

# iTRAC

## Investigation par Traitement et Analyse des cryptomonnaies

Sébastien Keller, Thales SIX GTS France, Paris, France ([sebastien.keller@thalesgroup.com](mailto:sebastien.keller@thalesgroup.com))

Le projet FUI 21 iTrac a pour objectif de développer et d'évaluer de nouveaux outils afin de détecter des comportements malveillants en corrélant les données issues du darkweb et les informations publiques fournies par la blockchain Bitcoins. Aujourd'hui quelques outils existent pour faire différentes analyses du ledger Bitcoins, des outils du web peuvent être adaptés pour effectuer des recherches dans le darkweb mais aucun outil ne cherche à corréler ces 2 sources d'information.

Le projet iTrac est porté par Thales SIX GTS France qui est numéro un européen des systèmes d'information et de communication sécurisés, notamment de la sécurisation des transactions bancaires. Sa Direction Technique développe des méthodes, des technologies et des outils d'analyse de l'information orientés Big Data, Big Analytics et Visual Analytics. Elle travaille déjà étroitement avec la Gendarmerie Nationale sur l'analyse de données sociales pour lutter contre la cybercriminalité. Le rôle technique de Thales dans ce projet est de participer à la collecte des besoins, d'intégrer l'ensemble des composants sur une plateforme big data et de développer les composants de collecte automatique de documents, de visualisation et d'aide à l'investigation.

Le consortium regroupe l'ensemble des forces nécessaires pour développer un outil de veille, d'investigation et de lutte contre la criminalité à destinations des autorités publiques :

- un grand groupe industriel (Thales) avec une forte expertise dans la fourniture de solution intégrée aux autorités publiques à des fins de sécurité,
- Une start-up spécialisée dans le secteur innovant des crypto-monnaies (PAYMIUM),
- Une PME spécialisée dans le traitement et l'analyse de documents textuels (Expert System),
- Un laboratoire spécialisé dans la fouille de grands graphes (LIP6 – Complex Network), particulièrement adaptée au graphe des transactions Bitcoin,
- Un laboratoire spécialiste (UM1 – DSP) des questions de cybercriminalité.

Le projet FUI 21 iTrac a été co-labellisé par les pôles Systematic, Cap Digital et Finance Innovation et est soutenu financièrement par la BPI et la région « Ile de France ». Ce projet a commencé le 01/06/2016 et s'achèvera le 01/06/2019.

Les principaux résultats sont :

- Crawler dark-web (Produit mature existant de Aleph Network, TRL 9, le projet a développé les formats d'export ainsi que différents filtres appliqués)
- Connecteurs temps réels à la Blockchain (Prototype TRL : 4)

- Analyse textuelle des documents collectés (Produit GOGITO de Expert System, TRL 9, le projet a développé des extractions spécifiques qui sont les adresses bitcoins, les noms de marketplaces ainsi que les dates)
- Outil d'analyse des graphes de transactions, des portefeuilles et des documents du darkweb (prototype TRL 4).

Ces différents résultats ont été fournis sous forme d'outils logiciels s'intégrant dans l'architecture décrite dans la figure suivante.

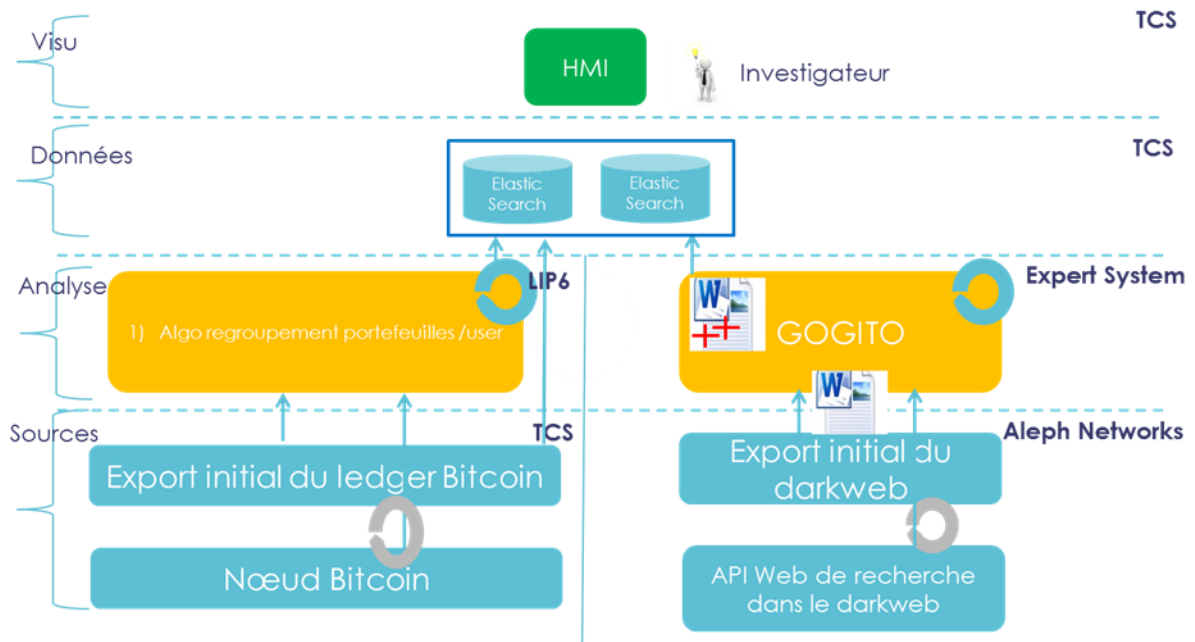


Figure 1 : Architecture du prototype