CRITICAL CHAINS

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

CRITICAL CHAINS

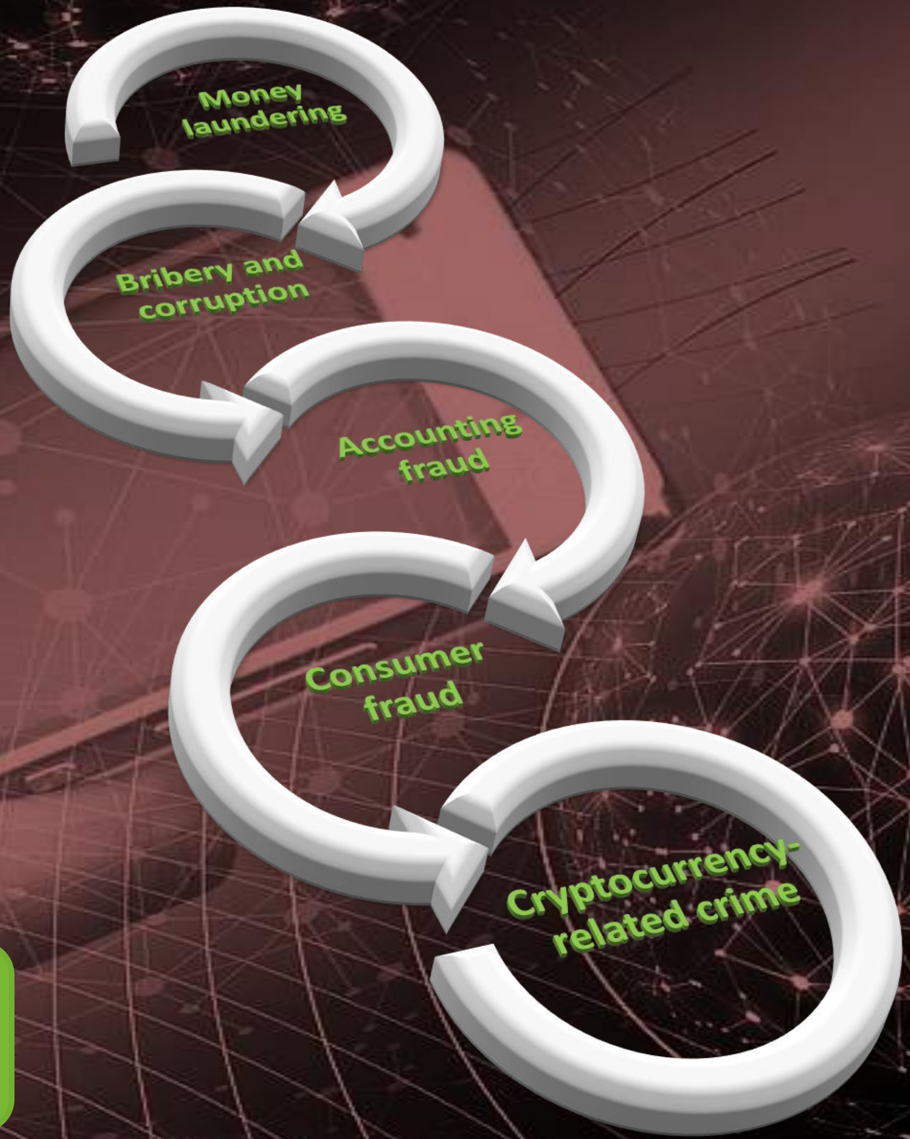
Cyber criminals have netted $4.3 billion from digital currency exchanges, investors and users in 2019.

#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

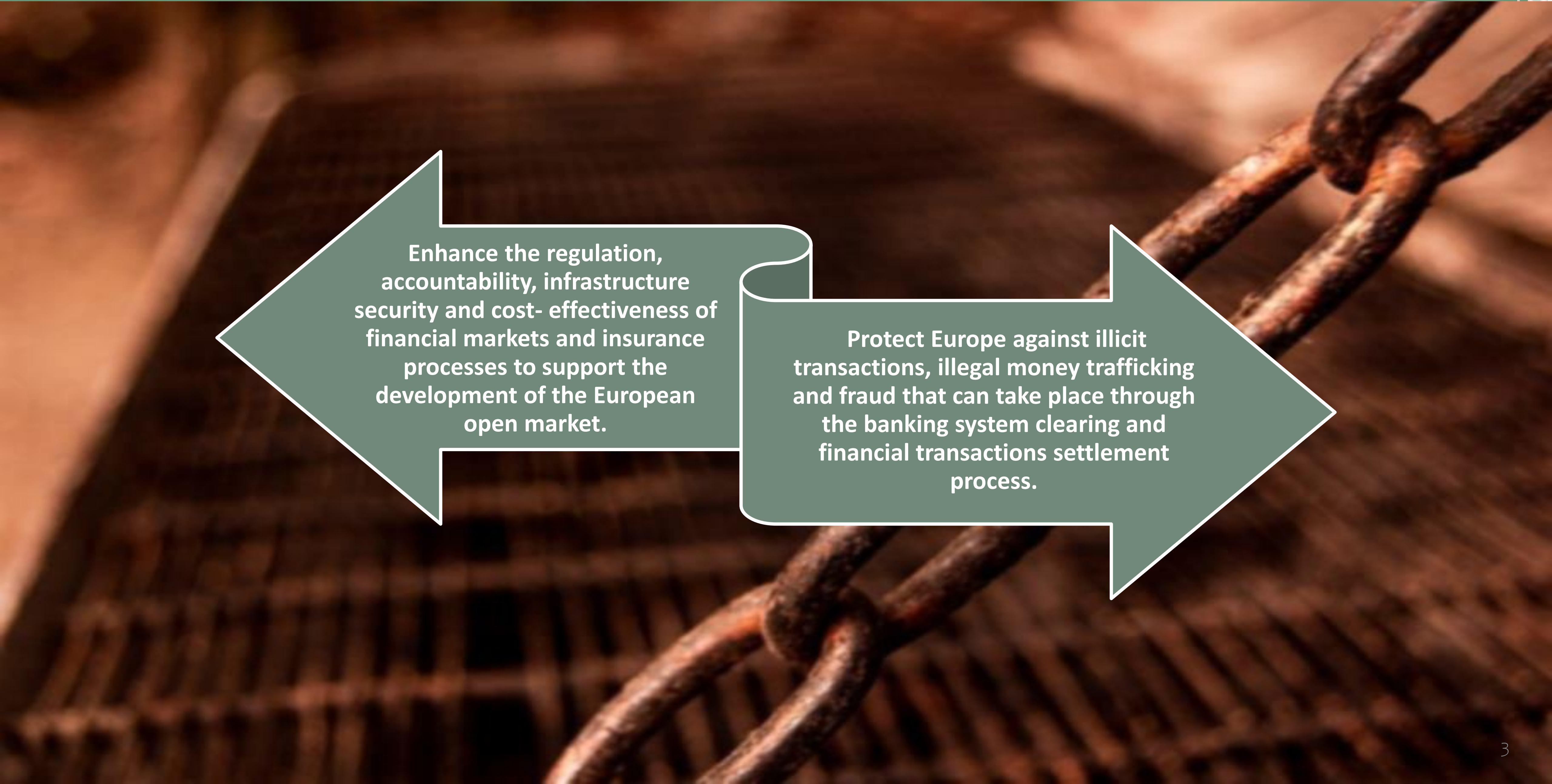


Digital technologies are profoundly changing the financial sector, but also a source of massive threat

https://cointelegraph.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study
https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2018---uk-findings.html
Kapersky. *Financial Cyber threats in 2018.* March 07, 2 https://securelist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019).

Image from https://www.piqsels.com

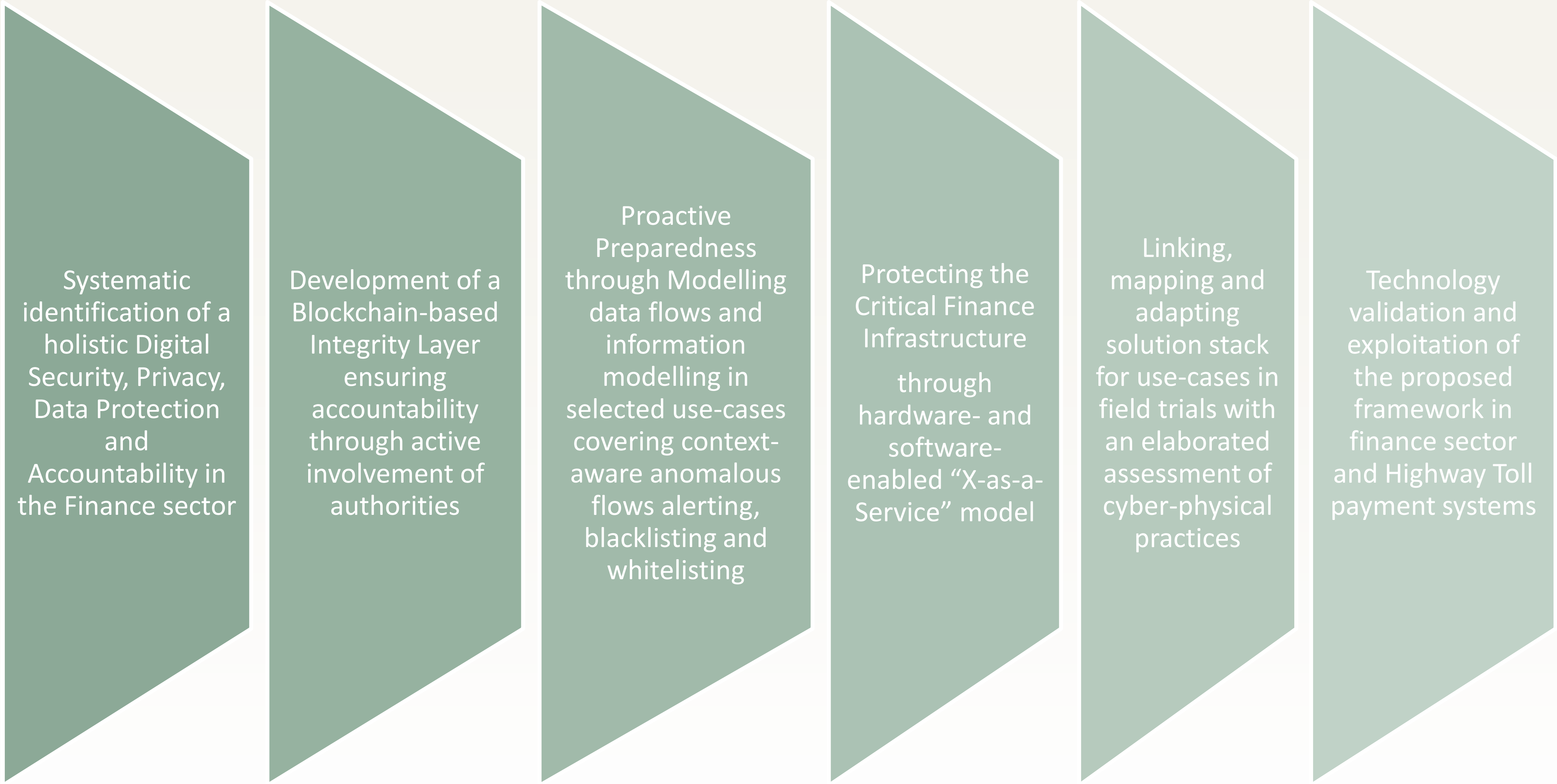
Strategic Objectives



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

Support cyber security, privacy, accountability and efficiency

Standardization

Enable the rapid adoption of cybersecurity best practices in the domain

Need to promote common standards

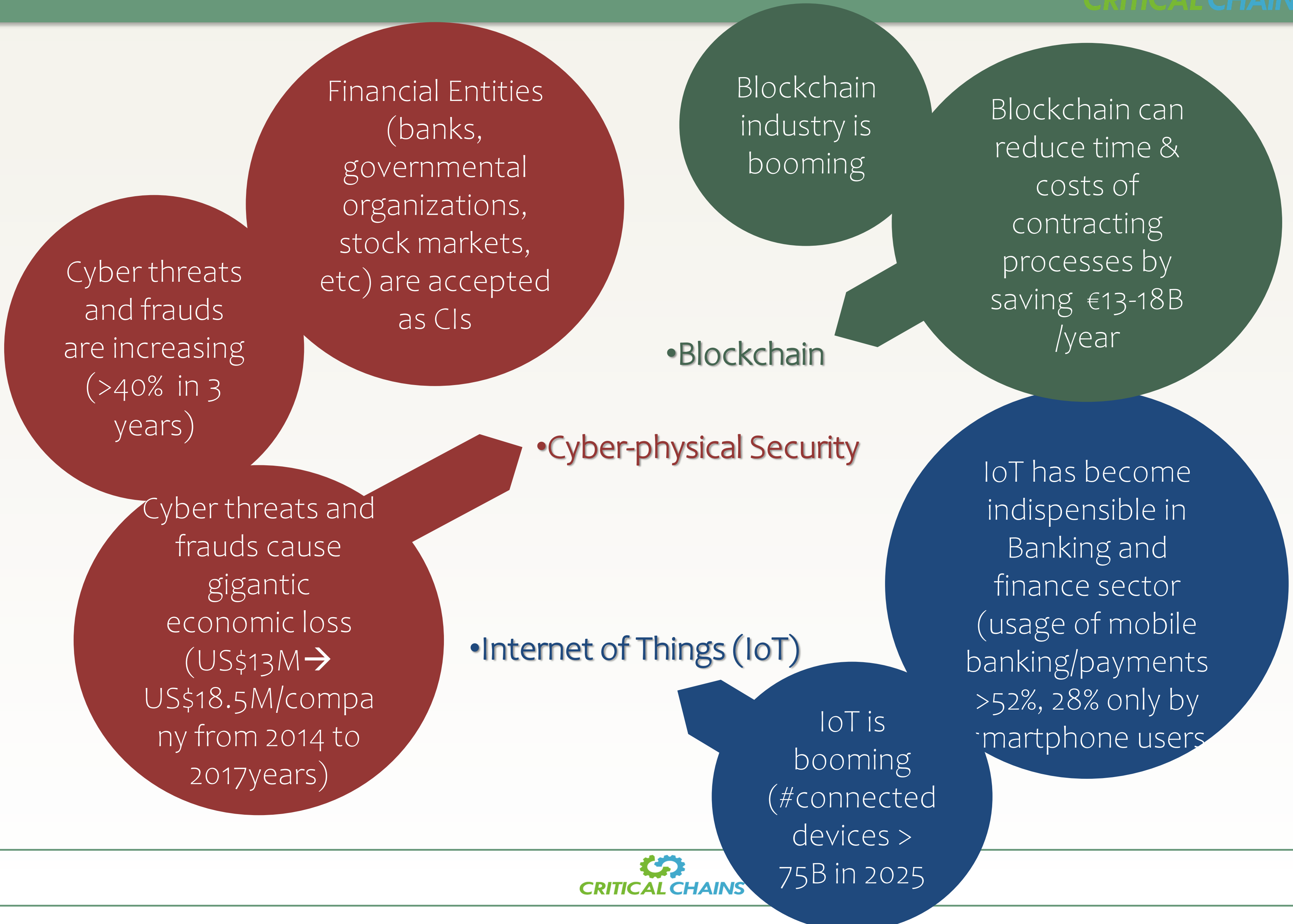
Conducting stress and resilience testing across systemic financial market infrastructures and institutions

Need to certify companies/organisations

Perform accredited conformity tests

Asymmetries: New Kids on the Block sometimes operating in a Regulatory Void

Opportunities



- Cyber-physical Security

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

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

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

- Blockchain

Blockchain industry is booming

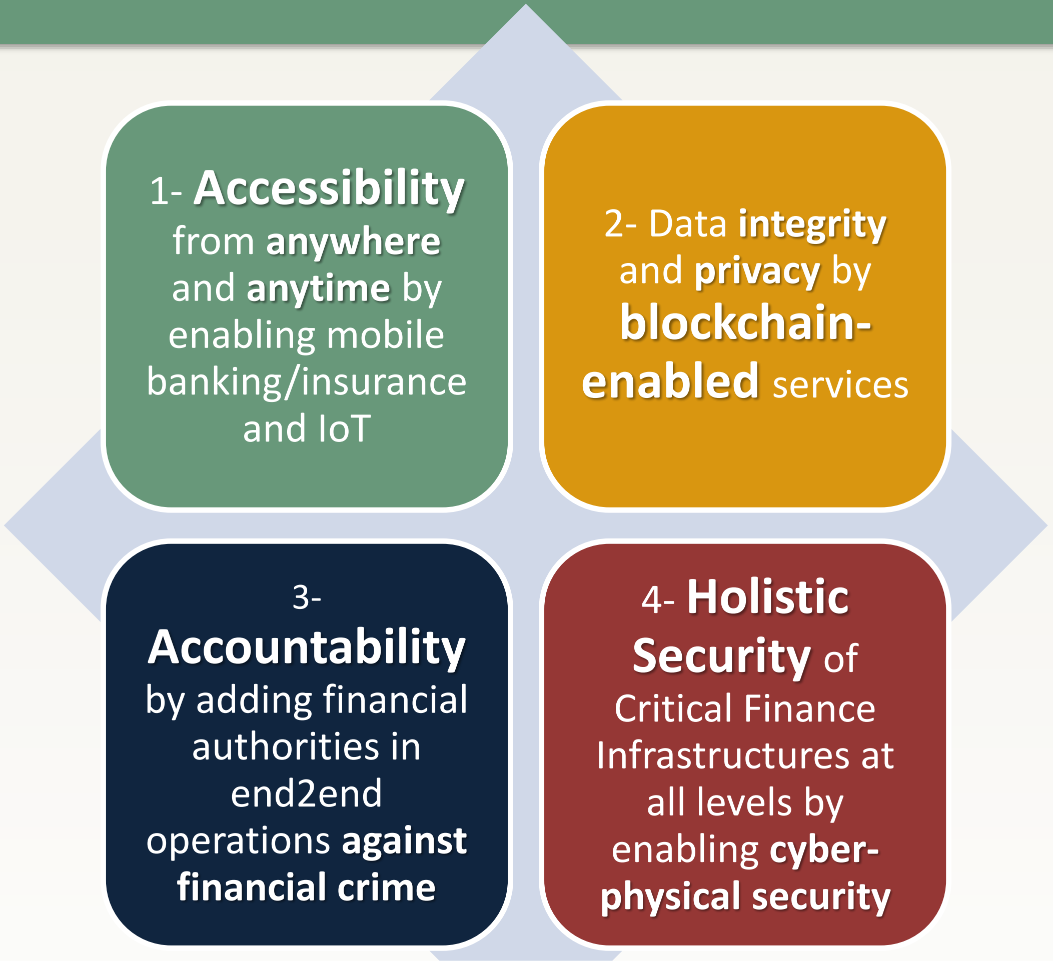
Blockchain can reduce time & costs of contracting processes by saving €13-18B /year

- Internet of Things (IoT)

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

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

Innovation Pillars



1- **Accessibility** from **anywhere** and **anytime** by enabling mobile banking/insurance and IoT

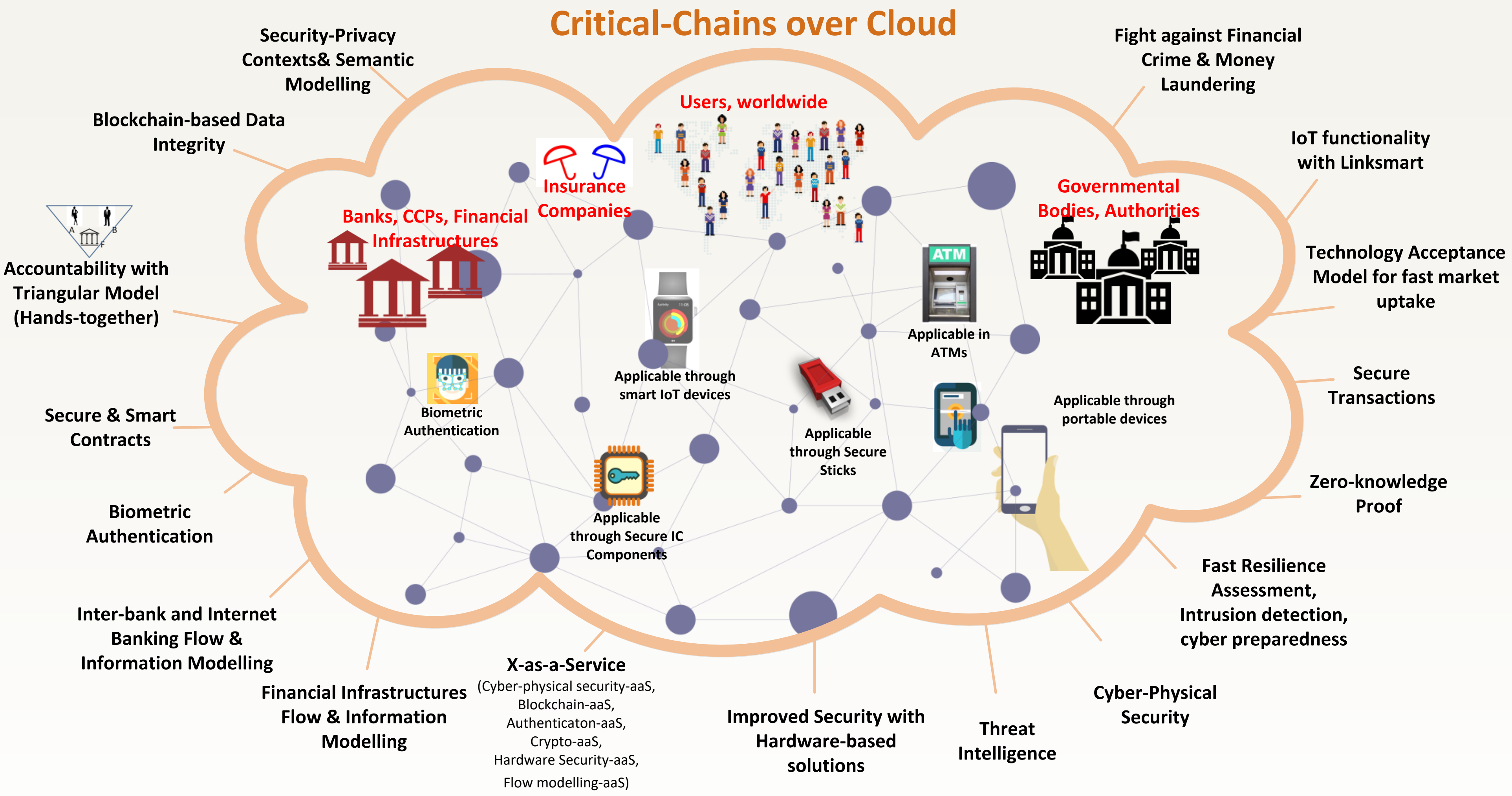
2- Data **integrity** and **privacy** by **blockchain-enabled** services

3- **Accountability** by adding financial authorities in end2end operations **against financial crime**

4- **Holistic Security** of Critical Finance Infrastructures at all levels by enabling **cyber-physical security**

5. Consider **privacy, ethical and legal concerns, socio-economic analysis, public acceptance** and elaborated **impact analysis** aligned with Fintech industry

Solution Stack



Critical-Chains over Cloud

Security-Privacy Contexts& Semantic Modelling

Blockchain-based Data Integrity

Accountability with Triangular Model (Hands-together)

Secure & Smart Contracts

Biometric Authentication

Inter-bank and Internet Banking Flow & Information Modelling

Financial Infrastructures Flow & Information Modelling

X-as-a-Service
(Cyber-physical security-aaS,
Blockchain-aaS,
Authenticaton-aaS,
Crypto-aaS,
Hardware Security-aaS,
Flow modelling-aaS)

Improved Security with Hardware-based solutions

Threat Intelligence

Cyber-Physical Security

Fast Resilience Assessment, Intrusion detection, cyber preparedness

Zero-knowledge Proof

Secure Transactions

Technology Acceptance Model for fast market uptake

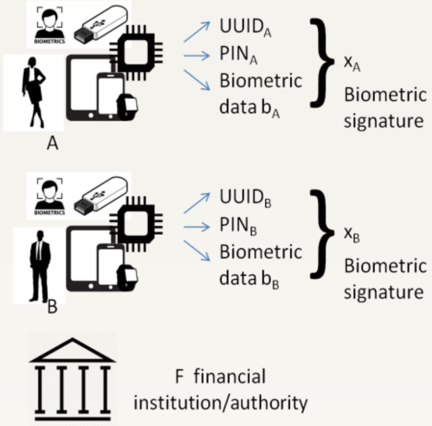
IoT functionality with Linksmart

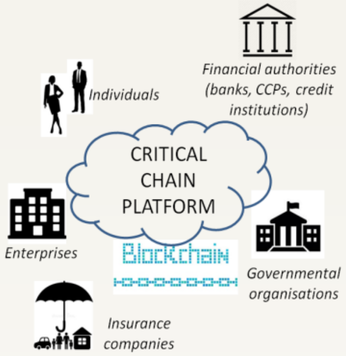
Fight against Financial Crime & Money Laundering

Users, worldwide
Insurance Companies
Banks, CCPs, Financial Infrastructures
Governmental Bodies, Authorities
ATM
Applicable in ATMs
Applicable through smart IoT devices
Biometric Authentication
Applicable through Secure Sticks
Applicable through portable devices
Applicable through Secure IC Components
A
B
F

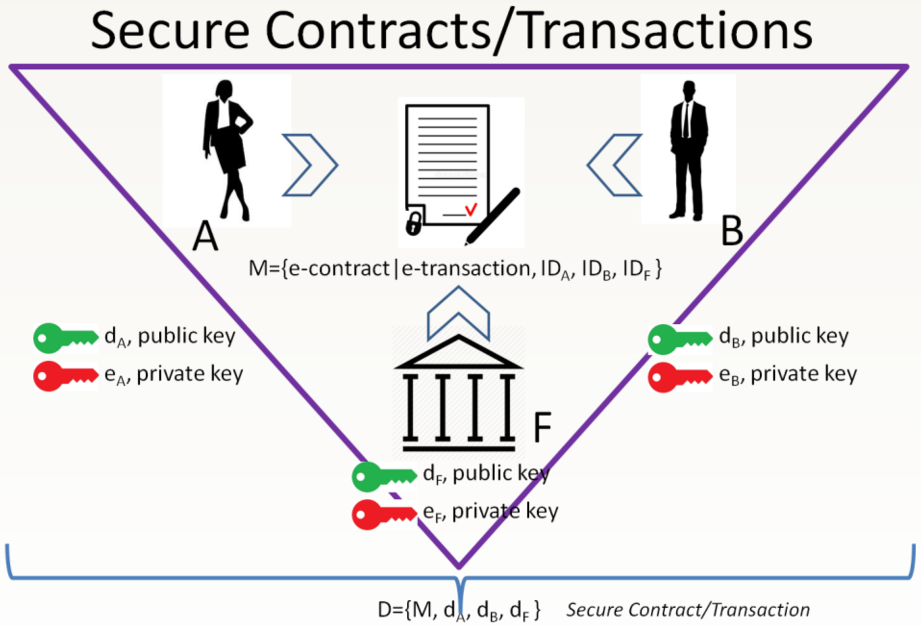
CRITICAL CHAINS

The Accountability Model

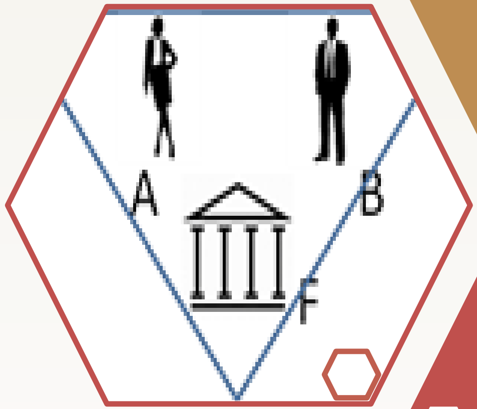



Individuals
Financial authorities (banks, CCPs, credit institutions)
CRITICAL CHAIN PLATFORM
Blockchain
Enterprises
Governmental organisations
Insurance companies

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
A
B
M={e-contract|e-transaction, ID$_A$, ID$_B$, ID$_F$ }
d$_A$, public key
e$_A$, private key
d$_B$, public key
e$_B$, private key
F
d$_F$, public key
e$_F$, private key
D={M, d$_A$, d$_B$, d$_F$ }
Secure Contract/Transaction

What’s new?



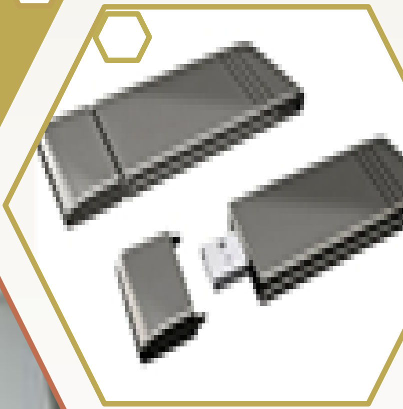
Elastic cyber-physical security and AI in the form of X-as-a-Service services over an integrated web-based cloud platform (holistic approach)

New accountability model by adding authorities in the decentralised network

New authentication/ authorisation mode with IoT-enabled cyber-physically-secure sticks and **biometric authentication over blockchain**

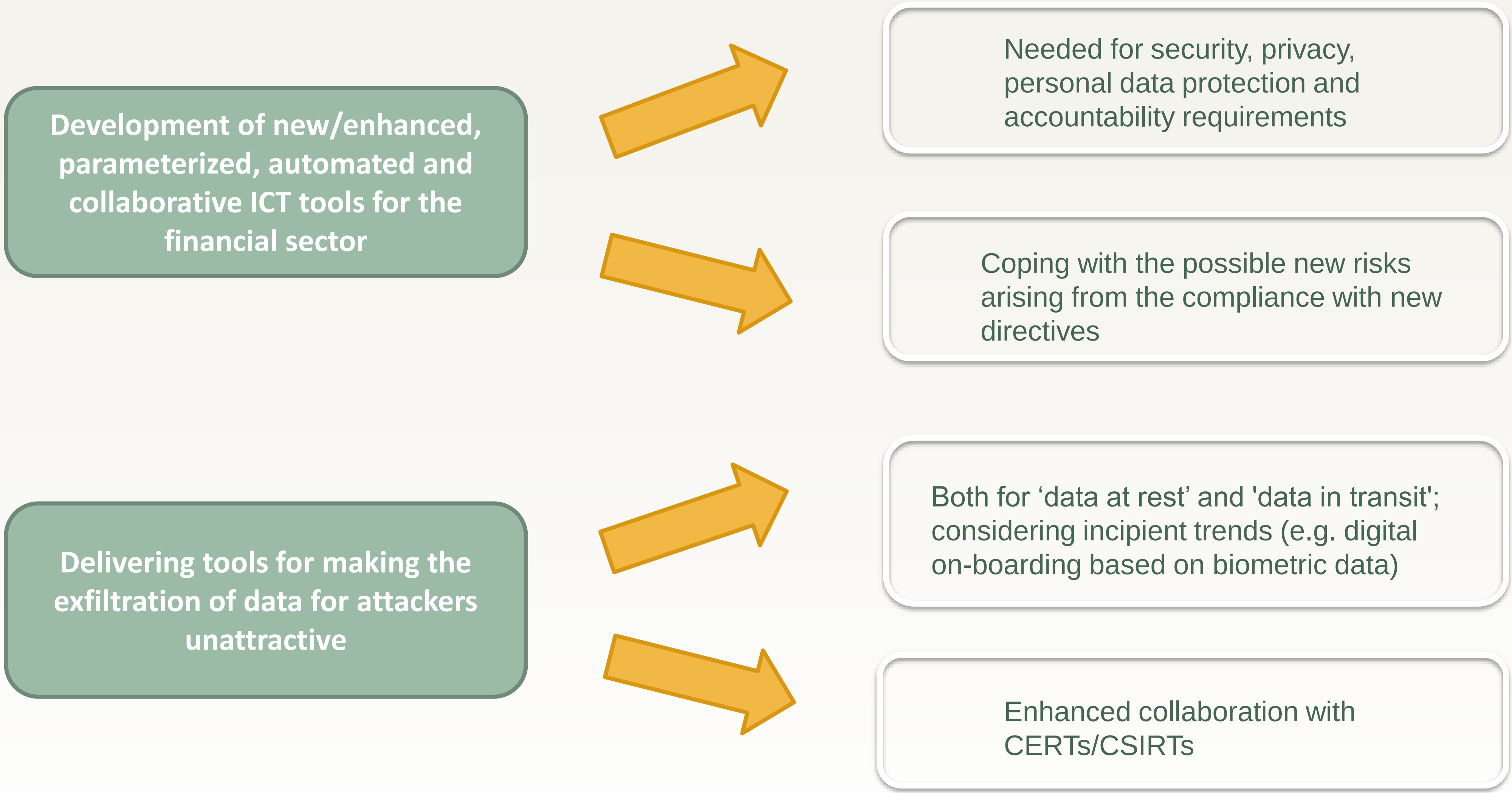
More **resilience with hardware-based cyber-physical security services** in XaaS form and smarter with effective flow and information models

Data integrity with blockchain & Audit and Compliance models applicable to the context.



Subjective assessment of technology and its uses in practical Fintech world

Expected Results



Development of new/enhanced, parameterized, automated and collaborative ICT tools for the financial sector

Needed for security, privacy, personal data protection and accountability requirements

Coping with the possible new risks arising from the compliance with new directives

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)

Enhanced collaboration with CERTs/CSIRTs

TRLs ranging from 5-6 initially and 7-9 as final deliverables

Expected Results

- ❑ **Critical-Chains Main Framework:**
  - Cloud-based data transmission, communication and financial transactions horizontal framework
- ❑ **Cyber-Physical Security as a Service**
  - Blockchain-as-a-Service
  - Authentication-as-a-Service: Authentication and authorization services using secure IoT sticks and biometric authentication.
  - Cryptography-as-a-Service
  - Data and information security and privacy preservation at all layer of cloud
- ❑ **Flow Modelling-as-a-Service:**
  - Data flow and information modelling
- ❑ **Audit and check the compliance of the entire Critical-Chains-supported financial processes to legislative framework**

Target End Users

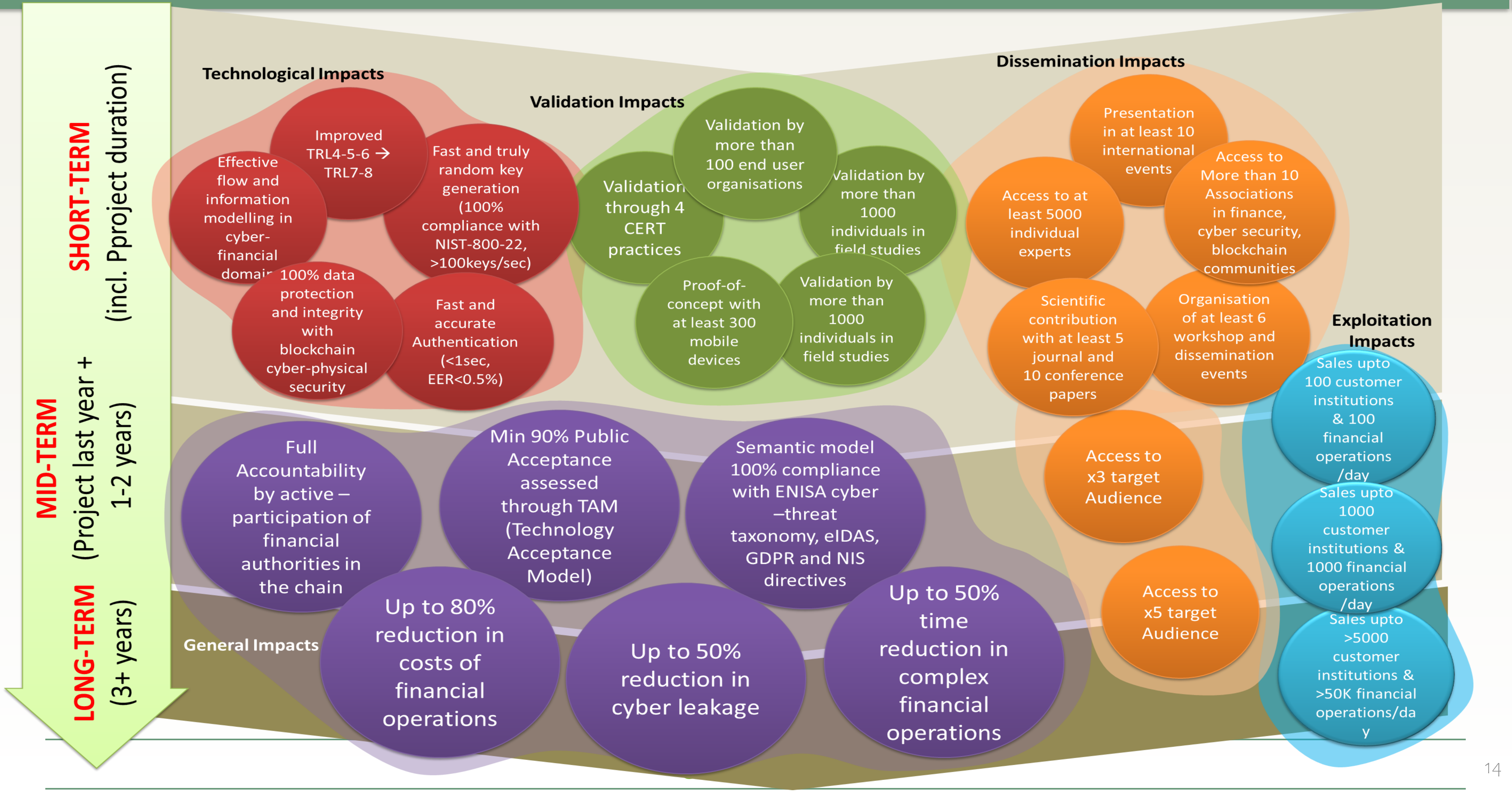
Use Cases and Target Sectors

Financial Sector, Internet Banking, Inter-Banking, Clearing

Insurance Processes

Highway Toll Collection

Impact



SHORT-TERM
(incl. Pproject duration)

MID-TERM
(Project last year + 1-2 years)

LONG-TERM
(3+ years)

Technological Impacts

Improved TRL4-5-6 → TRL7-8

Effective flow and information modelling in cyber-financial domain

Fast and truly random key generation (100% compliance with NIST-800-22, >100keys/sec)

100% data protection and integrity with blockchain cyber-physical security

Fast and accurate Authentication (<1sec, EER<0.5%)

Validation Impacts

Validation through 4 CERT practices

Validation by more than 100 end user organisations

Validation by more than 1000 individuals in field studies

Proof-of-concept with at least 300 mobile devices

Validation by more than 1000 individuals in field studies

Dissemination Impacts

Presentation in at least 10 international events

Access to at least 5000 individual experts

Access to More than 10 Associations in finance, cyber security, blockchain communities

Scientific contribution with at least 5 journal and 10 conference papers

Organisation of at least 6 workshop and dissemination events

Access to x3 target Audience

Access to x5 target Audience

Exploitation Impacts

Sales upto 100 customer institutions & 100 financial operations /day

Sales upto 1000 customer institutions & 1000 financial operations /day

Sales upto >5000 customer institutions & >50K financial operations/day

Full Accountability by active – participation of financial authorities in the chain

Min 90% Public Acceptance assessed through TAM (Technology Acceptance Model)

Semantic model 100% compliance with ENISA cyber –threat taxonomy, eIDAS, GDPR and NIS directives

General Impacts

Up to 80% reduction in costs of financial operations

Up to 50% reduction in cyber leakage

Up to 50% time reduction in complex financial operations

EU Policy Aspects, Data Protection, Scalability

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

Contact us!

Critical Chains Website: https://research.reading.ac.uk/critical-chains/

Twitter: https://twitter.com/ChainsH2020

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

Thank you for your kind attention!

Atta Badii – University of Reading

Critical Chains Project Coordinator

atta.badii@reading.ac.uk