

# Allstars contract

Rédacteur	Vérificateur	Approbateur

---




## 1 Introduction

Le projet d'analyse statique repose sur la détection de motif permettant la correspondance avec les codes des smart-contracts<sup>1</sup> étudiés.

## 2 Analyse statique

### 2.1 Contexte

L'analyse statique prend essentiellement en entrée le code source à analyser. Le langage principal sur lequel les motifs sont élaborées est Solidity . Cette analyse permet de vérifier l'inclusion de risques dans le code sources à partir d'une base de risques modélisés par Dowers de manière quasi instantanée. Cette base de risques est alimentée par la spécification des langages, les retours d'expérience.





Dépôt : [https://github.com/Dowers/tarkastus\\_backend](https://github.com/Dowers/tarkastus_backend)

La base de données de risques modélisées à ce jour est présentée dans le tableau ci-dessous :

<i>Verification implementees</i>	<i>H</i>	<i>M</i>	<i>L</i>	<i>G</i>	<i>NC</i>
64	5	12	13	19	13

### 2.2 Objectifs

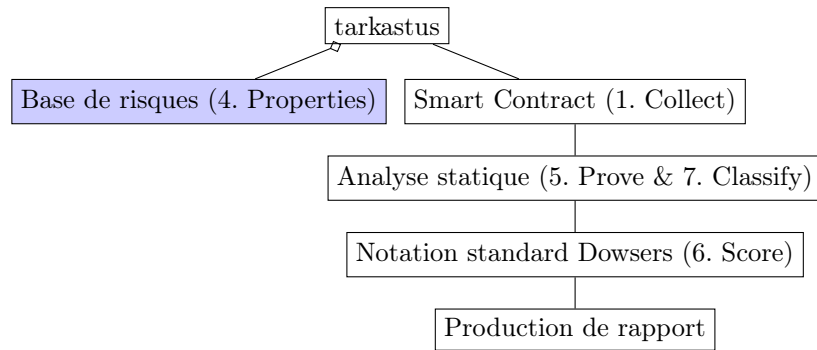
Les objectifs portent sur plusieurs points :

1. Amélioration continue de l'outil.
2. Enrichissement continue de la base de vérifications.
3. Ouverture à d'autre techniques de vérification portant sur le code compilé, métadonnées, arbre de la syntaxe abstraite...
4. Intégration d'un décompilateur Solidity .
5. Ouverture aux langages Rust , Cairo , WebAssembly .

---

1. Les contrats intelligents (en anglais : smart contracts) sont des protocoles informatiques qui facilitent, vérifient et exécutent la négociation ou l'exécution d'un contrat sous forme de code informatique.

## 2.3 Organisation fonctionnelle



### 2.3.1 tarkastus

Le module tarkastus est le principale lanceur des différentes analyses. Il agrège et organise les différentes étapes du logiciel.

### 2.3.2 Base de risques (4. Properties)

Le module tarkastus est le principale lanceur des différentes analyses. Il agrège et organise les différentes étapes du logiciel.

## 2.4 Planification

