Blockchain to protect individual rights

Massimiliano Sala - Univ. of Trento - De Componendis Cifris

Blockchain for social good -- **Turin** 15/12/2017

Who am I?

University of Trento

- Full Professor in Mathematics (Algebra and **Cryptography**)
- Laboratory of **Cryptography** (CryptoLabTN), Director

Italian Association of Cryptography **De Componendis Cifris**

- Acting Director

University of Trento spin-off company **Intellegit**

- Head of the Area **Cyber Security** **and** **Cryptography**

Blockchain: Cryptography at work

Cryptography has always been used to protect military and diplomatic secrets,

but nobody could have imagined the **amazing number** of important applications

Cryptography has now reached:

- from the protection of files in your smartphones,
- to the privacy-preserving communication you have in the Internet, including your chats and the secure sharing of your personal files, such as photos,
- to the last and most impressive application: Blockchain Technology

A blockchain: an infinite blackboard with no duster

Everybody can write on the blackboard, but Cryptography guarantees

1. the digital identity of the writer (public key) --> **who wrote?**
2. the impossibility to alter the content (hash function) --> **what was written?**
3. the public nature of the blackboard without losing its security
   everybody can read the blackboard and trust it !

Your rights are granted?

Say that:

1. you are **granted** a parking place (by your town)
   (or the right to vote, the right to health care, the right to paint red your door)

2. you park your car and when you come back --> you **find a fine**
   (in other words, you've been **denied** your right)

3. **what went wrong?**

What went wrong???

Many things might have happened:

1. the policeman could not see your parking permit

2. the policeman did see your permit, but it looked fake

3. the policeman did see your permit, he did realize it was real,
   but somehow he thought that the document did not refer to your car!

Just put your permit in the blockchain!

Remember, **Cryptography** is here to help:

1. the policeman will see it, because
   everyone can see what's written,

2. the policeman will be sure that it's **real**, because
   it is cryptographically signed by the **your town**

3. the policeman will be sure it refers to **your** car, because
   the content cannot be changed

Conclusions

Any time a **right is granted** to someone, **it** could be put on a **blockchain**!

This way, nobody would **deny** your right (except with malice).

As the Greek historian Polybius (203 BC – 120 BC) said:

*The order of battle used by the Roman army is very difficult to break through, since it allows **every man** to fight both **individually** and **collectively**.*