Teaching Critical-Safety systems considering Digital Ethics

Ethics4EU

Fatiha Zaïdi

June 15th 2021

université PARIS-SACLAY

LMF Laboratoire Méthodes Formelles

Outline

Definition

- Fundamental reflection that leads to a set of values that can be applied on a personal or professional level.
- It is necessary to make the difference between the law and the ethics.

Definition

- Laws are conceived from a set of rules (officials texts, jurisprudence, etc.) by a legitimate authority.
- The rules of law apply to a community and their violation leads to a sanction.
- The law aims to protect, fluidify and pacify relations within the community, to settle conflicts.

Definition

- Ethics is a reflection on the behaviours to be adopted to make the world humanly habitable: good behaviour, empowerment of each person, etc.
- In this, ethics is a search for an ideal of society and of the conduct of life. Ethics presupposes a reasonable dialogue, a "negotiation" between different people who pursue the same goal.
- This dialogue then gives rise to a standard that is likely to evolve, a standard that is intended to organise, if not the happiness of all, at least a collective well-being.

Operational Ethics

- Artificial Intelligence has contributed to a great deal of reflection, particularly with regard to the invasion of privacy, the violation of human dignity, the autonomy of systems and the socio-economic impacts
- Its reflection were structured around two main branches
  - Operational ethics, which is concerned with human ethics to guide the design, construction and use of artificially intelligent beings
  - Machine ethics, which is concerned with the moral behaviour of artificial moral agents.

Operational Ethics

In my case, I will focus my presentation on the operational ethics.

- Operational ethics for the design of digital systems has been the subject of reflection which has led to the organisation of its activities within committees, particularly in R & D centers and academic laboratories.
- These committees generally bring together specialists from several disciplines (law, philosopher, etc.) and aim to study and advise on any R & D and innovation activity, particularly in AI.

Operational Ethics: Research and Experimentation

- Deals with the various ethical issues involved in scientific experiments involving humans
- Assessing the usefulness and interest of the experience
- Assessing the impact on the lives of the subjects or the exploitation of their private data
  - Short and long term impact
  - Physiological, psychological, social, etc.
- Regulate the recording and use of experimental data
  - re-use of data, etc.
- Assessing the framework and context of the experience

Operational Ethics: Research and Experimentation

Various ethics committees have been set up in recent years:

- Allistene Commission on Research Ethics in Digital Science and Technology (CERNA) `https://www.allistene.fr/`
- CNRS Ethics Committee (COMETS): `http://www.cnrs.fr/comets/spip.php?article169`
- INSERM Ethics Committee (CEI): `https://www.inserm.fr/recherche-inserm/ethique/comite-ethique-inserm-cei-0`

These committees usually bring together specialists from several disciplines (law, philosopher, etc.) and their purpose is to study and advise on any R & D and innovation activity in particular.

Operational ethics: Project management

- The technological and societal purpose of the project
- The short and long term impact of the project and the final product (employment, performance, etc.)
- Conceptual and technical choices (taking into account the type of licences used, re-use of existing codes, etc.)
- Project documentation (in particular the capabilities and limitations of the system)
- The use of an eco-responsible approach (reducing ecological impact, reducing energy consumption)
- The issue of obsolescence and ageing of systems.

Ethics in driving research

- The experimentations have to be reproducible
- All the data to perform the experiments have also to be available
- When it is possible the software can be given to the community as a free software.
- The proofs are given as annexes in published papers and also on a web site. They are under the responsibility of the authors.
- Peers reviews help in avoiding plagiarism and in producing novelties.

Formal Methods

- Attack Tolerance
- Runtime verification: Monitoring
- Model checking

Attack Tolerance

Definition

Attack tolerance or intrusion tolerance is the capability of a system to continue to function properly with minimal degradation of performance, despite intrusions. The idea is to reduce the risk of attacks and to enable a continuity of service.

Issue

How can we **enable attack or intrusion tolerance** for systems ?

Attack Tolerance

Definition

Attack tolerance or intrusion tolerance is the capability of a system to continue to function properly with minimal degradation of performance, despite intrusions. The idea is to reduce the risk of attacks and to enable a continuity of service.

Issue

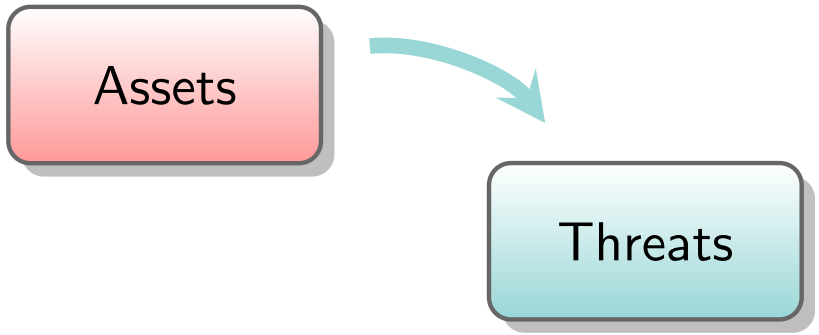
How can we **enable attack or intrusion tolerance** for systems ?

Attack tolerance

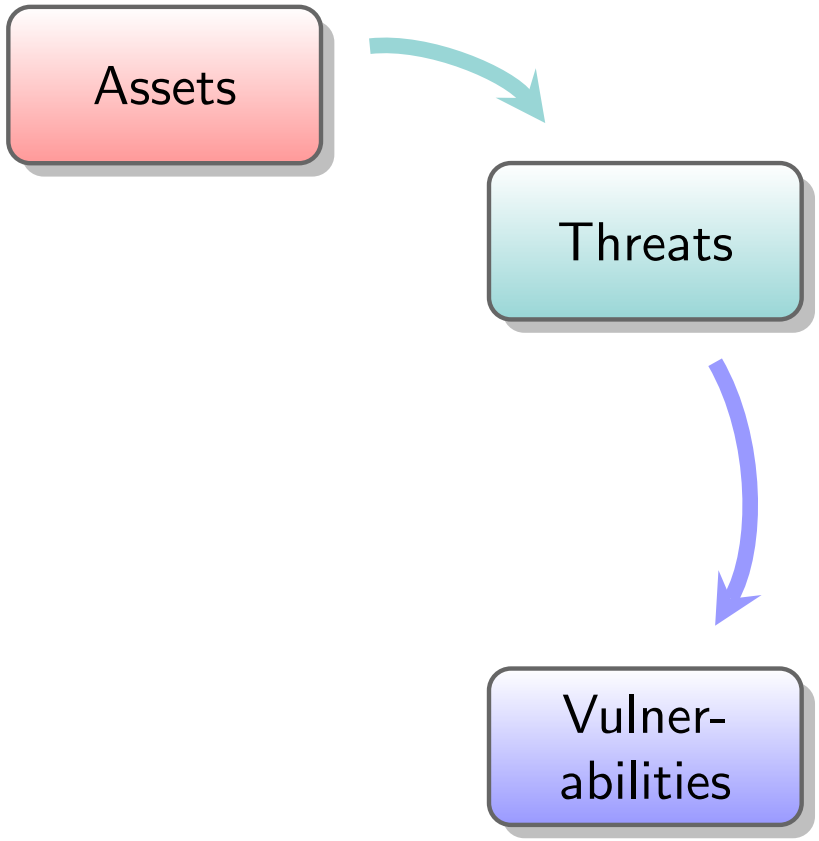
- We define a risk-based analysis. To ensure safety of the system is a kind of duty.
- We have to Leverage the level of security policy and user's experience

Risk-analysis overview

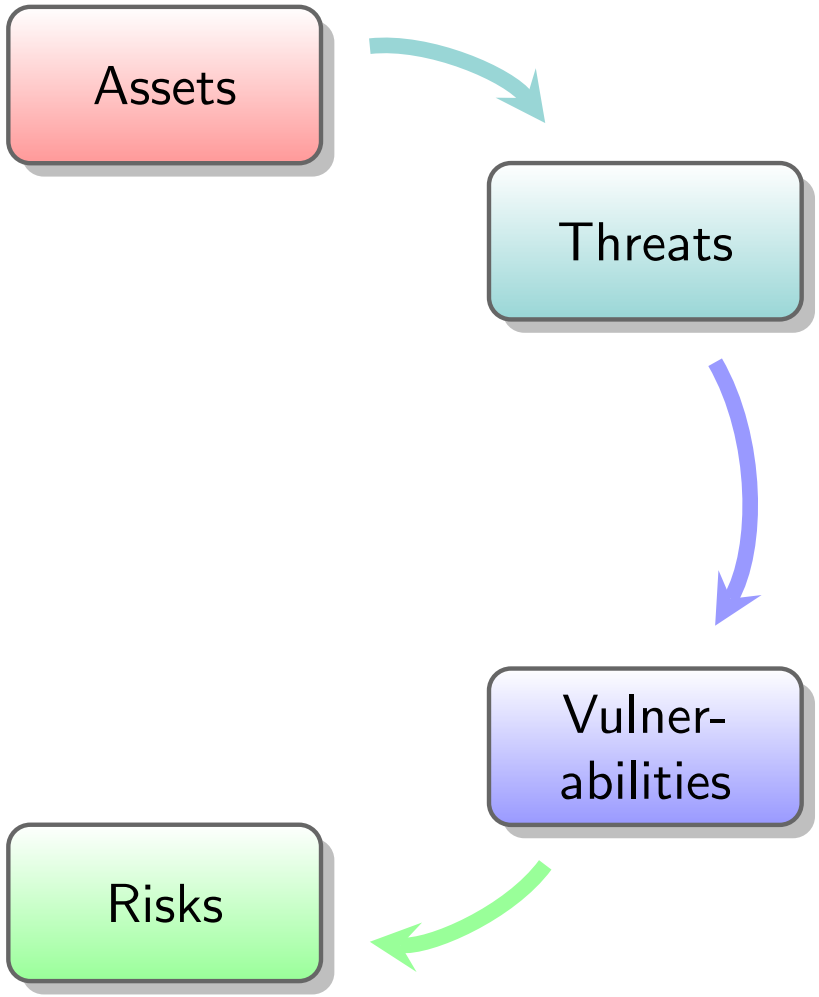
Risk-analysis overview



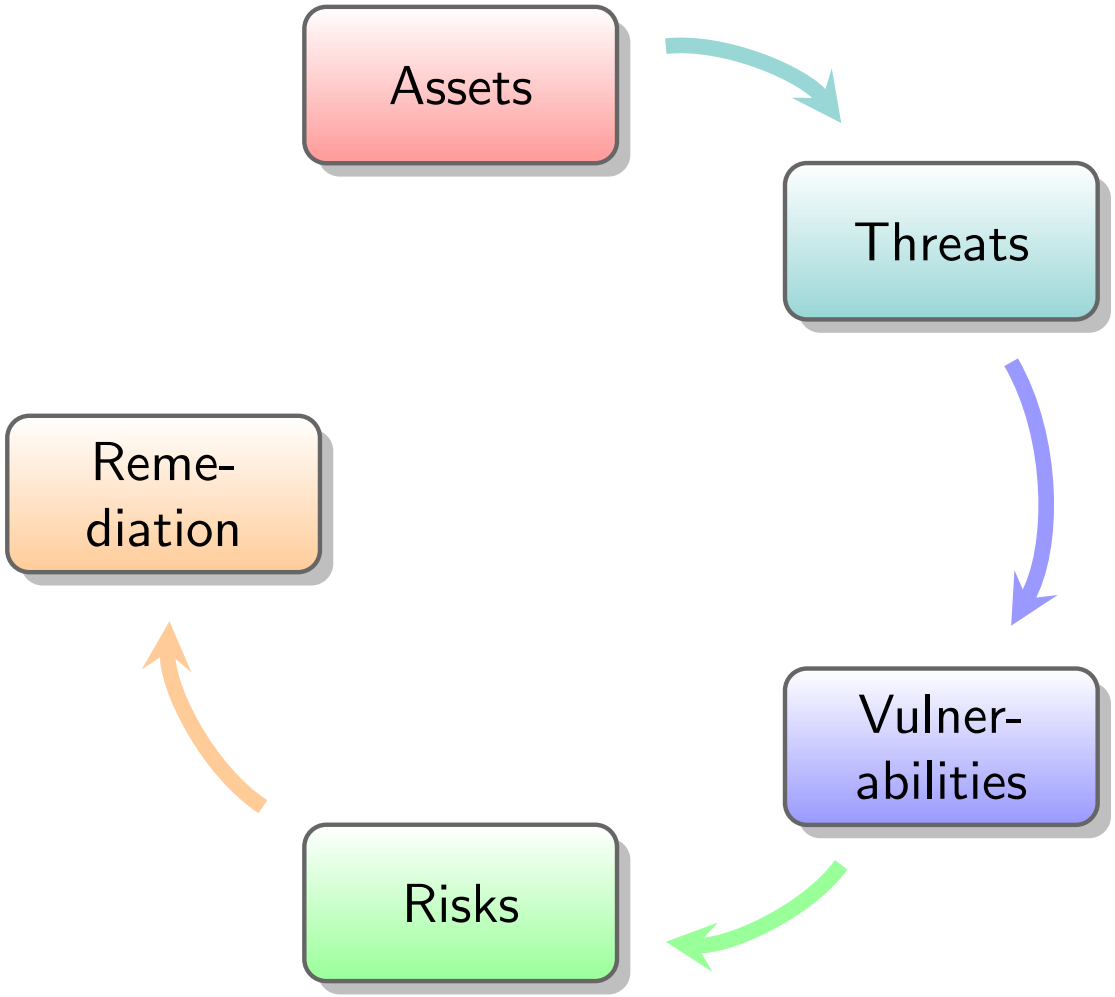
Risk-analysis overview



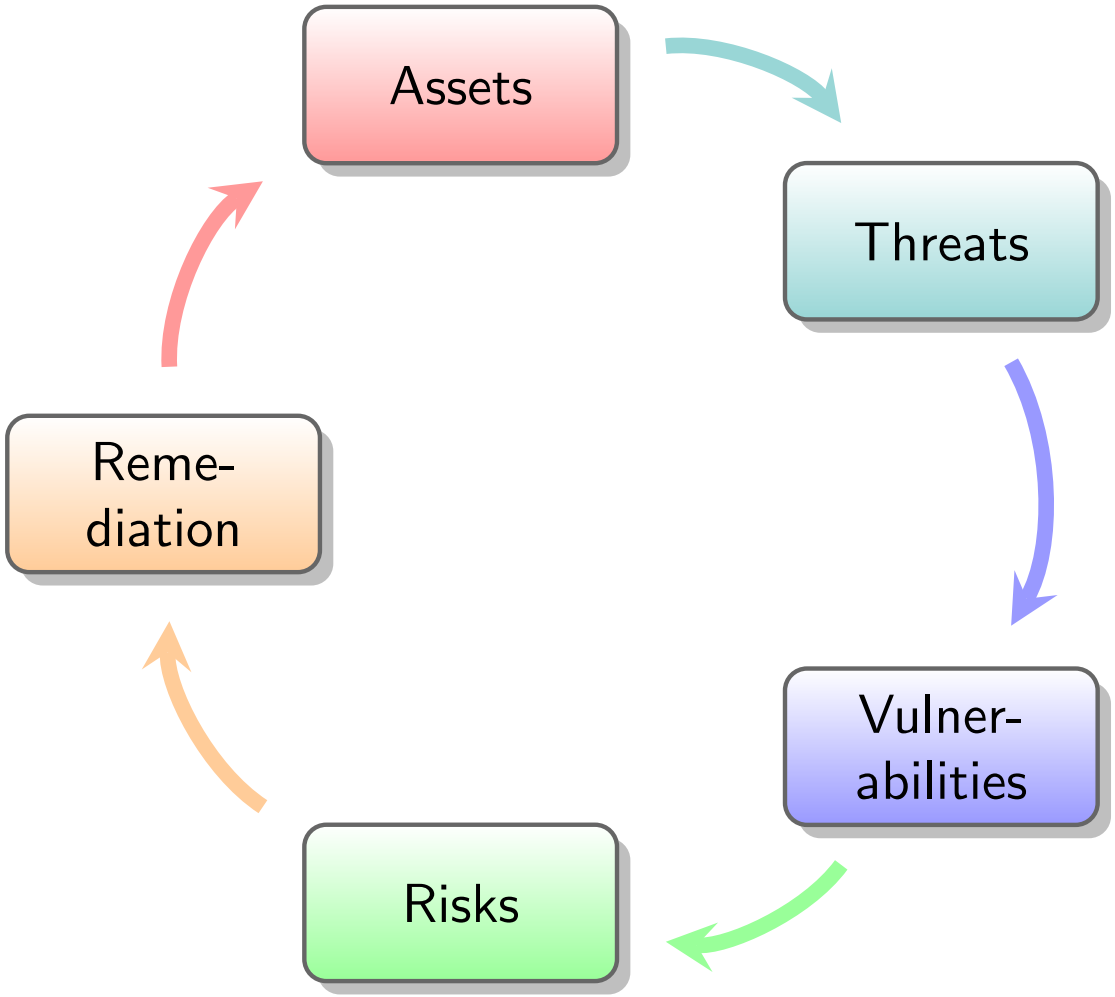
Risk-analysis overview



Risk-analysis overview



Risk-analysis overview



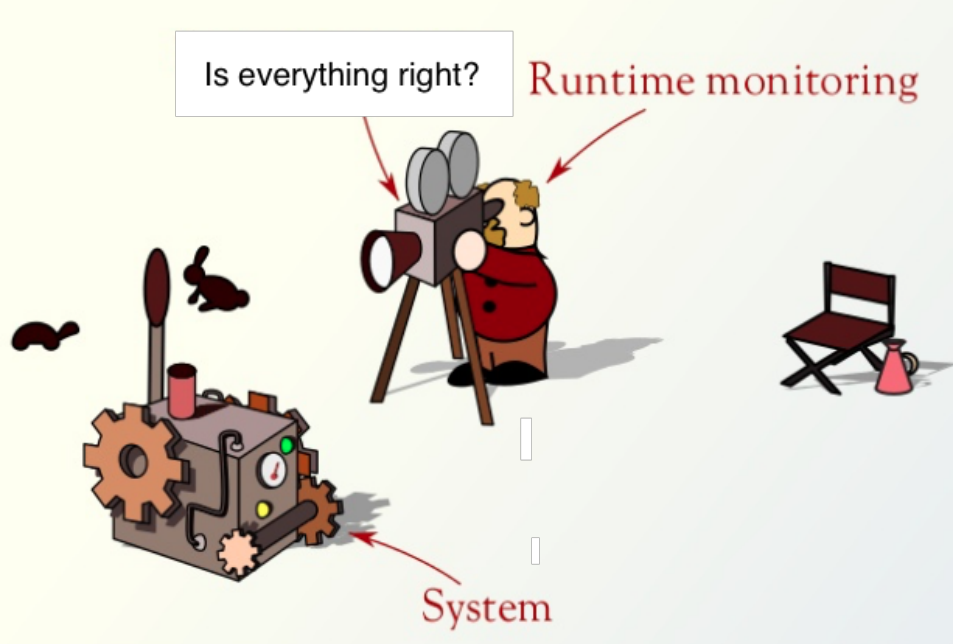
Ethics in attack tolerance

In case of system that have or wants to continue to function even when an attack is occurring, there are several concerns:

- A white-hat approach has to be followed, i.e. by trying to discover vulnerability of the system.
- by securing the sensitive part of the system
- by establishing good counter-measure to limit the effects of the attack.

Why runtime monitoring?

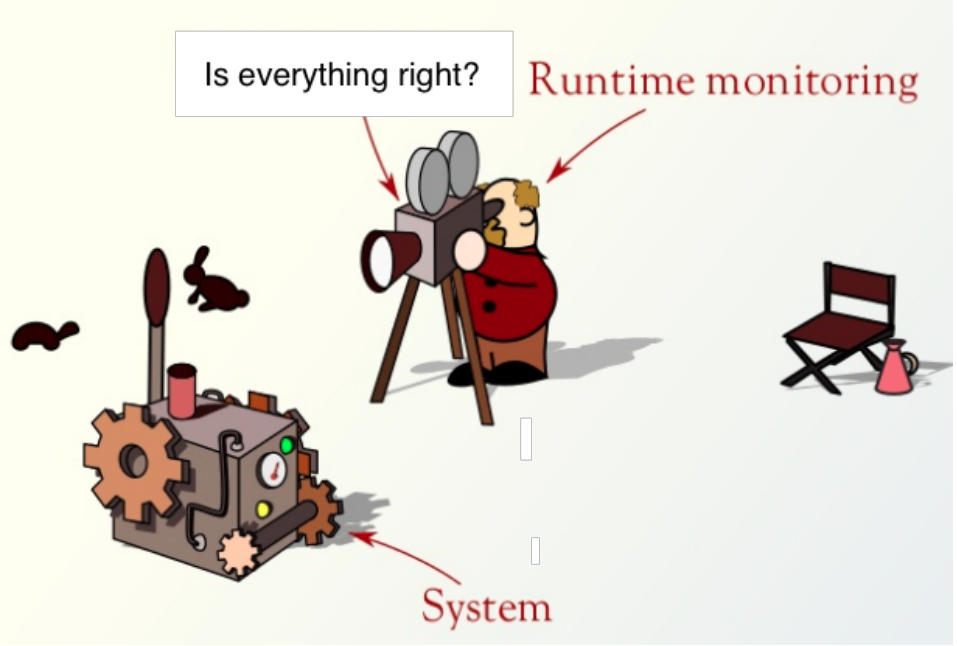
- For detecting the security threats, it is important to monitor the system at runtime.
- Runtime monitoring is the process of observing and verifying some properties of the system at runtime.



It helps to understand the behavior of the network and the application in order to detect faults and abnormal operations.

Why runtime monitoring?

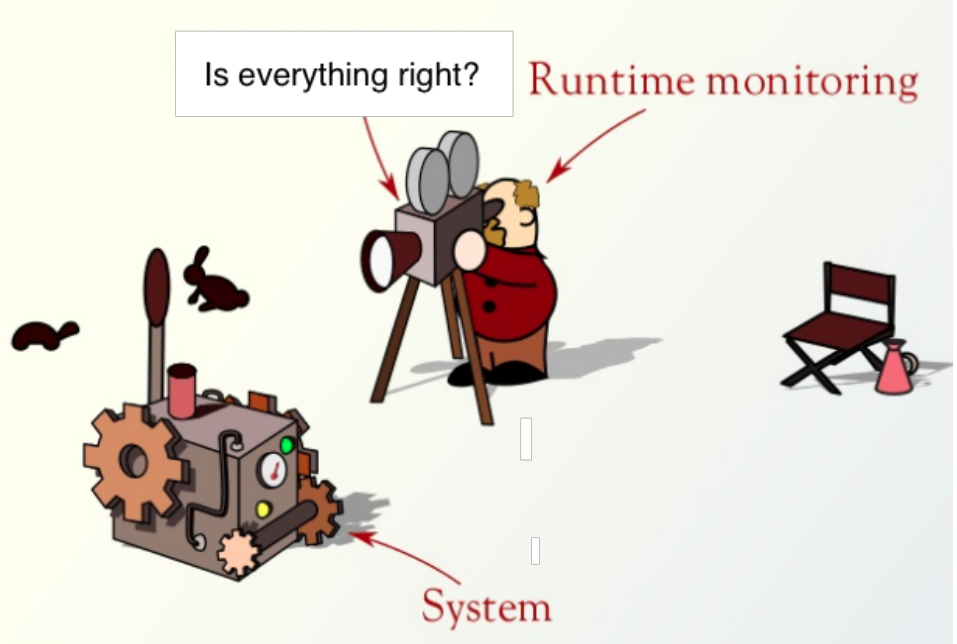
- For detecting the security threats, it is important to monitor the system at runtime.
- Runtime monitoring is the process of observing and verifying some properties of the system at runtime.



It helps to understand the behavior of the network and the application in order to detect faults and abnormal operations.

Why runtime monitoring?

- For detecting the security threats, it is important to monitor the system at runtime.
- Runtime monitoring is the process of observing and verifying some properties of the system at runtime.



It helps to understand the behavior of the network and the application in order to detect faults and abnormal operations.

Ethics with Monitoring

With monitoring approaches, data are kept to analyse the system. In this case, we need to address some issues regarding the data:

- Purpose of data storage
- Purpose of data processing
- People's rights
- Nature of store data (type of signal, sampling rates, etc.)
- The location of data storage and the regulations in force
- Information system security

Critical Safety systems

In case of critical systems, a correct code of conduct is to ensure safety.
The system has to be analysed, verified (tested intensively).
To apply formal methods, there is a significant effort that has to be done:

- To model formally the system
- To analyse the system
- to prove or test thoroughly the system
- and finally to produce a secure code

Products manufacturers have financial constraints and a time to market that can appear antagonist with formal approaches. As a result, the users are often the beta-tester of the products.
Hopefully, in very critical systems with possible massive loss of life, proof-based approaches are used.

Blockchain verification: smarts contracts verification

- Blockchain is a technology that allows a set of transactions to be recorded in a decentralised, secure and transparent manner in the form of a chain of blocks
- Smarts contracts are programs stored in a Blockchain
  - legal perspective (automated agreement)
  - no revocation modification (at least not easy)
  - code is law (no matter what it may end up doing)

But smarts contracts may have bugs (important financial risks).
Need to use formal methods to find bugs in smart contracts.

DAO flaw

- Coder(s) found a loophole in the procedure of the DAO.
- It was not checking whether there was a recursive call.
- The attacker managed to recursively call the split function and retrieved their funds multiple times before getting to the step where the code would check the balance.

DAO and Ethics

- For the attacker(s), the use of the smarts contracts was not an attack as in a Blockchain the code is law
- To undo the actions in a Blockchain is not an easy task (soft fork hard fork)

Even if code is law, to earn money because of a flaw in a code is not ethically acceptable.

Conclusion: From Ethics to Law

Ethical considerations have led to several legal advances

- General Data Protection Regulation (GDPR) (Adopted by the European Parliament in 2016 and applied in France in 2018)
- Personal Protection Committees (PPCs)
- Autonomous vehicles

Sources

I have constructed this presentation with different sources :

- Lecture of Thomas Baudel (Ethics and STICs)
- Lecture of Pr. Mehdi Ammi (IoT Ethics)
- Reading of CERNA reports, Comets
- GDPR