



# **IoT- & Blockchain-enabled Security Framework for New Generation Critical Cyber-physical Systems in Finance Sector**

Topic: SU-DS05-2018: Digital Security, Privacy, Data Protection and Accountability In Critical Sectors

**Grant Number: 833326**

**Coordinator:** Prof. Atta Badii, University of Reading, UK

# Challenges

Cyber criminals have netted \$4.3 billion from digital currency exchanges, investors and users in 2019.

#users attacked by banking malware (like Trojans) was about 900 thousand with ~16% increase as compared to 2017

#users who encountered Android banking malware tripled to 1.8 million worldwide.

Cybercrime is the most commonly experienced fraud- 31% globally (2018)

Data analytics detected only 1% of frauds in the UK (compared to a global average of 4%) as of 2018

**Digital technologies are profoundly changing the financial sector, but also a source of massive threat**

Money  
laundering

Bribery  
and  
corruption


Accounting  
fraud

Consumer  
fraud

Cryptocurrency-  
related crime



**Enhance the regulation, accountability, infrastructure security and cost- effectiveness of financial markets and insurance processes to support the development of the European open market.**



**Protect Europe against illicit transactions, illegal money trafficking and fraud that can take place through the banking system clearing and financial transactions settlement process.**

# Systemic Objectives

Systematic identification of a holistic Digital Security, Privacy, Data Protection and Accountability in the Finance sector

Development of a Blockchain-based Integrity Layer ensuring accountability through active involvement of authorities

Proactive Preparedness through Modelling data flows and information modelling in selected use-cases covering context-aware anomalous flows alerting, blacklisting and whitelisting

Protecting the Critical Finance Infrastructure through hardware- and software-enabled “X-as-a-Service” model

Linking, mapping and adapting solution stack for use-cases in field trials with an elaborated assessment of cyber-physical practices

Technology validation and exploitation of the proposed framework in finance sector and Highway Toll payment systems



- ❑ **Concept and approach**
- ❑ Increased digitization, growing complexity of cyber-attacks certain sectors/subsectors more critically exposed e.g. banking, and financial market infrastructures as part of critical infrastructure
- ❑ Digitally transformative innovation has to support cyber security, privacy, accountability and efficiency.
- ❑ Standardization has to enable the rapid adoption of cybersecurity best practices in the domain;
- ❑ Need to promote common standards for conducting stress and resilience testing across systemic financial market infrastructures and institutions
- ❑ Need to certify companies/organisations that can perform accredited conformity tests.
- ❑ Asymmetries: New Kids on the Block sometimes operating in a Regulatory Void

# Opportunities

Cyber threats and frauds are increasing (>40% in 3 years)

Financial Entities (banks, governmental organizations, stock markets, etc) are accepted as CIs

Cyber threats and frauds cause gigantic economic loss (US\$13M → US\$18.5M/company from 2014 to 2017 years)

Blockchain industry is booming

Blockchain can reduce time & costs of contracting processes by saving €13-18B /year

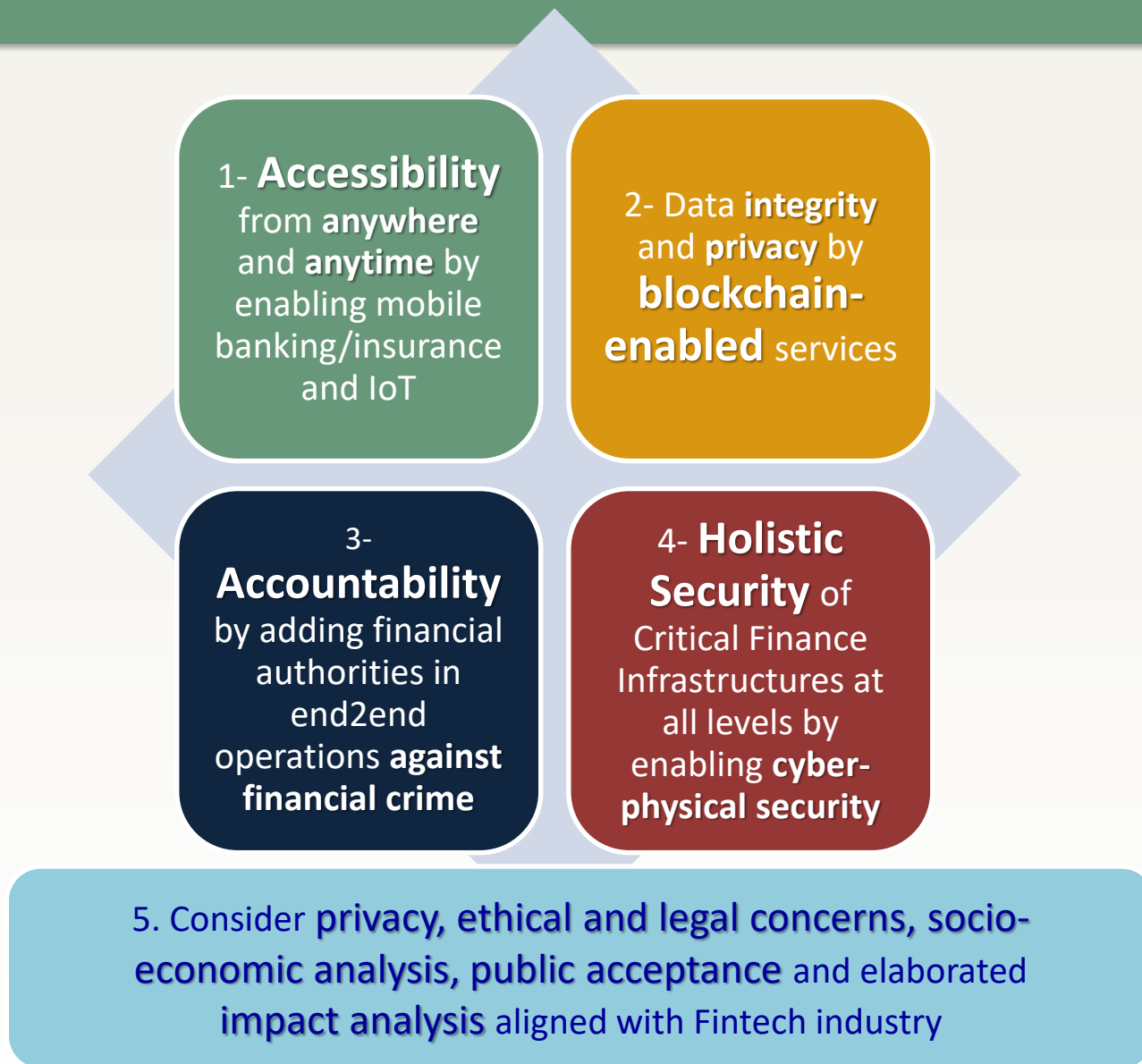
•Blockchain

•Cyber-physical Security

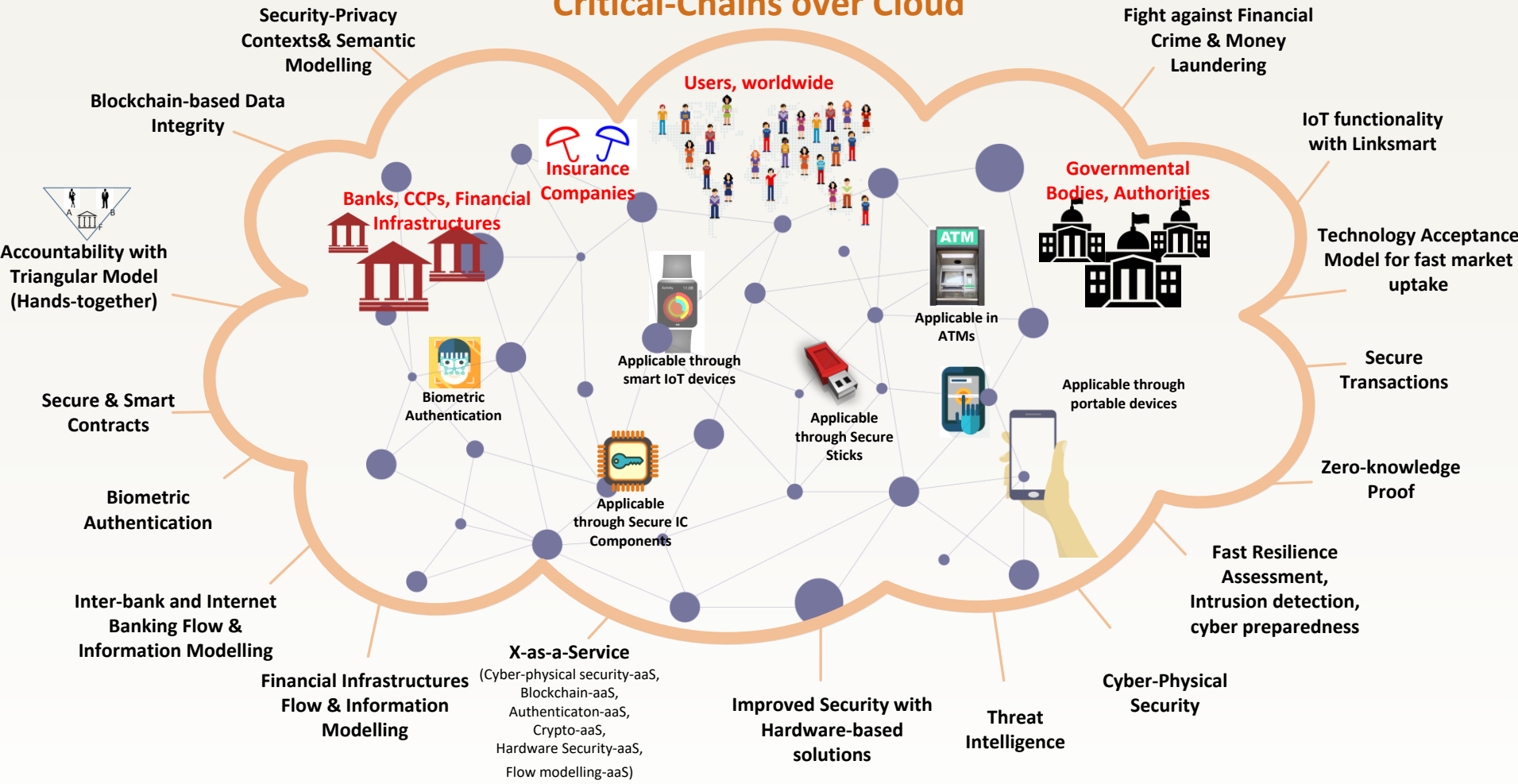
•Internet of Things (IoT)

IoT has become indispensable in Banking and finance sector (usage of mobile banking/payments >52%, 28% only by smartphone users)

IoT is booming (#connected devices > 75B in 2025)

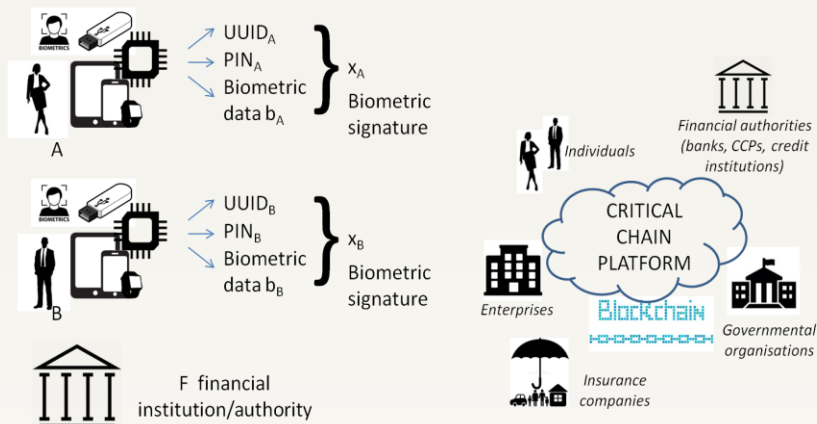


## Critical-Chains over Cloud



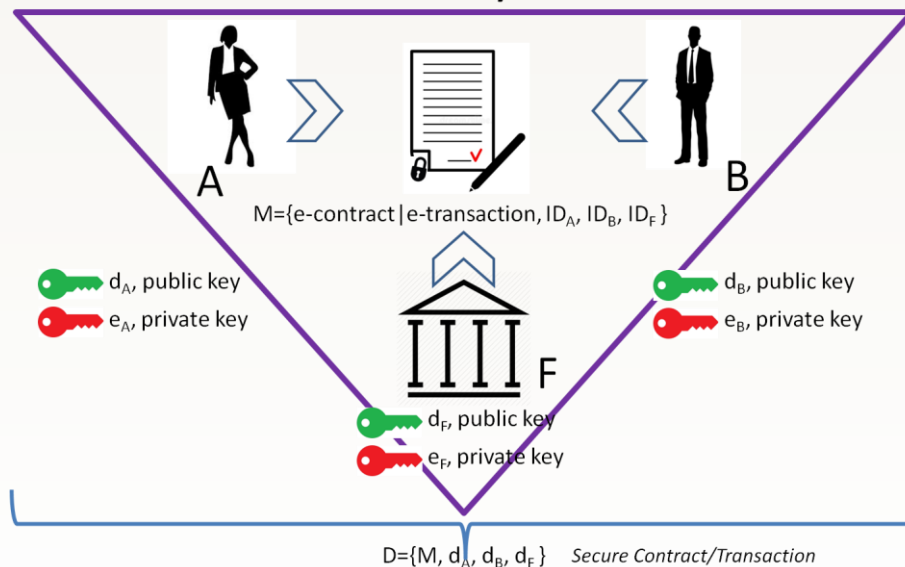


# The Accountability Model

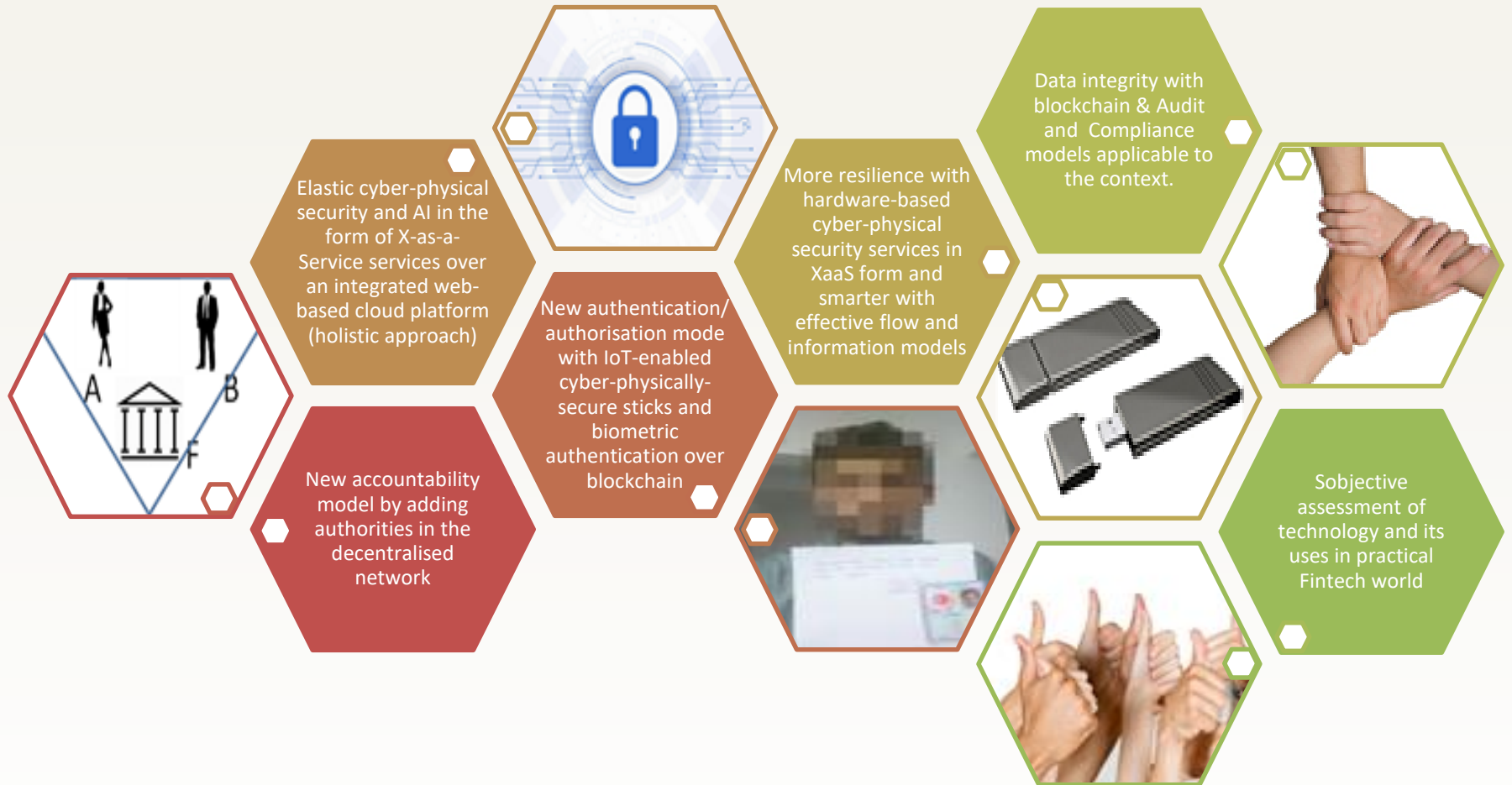


Accountability-by-design where financial authorities are put in multiparty blockchain-enabled triangular integrity and security for legal framework and further accreditation.

## Secure Contracts/Transactions



# What's new?



# Expected Results

- ❑ Development of new/enhanced, parameterized, automated and collaborative ICT tools for the financial sector as are needed for security, privacy, personal data protection and accountability requirements and to cope with the possible new risks arising from the compliance with new directives such as Open Banking (PSD2) and the EU Legislation on cybersecurity, privacy and personal data protection (GDPR) as well as cybersecurity standards (e.g. ISO27001, 27005).
- ❑ Delivering tools for making the exfiltration of data for attackers unattractive, both for 'data at rest' and 'data in transit'; considering incipient trends (e.g. digital on-boarding based on biometric data); and (iii) Enhanced collaboration with CERTs/CSIRTs.
- ❑ TRLs ranging from 5-6 initially and 7-9 as final deliverables

# Target End Users



Financial Sector,  
Internet Banking,  
Inter-Banking,  
Clearing



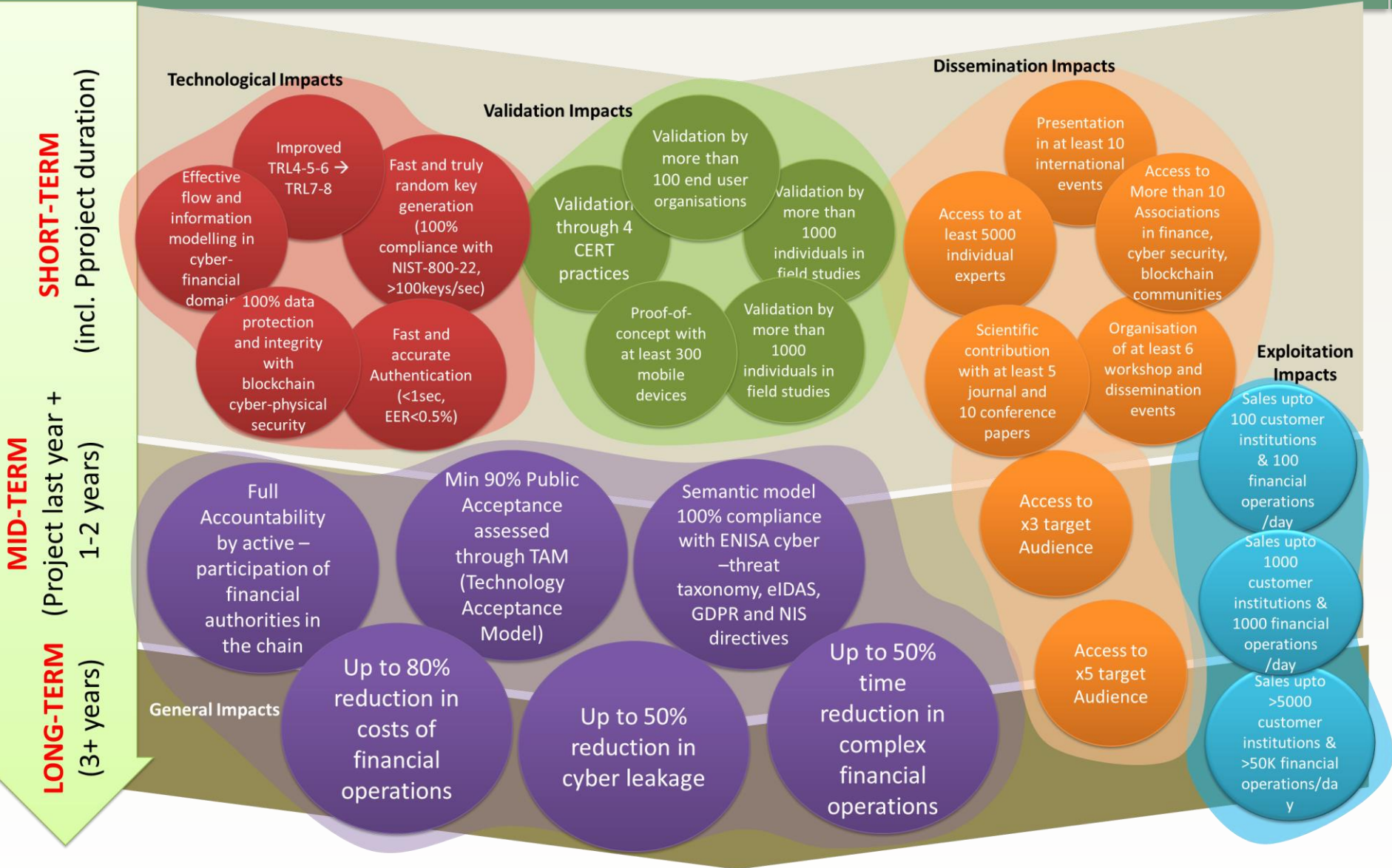
Insurance  
Processes



Highway Toll  
Collection



# Impact





**Development of resilience enhancing technologies and innovative solutions tailored for the finance domain, ensuring that a proactive preparedness helps financial market participants and infrastructures share information and better cope with technological shortfalls and support the objectives of regulated secure single open market in the financial sector.**

## Data Protection Aligned with GDPR

- Security & Intrusion Detection Data
- Requirement Engineering Data
- Usability Evaluation Data
- Highway Toll Data
- Website Click-through Cookies

## **Scalability:**

**Critical-Chains security measures for Blockchain transactions can also be used for cryptocurrencies**



# Main Project Events so far

- ❑ Project kick off meeting @ Reading, UK, 7-8 July 2019
- ❑ Clustering Workshop on “**Ethics of Blockchain**” on 17th December 2019, University of Reading, Park Campus, UK

## Workshop Themes:

- ❑ Avoiding Irreversibilities in BlockChain Futures
- ❑ No User Empowerment without User Informedness
- ❑ No Accountability without Answerability

