La *De Cifris* incontra Milano

Blockchain, White-box and High-speed Cryptography

Andrea VISCONTI

Dipartimento di Informatica
Università degli Studi di Milano

Blockchain: An example of a notary service

Blockchain: An example of a notary service

Blockchain and Cryptography...

- Hash Functions
  - Collision-free (collisions exist but we are not able to find them)
  - Preimage resistant (non-reversible)
  - Second preimage resistant
- Digital signature
- Merkle tree (binary tree)
- Zero-knowledge
- ...

Blockchain: An example of a notary service

Main idea

Art is a universal language. Why don't we share it?

We will **focus on young photographers** and their images.

We need to protect their artworks because

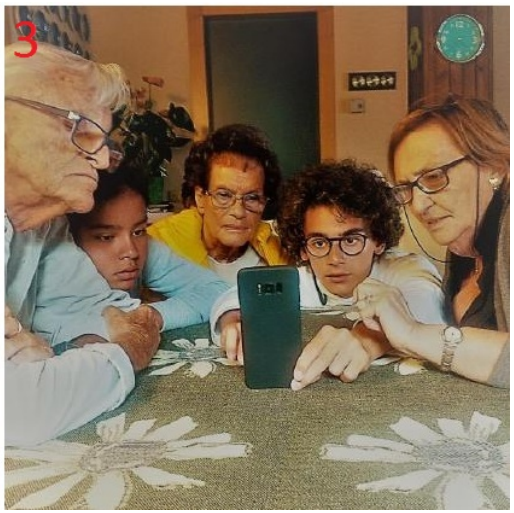
- photographers,
- auction houses,
- galleries,
- world's art collectors
- ...

may **have conflicting interests**!!

Blockchain: An example of a notary service

A simple challenge...

Photography is one of the best deal in the art market . . . Who would buy one of these images for $\$1,000$?



Which would you bet on?

. . . without expertise!

Blockchain: An example of a notary service

These images are not randomly chosen. Indeed...

Vibeke Tandberg is a Norwegian artists. She is known for manipulating her images to contort human figures and the spaces they occupy.

Estimated about $\$1,000$.

Blockchain: An example of a notary service

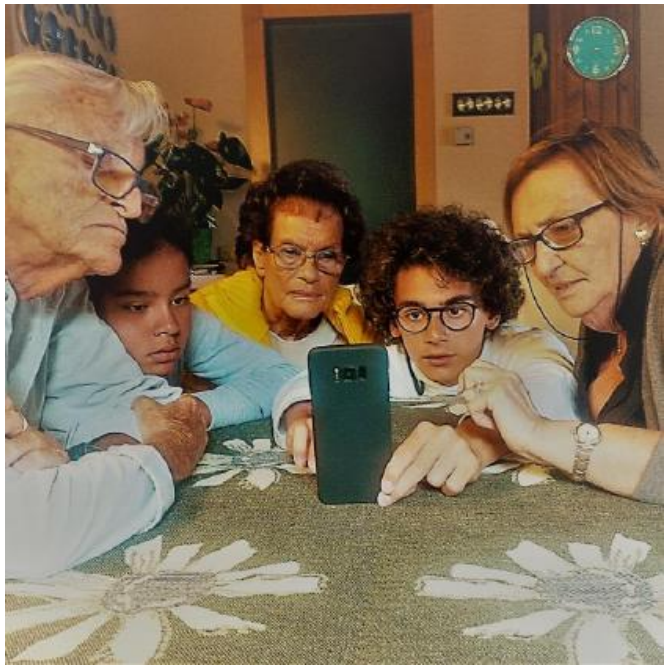
These images are not randomly chosen. Indeed...

Jeffrey Wall is a well-known Canadian artist. He is an influential photographer.

"*Card players*", estimated about $\$300,000 - \$400,000$.

Blockchain: An example of a notary service

These images are not randomly chosen. Indeed...



Maddalena is a professor @UniMI. She is not a photographer.

"Relatives", estimated about $0.

Blockchain: An example of a notary service

This simple challenge show us why **expertise is so important**.

A blockchain can be used **not only to store** the fingerprint of images!

We also need to store their **history**, what the viewer **observers**, **thinks**, and **feels** about these images.

. . . and to do so, we need to design and implement a smart contract application.

White-box Cryptography

White-box Cryptography

Cryptographic primitives are designed to protect data and keys in the **black-box attack model**, in which encryption/decryption operations cannot be tampered with.

These assumptions might not be applicable in some cases, for example DRM applications, Pay Tv, etc.

For this reason we refer to the **white-box model** as an attack model in which the adversary has total visibility of the software implementation of the cryptosystem, and full control over its execution platform.

White-box Cryptography

White-Box Cryptography was originally defined as an obfuscation technique intended to implement cryptographic primitives in such a way that an adversary having full access to the implementation and execution platform is **unable to extract the key**.

Why should an adversary be interested in recovering the key?

... DRM applications: a **key recovery attack** would allow an adversary to illegally **redistribute contents** to non-subscribers.

White-box Cryptography

2003–2011: White-Box implementations of **well-known cipher**.

These implementations are subjected to algebraic **attacks**, Differential Fault Analysis, Differential Computational Analysis, ...

Researchers have developed **dedicated** design approaches for white-box block ciphers.

PROS: interesting security properties.
CONS: efficiency could be a bottleneck.

Open problems: how to design a block cipher with a faster and secure key mixing.

High-speed Cryptography

High-speed Cryptography

Why is SW/HW **performance** so **important** for cryptography?

Efficient operations have high relevance both in HW and SW.

Usually **small speedups**: 3%, 5%, 10%.

Does the impact **justify the effort**?

High-speed Cryptography

A large **server farm**: –5/10% HW cost, –5/10% power cost, etc.

Constrained devices in the Internet of Things.

SW efficiency: data transfer cannot be bottlenecked by cryptography.

Could **careful implementation** of a cryptographic function improve performance?

It is possible to increase performance **by a factor of 10**!!

High-speed Cryptography

High-speed cryptography ==> High-speed **cryptanalysis**

To evaluate the **cipher strength** — e.g. computational resources required (time, memory, data)

To **try to gain access** to the contents of encrypted messages

The choice of mathematical structures are given by the **target cryptosystem**

Cryptanalytical implementations **do not take care about security**

Thanks for your attention!

andrea.visconti@unimi.it
www.di.unimi.it/visconti