Secure, Scalable Policy-enforced distributed data processing

using blockchain technologies

Example use-cases from airline industry relevant to digital marketplace (c1) & blockchain research (c2).

Improve passenger experience at airports

Improve efficiencies across multi modal logistic chains

iSHARE
powered by NLIP

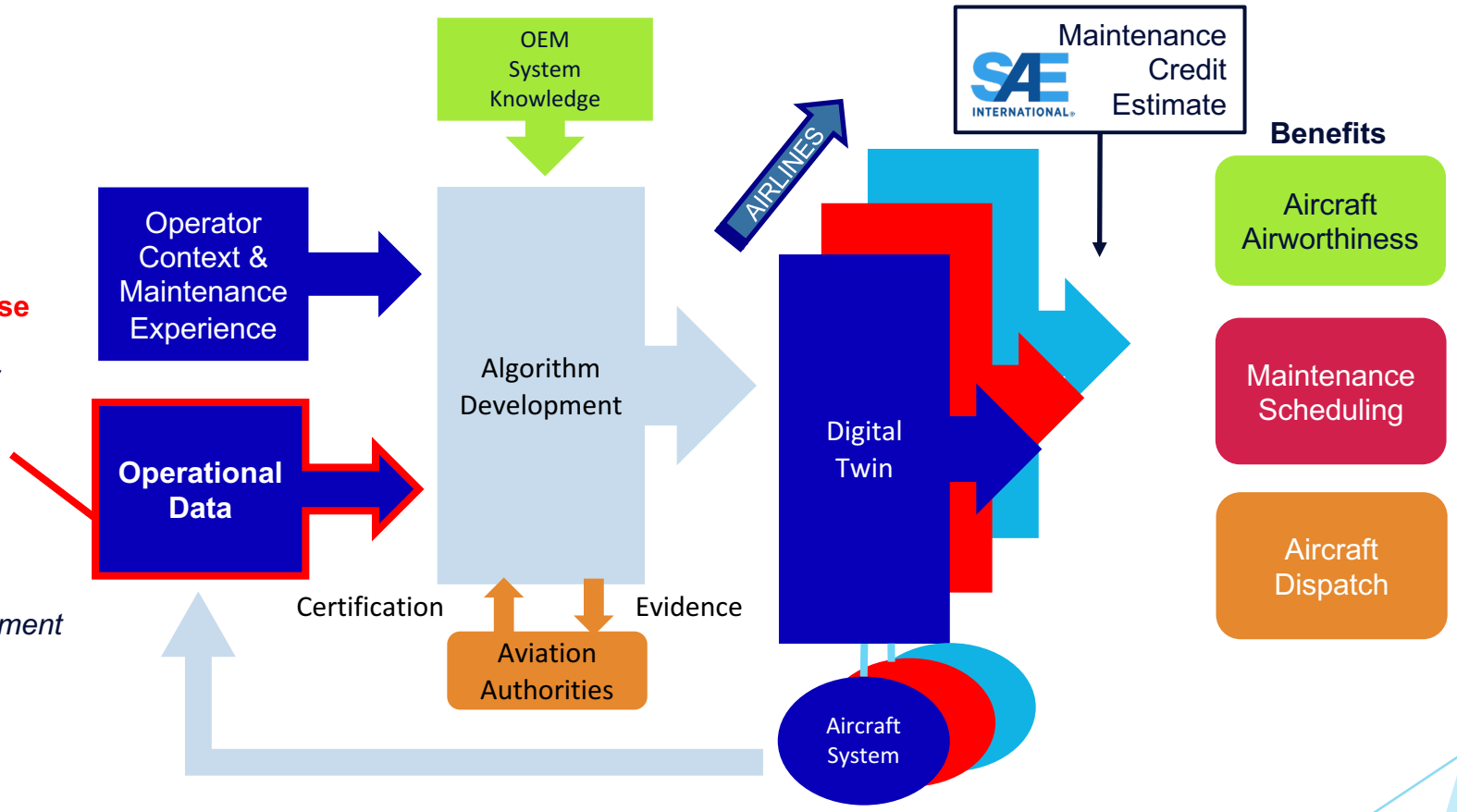
Increase fleet availability by improving maintenance scheduling by estimating maintenance credits from aircraft data.

SAE INTERNATIONAL

Maintenance Logistics driven by a digital twin

Research use case

How to unlock fair and economic big data asset sharing across airline operators as precondition for innovative algorithm development



Project description

Consider policy enforced data sharing and analysis across multiple IT domains based on negotiation of smart multi-party contracts to form temporary business alliances by:

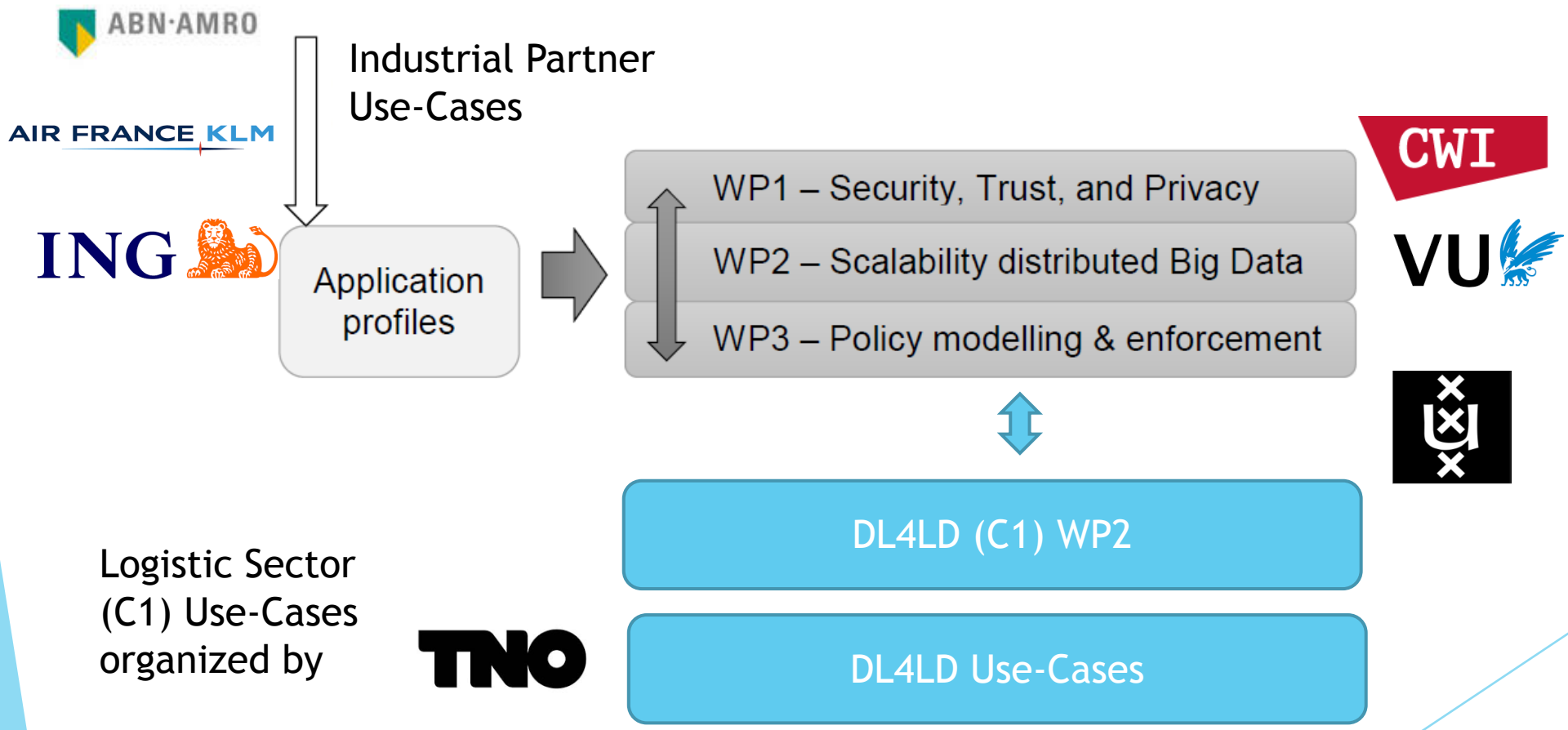
investigating the value that blockchain technology will bring

- Multidisciplinary fundamental and applied research
- Developing *integrated solution* for distributed dynamic data sharing
  - Secure
  - End-to-end trusted
  - Scalable
  - Future-proof
- Across multiple autonomous logistic domains
- Fundamental elements generically applicable

Project Goals

- Prove value of distributed Blockchain approaches to logistic use-cases
- Future proof cryptographic approach
  (against quantum computing and other high performance compute technologies)
- Provide an environment allowing parties to create data sharing agreements (compliant to rules and agreements within a digital market place) guaranteeing secure and trustworthy real time sharing of (big) data
- Provide secure and trustworthy mechanisms for compliancy checking using provenance trails and audit trails,
  and mechanisms for dispute settlement in case of breaches

Work packages



WP 1

Marc Stevens (PI), CWI Cryptology Group

Addresses challenges with future-proof (quantum-resistant) solutions based on cryptologic concepts that admit security proofs:

- Cryptographically secure ledger histories using non-parallelizable PoW systems;
- Robust consensus protocols compatible with non-parallelizable PoW systems;
- Admit light-weight clients that cannot store or process entire blockchain:
  - short cryptographic proofs of predicates,
    e.g., product stock is above order size, that a certain order has shipped;
- Mechanisms to share data privately to selected parties or specific purposes;
- Identity management, authentication and authorization

WP 2

Henri Bal, High.Perf. Dist.Comp G., VU

Develop a new high performance blockchain model

- High throughput of logistics information without scaling issues
- Bootstrapping, such that blockchain clients are able to synchronize blockchain data quickly with fewer data items to download, making it **acceptable for clients with restricted resources**
- high performance (cryptographic) primitives for accelerators (e.g. GPU, Xeon Phi) to increase throughput in verification of information transactions

WP3

Tom van Engers, Fac. of Law, UvA
Tijs van der Storm, Software Ana.&Transf., CWI
Cees de Laat, System and Network Eng.Lab, UvA
Sander Klous, Fac. of Science, UvA

Objectives of this work package

- Allowing parties to create data sharing agreements compliant to the digital market place policy thus guaranteeing secure and trustworthy real time sharing of big data.
- Augment the smart contract approach with additional expressiveness for modelling business and legal context.
- Leverage formal modelling, simulation and diagnosis of legal-institutional arrangements in business process compliance settings,
- Provide secure mechanisms for compliancy checking using provenance trails and audit trails, and mechanisms for dispute settlement in case of breaches.
- Secure a chain of custody, based on programmable distributed trust infrastructures developed with WP1 and WP2,

Data Logistics 4 Logistic Data (C1) + Secure scalable policy-enforced distributed data processing (C2) research proposal overview