Présentation du projet FUI iTrac

RESSI 2019

Sébastien Keller (Thales SIX GTS France)

16/05/2019

PROJET iTRAC

Agenda

- Contexte et Objectifs du projet
- Solution
- Résultats
- Conclusion

Contexte et Objectifs du projet

PROJET iTRAC

Objectif du projet iTrac – Contexte des crypto monnaies

« Un type de monnaie numérique non réglementée, émise et généralement contrôlée par ses développeurs, utilisée et acceptée par les membres d'une communauté virtuelle spécifique »

« Virtual currency schemes » : BCE, Fevr. 2015

Plusieurs monnaies existantes :

- Bitcoin, Ripple, Ethereum, Zcash…

Bitcoins (au 23/01/2019) :

- Capitalisation : de 55 Milliards d'euros.
- Volume échangé en 24h : 4,6 Milliards.

Objectif du projet iTrac – Contexte du darkweb

« Le dark web, Internet clandestin ou encore l'Internet sombre est le contenu du World Wide Web qui existe sur les darknets, des réseaux overlay qui utilisent l'internet public mais sont seulement accessibles via des logiciels, des configurations ou des autorisations spécifiques. Le dark web forme une petite partie de deep web, la partie du Web qui n'est pas indexée par les moteurs de recherche »

« https://fr.wikipedia.org/wiki/Dark_web »

Principales propriétés :

- Accès anonyme via le darknet.
- Usage pour des activités illicites ou pour des ONG par exemple.

Protocole TOR :

- Accès via un nœud TOR.
- Crawle des pages ouvertes.

Objectifs du projet iTrac - buts

Contribuer à la détection d'activités illicites :

- Vente de produits ou services illicites.
- Rançongiciels et ventes de produits pour hackeurs.
- Blanchiment d'argent.
- Détecter de nouveau comportements répréhensibles.

Enrichir et corréler les 2 sources d'information :

- Identifier des utilisateurs Bitcoin et des communautés.
- Caractériser de l'informations dans le darkweb.

Naviguer dans les données obtenues et les interpréter :

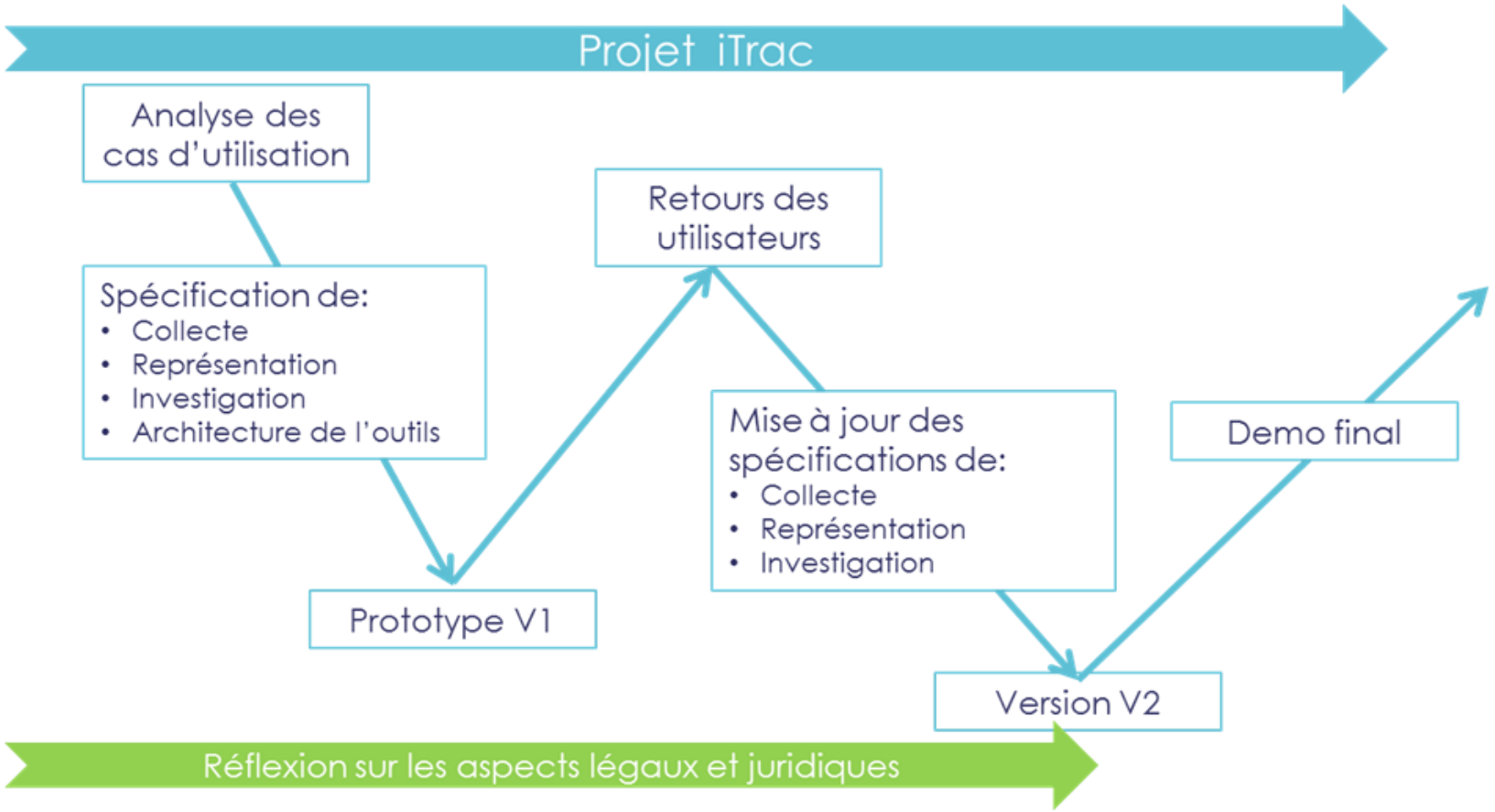
- Parcourir les données brutes et enrichies.
- Interpréter les données et les enrichir.

Solution

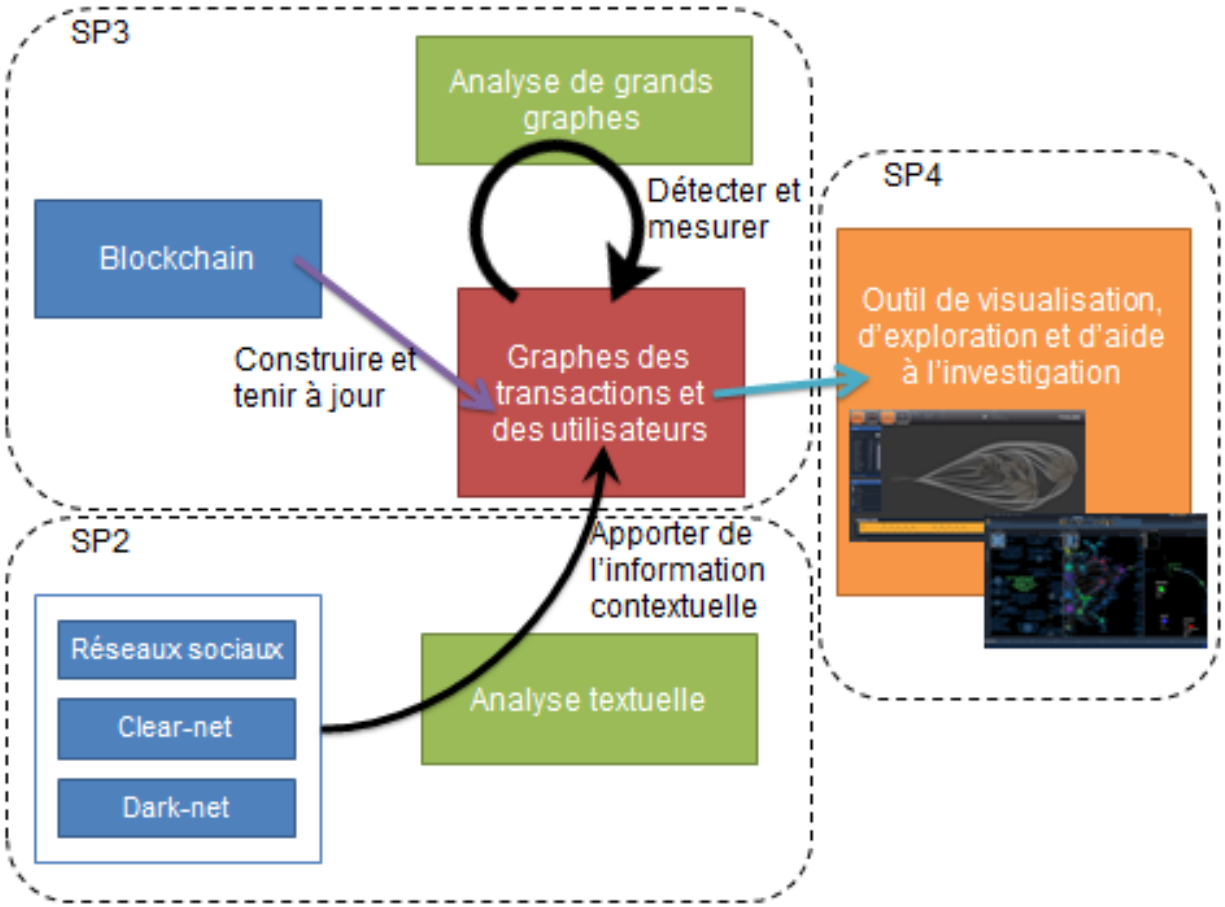
PROJET iTRAC

Solution – Approche

Approche



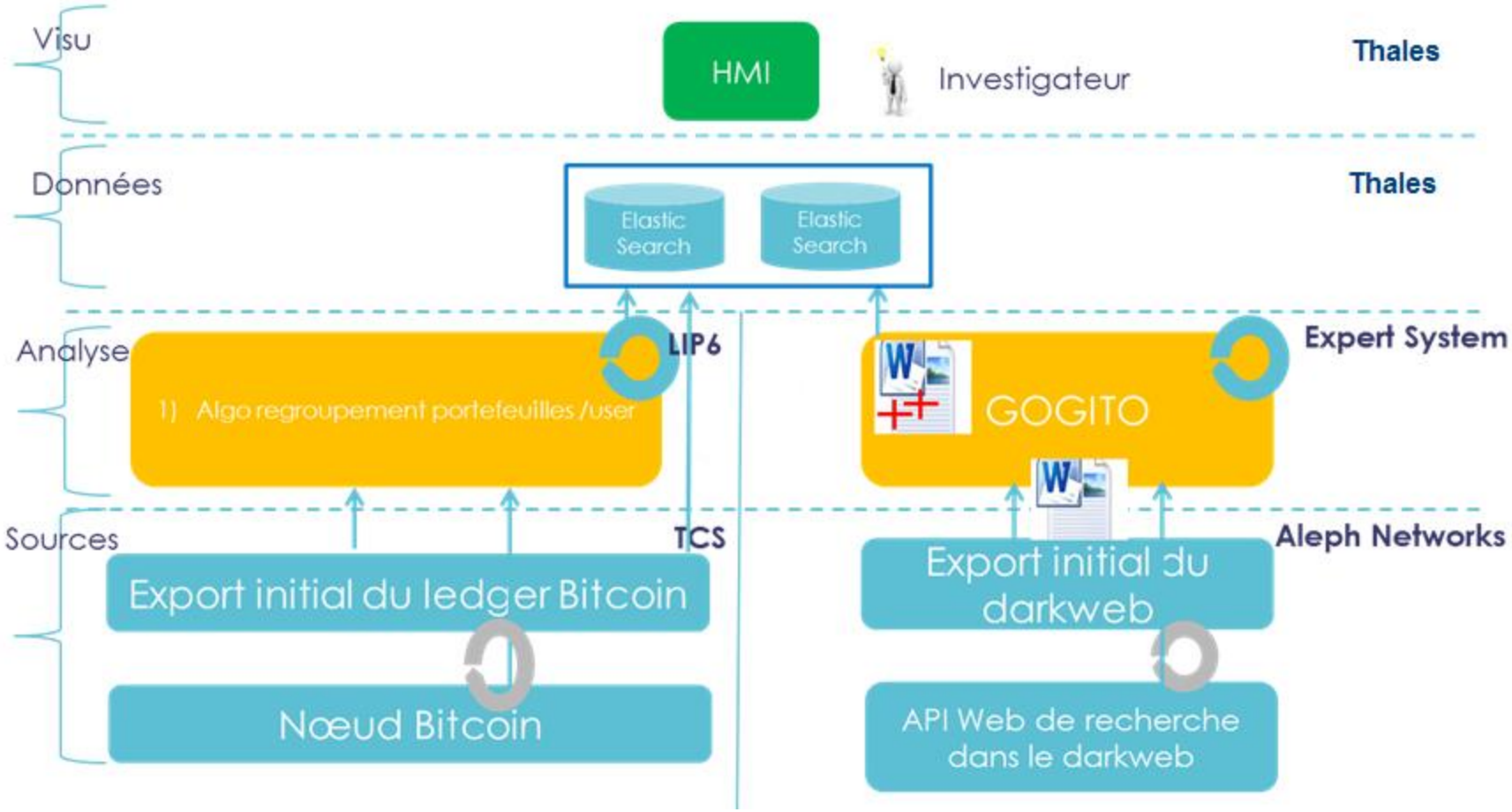
Solution – Organisation du travail



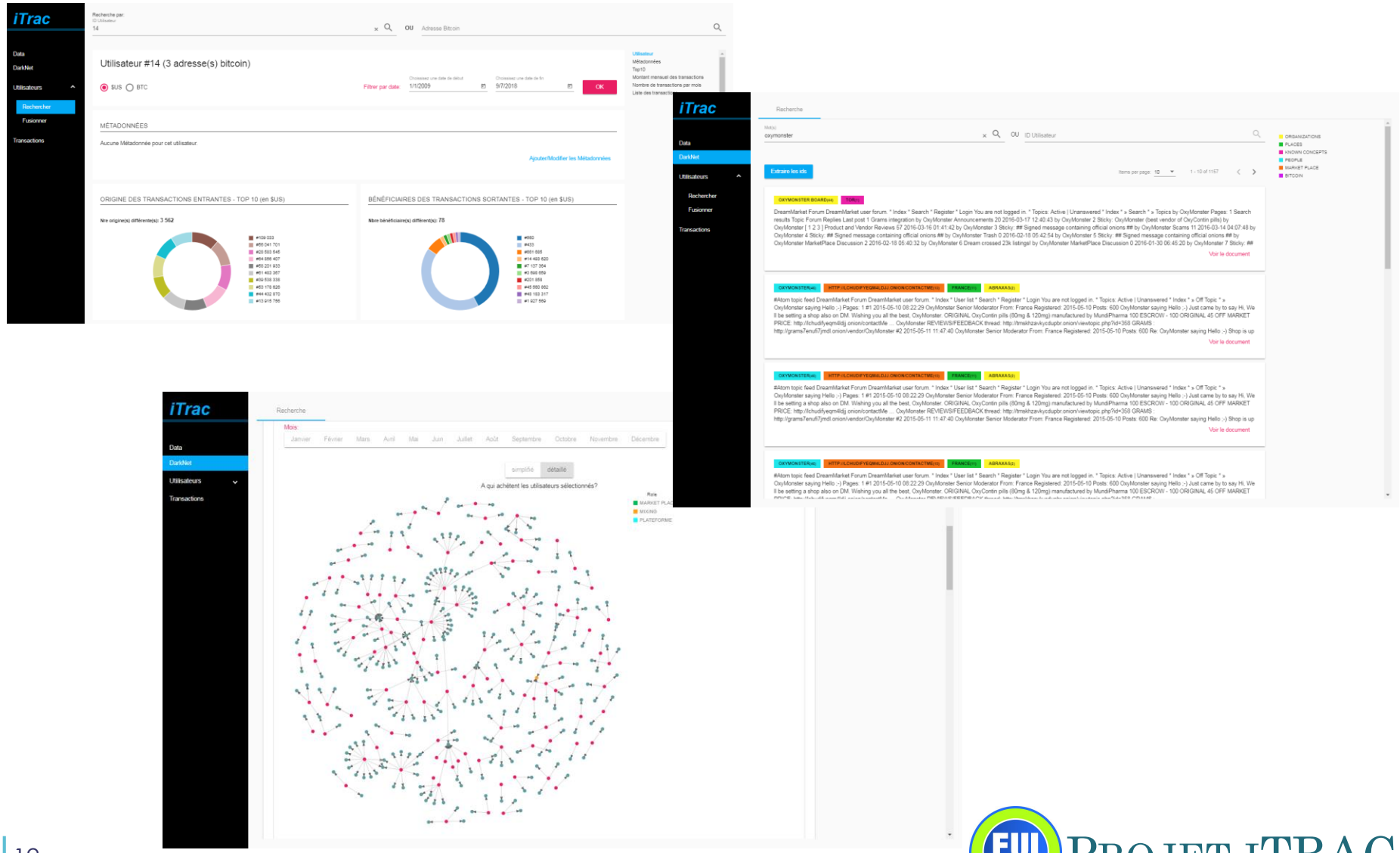
Résultats

PROJET iTRAC

Résultats – Outil de navigation



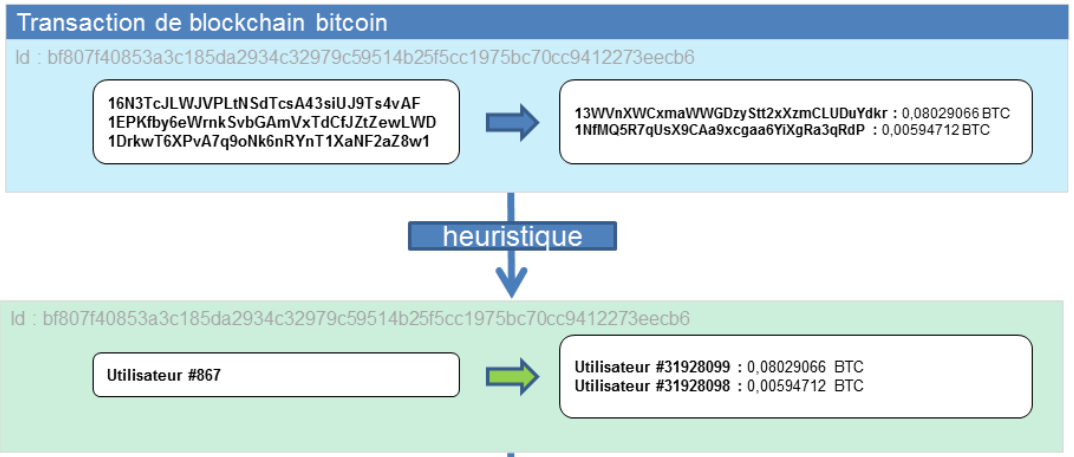
Résultats – Outil de navigation – Copies d'écran



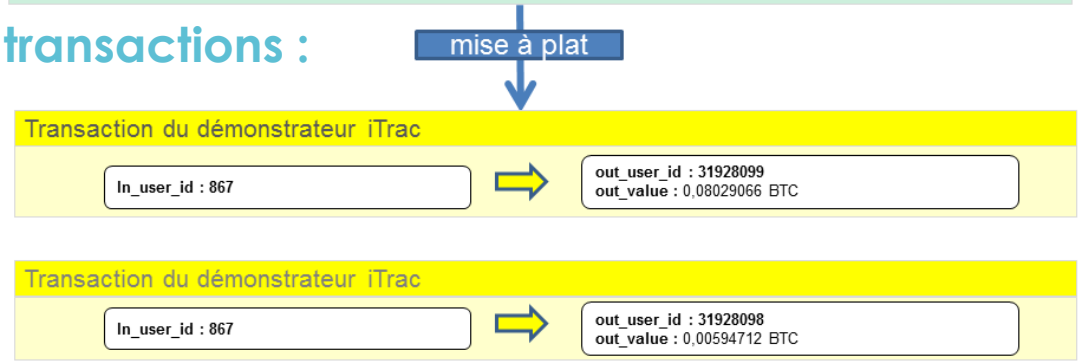
PROJET iTRAC

Résultats – Enrichissement et Analyse des données Bitcoins

Identification des utilisateurs :

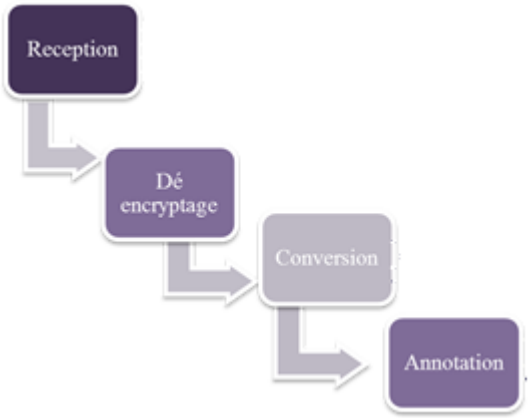


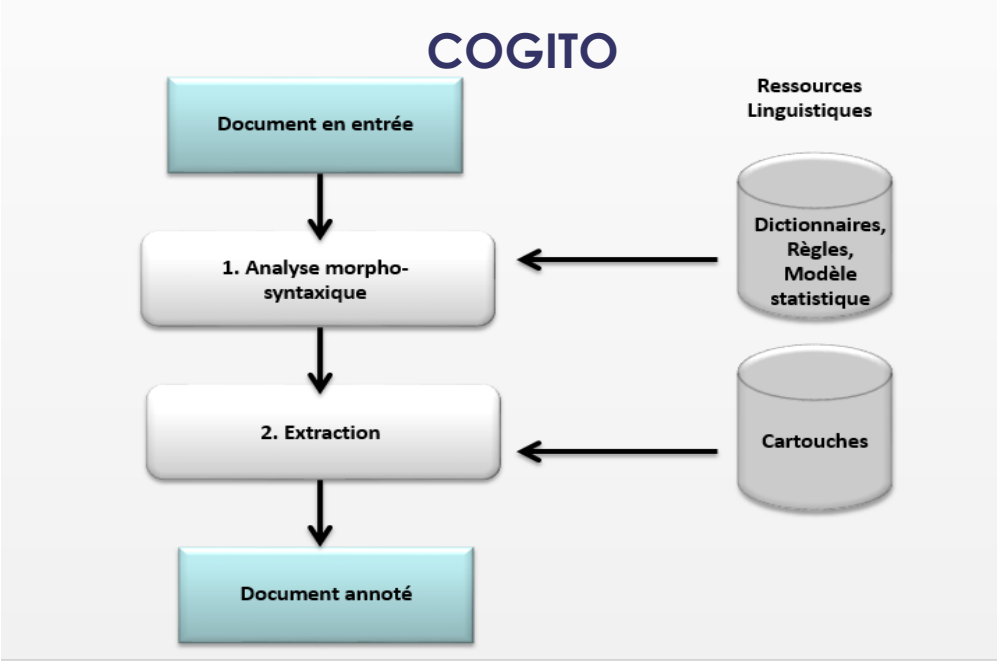
Mise à plat des transactions :



PROJET iTRAC

Résultats – Enrichissement et Analyse des données du darkweb





Cartouches utilisés par le modules d'extraction :

- CRIME TAX, basé sur Sensigrafo
- PATTERNS, utilisant des expressions régulières pour reconnaître les adresses bitcoin
- TM360, basé sur des lexiques pour extraire des entités nommées (noms, prénoms, pays, villes, montants, dates, etc.)

Résultats – Réflexion légale

- Analyse juridique des données en présence
- Analyse juridique des procédures applicables
- Analyse juridique des limites à l'utilisation de iTRAC
- Analyse juridique des traitements effectués

Conclusion

Principaux résultats:

- Un démonstrateur.
- Une réflexion sur les aspects légaux et juridiques.

Présentation à 2 utilisateurs potentiels et au ministère de la Justice:

- Tracfin.
- Cyber Douane.

Prochaines étapes:

- Prise en compte des contournements utilisés par les fraudeurs.
- Adaptation à d'autres crypto monnaies.

Systematic
Paris Region Digital Ecosystem

cap·digital
Paris Region

Finance Innovation
Projet labellisé

THALES

EXPERT SYSTEM

ALEPH

PAYMIUM

LIP6

PROJET iTRAC

bpifrance

îledeFrance

Caractéristiques du projet iTrac

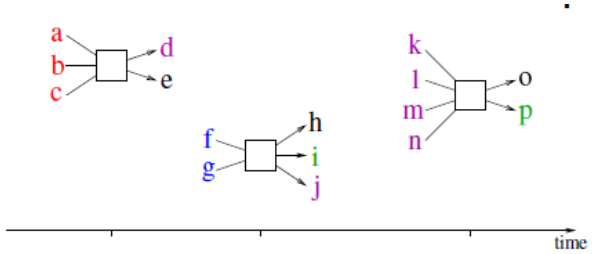
Nom du projet	iTRAC (Investigation par Traitement et Analyse des cryptomonnaies)
Appel à Projet	FUI 21
Date de début du projet	1er Juin 2016
Date de fin du projet	31 Mai 2019
Colabel des pôles	Cap Digital Finance Innovation Systematic
Financeurs	BPI Région Ile de France

Détails des traitements sur la chaine Bitcoin

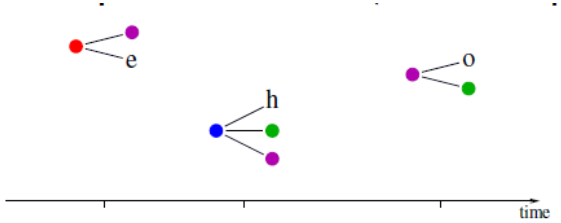
PROJET iTRAC

Conclusion

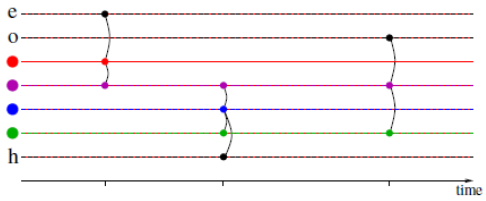
données brutes : transactions entre portefeuilles



fusion de portefeuilles (heuristiques)



transactions entre entités (individus, sociétés, ...)

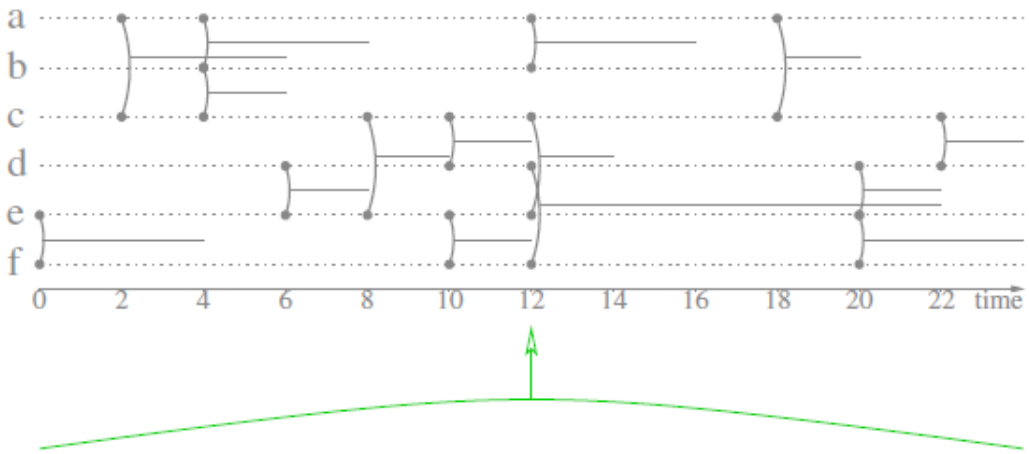


flot de liens entre entités (individus, sociétés, ...)

flots de liens – approche

analyser le flot de liens directement

flots de liens



graphes
et
réseaux

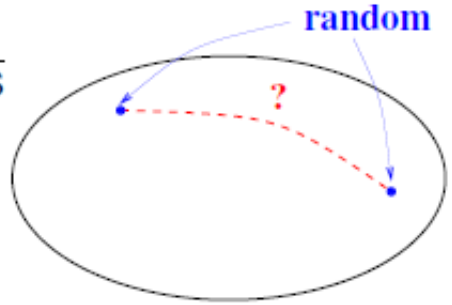
signaux, séries temporelles

flots de liens – densité

dans G :

proba que deux nœuds soient liés

$$\delta(G) = \frac{\text{nb liens}}{\text{nb liens possibles}} = \frac{2 \cdot m}{n \cdot (n-1)}$$

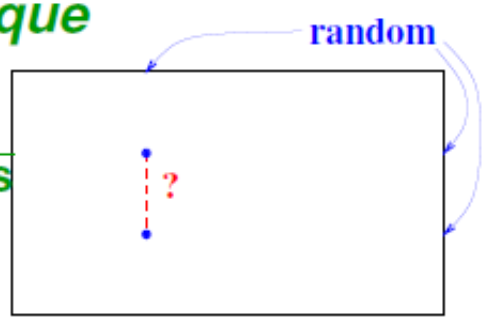


dans S :

proba que deux nœuds soient liés

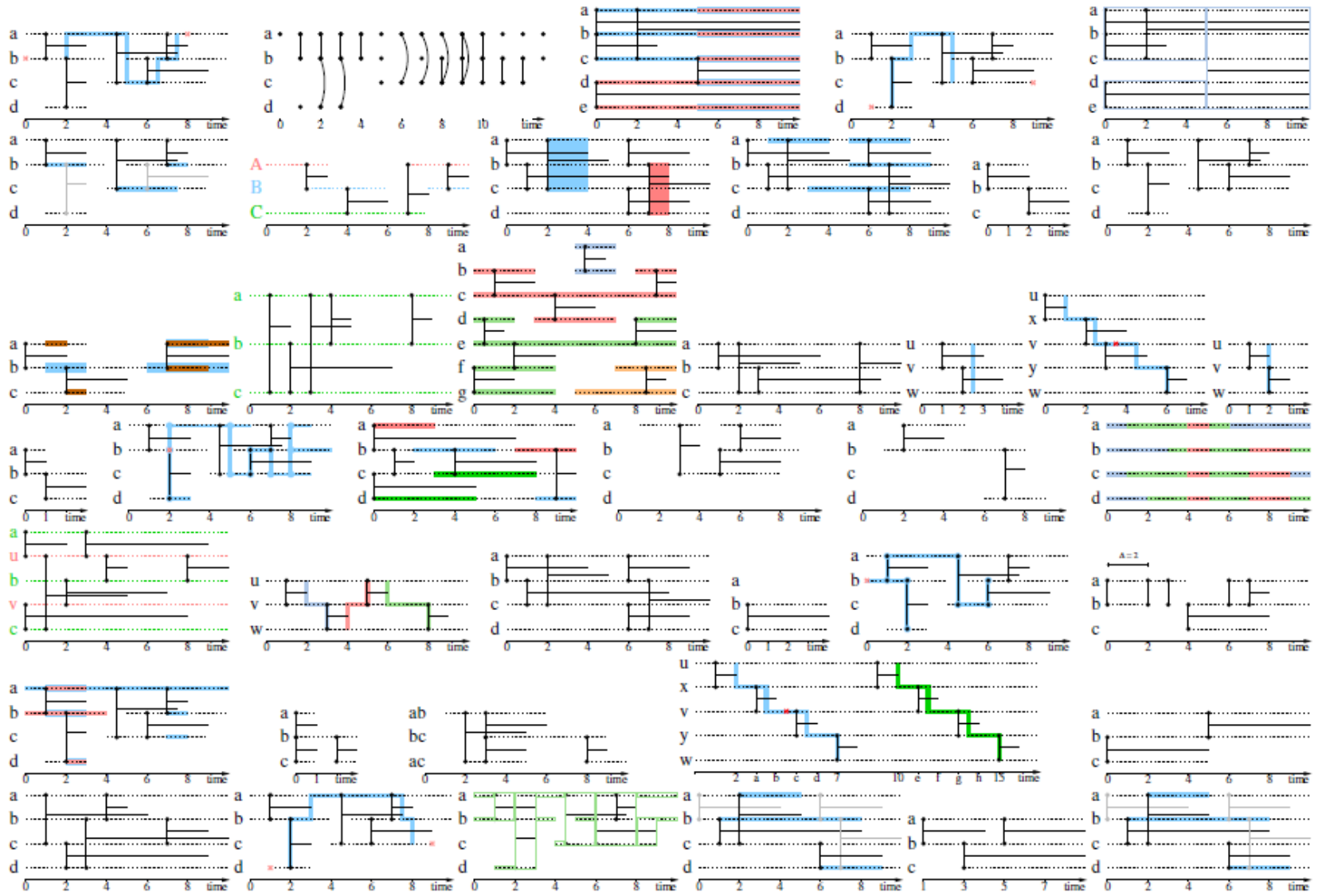
à un moment quelconque

$$\delta(S) = \frac{\text{nb liens}}{\text{nb liens possibles}} = \frac{\sum_{uv \in V \otimes V} |T_{uv}|}{\sum_{uv \in V \otimes V} |T_u \cap T_v|}$$



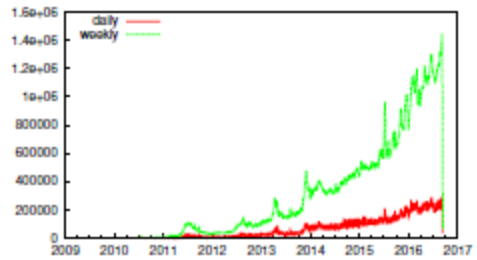
FUI FONDS UNIQUE INTERMINISTÉRIEL PROJET SÉLECTIONNÉ
PROJET iTRAC

formalisme flots de liens

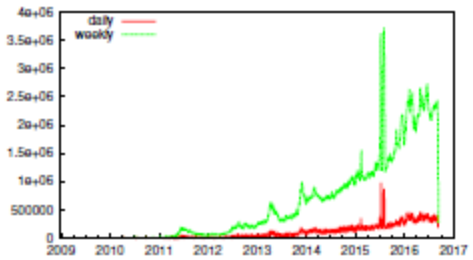


calculs sur les données

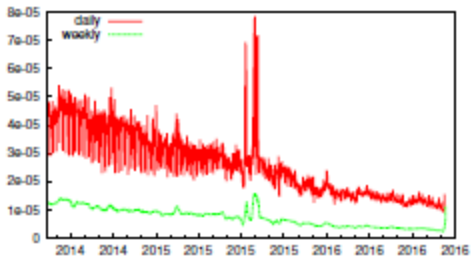
nb utilisateurs



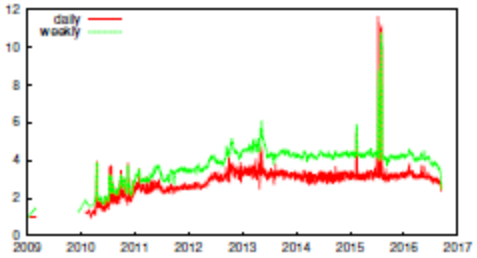
nb transactions



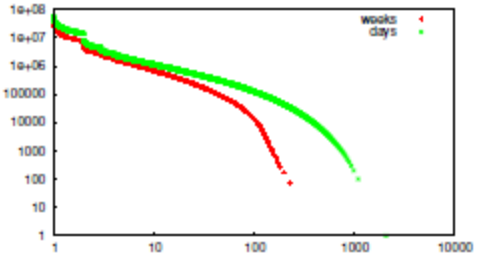
densité au cours du temps



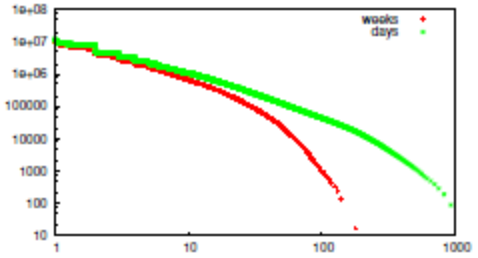
degré moyen au cours du temps



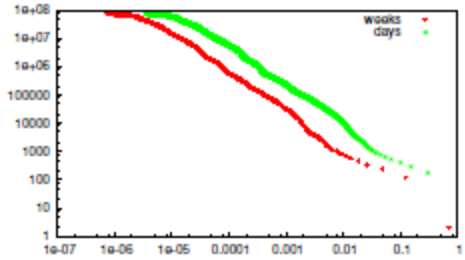
activité des nœuds



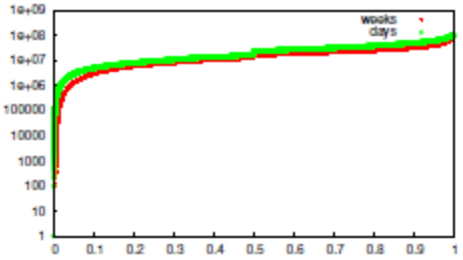
activité des liens



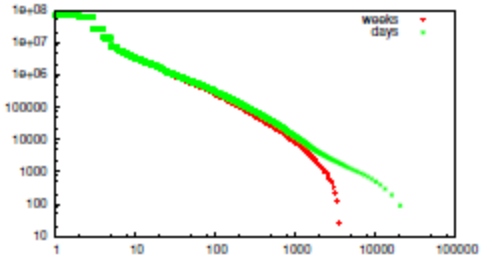
densité par nœud



densité par paire



distribution de degrés



Conclusion

Forte production scientifique :

- 7 journaux internationaux, 8 conférences internationales.
- + 2 conférences internationales invitées.
- + 3 thèses soutenues + 2 postdocs.

Briques logicielles et calculs :

- passage à l'échelle.
- librairie d'outils.

Fort enrichissement des données brutes :

- structure et dynamique.
- grand nombre de features.

Intégration dans le démonstrateur