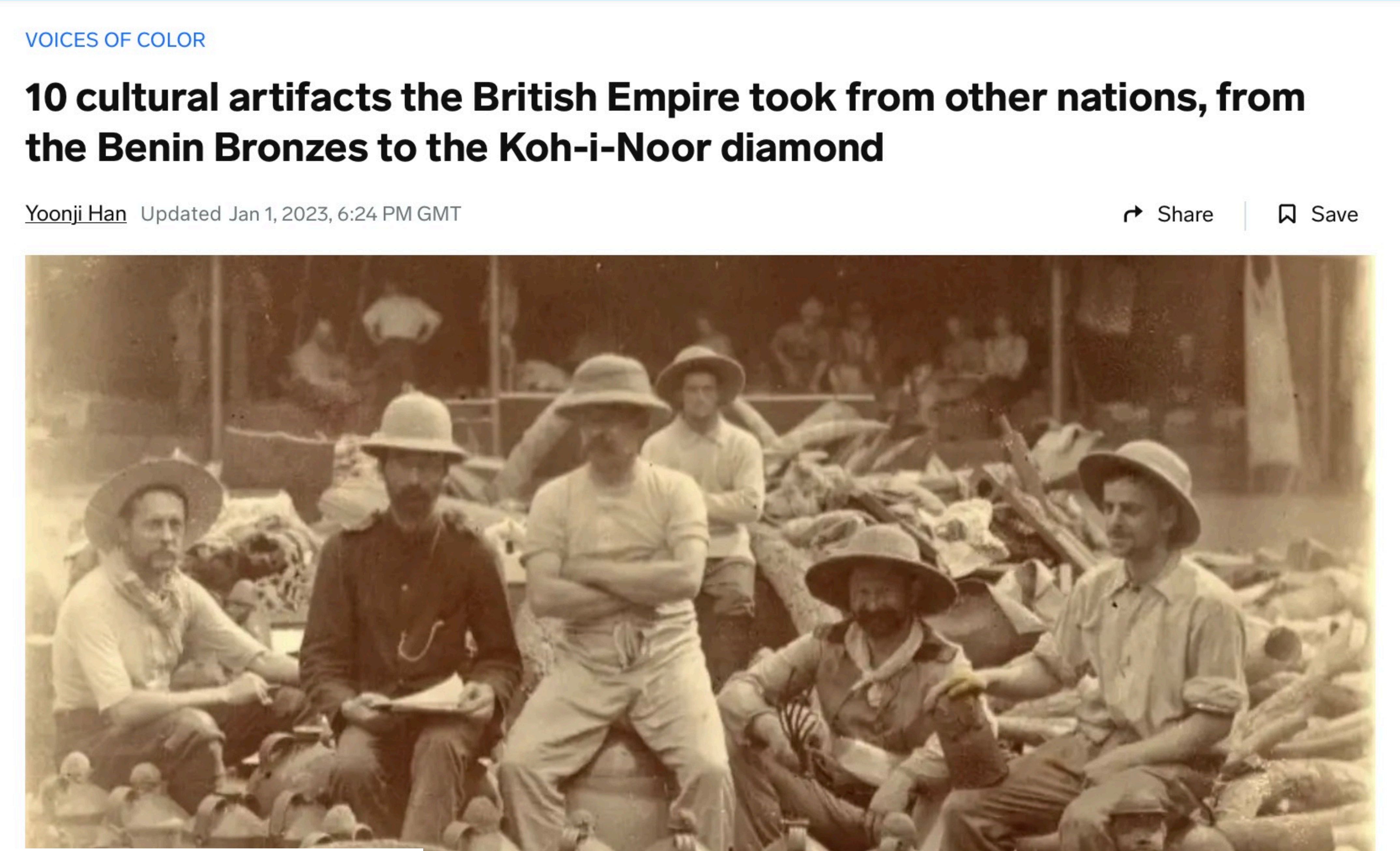


Artists 'steal' Queen Nefertiti bust by secretly scanning and releasing 3D printing data online

The artists were protesting Western museums' ownership of foreign artefacts

Elsa Vulliamy • Thursday 25 February 2016 12:51 GMT • Comments

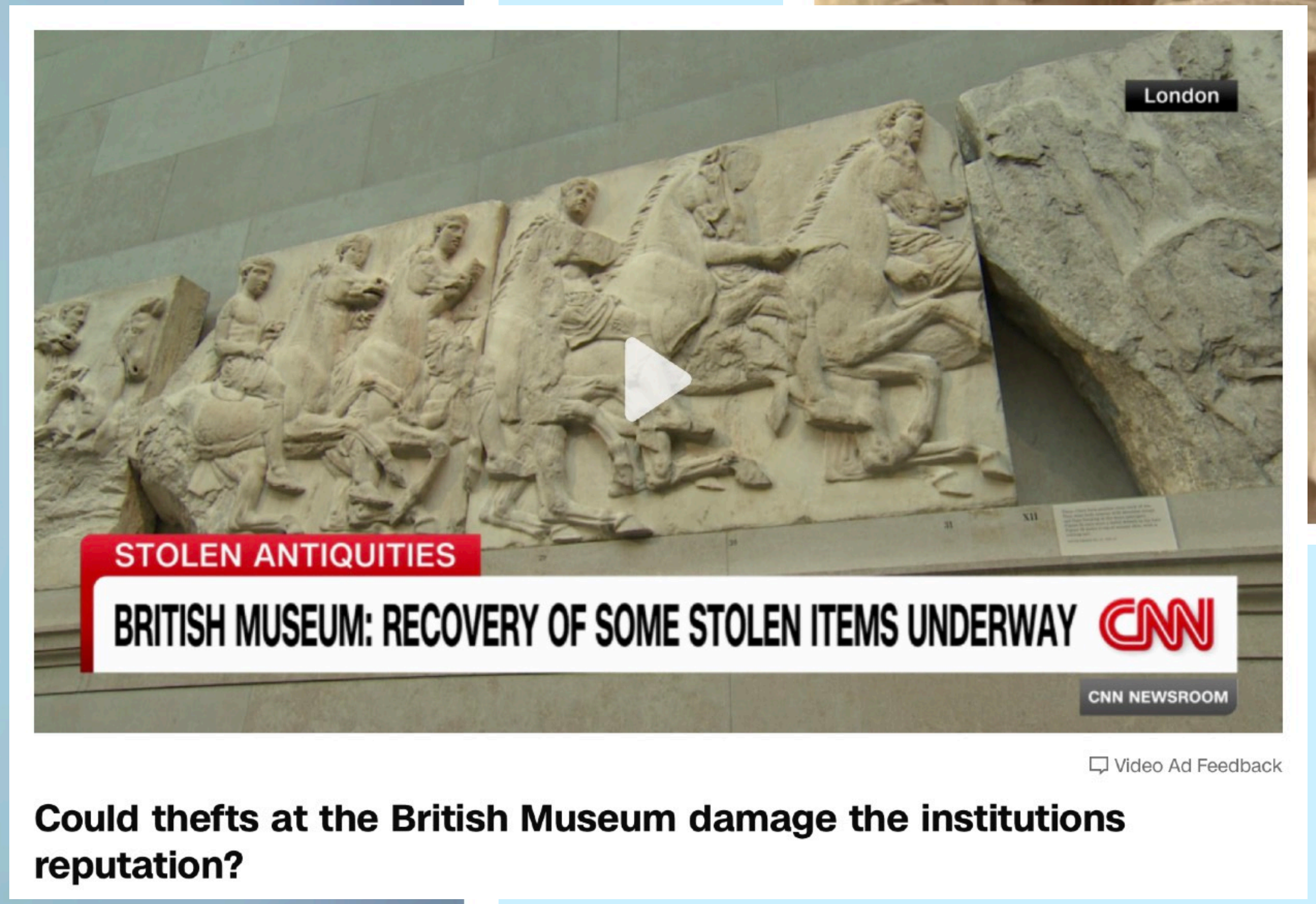
Germany and Egypt have disputed ownership of the bust *(Getty)*



VOICES OF COLOR

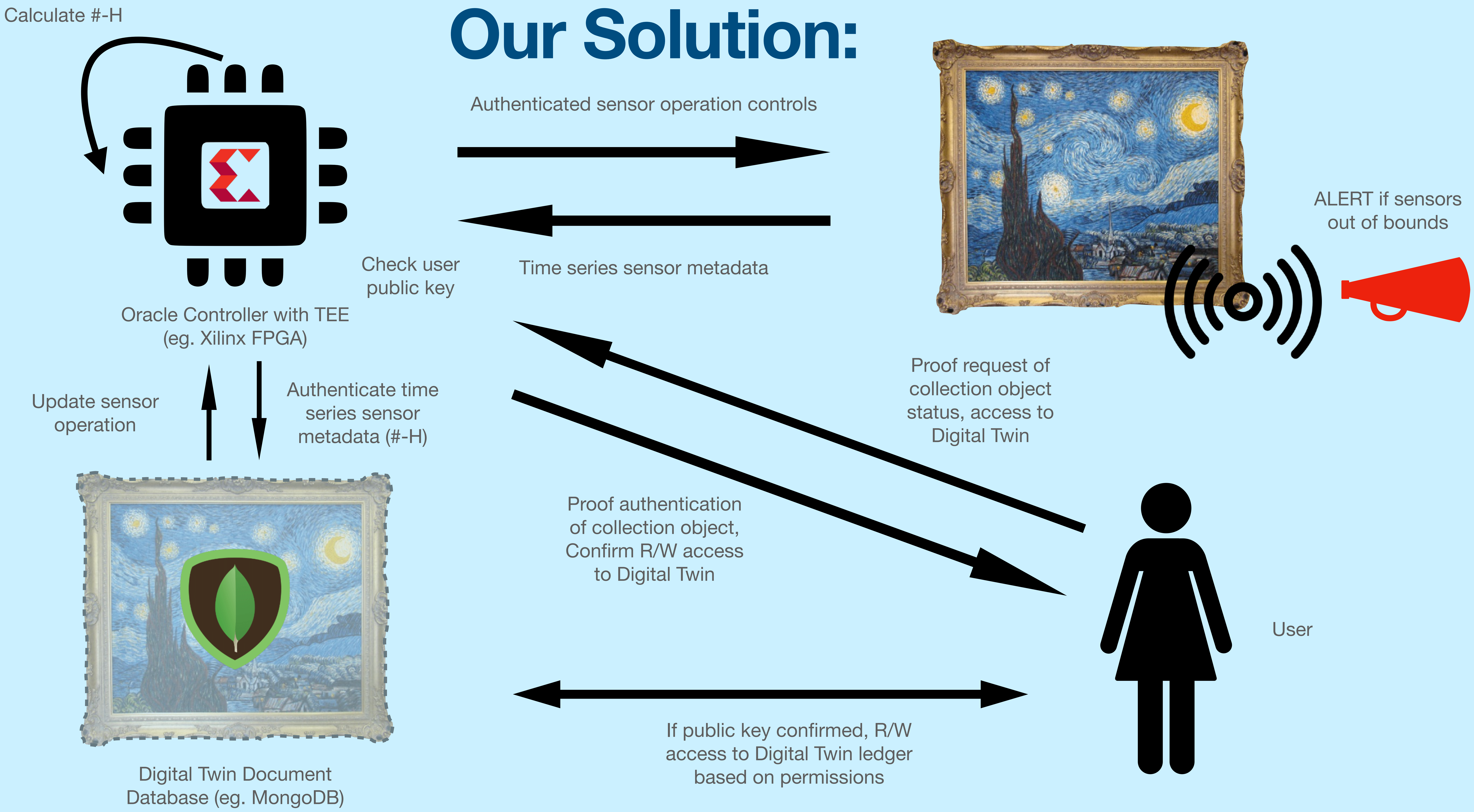
10 cultural artifacts the British Empire took from other nations, from the Benin Bronzes to the Koh-i-Noor diamond

Yoonji Han Updated Jan 1, 2023, 6:24 PM GMT



Could thefts at the British Museum damage the institutions reputation?

Our Solution:



Calculate #-H

Authenticated sensor operation controls

Time series sensor metadata

Check user public key

Oracle Controller with TEE (eg. Xilinx FPGA)

ALERT if sensors out of bounds

Update sensor operation

Authenticate time series sensor metadata (#-H)

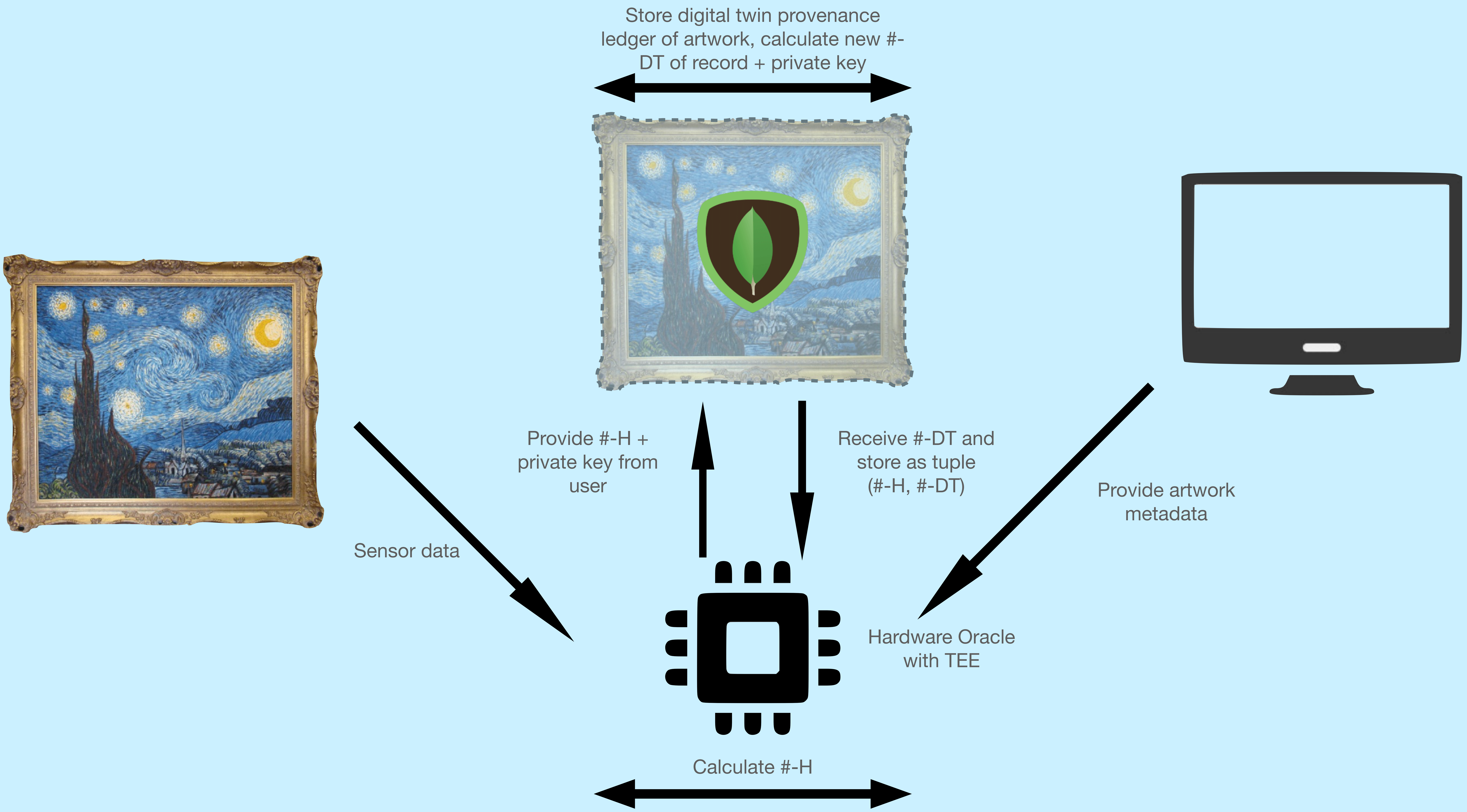
Proof request of collection object status, access to Digital Twin

Proof authentication of collection object, Confirm R/W access to Digital Twin

User

If public key confirmed, R/W access to Digital Twin ledger based on permissions

Digital Twin Document Database (eg. MongoDB)



Store digital twin provenance ledger of artwork, calculate new #-DT of record + private key

Provide #-H + private key from user

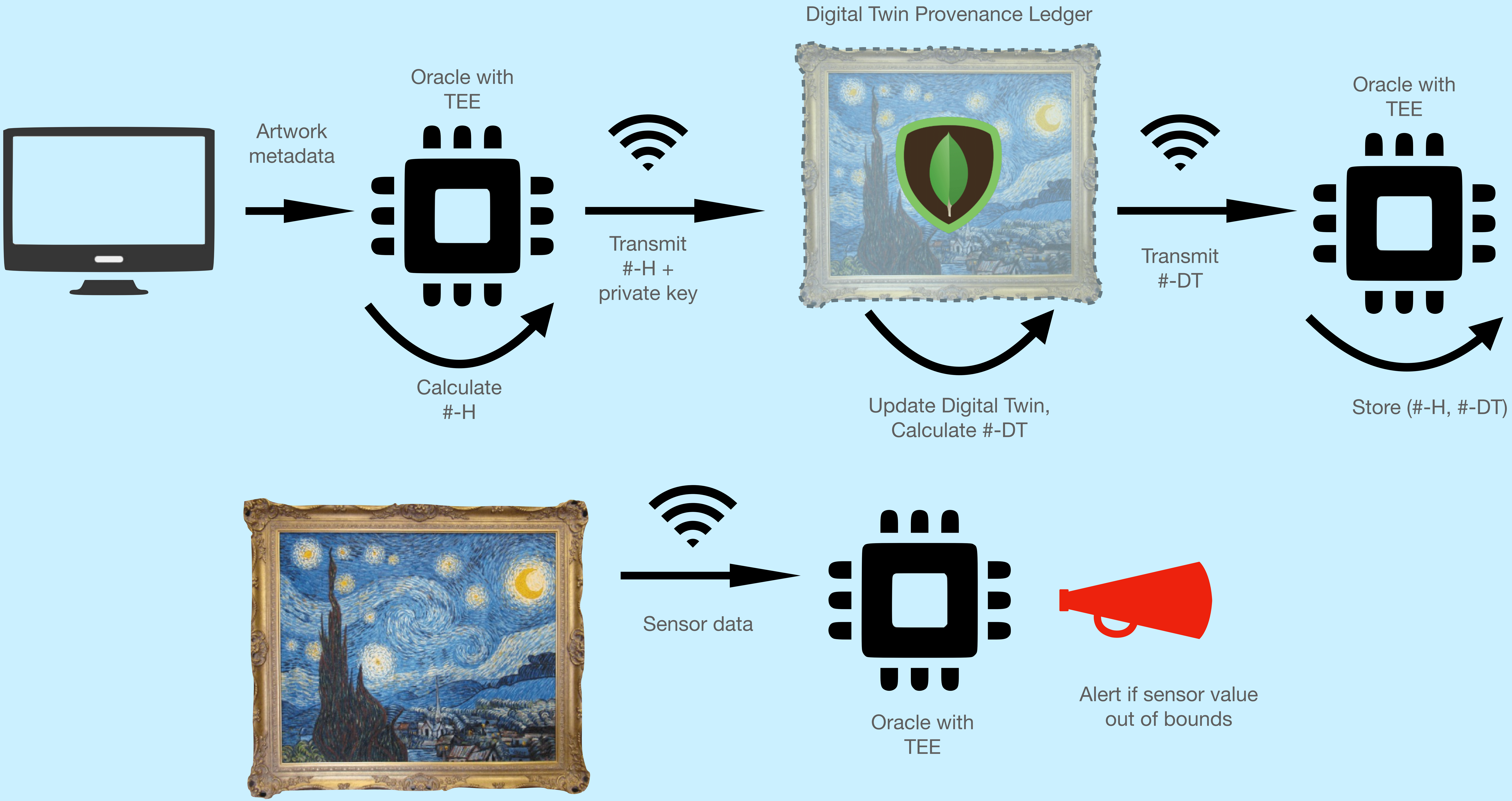
Receive #-DT and store as tuple (#-H, #-DT)

Provide artwork metadata

Sensor data

Hardware Oracle with TEE

Calculate #-H



Digital Twin Provenance Ledger

Artwork metadata

Oracle with TEE

Calculate #-H

Transmit #-H + private key

Update Digital Twin, Calculate #-DT

Transmit #-DT

Oracle with TEE

Store (#-H, #-DT)

Sensor data

Oracle with TEE

Alert if sensor value out of bounds

Design Features

Controller	PHYS layer Low cost, real time
Access	Permissioned, different user groups
Memory	Read: check provenance (public) Write: add provenance events (permissioned)
Network	Https compatible Push/pull ability
Authenication	Local (controller) Distributed (database, DLT)
Algorithmic	Cryptographic # (eg. ShA-256)
Oracle	TEE for IoT interface with DLT
Communication	Bi-directional between object and custodian
Monitoring	Real time localization and health status of object (IoT sensors)
Extensible	IoT sensors Customizable object metadata, records
Alert	Ability to push alert if object is at risk Machine learning to establish expected sensor ranges

Database Evaluation

Database	Pros	Cons
SQL	Simple & standardized Efficient	Enterprise ($) Known security issues Non-flexible
Column	Compressible, self-indexing Fast queries	Poor for incremental data Rigid (know structure in advance)
Relational	Accuracy (key pair) Security	Not scalable Enterprise ($)
Graph	Object oriented (data nodes, relationship edges) Flexible	Cannot network partition (due to edges) Not scalable
Document	Rapid & flexible support of different data types Secure: key pair	Increase in complexity with increased interconnectivity Less scalable
Time Series	Track (sensor) data over time Compare multiple data streams	Sensitive to data fluctuations High memory requirements

MongoDB has both!

Oracle Problem

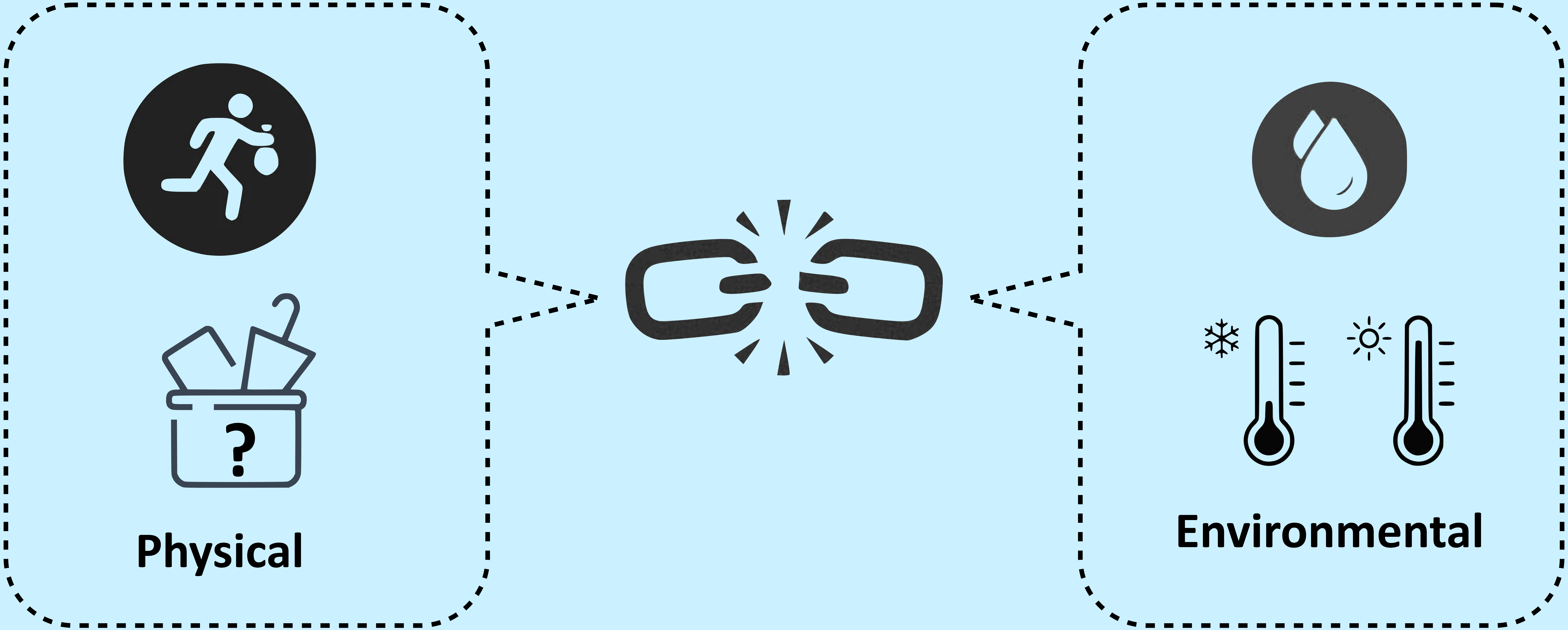
- Blockchain trust with trustless users via
  - Decentralization
  - Consensus via voting
- Deterministic, sequential so needs intermediary to use external, non-deterministic data in smart contracts (eg. IoT sensors)
- External data often doesn’t have same trust
  - Lack of attribution
  - Hierarchical (centralized)

Solution: trusted execution environments (TEE) for oracles

Trusted Execution Environment

- **Distributed System Requirements:**
    - Safety (no smart contract written with incorrect data)
    - Correctness (authenticity and integrity of data)
    - Liveness (Tx not lost, minimal outages IoT, Gas fee - ETH)
    - Truthfulness (data accountable and attributable)
- **Stock Hardware TEE: Ultimately inflexible**
    - Intel SGX (eg. TownCrier, Provable):
        - Safe CPU enclave
        - Root of Trust: System boot in enclave, attribution via PKI
        - High energy, desktop computers or servers
        - Security breaches
    - ARM TrustZone
        - Secure world CPU partition
        - Similar RoT
        - Suitable for mobile devices

Threat Models



Physical

Environmental

Thank you

Questions?

Blockchain @UBC