Critical-Chains

Collaborative Project

Project Start Date 1st July 2019

Duration 36 Months

Deliverable D7.2 (Public)

Critical-Chains Bulletin: a report on dissemination, exploitation and list of outcomes (b)

Published by the Critical-Chains Consortium

Version 6.2 Date: 30/06/2021

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP7

Document Responsible: RINA-C

Contributors: All

Status: Final

ABSTRACT

D7.2 “Critical-Chains Bulletin: A report on dissemination, exploitation and list of outcomes (b)” has been submitted in the framework of Critical-Chains WP7 “Dissemination, Standardisation, Exploitation and Innovation Management”.

The aim of this deliverable is to:

- Present the communication strategies to deliver Critical-Chains innovation across Europe
- Shows all the content created to promote the Critical-Chains project
- Provides an overview of links with relevant projects/initiatives/experts in the field to disseminate project results and facilitate exchange of knowledge in workshops, conferences etc.
- Lists all the communication and dissemination activities performed to promote the project
- Presents the exploitation strategy building process and preliminary analysis to inform the Critical- Chains value proposition and exploitation planning

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Deliverable D7.1 Document History

Versioning			
Version Number	**Date**	**Contributors' name and organisation**	**Changes**
V0	30-05-2021	RINA-C	1st Draft
V6	09-02-2022	UREAD	Various changes post establishment of the limits of actual R&D effort of respective Partners and the clarification of the exploitation plans
V6.1	20-06-2022	RINA-C	Enhancement of the quality of diagrams
V6.2	30-06-2022	UREAD	Review, edits throughout and re-formatting

Internal Review History

Internal Reviewers	**Date**	**Comments**
Atta Badii	01-02-2022	C&D table and Exploitation tables need to be finalised
Srivenkata Srikanth	03-01-2022	Quality Check and lay-out refinements

Table of Contents

Table of Figures

List of Tables

Executive Summary

D7.2 aims at highlighting all the outcomes achieved from M12 to M24 in the context of the communication, dissemination, and exploitation strategy of Critical-Chains.

This includes the following main results:

- Outcome 1: Project Identity
- Outcome 2: Communication & Dissemination Strategy
- Outcome 3: Channels
- Outcome 4: Editorial Plan
- Outcome 5: Project Promotional Contents
- Outcome 6: Performed Events
- Outcome 7: Exploitation Strategy building up process

1 Introduction

The Project Objectives are to develop an integrated effective, accessible, fast, secure and privacy-preserving financial contracts and transaction solutions. This is to protect against illicit transactions, illegal money trafficking and fraud that can take place through the banking clearing system and financial transactions settlement process. Thus, the objectives of the project are in the public interest. The planned Research and Innovation work involves the use of the following data types of the participants for their respective purposes as outlined in this section:

- Anonymised Inter-bank data relating to fund transfers as required for clearing funds;
- Anonymised fund transfers from sender to receiver accounts;
- Anonymised user-expressed system requirements and usability evaluation data;
- Minimal profiling of data as essential for anonymized users' requirements and usability clustering analysis, or anonymised transactions for clustering and aggregated analysis;
- Facial Images which are encrypted and stored for authentication and identity management. This is needed to support authentication, auditability and accountability. The "Critical-Chains" system will not have any access to the encrypted images but will receive the results of the success or failure of the authentication process.

The technologies to be deployed consist of:

- transaction and financial dataflow analytics and modelling of the financial transactions clearing and claim settlement processes;
- secure and smart use of Blockchain for data integrity checking, by involving financial institutions in the distributed Blockchain network;
- cyber security protection of Inter-Banks and Internet Banking, insurance and financial market infrastructures;
- Privacy protection through secure access supported by embedded systems and Internet-of-Things security;
- Critical-Chains is to be validated using four case studies aligned with four critical sectors: banking, financial market infrastructures, the insurance sector, and Highway Toll collection. The validation will include evaluating system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy to the rest of the world. The Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector.

1.1 Scope of the Deliverable

This deliverable reports on the entire set of the dissemination activities undertaken by the Critical-Chains Consortium during the first two years of the project. This includes the description of each activity type in terms of dissemination channel, space, place and focus of the activity and the outcomes as shallbe detailed in the following sections.

2 Outcome 1: Project Identity

In order to make the project stand out and to build a solid and long-lasting visual identity that can be easily recognised by potential stakeholders, a project identity has been developed by RINA C.

The project identity is made up of:

- Critical-Chains Logo
- Promotional Payoff

2.1 Logo

According to the Psychology of colours, blue and green provide a sense of security and promote trust in a brand. Both colours are associated with reliability.

Therefore, the Critical-Chains logo has been designed in green and blue to inspire trust in the project.

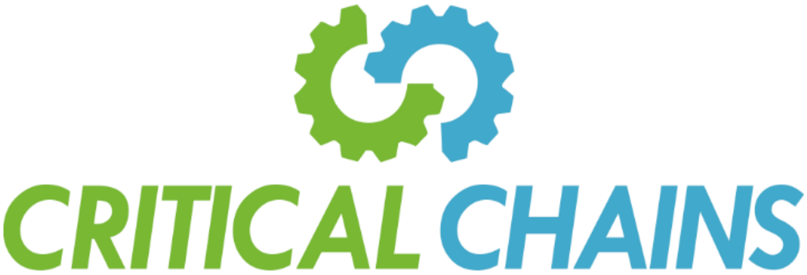


Figure 1: Critical-Chains Project Logo

2.2 Promotional Payoff

A promotional payoff is a verbal element which, combined with the logo, establishes the brand identity of a particular project.

To make the project objective clear and effective for the general audience, the following promotional payoff has been developed: “Critical-Chains: Cybersecurity in the FinTech World is real”.

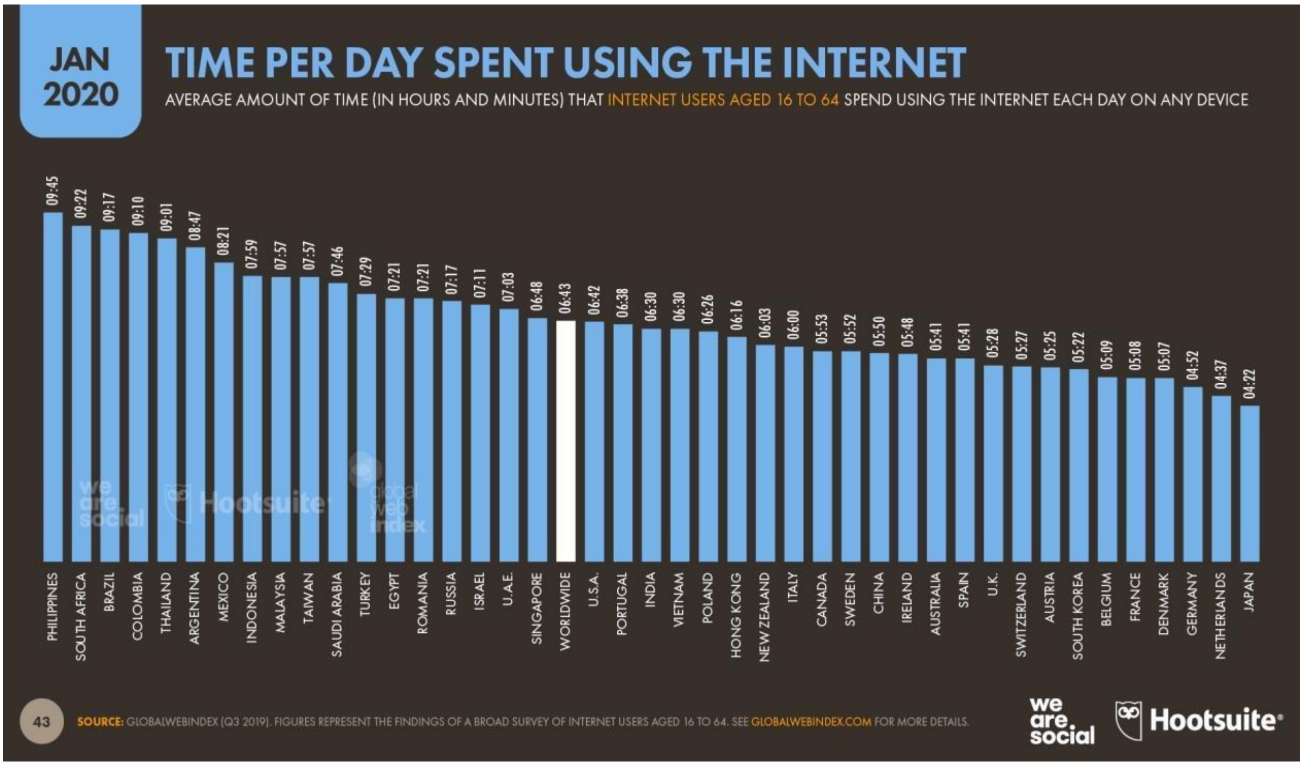
3 Outcome 2: Communication & Dissemination Strategy

According to “Digital 2020 – Global Digital Overview” (https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media), digital, mobile, and social media have become an indispensable part of everyday life for people all over the world. More than 4.5 billion people now use the Internet, while social media users have passed the 3.8 billion mark. In addition, the world’s Internet users will spend a cumulative 1.25 billion years online in 2020, with more than one-third of that time spent using social media.

For this reason, the Critical-Chains Project Consortium decided to develop a Communication and Dissemination Strategy that mainly relies on digital channels.

The Critical-Chains communication and dissemination strategy is based on the creation and distribution of valuable, relevant and consistent content to attract and retain a clearly defined audience.

Instead of pitching the innovative technologies of the Project, Critical-Chains will deliver information that is valuable and useful and will follow a specific editorial plan (planned in advance; regularly up-dated with new content ideas and customised according to target audiences


JAN 2020

TIME PER DAY SPENT USING THE INTERNET

AVERAGE AMOUNT OF TIME (IN HOURS AND MINUTES) THAT INTERNET USERS AGED 16 TO 64 SPEND USING THE INTERNET EACH DAY ON ANY DEVICE

SOURCE: GLOBALWEBINDEX (Q3 2019). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.

Figure 2: Time per day spent using the internet

In particular, Critical-Chains communication and dissemination strategy is mainly divided into 3 phases:

1. **Awareness (M1-M12):** the objective is to attract potential stakeholders mainly through communication activities (project promotional materials, general presentations, press releases, videos)
2. **Consideration (M12-M24)**: the objective is to produce valuable content that can be interesting and useful for the stakeholders in order to convince them to finally become part of the Critical-Chains community (scientific/technical magazines and oral/poster presentations at conferences, seminars, workshops, etc.)
3. **Decision (M24-M36):** the objective is to retain stakeholders through valuable content, such as the project e-publication with all public results.

Finally, the project communication and dissemination strategy take into consideration all the following elements in order to maximize its efficiency:

- **Objectives**
- **Target Audience**
- **Communication mix to reach the target audience**
- **Definition of the most efficient content formats for the target audience**
- **Editorial Plan**
- **Key Performance Indicators**

3.1 Dissemination Strategy Implementation Plan

At the beginning of the second phase of the project, a dissemination strategy implementation plan has been elaborated.
It is based on the below four strategic objectives:

- **Objective 1**: strengthening the link to other H2020 sister projects in finance sector by trying to create a sort of Network - community building and leading, that helps widening the impact.
    - Means: specific thematic webinars where 2-3 project coordinators discuss about precise topics. The topics are based on the similarities (or differences) among the projects. –

sharing insights, leveraging synergies amongst projects e.g., mutual exchange of synthetic data etc.

- **Objective 2**: increased robustness of Critical-Chains innovations and results by building a stakeholder community and engaging them in validation to support our "co-design" methodological framework.
    - Means:
        - Specific workshops presenting Critical-Chains results or specific technologies with the aim to survey the community, strengthen requirements and/or validation, extracting information.
        - Stakeholder listing on project website, linking to stakeholder and or allowing them a motivations and interests page each – we can offer "visibility" in exchange of useful and usable information.
    - Best use-case: stakeholder available to provide access/use on their dataset to validate a Critical-Chains technology, which can lead to either of the following managed outcomes:
        - Satisfactory results: being acceptable to publish a paper with acknowledging stakeholder involvement (or even co-authoring).
        - Not satisfactory results: dissemination over website of validation with an external stakeholder.
- **Objective 3**: strengthening project positioning in the Research Community by having a strong publication/editorial plan and deciding the target conferences on which the Consortium can produce joint publications on collaborative project innovations - normal expectation of the Commission Evaluators.
    - Means: Rules for publication/editorial plan
- **Objective 4**: making the project "warmer" by dynamically using communication channels. A way could be bringing partners closer to the community with a series of carefully edited and quality checked to ensure equitable treatment of the Partners, short video interviews explaining innovations, key details of the project, benefits to the users, expected impacts. These can be posted on the project website, LinkedIn group, twitter.
    - Means:
        - Series of videos (indications as to how to make a selfie video);
        - Newsletter (to be linked with the engagement of stakeholder community)
        - Reposting news on Finance, technologies in the sector and cybersecurity on twitter or LinkedIn - very carefully to ensure no risk of reputational damage to the Consortium and/or inequitable treatment due to imbalanced positioning and visibility of any partner.

4 Objectives

The general purpose of the dissemination of European projects is to promote European collaborative research and innovation. The Critical-Chains project communication and dissemination objectives are:

- Raise public awareness and ensure maximum visibility of the project key milestones, objectives, activities and findings among EU member states.
- Announce and promote Critical-Chains events, contributing to upgrade its attendance and engagement potential.
- Reach the wider European FinTech and security community

5 Target

As stated in the previous chapters, an audience is imperative to develop a successful communication and dissemination strategy, the Project Consortium carefully identified the target audiences in order to maximise the impact of Critical-Chains.

Knowing the audience is fundamental for the stage of content creation: by understanding the informational needs, the preferred content formats, and the most used channels by our target audiences it is possible to create valuable content and disseminate the project results in an effective way. Therefore, Critical-Chains Communication & Dissemination strategy targets are:

- Key decision-makers, public bodies and authorities in the FinTech domain such as governmental organisations, ministries, national and international associations
- End users and practitioners in priority sectors
- Direct consumers enterprises
- Solution partners
- Public citizens

In particular, specific actions have been foreseen in order to reach the target audiences, as listed in the following table.

Table 1: Critical-Chains Target Groups

Target Group	What do we want to achieve	How do we reach target groups
Key decision makers, public bodies and authorities in the FinTech domain such as governmental organisations, ministries, national & international associations (bank associations, etc.)	• Provide solutions to the challenges of risk analysis in the context of modern financial infrastructure, assisting to shape the future direction of research; • Give visibility to the innovation activity realized during the project implementation, raise awareness about the possible uses of the project solution in different domains • Disseminate the Critical-Chains solution to find out how it can improve some processes such as audits and fraud detection related to tax payment • Create an image as a trustful partner for the latest security research and innovation	• Policy reports, meetings, conferences, workshops, social media, own events/summits • Suggestion papers for common standards in the field of cyber-physical security, blockchain- enabled triangular model, consolidation as expert on the topic
End users & practitioners in priority sectors	• Cultivation of existing and further development of new business relations; • Enhance visibility of project results, improve end user awareness towards secure Blockchain based solutions and related services • Increase awareness on new markets for solutions on this topic	• Existing business relationships, • Bilateral discussions in meetings, conferences, seminars/workshops, own events/summits • Include them in Advisory Board

Target Group	What do we want to achieve	How do we reach Target groups
	• include banks, insurance companies, financial organisations (mid-parties in triangular accountability model)	• Send them regular newsletters, • Direct and personal contacts to the financial IT managers; • Discussion group meetings with partners
	•	•
Direct customers, enterprises	• Cultivate existing and further development of new business relations • Increase awareness of the secure financial operations (transactions, secure and smart contracting) • Increase awareness of using the proposed framework as a facilitator in business operations and models	• Promotional activities over media (including social media) • Activate practitioners' existing customer portfolio to increase their awareness • Business relations, own events/summits
Solution partners	• Relationships for future projects and exchange of expertise, new input for research • New and innovative solutions in the blockchain enabled secure FinTech areas • Forecast possible future threats and solutions to overcome them • Licensing agreements for technologies developed in the project	• Organise or participate in workshops for hands-on-experience • Activate existing business relations • Visibility in top scientific conferences • Open booths in brokerage events, summits or fairs to reach the solution partners • Presentation of Critical-Chains innovative solutions on conferences, own events/summits
Public, citizens	• Dissemination of knowledge and advancement of society, according to general orientation of Consortium society; • Enhance visibility of project results, improve end user awareness towards secure Blockchain based solutions and related services • Increased awareness for the specific topics of Critical-Chains;	• Online dissemination (e.g., posts/news on project website) • Dissemination through social media, media, news • Share videos and animations over Internet
Company internal stakeholders	• Knowledge transfer & awareness raising • Transfer project generated knowledge towards security practitioners, professionals working in the banking divisions, professionals working in the trust services' departments	• Organisation of dedicated workshops and seminars

6 Outcome 3: Project Channels

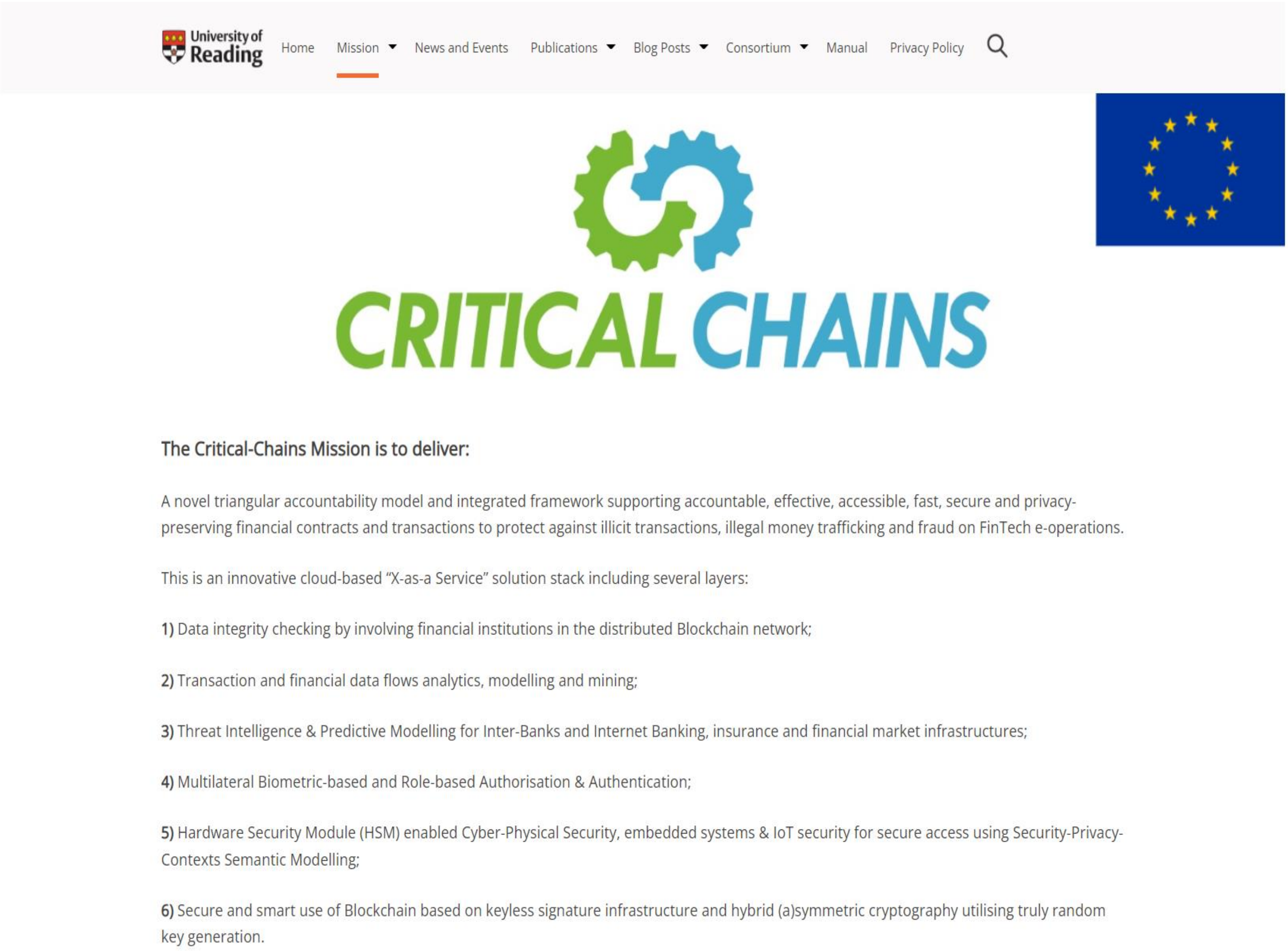
6.1 Website

Critical-Chains project website (https://research.reading.ac.uk/critical-chains/) has been **developed by UREAD (the Coordinator)** and it constitutes a key communication tool to increase the project visibilityand impact, especially towards the wider FinTech community and also to the security community andgeneral public. It is **constantly updated** and will contain **all relevant information about the project** (project objectives, information, news, event announcements, public reports, and analysis) and it alsoserves as communication tool.

The website is **compliant with art.29 GA** as it contains the disclaimer "This project has received funding from the European Union Horizon 2020 Research and Innovation Programme under Grant AgreementNo 833326. This project website reflects only the Critical-Chains Consortium views, the European Commission is not responsible for any use that may be made of the information contained on this website."

The homepage also contains the project video and the link to all the main web pages:

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



The Critical-Chains Mission is to deliver:

A novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations.

This is an innovative cloud-based "X-as-a Service" solution stack including several layers:

1) Data integrity checking by involving financial institutions in the distributed Blockchain network;

2) Transaction and financial data flows analytics, modelling and mining;

3) Threat Intelligence & Predictive Modelling for Inter-Banks and Internet Banking, insurance and financial market infrastructures;

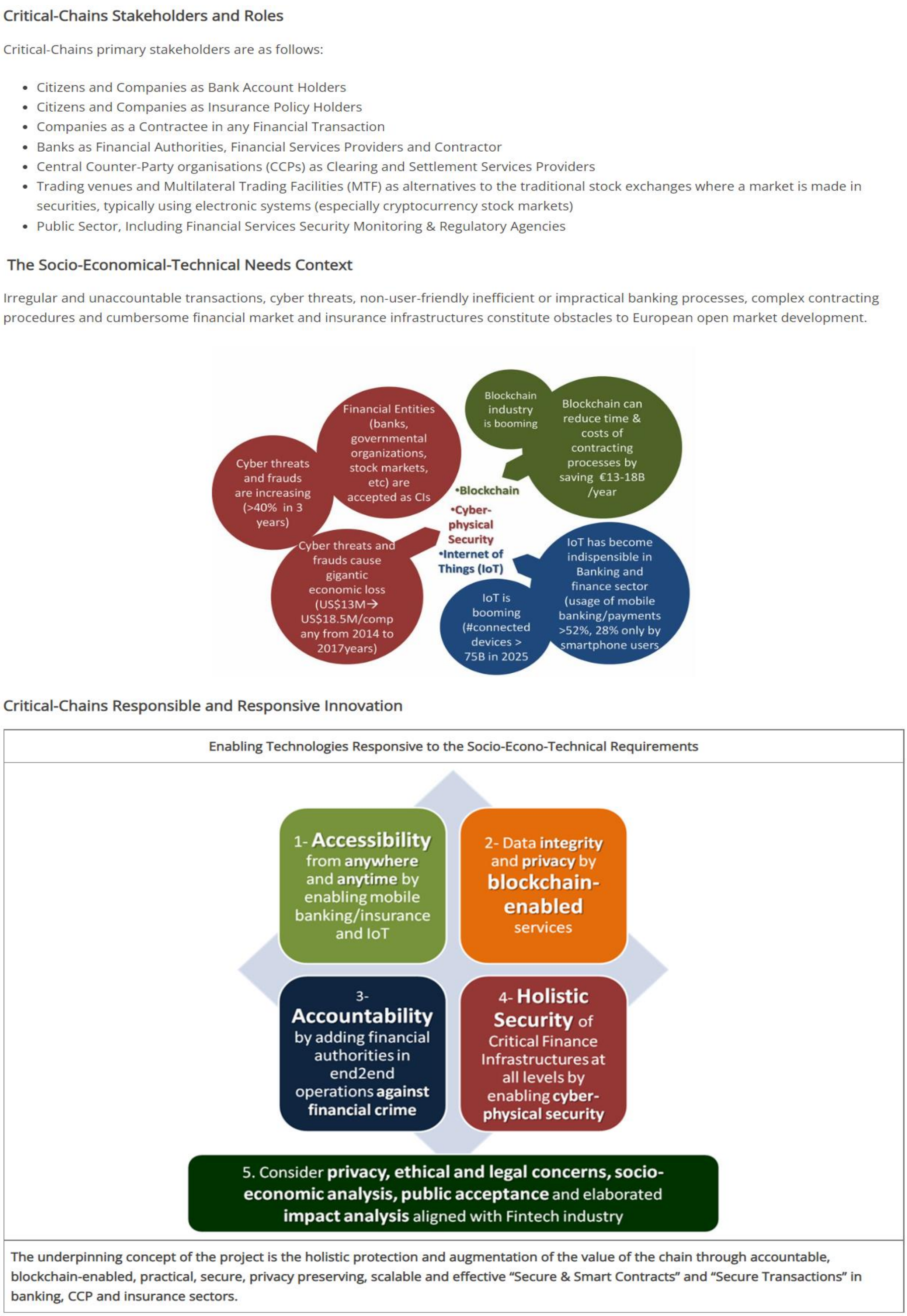
4) Multilateral Biometric-based and Role-based Authorisation & Authentication;

5) Hardware Security Module (HSM) enabled Cyber-Physical Security, embedded systems & IoT security for secure access using Security-Privacy-Contexts Semantic Modelling;

6) Secure and smart use of Blockchain based on keyless signature infrastructure and hybrid (a)symmetric cryptography utilising truly random key generation.

Figure 3: Critical-Chains Mission webpage

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



Critical-Chains Stakeholders and Roles

Critical-Chains primary stakeholders are as follows:

- Citizens and Companies as Bank Account Holders
- Citizens and Companies as Insurance Policy Holders
- Companies as a Contractee in any Financial Transaction
- Banks as Financial Authorities, Financial Services Providers and Contractor
- Central Counter-Party organisations (CCPs) as Clearing and Settlement Services Providers
- Trading venues and Multilateral Trading Facilities (MTF) as alternatives to the traditional stock exchanges where a market is made in securities, typically using electronic systems (especially cryptocurrency stock markets)
- Public Sector, Including Financial Services Security Monitoring & Regulatory Agencies

The Socio-Economical-Technical Needs Context

Irregular and unaccountable transactions, cyber threats, non-user-friendly inefficient or impractical banking processes, complex contracting procedures and cumbersome financial market and insurance infrastructures constitute obstacles to European open market development.

Cyber threats and frauds are increasing (>40% in 3 years)
Financial Entities (banks, governmental organizations, stock markets, etc) are accepted as CIs
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)
Cyber threats and frauds cause gigantic economic loss (US$13M→US$18.5M/company from 2014 to 2017years)
IoT is booming (#connected devices > 75B in 2025
IoT has become indispensible in Banking and finance sector (usage of mobile banking/payments >52%, 28% only by smartphone users

Critical-Chains Responsible and Responsive Innovation

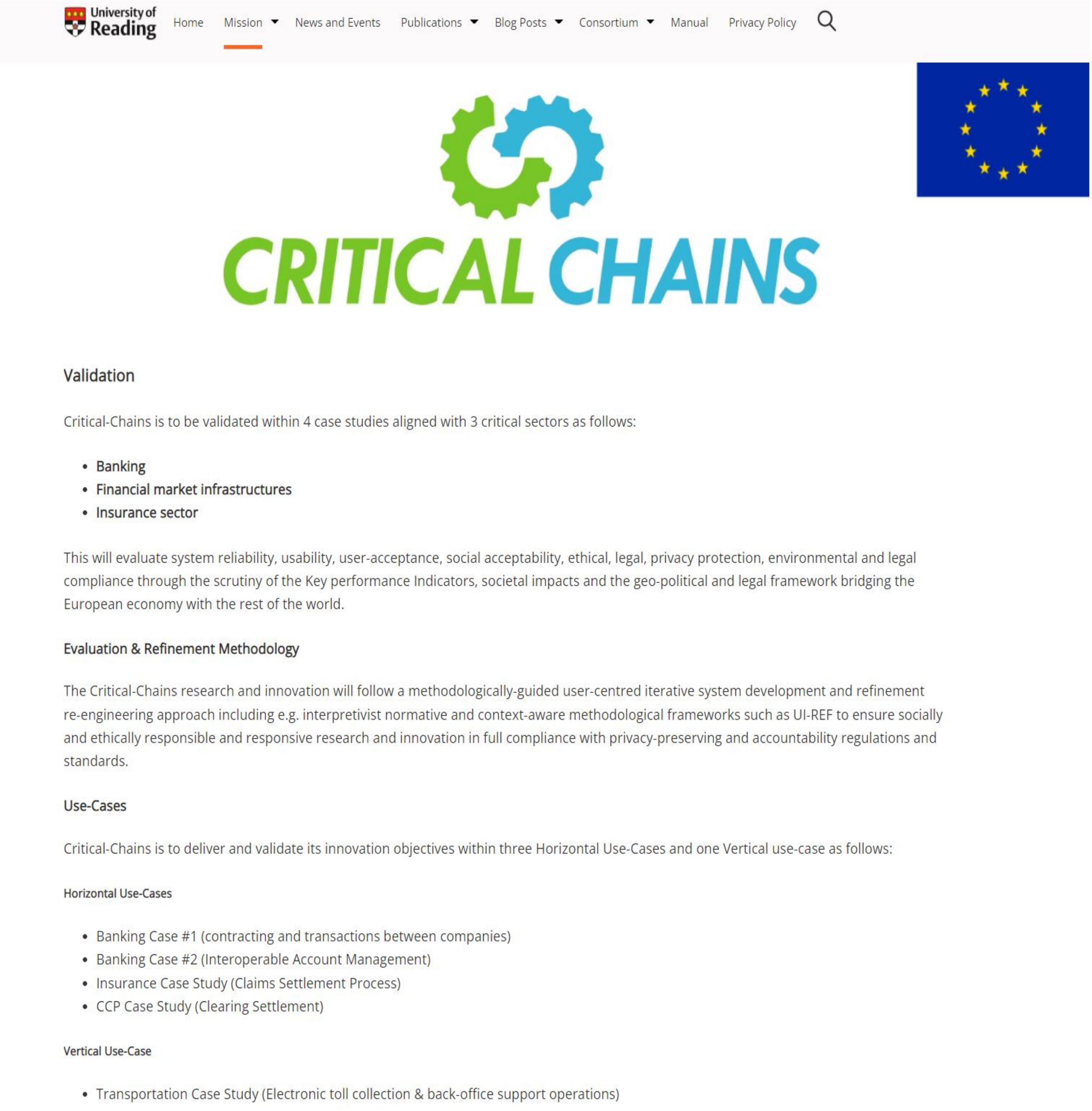
Enabling Technologies Responsive to the Socio-Econo-Technical Requirements

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

The underpinning concept of the project is the holistic protection and augmentation of the value of the chain through accountable, blockchain-enabled, practical, secure, privacy preserving, scalable and effective "Secure & Smart Contracts" and "Secure Transactions" in banking, CCP and insurance sectors.

Figure 4: Critical-Chains Innovation webpage

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



Validation

Critical-Chains is to be validated within 4 case studies aligned with 3 critical sectors as follows:

- Banking
- Financial market infrastructures
- Insurance sector

This will evaluate system reliability, usability, user-acceptance, social acceptability, ethical, legal, privacy protection, environmental and legal compliance through the scrutiny of the Key performance Indicators, societal impacts and the geo-political and legal framework bridging the European economy with the rest of the world.

Evaluation & Refinement Methodology

The Critical-Chains research and innovation will follow a methodologically-guided user-centred iterative system development and refinement re-engineering approach including e.g. interpretivist normative and context-aware methodological frameworks such as UI-REF to ensure socially and ethically responsible and responsive research and innovation in full compliance with privacy-preserving and accountability regulations and standards.

Use-Cases

Critical-Chains is to deliver and validate its innovation objectives within three Horizontal Use-Cases and one Vertical use-case as follows:

Horizontal Use-Cases

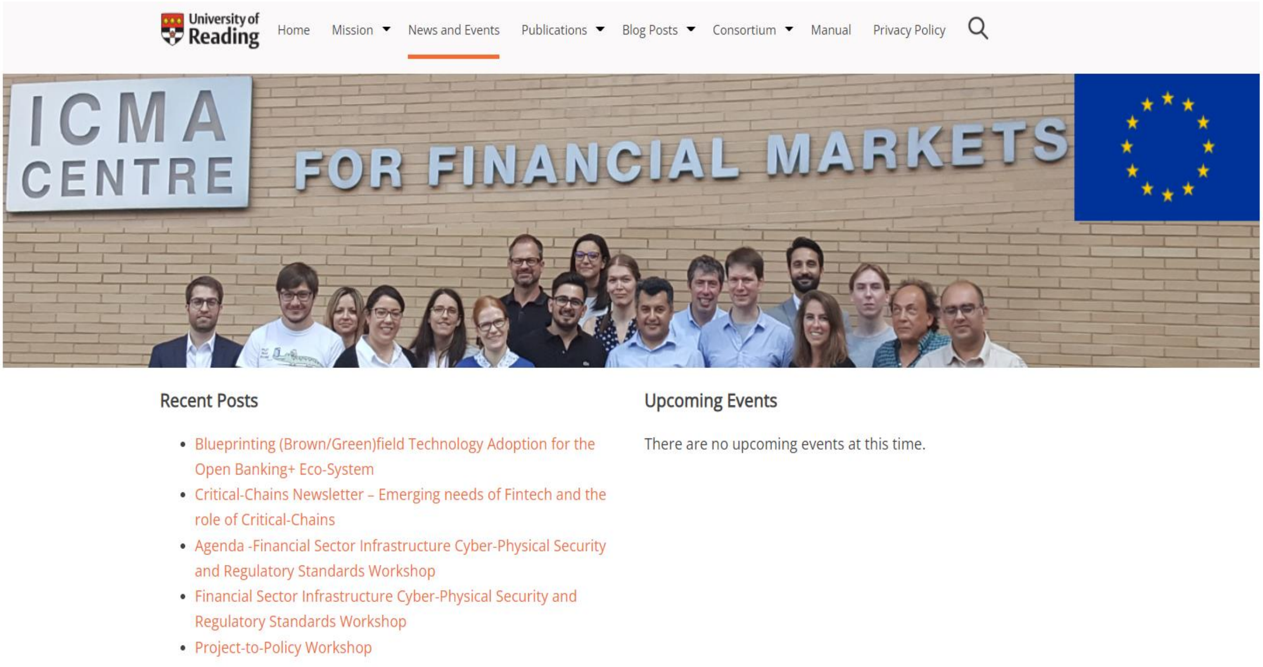
- Banking Case #1 (contracting and transactions between companies)
- Banking Case #2 (Interoperable Account Management)
- Insurance Case Study (Claims Settlement Process)
- CCP Case Study (Clearing Settlement)

Vertical Use-Case

- Transportation Case Study (Electronic toll collection & back-office support operations)

Figure 5: Critical-Chains Validation webpage

- News and Events: https://research.reading.ac.uk/critical-chains/news-and-events/



Recent Posts

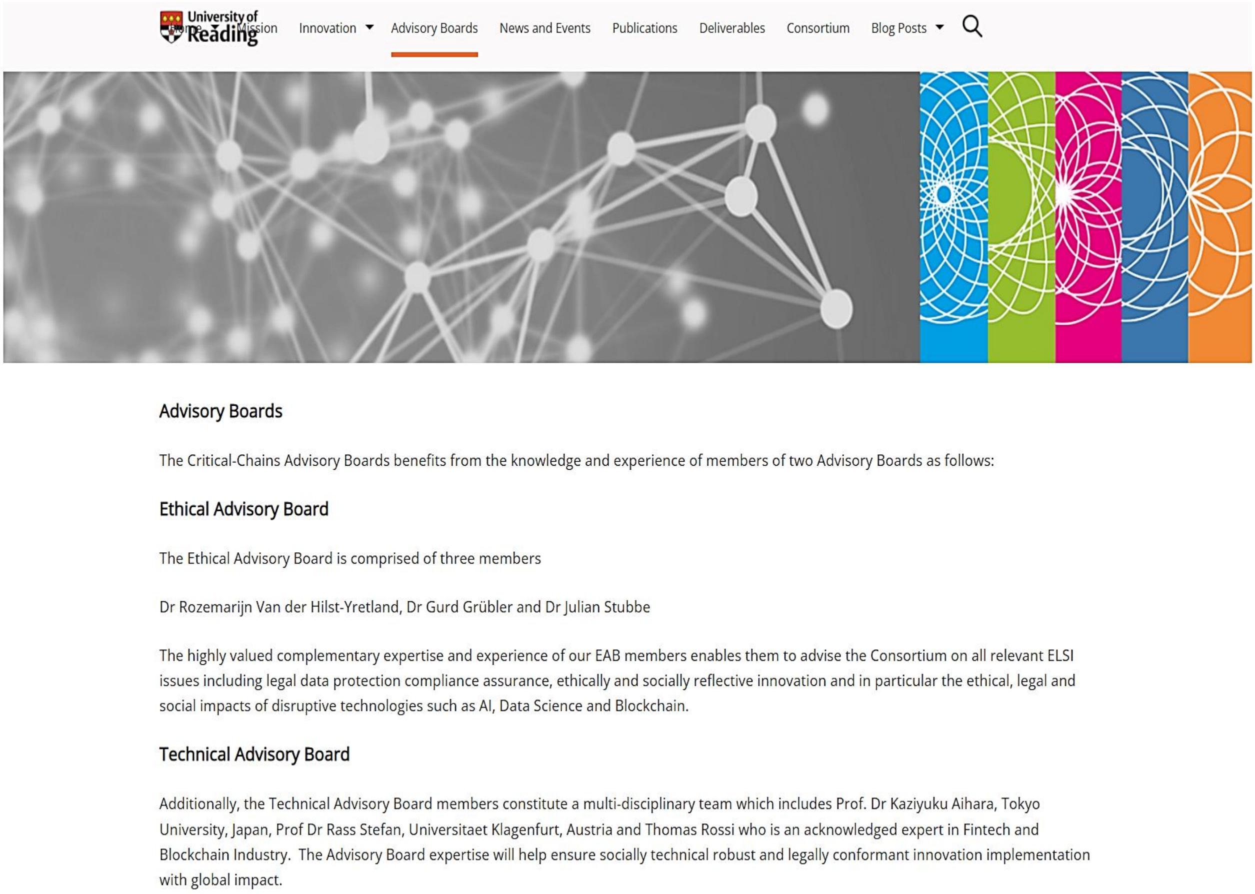
- Blueprinting (Brown/Green)field Technology Adoption for the Open Banking+ Eco-System
- Critical-Chains Newsletter – Emerging needs of Fintech and the role of Critical-Chains
- Agenda -Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop
- Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop
- Project-to-Policy Workshop

Upcoming Events

There are no upcoming events at this time.

Figure 6: Critical-Chains News and Events webpage

- Advisory Boards: https://research.reading.ac.uk/critical-chains/advisory-boards/



Advisory Boards

The Critical-Chains Advisory Boards benefits from the knowledge and experience of members of two Advisory Boards as follows:

Ethical Advisory Board

The Ethical Advisory Board is comprised of three members

Dr Rozemarijn Van der Hilst-Yretland, Dr Gurd Grübler and Dr Julian Stubbe

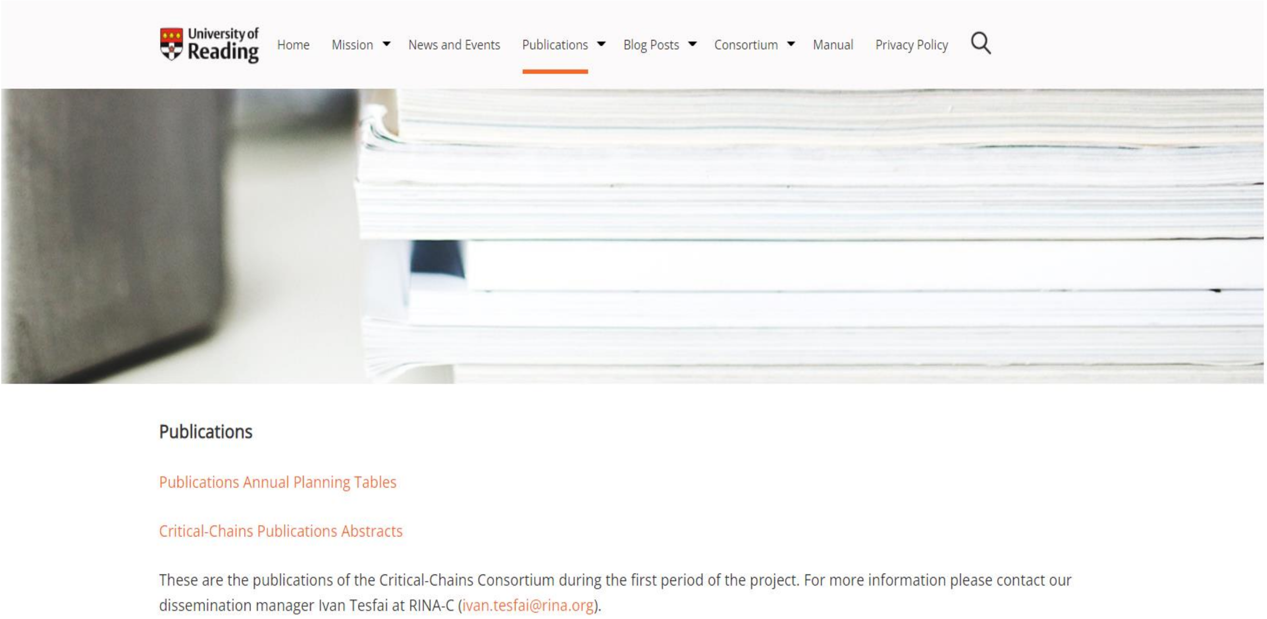
The highly valued complementary expertise and experience of our EAB members enables them to advise the Consortium on all relevant ELSI issues including legal data protection compliance assurance, ethically and socially reflective innovation and in particular the ethical, legal and social impacts of disruptive technologies such as AI, Data Science and Blockchain.

Technical Advisory Board

Additionally, the Technical Advisory Board members constitute a multi-disciplinary team which includes Prof. Dr Kaziyuku Aihara, Tokyo University, Japan, Prof Dr Rass Stefan, Universitaet Klagenfurt, Austria and Thomas Rossi who is an acknowledged expert in Fintech and Blockchain Industry. The Advisory Board expertise will help ensure socially technical robust and legally conformant innovation implementation with global impact.

Figure 7: Critical-Chains Advisory Boards webpage

- Publications : https://research.reading.ac.uk/critical-chains/publications/



Publications

Publications Annual Planning Tables

Critical-Chains Publications Abstracts

These are the publications of the Critical-Chains Consortium during the first period of the project. For more information please contact our dissemination manager Ivan Tesfai at RINA-C (ivan.tesfai@rina.org).

Figure 8: Critical-Chains Publications webpage

6.2 Social Media

Specific banners have been created by RINA for Critical-Chains social media pages.

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

Figure 9: Critical-Chains social media banner

Twitter is a conversation-based social media and 47% of marketers agree that Twitter is the best social media channel for customer engagement.

For this reason, the Critical-Chains Project Consortium has decided to open the project Twitteraccount, which is managed by RINA (https://twitter.com/ChainsH2020).

All **strategic hashtags** are included in Critical-Chains project tweets (such as #H2020, #Cyberattacks etc.) in order to give more visibility to the project.

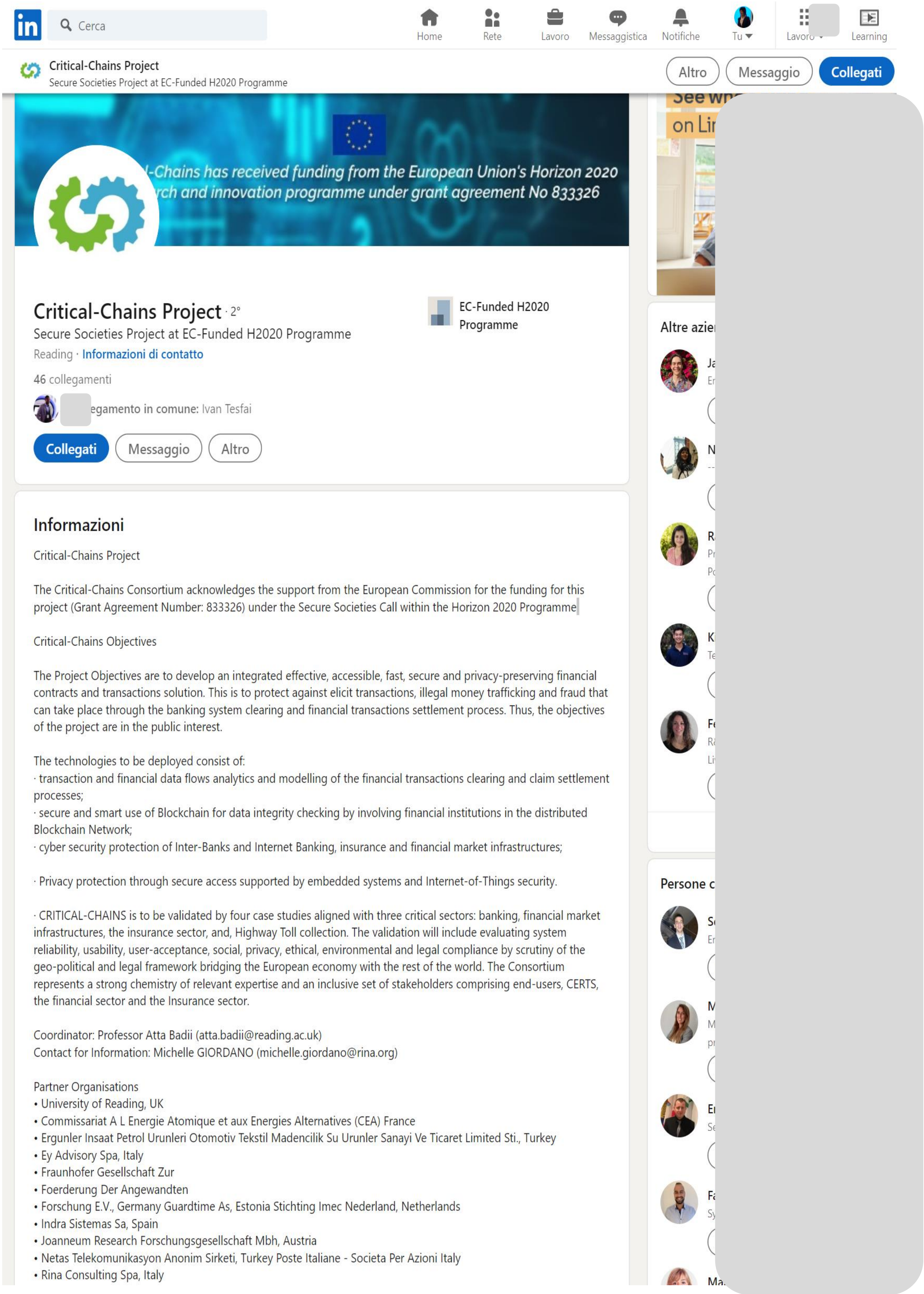
In addition, **trending hashtags of the day** relevant for Critical-Chains project (#CyberSecurityDay) will be exploited to maximise the impact of this project on Twitter community.

The style of Critical-Chains tweets is conversational in order to create online debates on the project. Moreover, **other accounts** (partners, events' account, h2020 accounts, journalists, etc.) are always mentioned in the project tweets to promote social engagement.

Last but not least, **images or videos** to attract are always included in the project tweets in order to catch the followers' attention more easily.

Critical-Chains can be found on LinkedIn at https://www.linkedin.com/in/critical-chains-project-55a3501a3/

The profile page includes information about the project, and the partners involved.



Critical-Chains Project
Secure Societies Project at EC-Funded H2020 Programme

-Chains has received funding from the European Union's Horizon 2020 rch and innovation programme under grant agreement No 833326

Critical-Chains Project · 2°
Secure Societies Project at EC-Funded H2020 Programme
Reading · Informazioni di contatto

EC-Funded H2020 Programme

46 collegamenti

[redacted] egamento in comune: Ivan Tesfai

[redacted]

Informazioni

Critical-Chains Project

The Critical-Chains Consortium acknowledges the support from the European Commission for the funding for this project (Grant Agreement Number: 833326) under the Secure Societies Call within the Horizon 2020 Programme

Critical-Chains Objectives

The Project Objectives are to develop an integrated effective, accessible, fast, secure and privacy-preserving financial contracts and transactions solution. This is to protect against elicit transactions, illegal money trafficking and fraud that can take place through the banking system clearing and financial transactions settlement process. Thus, the objectives of the project are in the public interest.

The technologies to be deployed consist of:
· transaction and financial data flows analytics and modelling of the financial transactions clearing and claim settlement processes;
· secure and smart use of Blockchain for data integrity checking by involving financial institutions in the distributed Blockchain Network;
· cyber security protection of Inter-Banks and Internet Banking, insurance and financial market infrastructures;

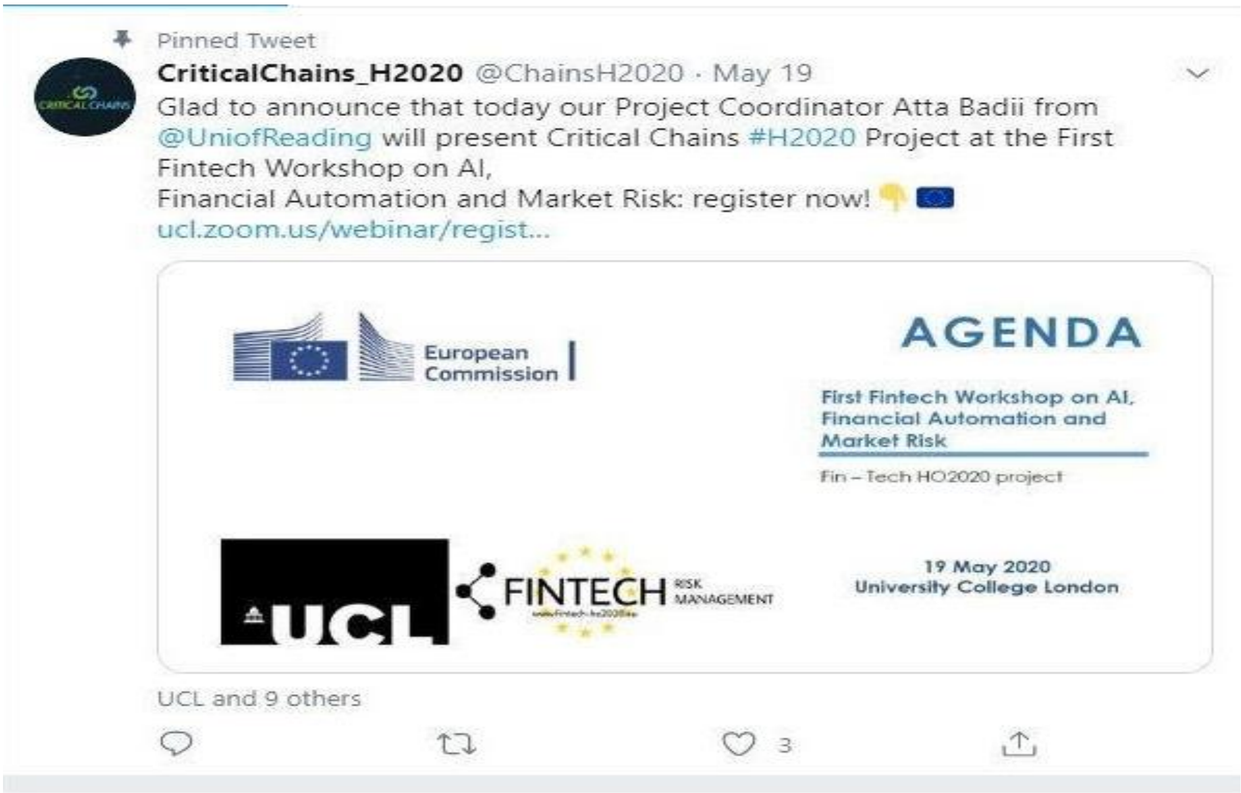
· Privacy protection through secure access supported by embedded systems and Internet-of-Things security.

· CRITICAL-CHAINS is to be validated by four case studies aligned with three critical sectors: banking, financial market infrastructures, the insurance sector, and, Highway Toll collection. The validation will include evaluating system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy with the rest of the world. The Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users, CERTS, the financial sector and the Insurance sector.

Coordinator: Professor Atta Badii (atta.badii@reading.ac.uk)
Contact for Information: Michelle GIORDANO (michelle.giordano@rina.org)

Partner Organisations
- University of Reading, UK
- Commissariat A L Energie Atomique et aux Energies Alternatives (CEA) France
- Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik Su Urunler Sanayi Ve Ticaret Limited Sti., Turkey
- Ey Advisory Spa, Italy
- Fraunhofer Gesellschaft Zur
- Foerderung Der Angewandten
- Forschung E.V., Germany Guardtime As, Estonia Stichting Imec Nederland, Netherlands
- Indra Sistemas Sa, Spain
- Joanneum Research Forschungsgesellschaft Mbh, Austria
- Netas Telekomunikasyon Anonim Sirketi, Turkey Poste Italiane - Societa Per Azioni Italy
- Rina Consulting Spa, Italy

Figure 10: LinkedIn webpage



Pinned Tweet

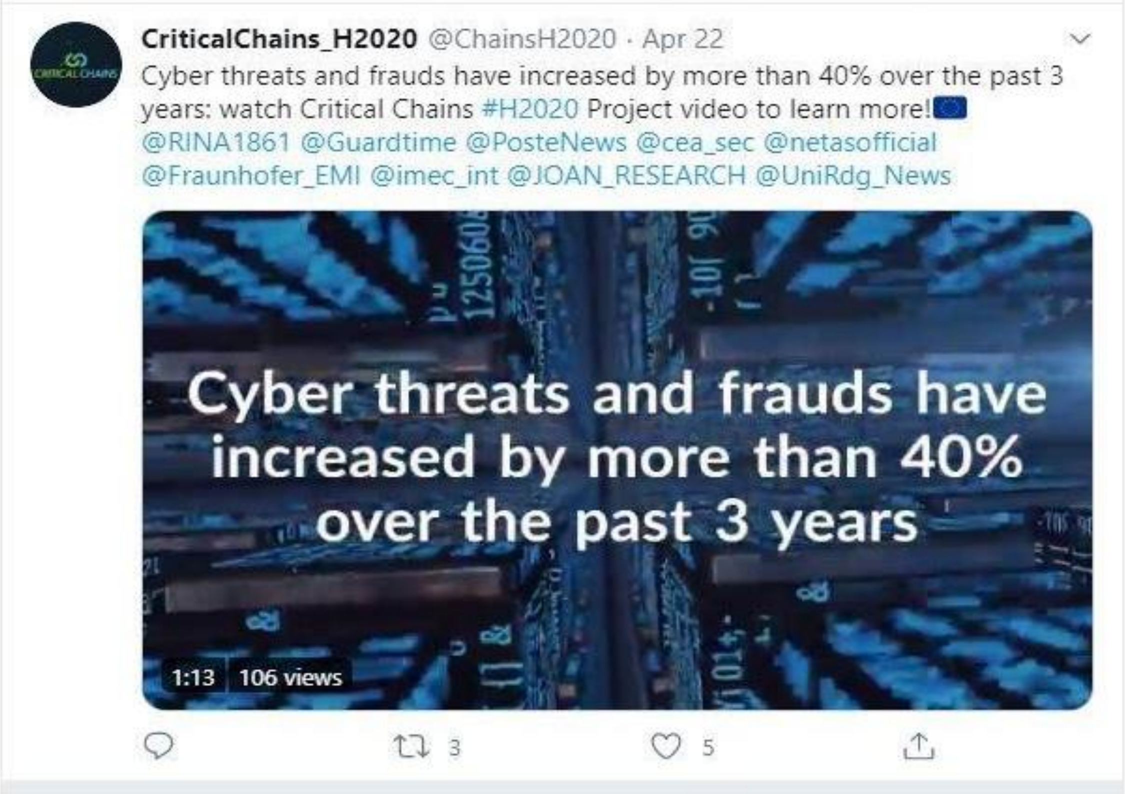
CriticalChains_H2020 @ChainsH2020 · May 19

Glad to announce that today our Project Coordinator Atta Badii from @UniofReading will present Critical Chains #H2020 Project at the First Fintech Workshop on AI,
Financial Automation and Market Risk: register now! 👇 🇪🇺
ucl.zoom.us/webinar/regist...

European Commission
AGENDA
First Fintech Workshop on AI, Financial Automation and Market Risk
Fin – Tech HO2020 project
19 May 2020
University College London
UCL
FINTECH RISK MANAGEMENT

UCL and 9 others

Figure 11: Example of Promotional Tweet



CriticalChains_H2020 @ChainsH2020 · Apr 22

Cyber threats and frauds have increased by more than 40% over the past 3 years: watch Critical Chains #H2020 Project video to learn more! 🇪🇺
@RINA1861 @Guardtime @PosteNews @cea_sec @netasofficial @Fraunhofer_EMI @imec_int @JOAN_RESEARCH @UniRdg_News

Cyber threats and frauds have increased by more than 40% over the past 3 years
1:13 106 views
3
5

Figure 12 : Example of Promotional Tweet

YouTube Channel

https://www.youtube.com/channel/UCa3QA5cOLRMR8bPeGIvsVWg

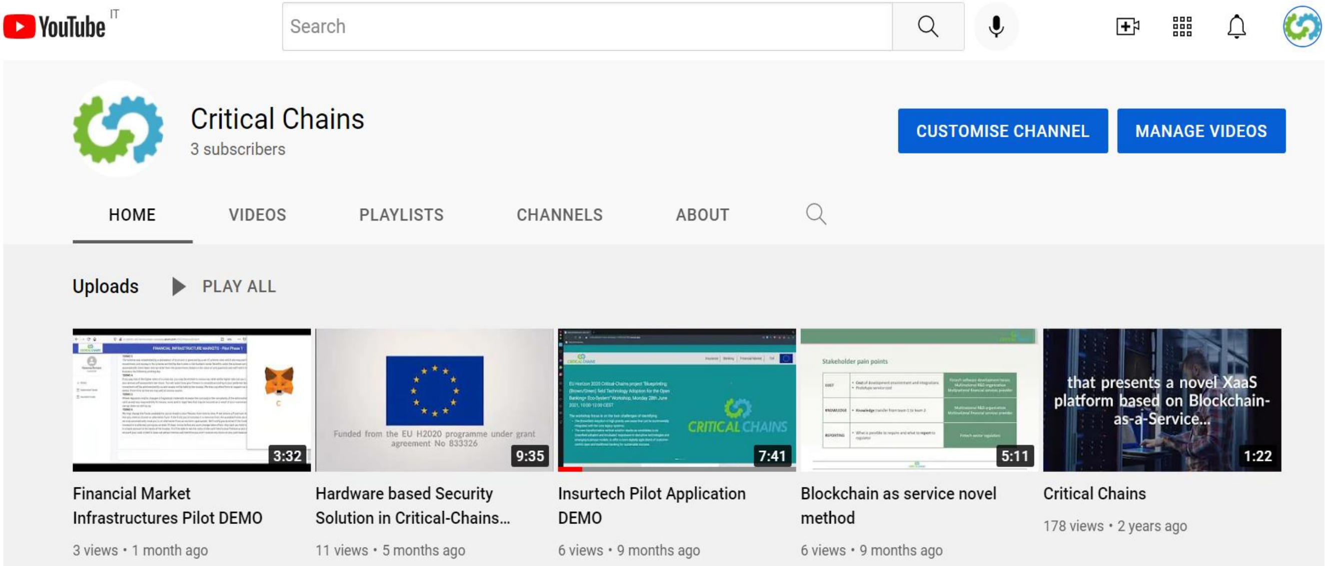
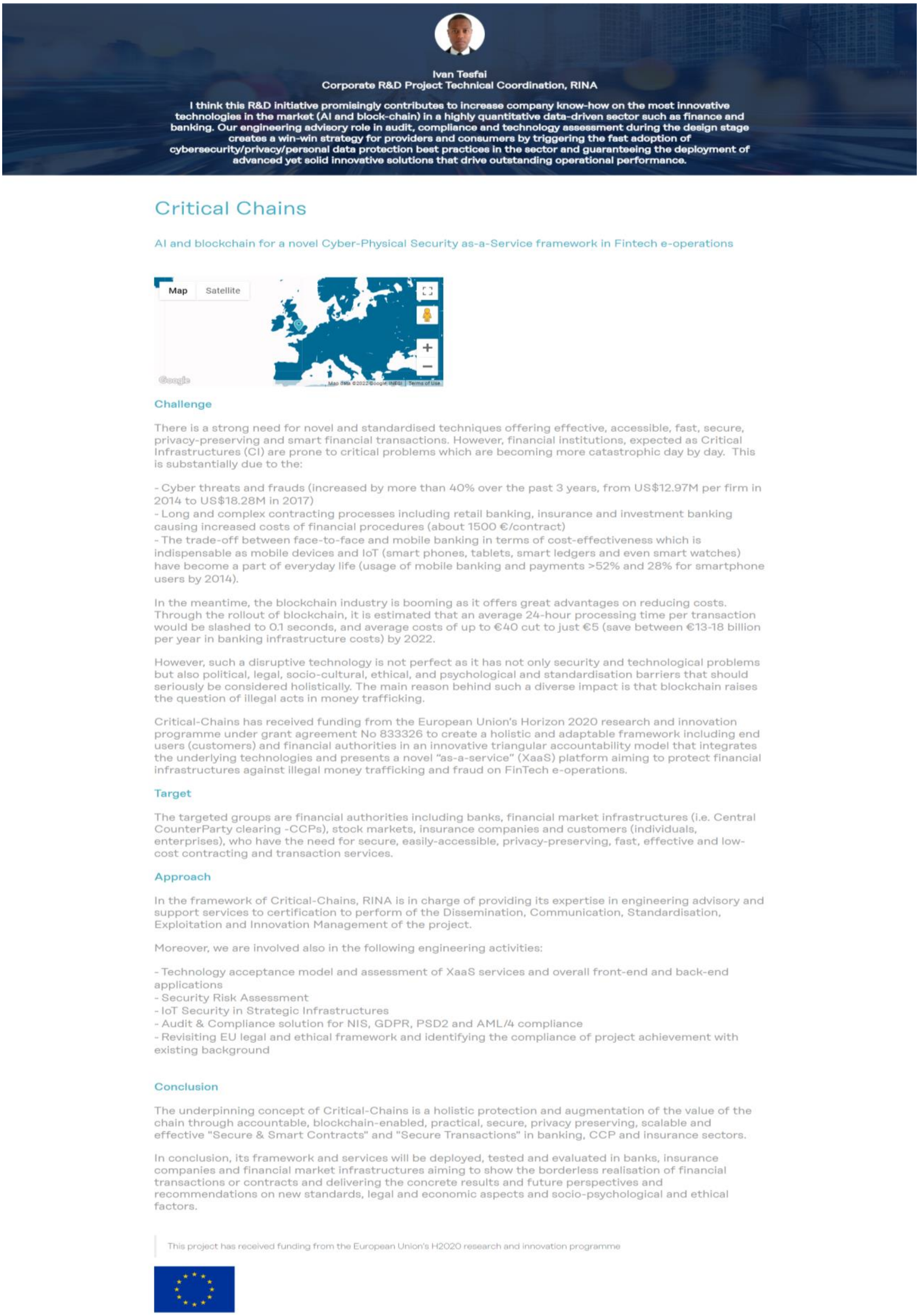


Figure 13: Critical-Chains YouTube Channel

7 Outcome 4: Editorial Plan

7.1 Promotion through Partner’s channels

Project partners promoted Critical-Chains also on their own communication channels. For example, RINA-C promoted the project on its website (https://www.rina.org/en/media/casestudies/critical-chains) and social media.



Ivan Tesfai
Corporate R&D Project Technical Coordination, RINA

I think this R&D initiative promisingly contributes to increase company know-how on the most innovative technologies in the market (AI and block-chain) in a highly quantitative data-driven sector such as finance and banking. Our engineering advisory role in audit, compliance and technology assessment during the design stage creates a win-win strategy for providers and consumers by triggering the fast adoption of cybersecurity/privacy/personal data protection best practices in the sector and guaranteeing the deployment of advanced yet solid innovative solutions that drive outstanding operational performance.

Critical Chains

AI and blockchain for a novel Cyber-Physical Security as-a-Service framework in Fintech e-operations

Challenge

There is a strong need for novel and standardised techniques offering effective, accessible, fast, secure, privacy-preserving and smart financial transactions. However, financial institutions, expected as Critical Infrastructures (CI) are prone to critical problems which are becoming more catastrophic day by day. This is substantially due to the:

- Cyber threats and frauds (increased by more than 40% over the past 3 years, from US$12.97M per firm in 2014 to US$18.28M in 2017)
- Long and complex contracting processes including retail banking, insurance and investment banking causing increased costs of financial procedures (about 1500 €/contract)
- The trade-off between face-to-face and mobile banking in terms of cost-effectiveness which is indispensable as mobile devices and IoT (smart phones, tablets, smart ledgers and even smart watches) have become a part of everyday life (usage of mobile banking and payments >52% and 28% for smartphone users by 2014).

In the meantime, the blockchain industry is booming as it offers great advantages on reducing costs. Through the rollout of blockchain, it is estimated that an average 24-hour processing time per transaction would be slashed to 0.1 seconds, and average costs of up to €40 cut to just €5 (save between €13-18 billion per year in banking infrastructure costs) by 2022.

However, such a disruptive technology is not perfect as it has not only security and technological problems but also political, legal, socio-cultural, ethical, and psychological and standardisation barriers that should seriously be considered holistically. The main reason behind such a diverse impact is that blockchain raises the question of illegal acts in money trafficking.

Critical-Chains has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326 to create a holistic and adaptable framework including end users (customers) and financial authorities in an innovative triangular accountability model that integrates the underlying technologies and presents a novel "as-a-service" (XaaS) platform aiming to protect financial infrastructures against illegal money trafficking and fraud on FinTech e-operations.

Target

The targeted groups are financial authorities including banks, financial market infrastructures (i.e. Central CounterParty clearing -CCPs), stock markets, insurance companies and customers (individuals, enterprises), who have the need for secure, easily-accessible, privacy-preserving, fast, effective and low-cost contracting and transaction services.

Approach

In the framework of Critical-Chains, RINA is in charge of providing its expertise in engineering advisory and support services to certification to perform of the Dissemination, Communication, Standardisation, Exploitation and Innovation Management of the project.

Moreover, we are involved also in the following engineering activities:

- Technology acceptance model and assessment of XaaS services and overall front-end and back-end applications
- Security Risk Assessment
- IoT Security in Strategic Infrastructures
- Audit & Compliance solution for NIS, GDPR, PSD2 and AML/4 compliance
- Revisiting EU legal and ethical framework and identifying the compliance of project achievement with existing background

Conclusion

The underpinning concept of Critical-Chains is a holistic protection and augmentation of the value of the chain through accountable, blockchain-enabled, practical, secure, privacy preserving, scalable and effective "Secure & Smart Contracts" and "Secure Transactions" in banking, CCP and insurance sectors.

In conclusion, its framework and services will be deployed, tested and evaluated in banks, insurance companies and financial market infrastructures aiming to show the borderless realisation of financial transactions or contracts and delivering the concrete results and future perspectives and recommendations on new standards, legal and economic aspects and socio-psychological and ethical factors.

This project has received funding from the European Union's H2020 research and innovation programme

Figure 14: Critical-Chains project on RINA website

Similar internal communications were performed by JR, NETAS and other partners.

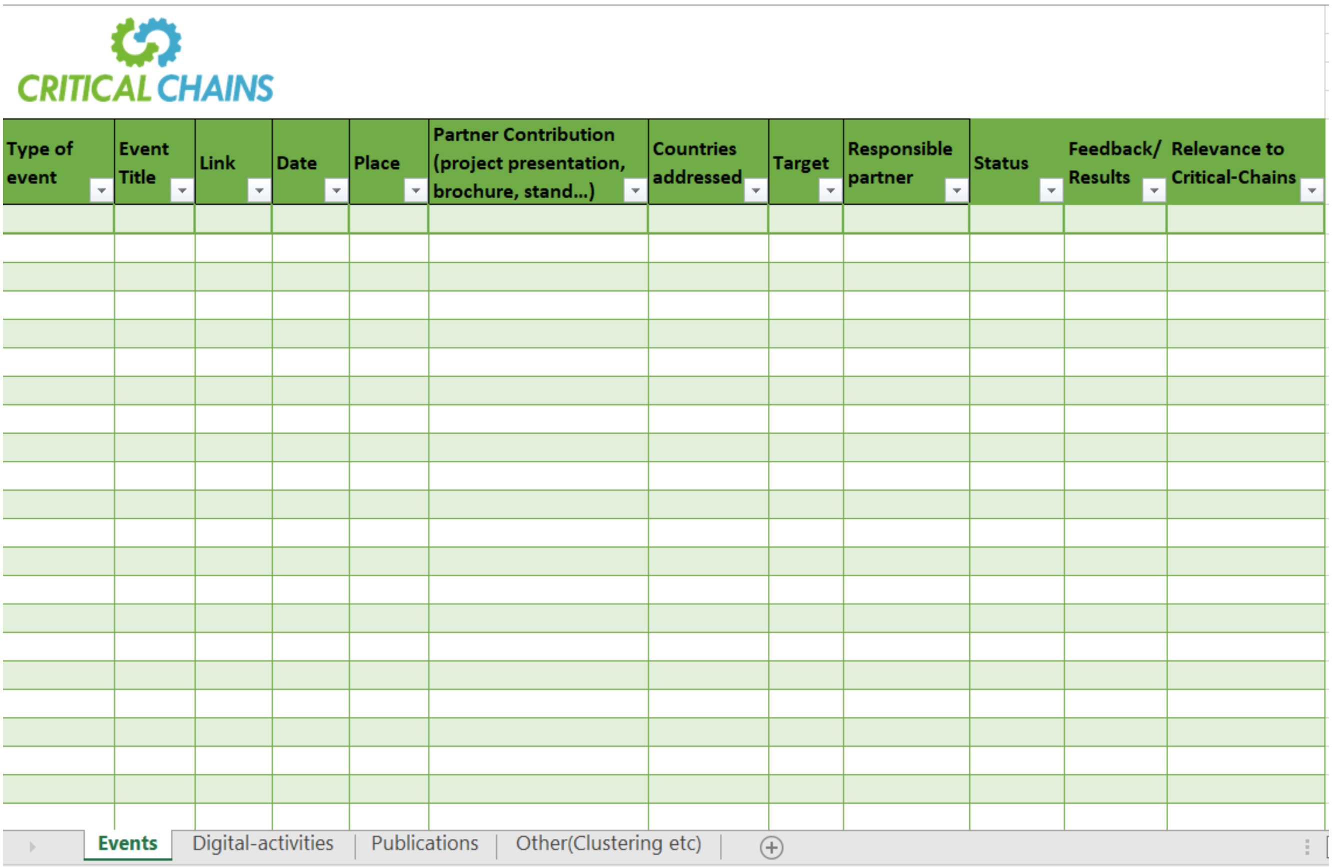
7.2 Communication & Dissemination Tracking File

A specific communication and dissemination tracking file has been developed and shared with the whole Project Consortium every 6 months in order to keep track of all the performed communication and dissemination activities.

All project partners are to duly submit the detail of their proposed dissemination activities (event, date, proposed content of the publication) to Dr Katharina Ross Project Security Officer, FHG, in accordance with the provisions of Consortium Agreement. For Awareness Raising presentations Partners have been advised to make available their proposed presentation to RINA-C as the Dissemination Manager who is responsible to support such activities by ensuring that the proposed presentation is consistent with project abstract as appears on the website and the project poster; follows the logo and branding style as established for the project as well as including the acknowledgement to the EC.

Critical-Chains Communication & Dissemination record of dissemination activities deals with 4 aspects of disseminations as follows:

- Events (conferences, workshop, trade fairs etc) in which project partners presented/plan to present Critical-Chains
- Information about online promotion (news on partners' website and/or social media, publication in online magazines, newsletters etc)
- Information about scientific publications
- Other actions



Type of event	Event Title	Link	Date	Place	Partner Contribution (project presentation, brochure, stand...)	Countries addressed	Target	Responsible partner	Status	Feedback/ Results	Relevance to Critical-Chains

Figure 15: Critical-Chains C&D Tracking File

All project partners are aware that all their communication and dissemination actions need to be compliant with the following articles of the Grant Agreement:

- Art 29.4 – EU acknowledgement: “Critical-Chains has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833326”
- Art. 9.2 - Open access to scientific publications: each beneficiary must ensure open access (free of charge, online access for any user) to all peer-reviewed scientific publications relating to its results.

8 Outcome 5: Project Promotional Contents

8.1 Video

RINA developed a project promotional video motivated by the following persuasive facts:

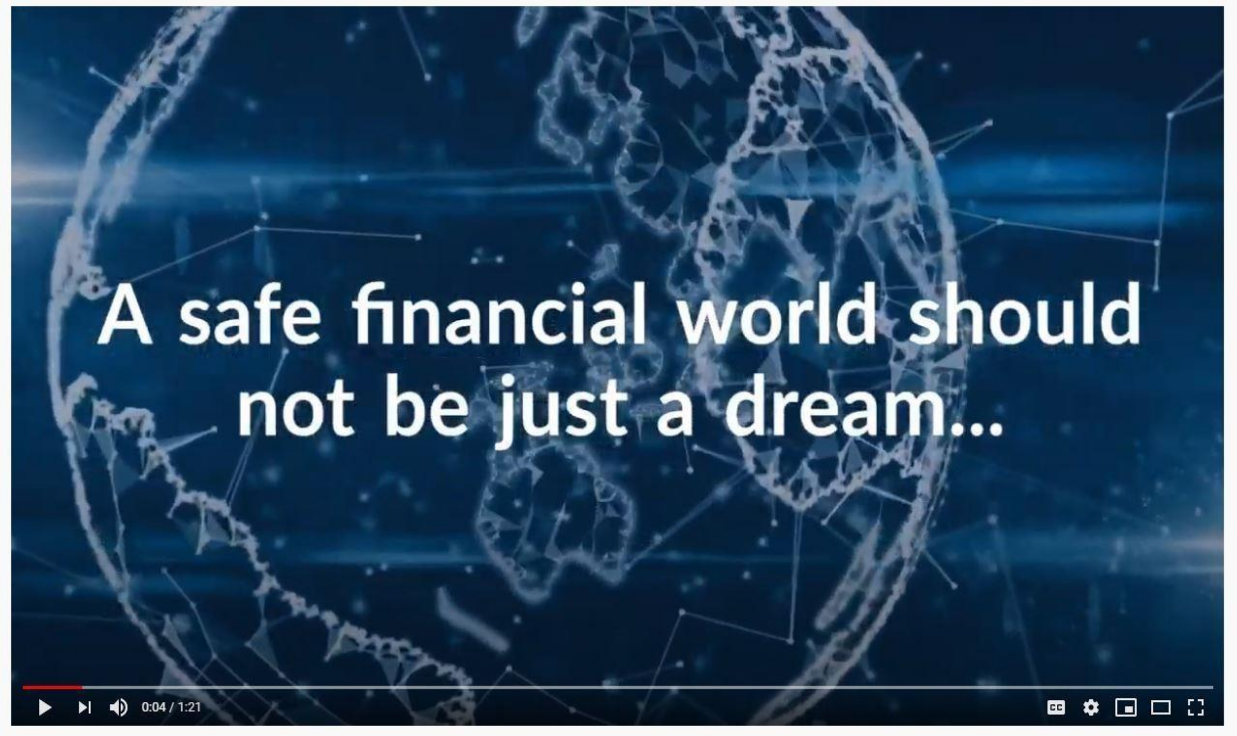
- 78% of people watch online videos every week, and 55% view online videos every day (HubSpot);
- 55% of people pay close attention when watching videos, more than all other types of content (HubSpot);
- Social video generates 1200% more shares than text and image content combined (WordStream);
- 52% of marketers say video is the type of content with the best ROI (Return of Investment) (HubSpot);

The Critical-Chains promotional project video (https://www.youtube.com/watch?v=7NUIdjFHMhI) is 1.22 minutes long and the message can be understood also without audio because videos are usually watched on auto-play on social media. It is consistent with the project brand identity as it is designed using the same colour palette as the project logo.

Ideally, it is divided in 3 main parts:

- Project challenge
- Project innovation
- Final “call to action” which invites users to visit project website to learn more

The project video has been shared on the Critical-Chains website and social media and on partners’ communication channels.



A safe financial world should not be just a dream...

Figure 16: Critical-Chains Promotional Video

Critical-Chains H2020 Project will create a holistic and adaptable framework

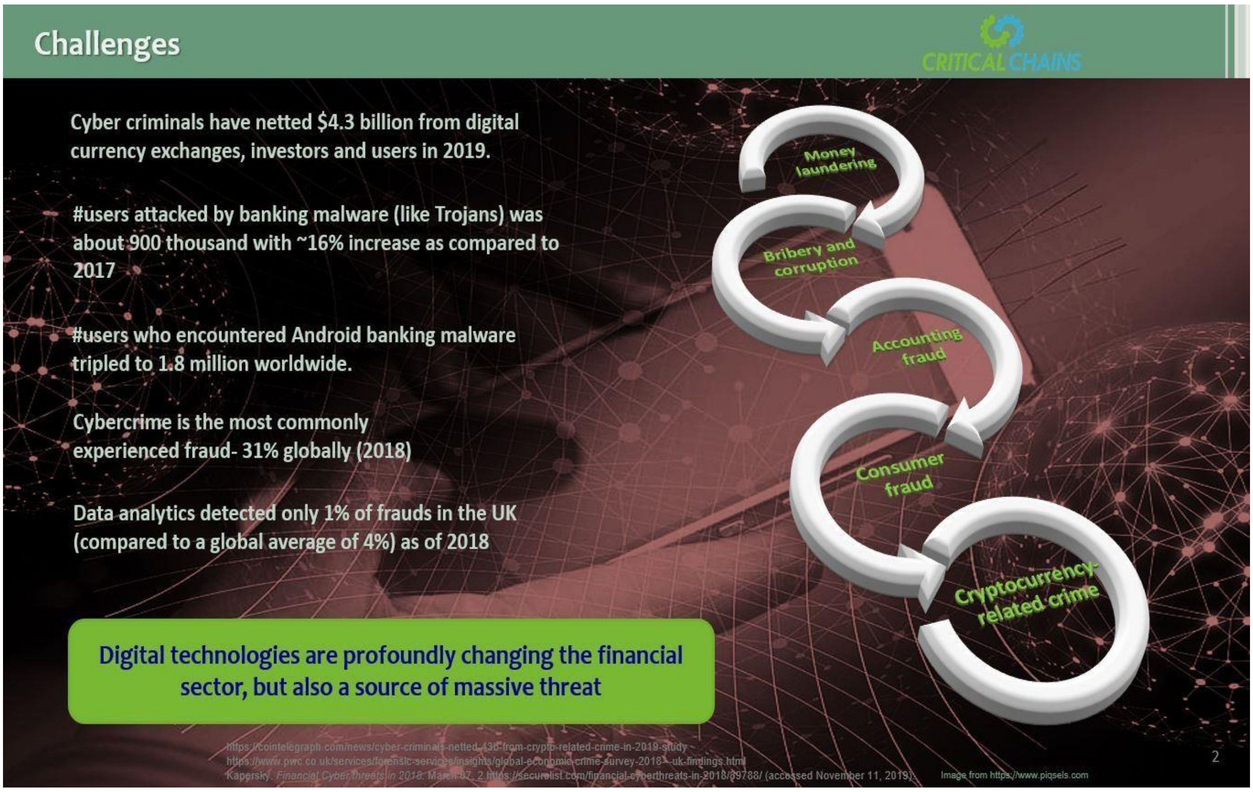
Figure 17: Critical-Chains Promotional Video

Critical-Chains: cyber-security in the FinTech world is real

Figure 18: Critical-Chains Promotional Video

8.2 Presentation

A project presentation has been developed by UREAD and RINA C and made available for all project partners. It will be regularly updated with all project results.



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)

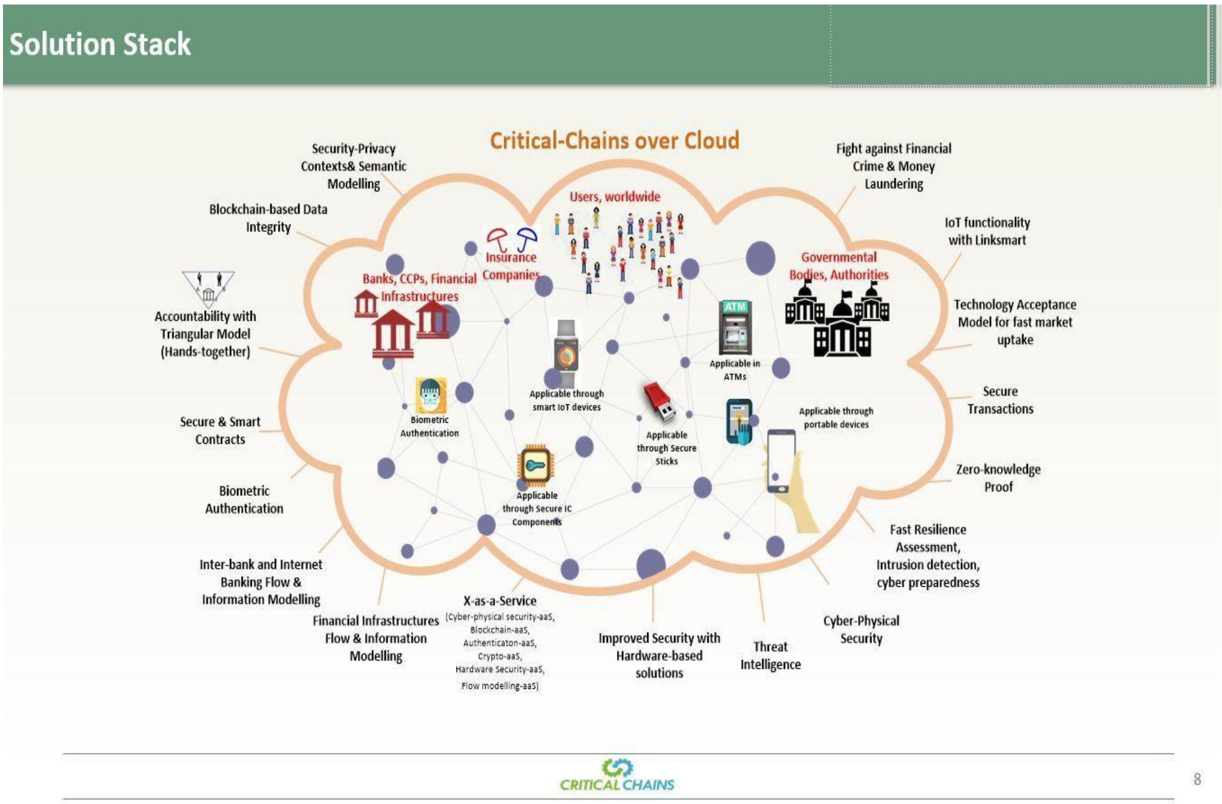
Data analytics detected only 1% of frauds in the UK (compared to a global average of 4%) as of 2018

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

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 Cyberthreats in 2018*. March 07, 2 https://securelist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019). Image from https://www.piqsels.com

2

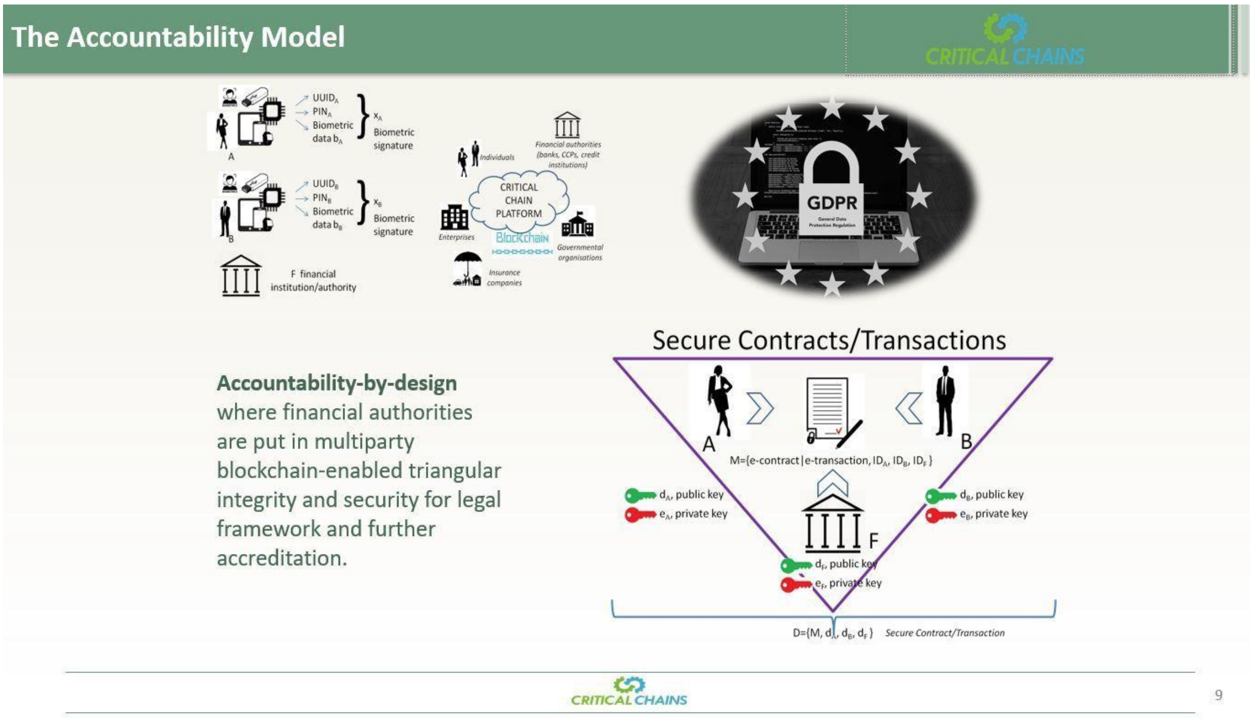
Figure 19: Critical-Chains project presentation



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
Biometric Authentication
Applicable through smart IoT devices
Applicable through Secure Sticks
Applicable through portable devices
Applicable through Secure IC Components
CRITICAL CHAINS
8

Figure 20: Critical-Chains project presentation



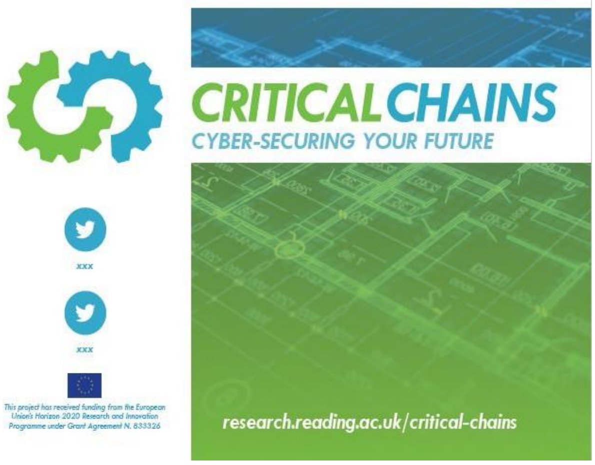
The Accountability Model

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

Figure 21: Critical-Chains project presentation

8.3 Brochure

RINA developed a project brochure to disseminate Critical-Chains to the general public.



CRITICAL CHAINS

CYBER-SECURING YOUR FUTURE

xxx

xxx

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N. 833326

research.reading.ac.uk/critical-chains

PROJECT CONSORTIUM

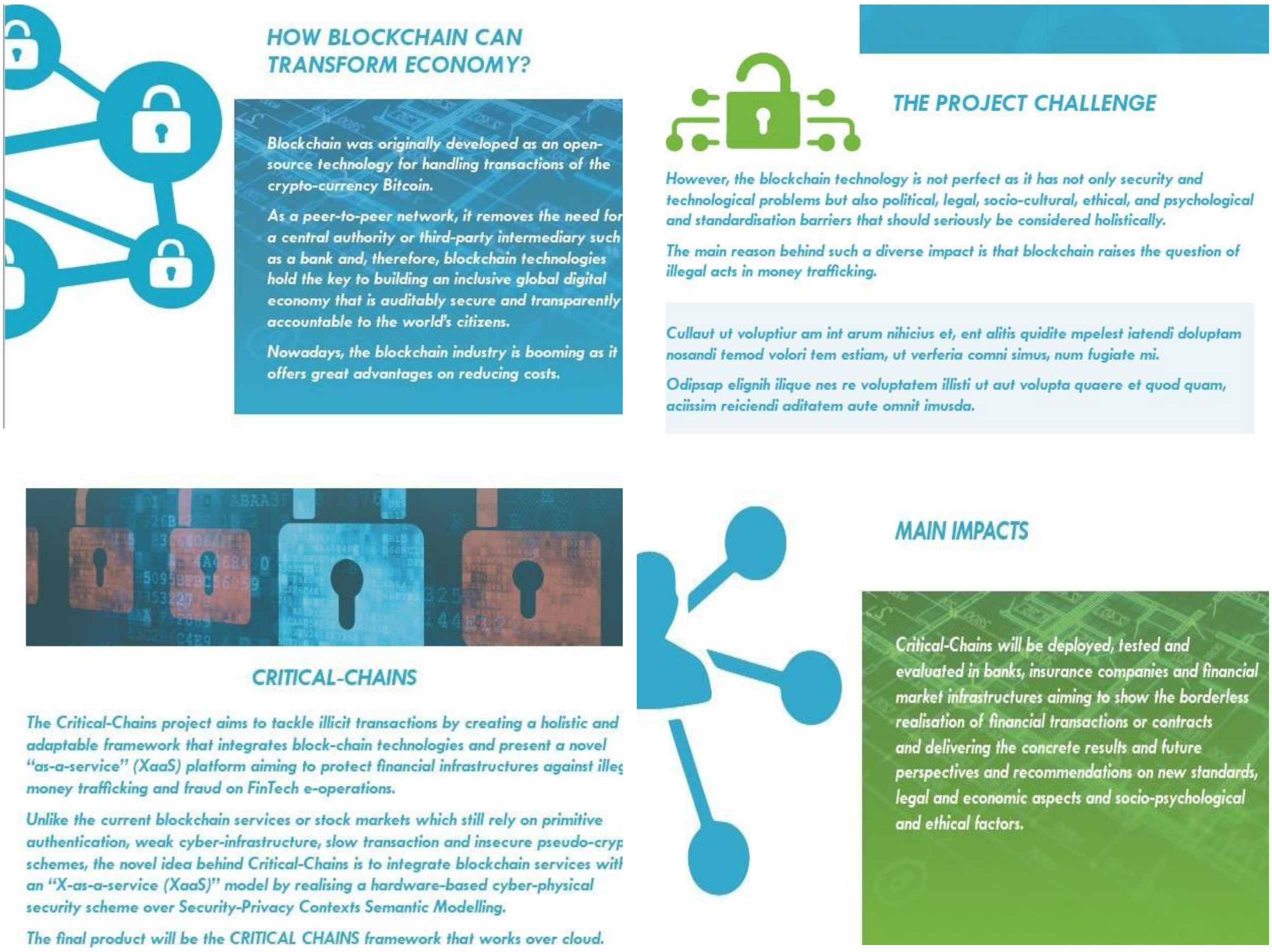
University of Reading
cea
ERGE
EY
NETAS
RINA
indra
Fraunhofer EMI
guardtime
imec
JOANNEUM RESEARCH
Posteitaliane

xxx

xxx

xxx

CONTACT:
Atta Badii – atta.badii@reading.ac.uk
research.reading.ac.uk/critical-chains



HOW BLOCKCHAIN CAN TRANSFORM ECONOMY?

Blockchain was originally developed as an open-source technology for handling transactions of the crypto-currency Bitcoin.

As a peer-to-peer network, it removes the need for a central authority or third-party intermediary such as a bank and, therefore, blockchain technologies hold the key to building an inclusive global digital economy that is auditably secure and transparently accountable to the world's citizens.

Nowadays, the blockchain industry is booming as it offers great advantages on reducing costs.

THE PROJECT CHALLENGE

However, the blockchain technology is not perfect as it has not only security and technological problems but also political, legal, socio-cultural, ethical, and psychological and standardisation barriers that should seriously be considered holistically.

The main reason behind such a diverse impact is that blockchain raises the question of illegal acts in money trafficking.

Cullaut ut voluptiur am int arum nihicius et, ent alitis quidite mpelest iatendi doluptam nosandi temod volori tem estiam, ut verferia comni simus, num fugiate mi.

Odipsap elignih ilique nes re voluptatem illisti ut aut volupta quaere et quod quam, aciissim reiciendi aditatem aute omnit imusda.

CRITICAL-CHAINS

The Critical-Chains project aims to tackle illicit transactions by creating a holistic and adaptable framework that integrates block-chain technologies and present a novel "as-a-service" (XaaS) platform aiming to protect financial infrastructures against illeg money trafficking and fraud on FinTech e-operations.

Unlike the current blockchain services or stock markets which still rely on primitive authentication, weak cyber-infrastructure, slow transaction and insecure pseudo-cryp schemes, the novel idea behind Critical-Chains is to integrate blockchain services wit an "X-as-a-service (XaaS)" model by realising a hardware-based cyber-physical security scheme over Security-Privacy Contexts Semantic Modelling.

The final product will be the CRITICAL CHAINS framework that works over cloud.

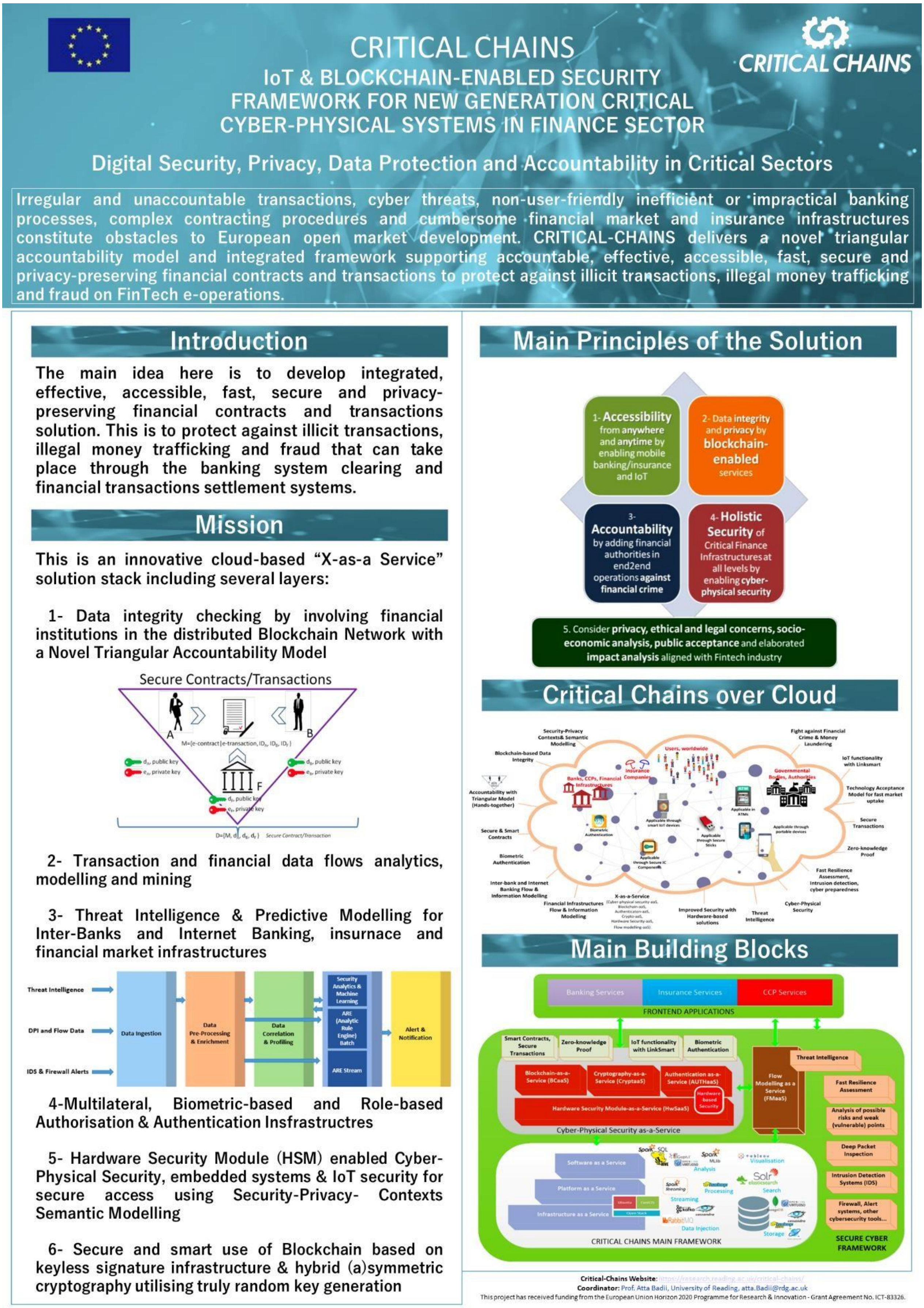
MAIN IMPACTS

Critical-Chains will be deployed, tested and evaluated in banks, insurance companies and financial market infrastructures aiming to show the borderless realisation of financial transactions or contracts and delivering the concrete results and future perspectives and recommendations on new standards, legal and economic aspects and socio-psychological and ethical factors.

Figure 22:Critical-Chains project brochure

8.4 Posters

Project poster with technical content has been prepared by NETAS



CRITICAL CHAINS

IoT & BLOCKCHAIN-ENABLED SECURITY FRAMEWORK FOR NEW GENERATION CRITICAL CYBER-PHYSICAL SYSTEMS IN FINANCE SECTOR

CRITICAL CHAINS

Digital Security, Privacy, Data Protection and Accountability in Critical Sectors

Irregular and unaccountable transactions, cyber threats, non-user-friendly inefficient or impractical banking processes, complex contracting procedures and cumbersome financial market and insurance infrastructures constitute obstacles to European open market development. CRITICAL-CHAINS delivers a novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations.

Introduction

The main idea here is to develop integrated, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions solution. This is to protect against illicit transactions, illegal money trafficking and fraud that can take place through the banking system clearing and financial transactions settlement systems.

Mission

This is an innovative cloud-based "X-as-a Service" solution stack including several layers:

1- Data integrity checking by involving financial institutions in the distributed Blockchain Network with a Novel Triangular Accountability Model

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

2- Transaction and financial data flows analytics, modelling and mining

3- Threat Intelligence & Predictive Modelling for Inter-Banks and Internet Banking, insurnace and financial market infrastructures

Threat Intelligence
DPI and Flow Data
IDS & Firewall Alerts
Data Ingestion
Data Pre-Processing & Enrichment
Data Correlation & Profiling
Security Analytics & Machine Learning
ARE (Analytic Rule Engine) Batch
ARE Stream
Alert & Notification

4-Multilateral, Biometric-based and Role-based Authorisation & Authentication Insfrastructres

5- Hardware Security Module (HSM) enabled Cyber-Physical Security, embedded systems & IoT security for secure access using Security-Privacy- Contexts Semantic Modelling

6- Secure and smart use of Blockchain based on keyless signature infrastructure & hybrid (a)symmetric cryptography utilising truly random key generation

Main Principles of the Solution

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

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
Biometric Authentication
Applicable through smart IoT devices
Applicable in ATMs
Applicable through Secure Sticks
Applicable through portable devices
Applicable through Secure IC Component

Main Building Blocks

Banking Services
Insurance Services
CCP Services
FRONTEND APPLICATIONS
Smart Contracts, Secure Transactions
Zero-knowledge Proof
IoT functionality with LinkSmart
Biometric Authentication
Blockchain-as-a-Service (BCaaS)
Cryptography-as-a-Service (CryptaaS)
Authentication as-a-Service (AUTHaaS)
Hardware-based Security
Hardware Security Module-as-a-Service (HwSaaS)
Cyber-Physical Security as-a-Service
Flow Modelling as a Service (FMaaS)
Threat Intelligence
Fast Resilience Assessment
Analysis of possible risks and weak (vulnerable) points
Deep Packet Inspection
Intrusion Detection Systems (IDS)
Firewall, Alert systems, other cybersecurity tools...
SECURE CYBER FRAMEWORK
Software as a Service
Platform as a Service
Infrastructure as a Service
Open Stack
Spark SQL
Spark MLlib
Analysis
Visualisation
Spark Streaming
Streaming
Processing
Solr
elasticsearch
Search
kafka
cassandra
RabbitMQ
Data Injection
Storage
CRITICAL CHAINS MAIN FRAMEWORK

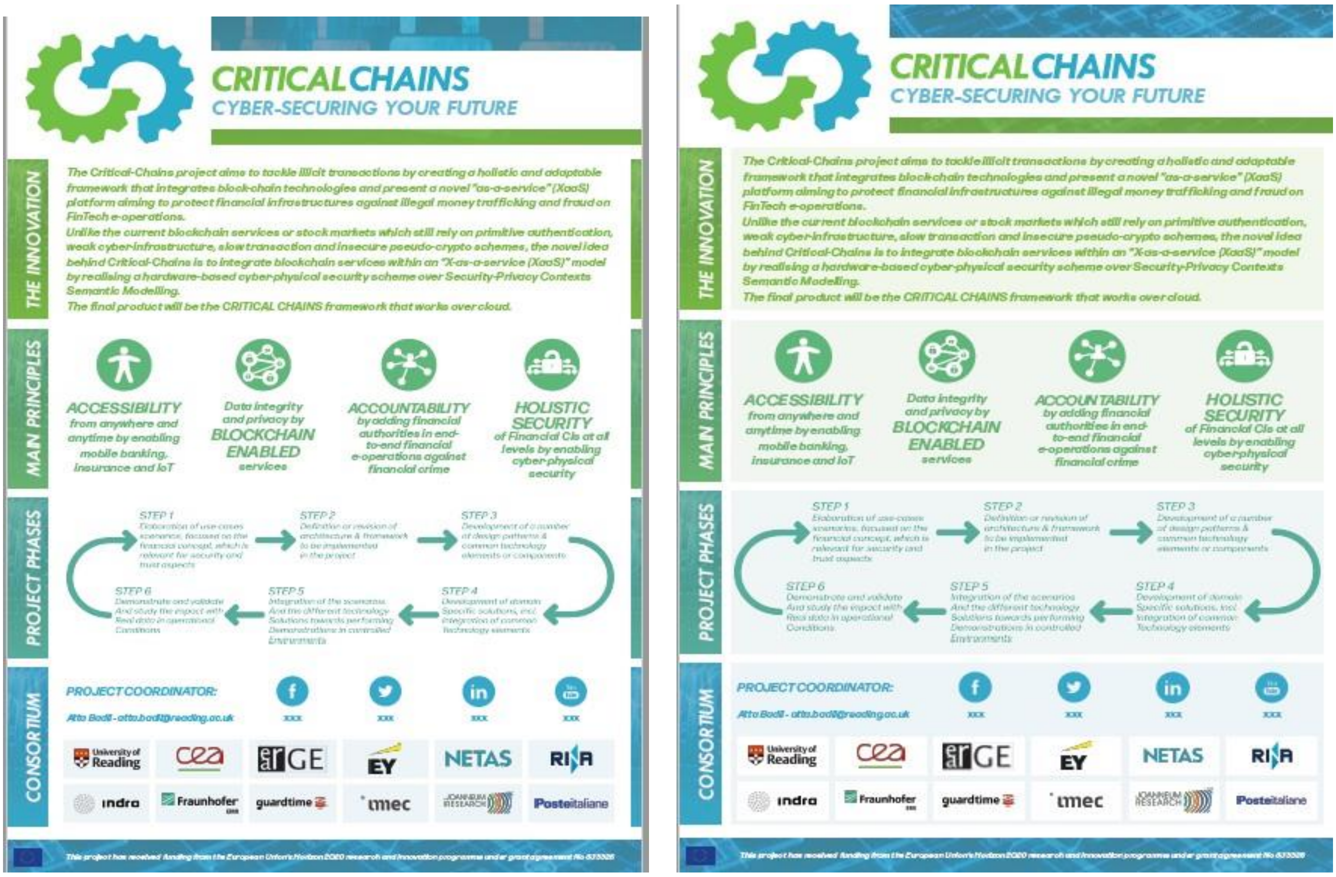
Critical-Chains Website: https://research.reading.ac.uk/critical-chains/

Coordinator: Prof. Atta Badii, University of Reading, atta.Badii@rdg.ac.uk

This project has received funding from the European Union Horizon 2020 Programme for Research & Innovation - Grant Agreement No. ICT-83326.

Figure 23: Critical-Chains project poster-2 (NETAS)

RINA-C developed a more generic project poster to reach a wider group of audience.



CRITICAL CHAINS
CYBER-SECURING YOUR FUTURE

THE INNOVATION

The Critical-Chains project aims to tackle illicit transactions by creating a holistic and adaptable framework that integrates block-chain technologies and present a novel "as-a-service" (XaaS) platform aiming to protect financial infrastructures against illegal money trafficking and fraud on FinTech e-operations.
Unlike the current blockchain services or stock markets which still rely on primitive authentication, weak cyber-infrastructure, slow transaction and insecure pseudo-crypto schemes, the novel idea behind Critical-Chains is to integrate blockchain services within an "X-as-a-service (XaaS)" model by realising a hardware-based cyber-physical security scheme over Security-Privacy Contexts Semantic Modelling.
The final product will be the CRITICAL CHAINS framework that works over cloud.

MAIN PRINCIPLES

ACCESSIBILITY from anywhere and anytime by enabling mobile banking, insurance and IoT

Data integrity and privacy by BLOCKCHAIN ENABLED services

ACCOUNTABILITY by adding financial authorities in end-to-end financial e-operations against financial crime

HOLISTIC SECURITY of Financial CIs at all levels by enabling cyber-physical security

PROJECT PHASES

STEP 1 Elaboration of use cases scenarios, focused on the financial concept, which is relevant for security and trust aspects

STEP 2 Definition or revision of architecture & framework to be implemented in the project

STEP 3 Development of a number of design patterns & common technology elements or components

STEP 4 Development of domain Specific solutions, incl. integration of common Technology elements

STEP 5 Integration of the scenarios And the different technology Solutions towards performing Demonstrations in controlled Environments

STEP 6 Demonstrate and validate And study the impact with Real data in operational Conditions

CONSORTIUM

PROJECT COORDINATOR:
Atta Badii - atta.badii@reading.ac.uk

xxx xxx xxx xxx

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

Figure 24: Critical-Chains project poster-3 (RINA)

8.5 Project Output Videos

With the purpose to increase Critical-Chains visibility, several videos about Critical-Chains outputs have been created.
The plan is to share the video on project social media accounts and to repost them on partners channels. A guideline for the video making has been shared with project partners by RINA–C.

By M24 two videos about Critical-Chains solution had been shared, the other videos are planned to be shared at ten days interval, as per editorial plan.

In particular:

- the video about Blockchain as service method has been shared on 23rd of June 2021 on LinkedIn project account and reposted by the consortium partners.

  To watch the video:

  https://www.linkedin.com/feed/update/urn:li:activity:6813384896397103104

- On the 29th of June 2021, the Demonstration of the Toll Collection pilot application shared on LinkedIn and Twitter Project account.

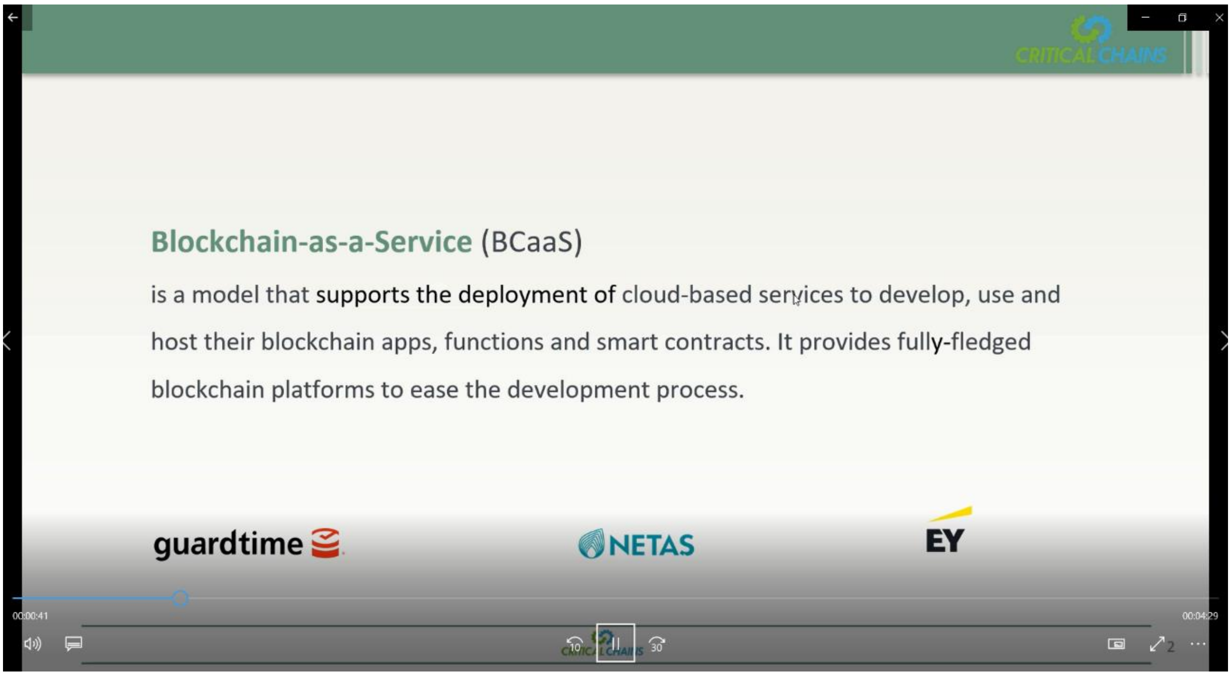
  To watch the video:

  https://www.linkedin.com/feed/update/urn:li:activity:6815599478427541504

Here below some screenshot of the produced videos:

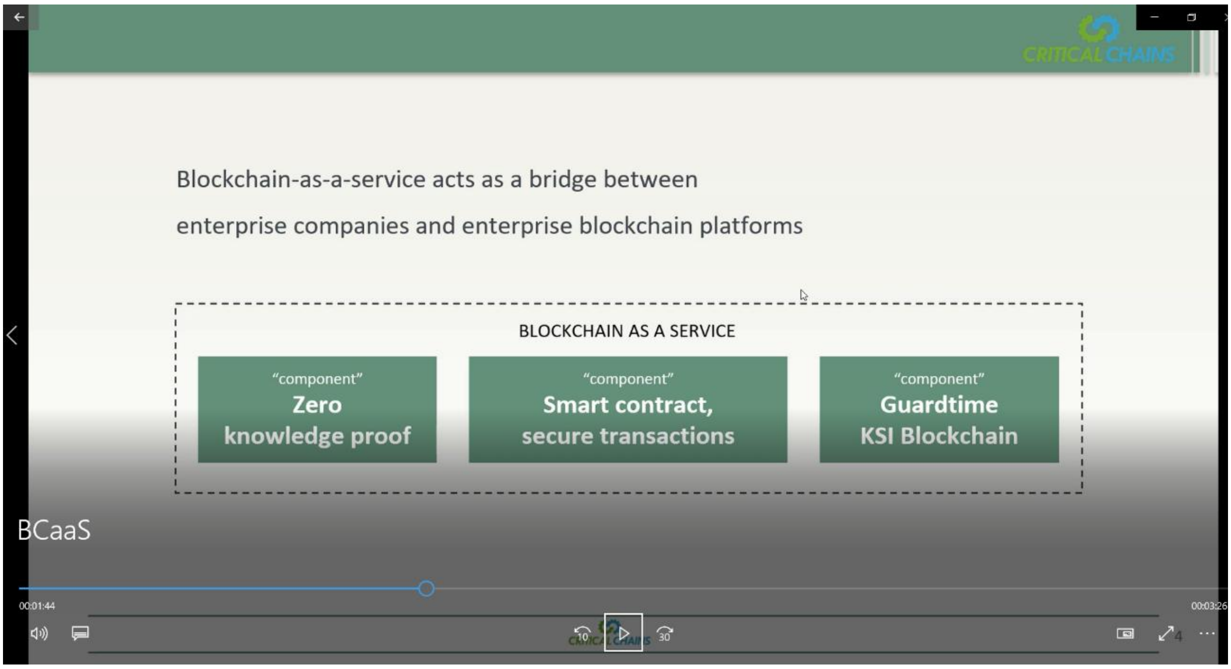
- **BCaaS Video**

  The video briefly explains the novel Blockchain as a service method developed within the context of Critical-Chains.



Blockchain-as-a-Service (BCaaS)

is a model that supports the deployment of cloud-based services to develop, use and host their blockchain apps, functions and smart contracts. It provides fully-fledged blockchain platforms to ease the development process.



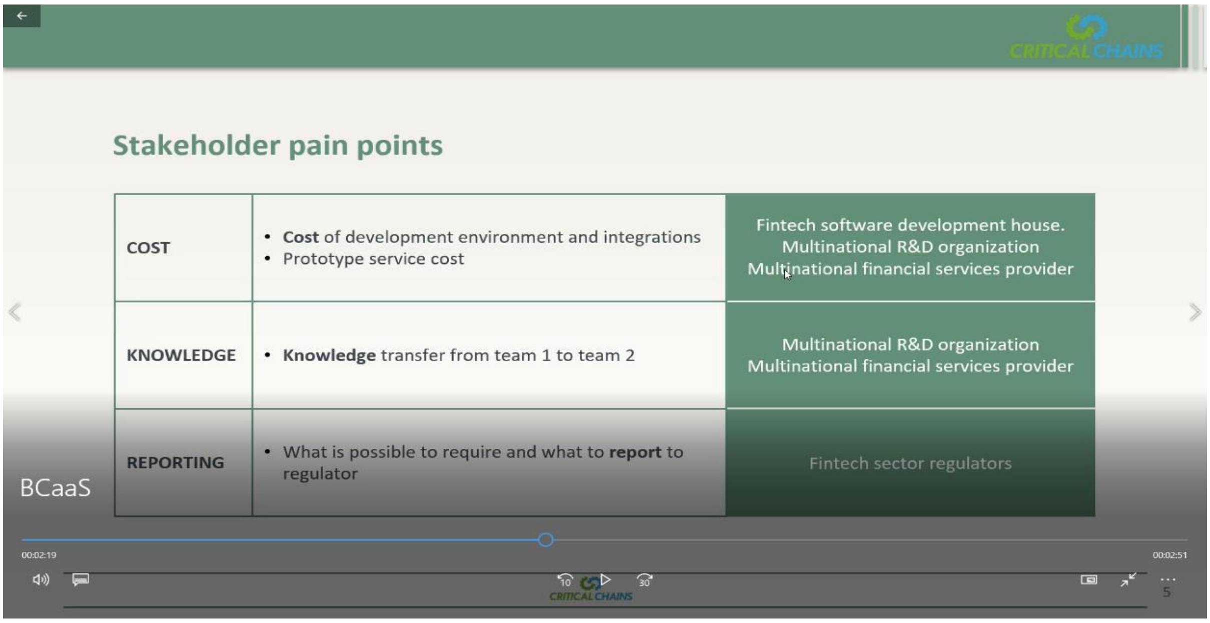
Blockchain-as-a-service acts as a bridge between enterprise companies and enterprise blockchain platforms

BLOCKCHAIN AS A SERVICE

"component" **Zero knowledge proof**

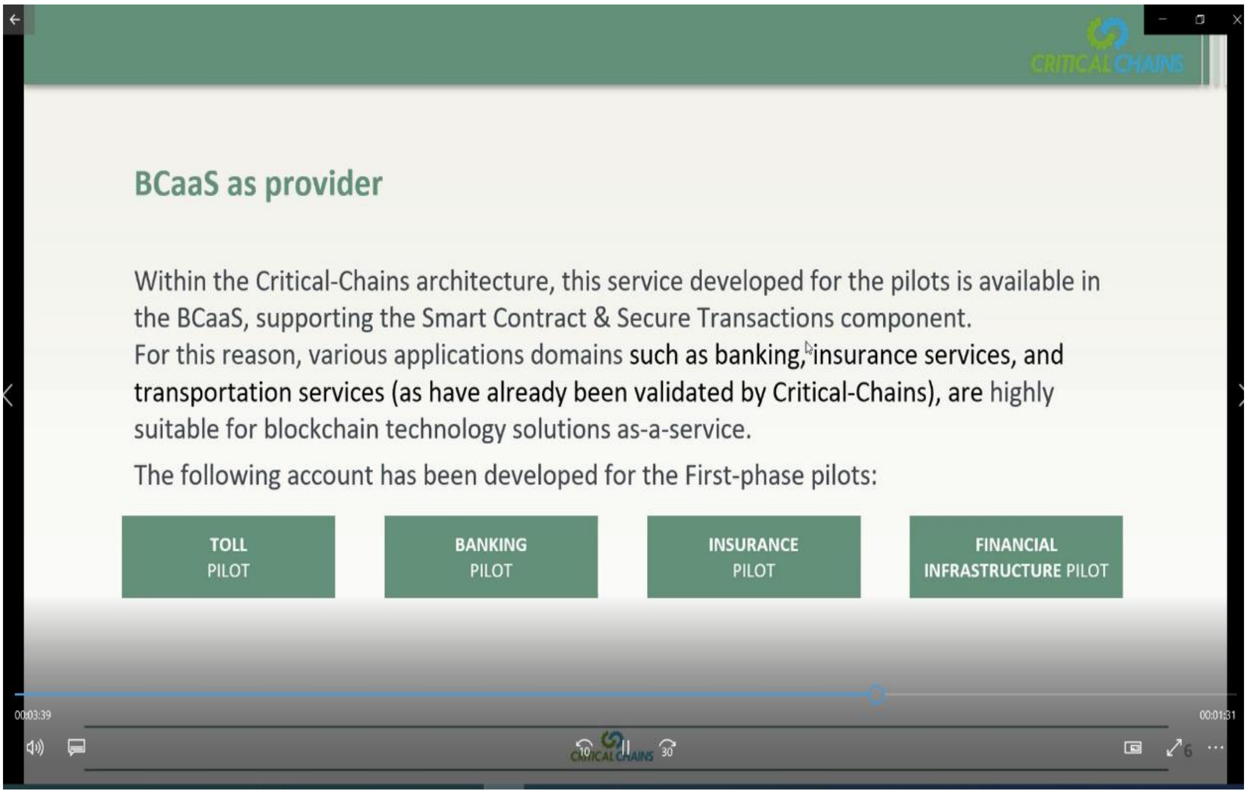
"component" **Smart contract, secure transactions**

"component" **Guardtime KSI Blockchain**



Stakeholder pain points

COST	• **Cost** of development environment and integrations • Prototype service cost	Fintech software development house. Multinational R&D organization Multinational financial services provider
KNOWLEDGE	• **Knowledge** transfer from team 1 to team 2	Multinational R&D organization Multinational financial services provider
REPORTING	• What is possible to require and what to **report** to regulator	Fintech sector regulators



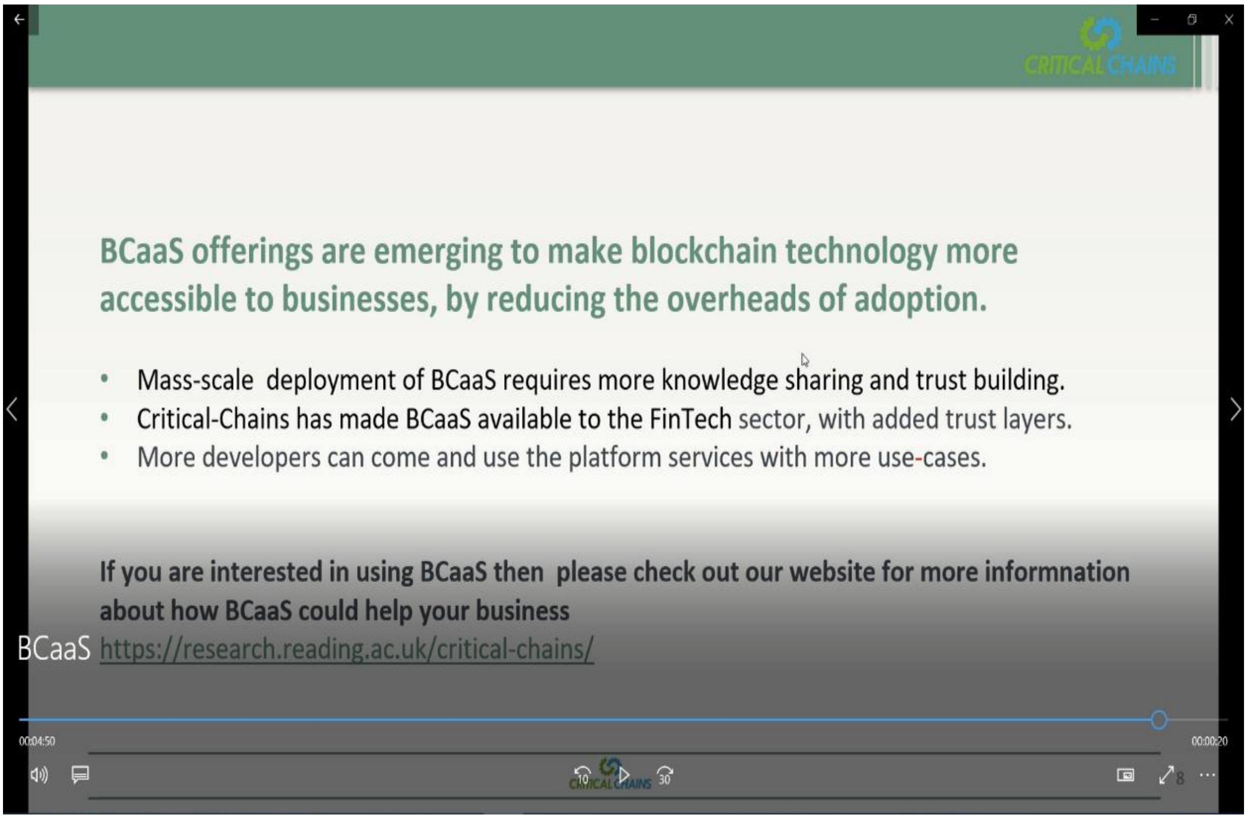
CRITICAL CHAINS

BCaaS as provider

Within the Critical-Chains architecture, this service developed for the pilots is available in the BCaaS, supporting the Smart Contract & Secure Transactions component.
For this reason, various applications domains such as banking, insurance services, and transportation services (as have already been validated by Critical-Chains), are highly suitable for blockchain technology solutions as-a-service.

The following account has been developed for the First-phase pilots:

TOLL PILOT | BANKING PILOT | INSURANCE PILOT | FINANCIAL INFRASTRUCTURE PILOT



CRITICAL CHAINS

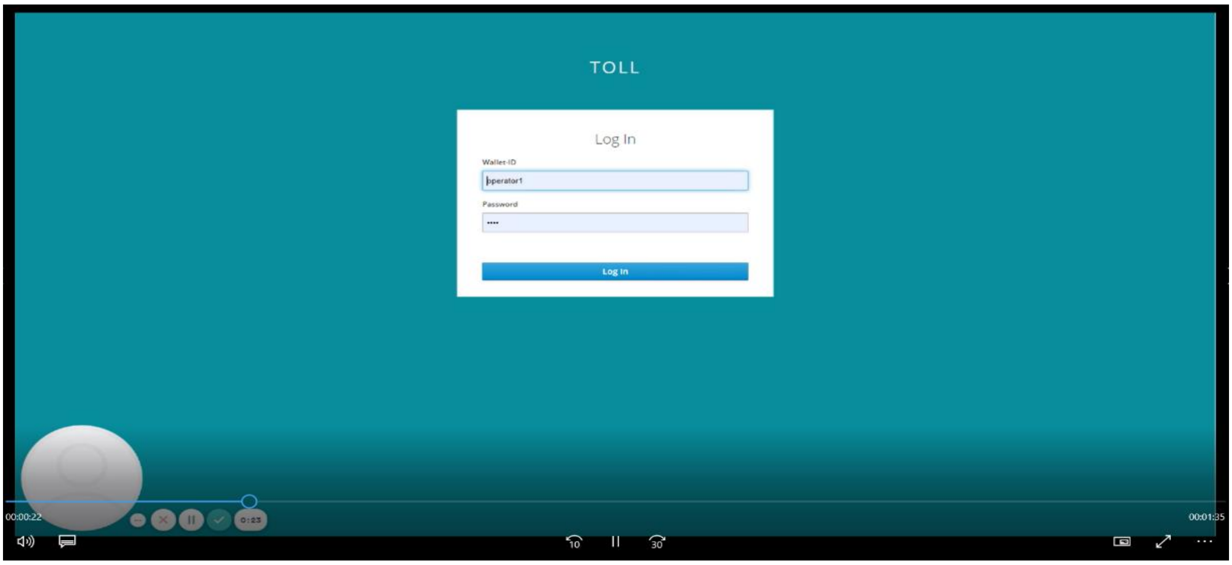
BCaaS offerings are emerging to make blockchain technology more accessible to businesses, by reducing the overheads of adoption.

- Mass-scale deployment of BCaaS requires more knowledge sharing and trust building.
- Critical-Chains has made BCaaS available to the FinTech sector, with added trust layers.
- More developers can come and use the platform services with more use-cases.

If you are interested in using BCaaS then please check out our website for more informnation about how BCaaS could help your business

BCaaS https://research.reading.ac.uk/critical-chains/

- **Toll Collection Pilot Application Demonstration**
  The video shows the demonstration of the toll collection pilot application accessible from the Critical-Chains main page.



TOLL

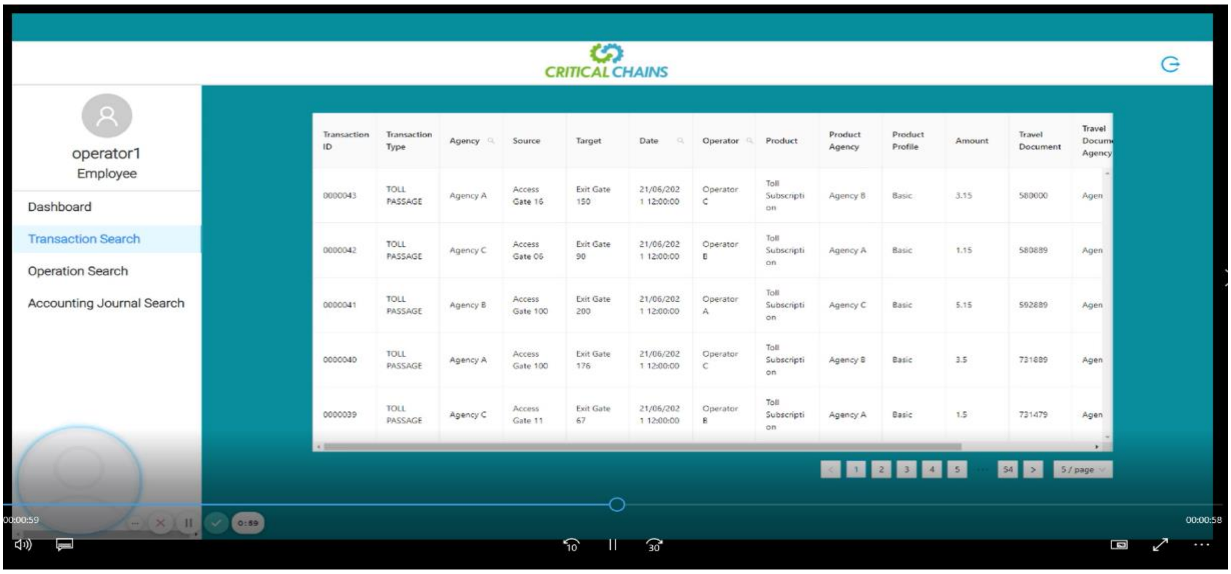
Log In

Wallet-ID

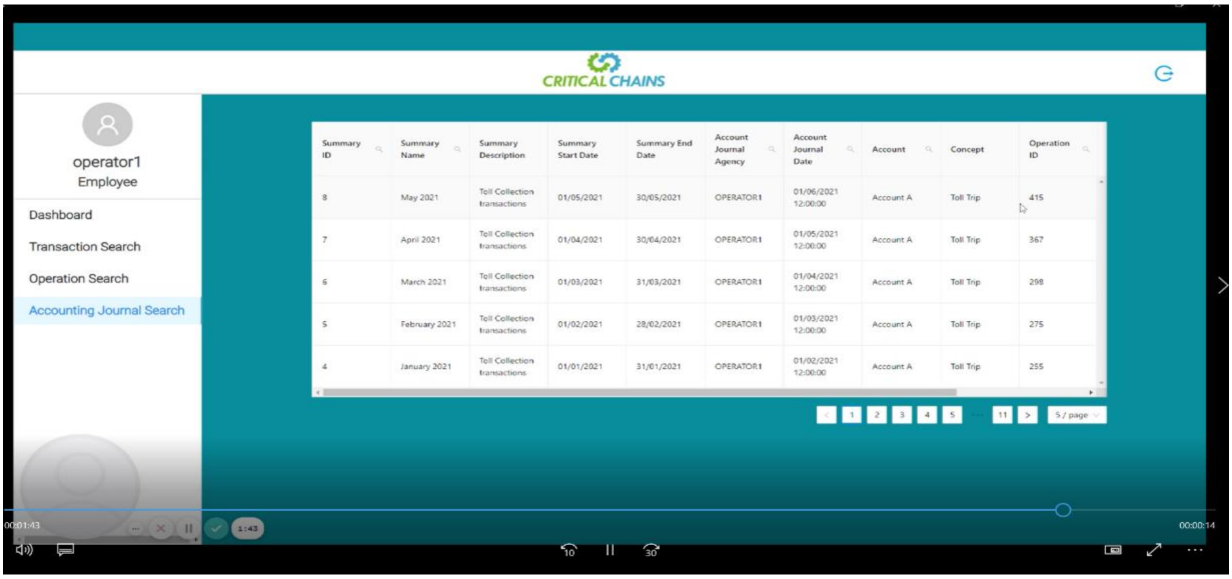
operator1

Password

••••



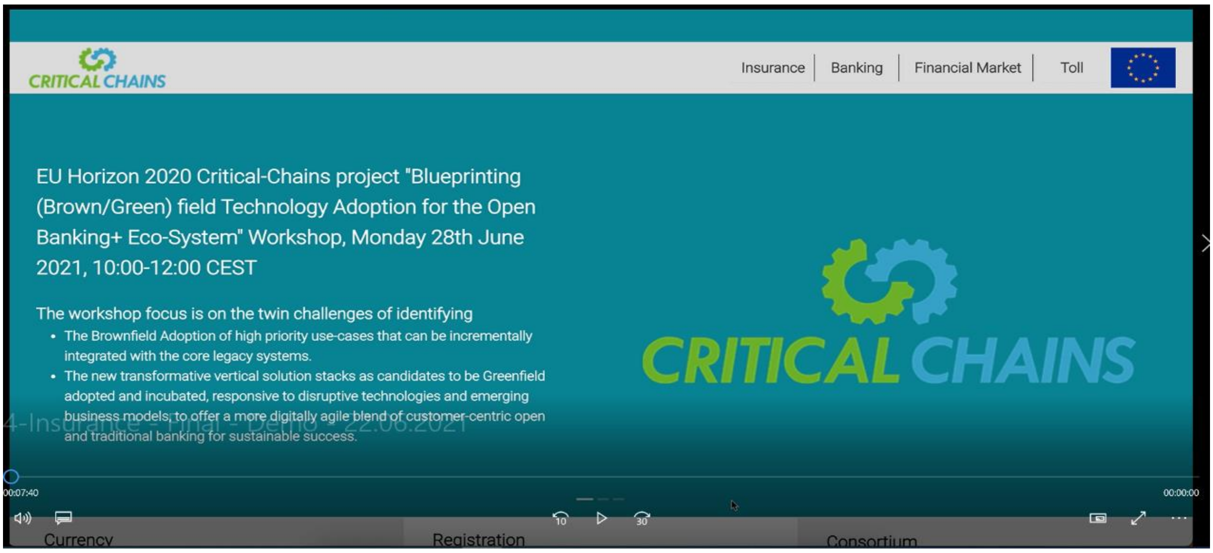
Transaction ID	Transaction Type	Agency	Source	Target	Date	Operator	Product	Product Agency	Product Profile	Amount	Travel Document	Travel Docum Agency
0000043	TOLL PASSAGE	Agency A	Access Gate 16	Exit Gate 150	21/06/202 1 12:00:00	Operator C	Toll Subscripti on	Agency B	Basic	3.15	580000	Agen
0000042	TOLL PASSAGE	Agency C	Access Gate 06	Exit Gate 90	21/06/202 1 12:00:00	Operator B	Toll Subscripti on	Agency A	Basic	1.15	580889	Agen
0000041	TOLL PASSAGE	Agency B	Access Gate 100	Exit Gate 200	21/06/202 1 12:00:00	Operator A	Toll Subscripti on	Agency C	Basic	5.15	592889	Agen
0000040	TOLL PASSAGE	Agency A	Access Gate 100	Exit Gate 176	21/06/202 1 12:00:00	Operator C	Toll Subscripti on	Agency B	Basic	3.5	731889	Agen
0000039	TOLL PASSAGE	Agency C	Access Gate 11	Exit Gate 67	21/06/202 1 12:00:00	Operator B	Toll Subscripti on	Agency A	Basic	1.5	731479	Agen



Summary ID	Summary Name	Summary Description	Summary Start Date	Summary End Date	Account Journal Agency	Account Journal Date	Account	Concept	Operation ID
8	May 2021	Toll Collection transactions	01/05/2021	30/05/2021	OPERATOR1	01/06/2021 12:00:00	Account A	Toll Trip	415
7	April 2021	Toll Collection transactions	01/04/2021	30/04/2021	OPERATOR1	01/05/2021 12:00:00	Account A	Toll Trip	367
6	March 2021	Toll Collection transactions	01/03/2021	31/03/2021	OPERATOR1	01/04/2021 12:00:00	Account A	Toll Trip	298
5	February 2021	Toll Collection transactions	01/02/2021	28/02/2021	OPERATOR1	01/03/2021 12:00:00	Account A	Toll Trip	275
4	January 2021	Toll Collection transactions	01/01/2021	31/01/2021	OPERATOR1	01/02/2021 12:00:00	Account A	Toll Trip	255

- **Insurtech Pilot Application Demonstration**

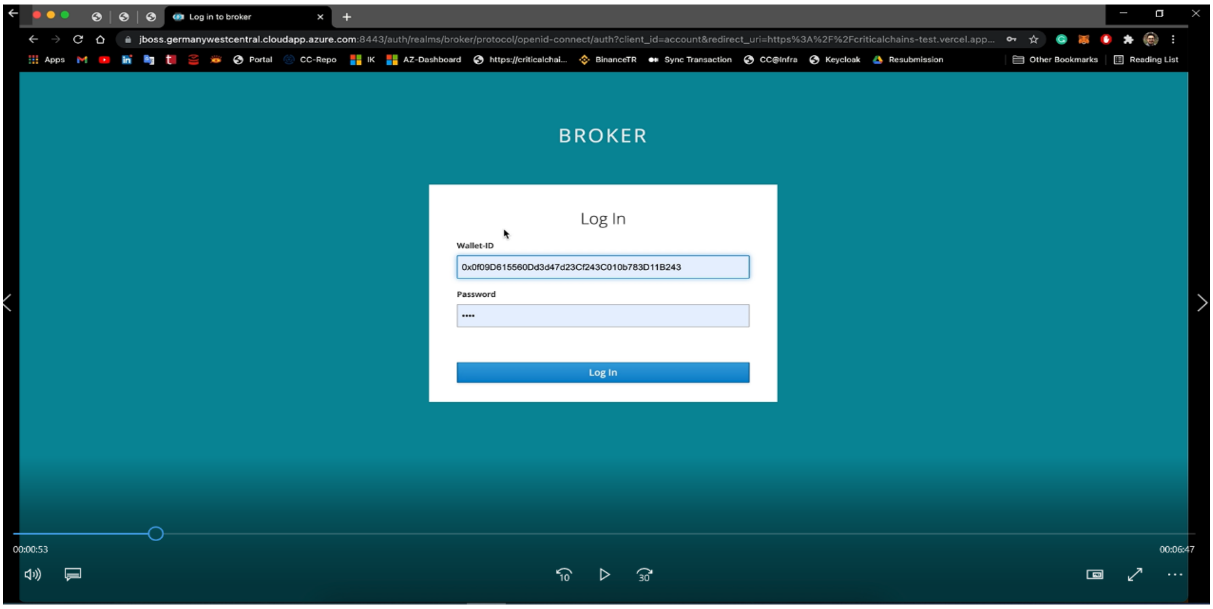
  The demonstration presents the Insurtech Pilot application focusing on the crop insurance use case.



EU Horizon 2020 Critical-Chains project "Blueprinting (Brown/Green) field Technology Adoption for the Open Banking+ Eco-System" Workshop, Monday 28th June 2021, 10:00-12:00 CEST

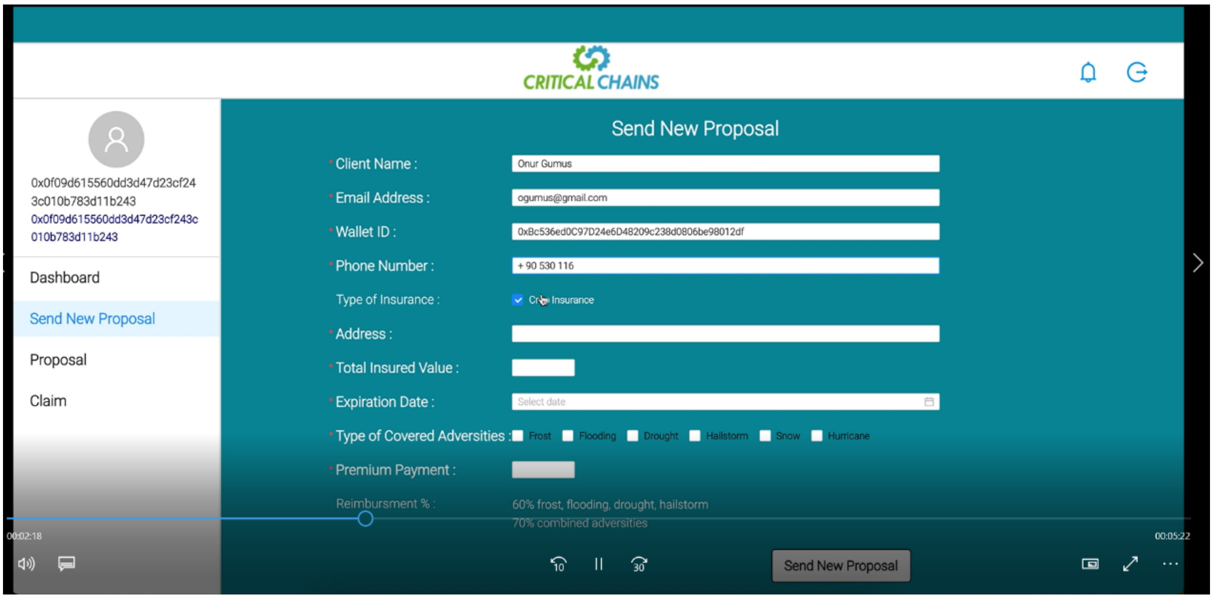
The workshop focus is on the twin challenges of identifying

- The Brownfield Adoption of high priority use-cases that can be incrementally integrated with the core legacy systems.
- The new transformative vertical solution stacks as candidates to be Greenfield adopted and incubated, responsive to disruptive technologies and emerging business models, to offer a more digitally agile blend of customer-centric open and traditional banking for sustainable success.



Wallet-ID: 0x0f09D615560Dd3d47d23Cf243C010b783D11B243

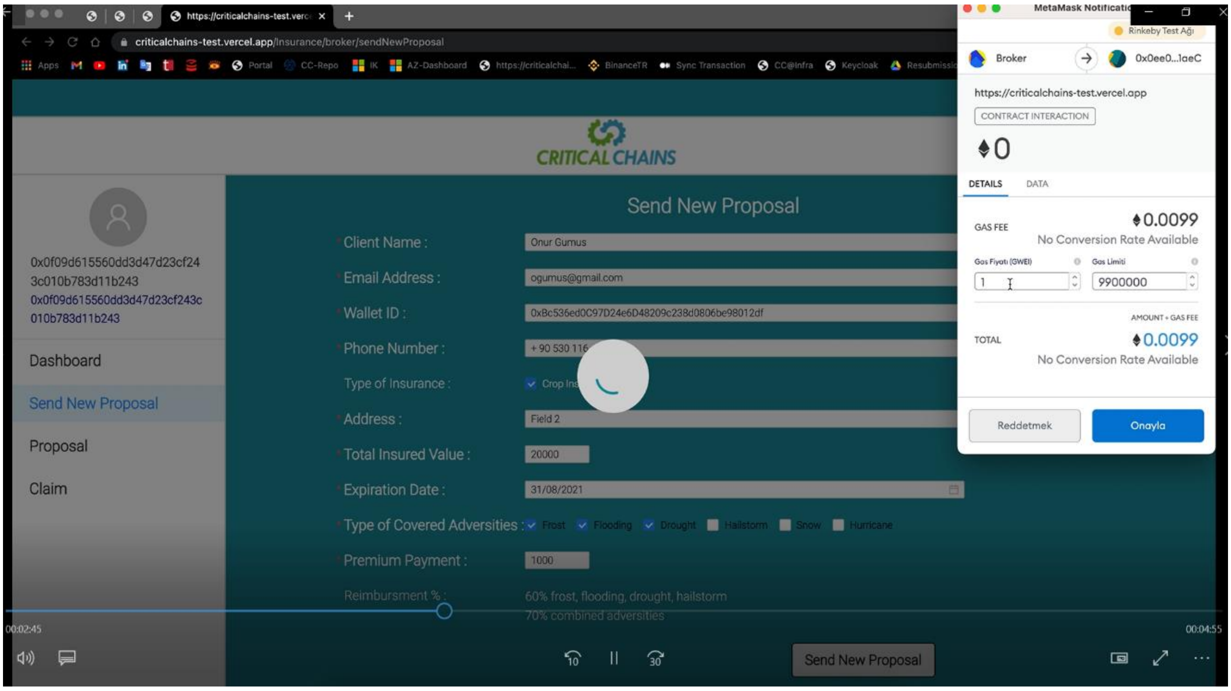
Password: ····



0x0f09d615560dd3d47d23cf24 3c010b783d11b243
0x0f09d615560dd3d47d23cf243c 010b783d11b243

Send New Proposal

Client Name :	Onur Gumus
Email Address :	ogumus@gmail.com
Wallet ID :	0xBc536ed0C97D24e6D48209c238d0806be98012df
Phone Number :	+ 90 530 116
Type of Insurance :	☑ Crop Insurance
Address :	
Total Insured Value :	
Expiration Date :	Select date
Type of Covered Adversities :	□ Frost □ Flooding □ Drought □ Hailstorm □ Snow □ Hurricane
Premium Payment :	
Reimbursment % :	60% frost, flooding, drought, hailstorm 70% combined adversities



https://criticalchains-test.verc
criticalchains-test.vercel.app/Insurance/broker/sendNewProposal
Apps Portal CC-Repo IK AZ-Dashboard https://criticalchai... BinanceTR Sync Transaction CC@Infra Keycloak Resubmissi
CRITICAL CHAINS
Dashboard
Send New Proposal
Proposal
Claim
Send New Proposal
00:02:45
00:04:55
MetaMask Notificati
Rinkeby Test Ağı
Broker
0x0ee0...1aeC
CONTRACT INTERACTION
DETAILS
DATA
Reddetmek
Onayla

0x0f09d615560dd3d47d23cf24
3c010b783d11b243
0x0f09d615560dd3d47d23cf243c
010b783d11b243

Send New Proposal

Client Name : Onur Gumus

Email Address : ogumus@gmail.com

Wallet ID : 0xBc536ed0C97D24e6D48209c238d0806be98012df

Phone Number : + 90 530 116

Type of Insurance : ☑ Crop Ins

Address : Field 2

Total Insured Value : 20000

Expiration Date : 31/08/2021

Type of Covered Adversities : ☑ Frost ☑ Flooding ☑ Drought □ Hailstorm □ Snow □ Hurricane

Premium Payment : 1000

Reimbursment % : 60% frost, flooding, drought, hailstorm
70% combined adversities

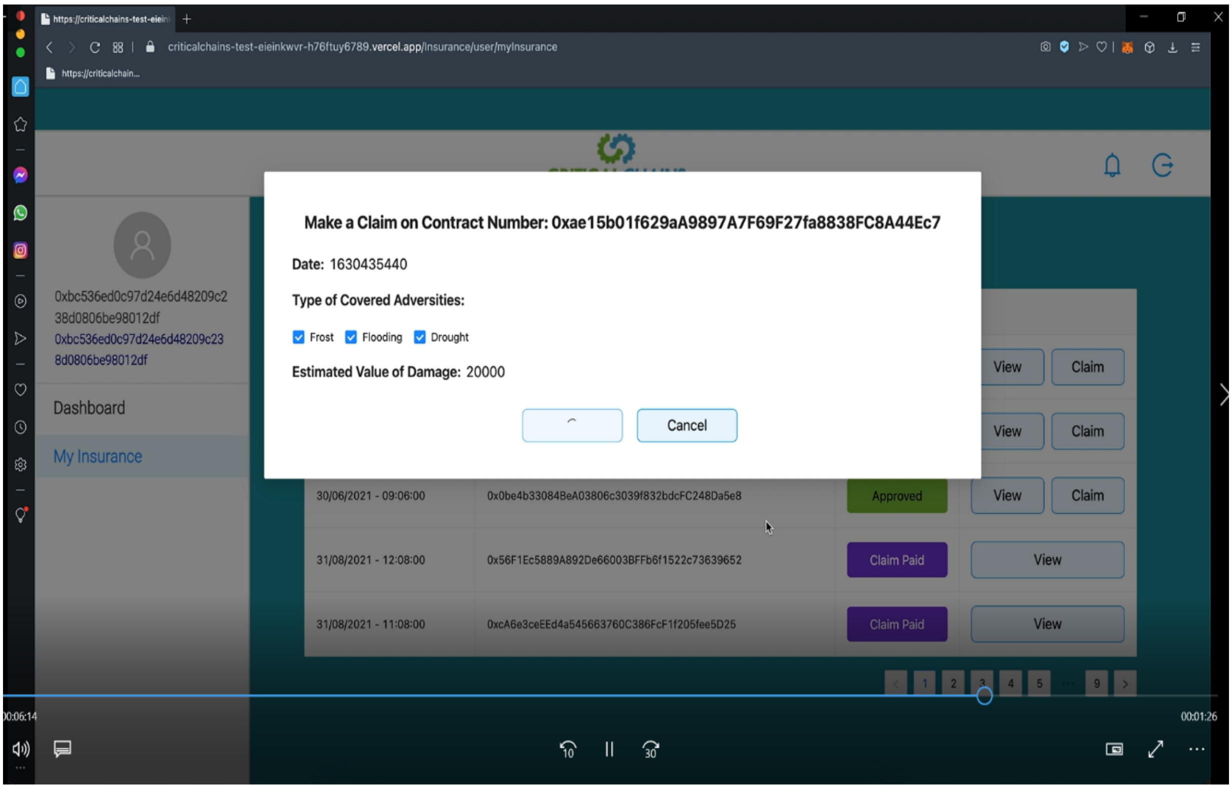
https://criticalchains-test.vercel.app

0

GAS FEE 0.0099
No Conversion Rate Available

Gas Fiyatı (GWEI) 1
Gas Limiti 9900000

AMOUNT + GAS FEE
TOTAL 0.0099
No Conversion Rate Available



https://criticalchains-test-eiein
criticalchains-test-eieinkwvr-h76ftuy6789.vercel.app/Insurance/user/myInsurance
https://criticalchain...
Dashboard
My Insurance
Cancel
View
Claim
1
2
3
4
5
9
00:06:14
00:01:26

0xbc536ed0c97d24e6d48209c2
38d0806be98012df
0xbc536ed0c97d24e6d48209c23
8d0806be98012df

Make a Claim on Contract Number: 0xae15b01f629aA9897A7F69F27fa8838FC8A44Ec7

Date: 1630435440

Type of Covered Adversities:

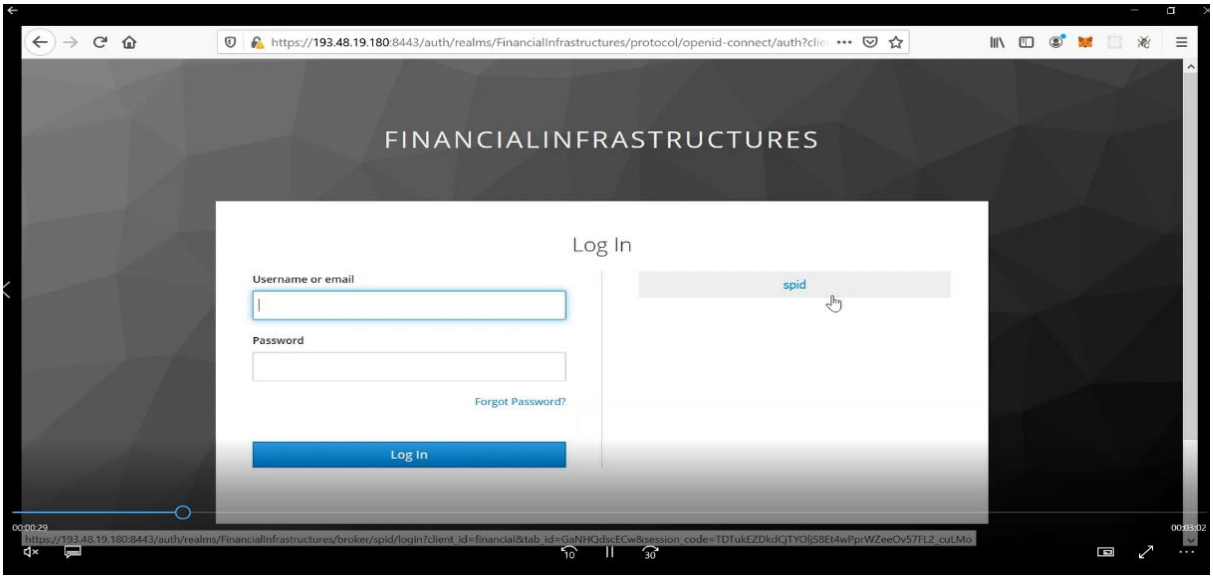
☑ Frost ☑ Flooding ☑ Drought

Estimated Value of Damage: 20000

30/06/2021 - 09:06:00	0x0be4b33084BeA03806c3039f832bdcFC248Da5e8	Approved	View Claim
31/08/2021 - 12:08:00	0x56F1Ec5889A892De66003BFFb6f1522c73639652	Claim Paid	View
31/08/2021 - 11:08:00	0xcA6e3ceEEd4a545663760C386FcF1f205fee5D25	Claim Paid	View

- **Financial Market Pilot Application**

  The video is a demonstration of the financial market infrastructures pilot application developed in the first phase of Critical-Chains project (pension fund application).



https://193.48.19.180:8443/auth/realms/FinancialInfrastructures/protocol/openid-connect/auth?clie

FINANCIALINFRASTRUCTURES

Log In

Username or email

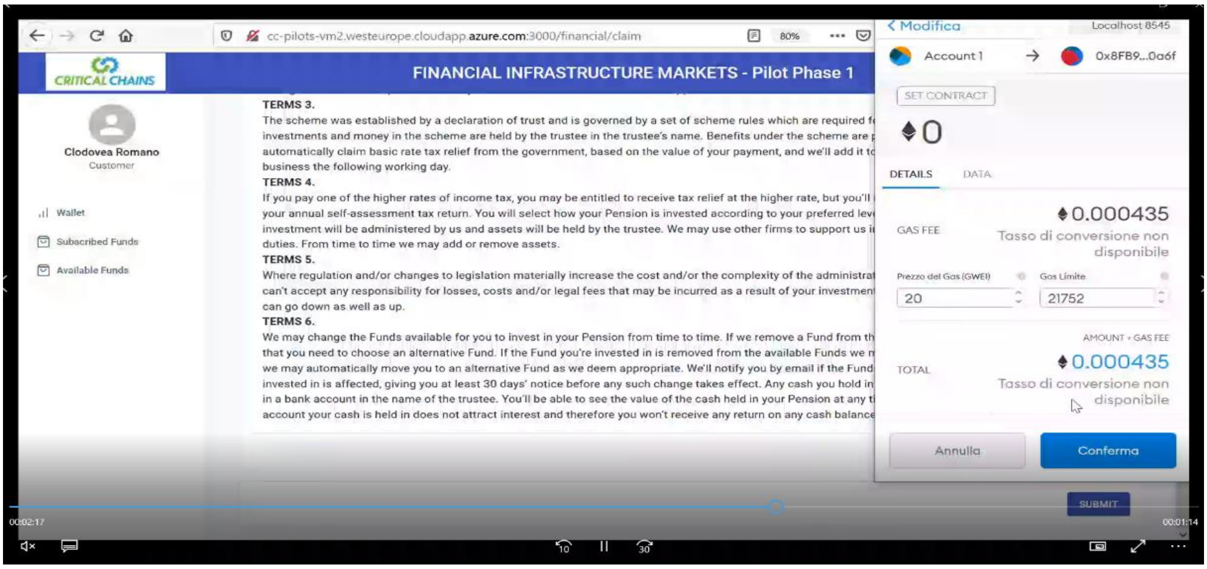
Password

Forgot Password?

Log In

spid

https://193.48.19.180:8443/auth/realms/FinancialInfrastructures/broker/spid/login?client_id=financial&tab_id=GaNHQdscECw&session_code=TDTukEZDkdCjTYOljS8Et4wPprWZeeOv57FL2_cuLMo



cc-pilots-vm2.westeurope.cloudapp.azure.com:3000/financial/claim

FINANCIAL INFRASTRUCTURE MARKETS - Pilot Phase 1

Clodovea Romano
Customer

Wallet
Subscribed Funds
Available Funds

TERMS 3.
The scheme was established by a declaration of trust and is governed by a set of scheme rules which are required f
investments and money in the scheme are held by the trustee in the trustee's name. Benefits under the scheme are p
automatically claim basic rate tax relief from the government, based on the value of your payment, and we'll add it to
business the following working day.
TERMS 4.
If you pay one of the higher rates of income tax, you may be entitled to receive tax relief at the higher rate, but you'll
your annual self-assessment tax return. You will select how your Pension is invested according to your preferred lev
investment will be administered by us and assets will be held by the trustee. We may use other firms to support us i
duties. From time to time we may add or remove assets.
TERMS 5.
Where regulation and/or changes to legislation materially increase the cost and/or the complexity of the administrat
can't accept any responsibility for losses, costs and/or legal fees that may be incurred as a result of your investmen
can go down as well as up.
TERMS 6.
We may change the Funds available for you to invest in your Pension from time to time. If we remove a Fund from th
that you need to choose an alternative Fund. If the Fund you're invested in is removed from the available Funds we n
we may automatically move you to an alternative Fund as we deem appropriate. We'll notify you by email if the Fund
invested in is affected, giving you at least 30 days' notice before any such change takes effect. Any cash you hold in
in a bank account in the name of the trustee. You'll be able to see the value of the cash held in your Pension at any ti
account your cash is held in does not attract interest and therefore you won't receive any return on any cash balance

< Modifica Localhost 8545

Account 1 → 0x8FB9...0a6f

SET CONTRACT

0

DETAILS DATA

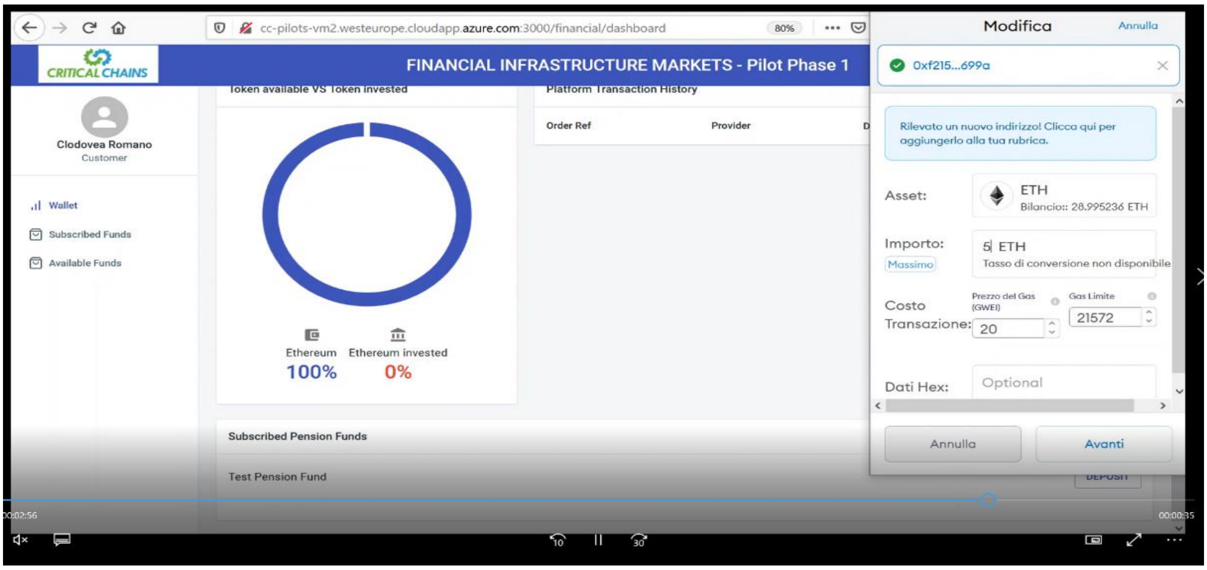
GAS FEE 0.000435
Tasso di conversione non disponibile

Prezzo del Gas (GWEI): 20
Gas Limite: 21752

AMOUNT + GAS FEE
TOTAL 0.000435
Tasso di conversione non disponibile

Annulla | Conferma

SUBMIT



cc-pilots-vm2.westeurope.cloudapp.azure.com:3000/financial/dashboard

FINANCIAL INFRASTRUCTURE MARKETS - Pilot Phase 1

Clodovea Romano
Customer

Wallet
Subscribed Funds
Available Funds

Token available VS Token invested

Ethereum 100%
Ethereum invested 0%

Platform Transaction History

Order Ref | Provider

Subscribed Pension Funds

Test Pension Fund

Modifica Annulla

0xf215...699a

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

Asset: ETH Bilancio:: 28.995236 ETH

Importo: 5 ETH
Massimo
Tasso di conversione non disponibile

Costo Transazione: Prezzo del Gas (GWEI) 20 Gas Limite 21572

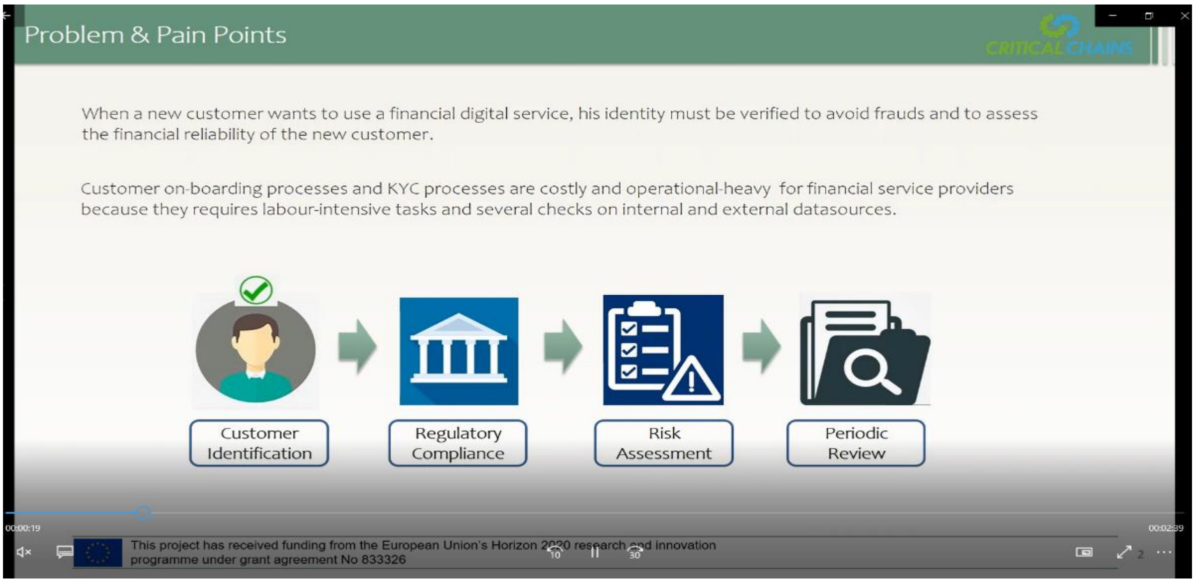
Dati Hex: Optional

Annulla | Avanti

DEPOSIT

- **Critical-Chains SPID Authentication**

The video shows the eIDAS compliance authentication access to the Critical-Chains main framework using the national digital identity SPID.

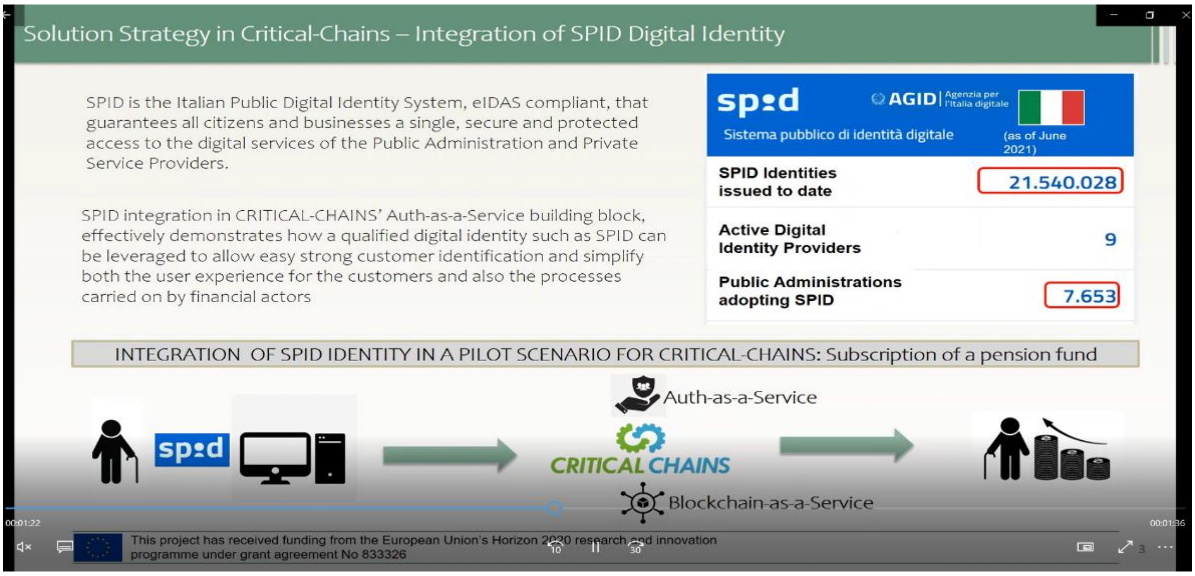


Problem & Pain Points

When a new customer wants to use a financial digital service, his identity must be verified to avoid frauds and to assess the financial reliability of the new customer.

Customer on-boarding processes and KYC processes are costly and operational-heavy for financial service providers because they requires labour-intensive tasks and several checks on internal and external datasources.

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



Solution Strategy in Critical-Chains – Integration of SPID Digital Identity

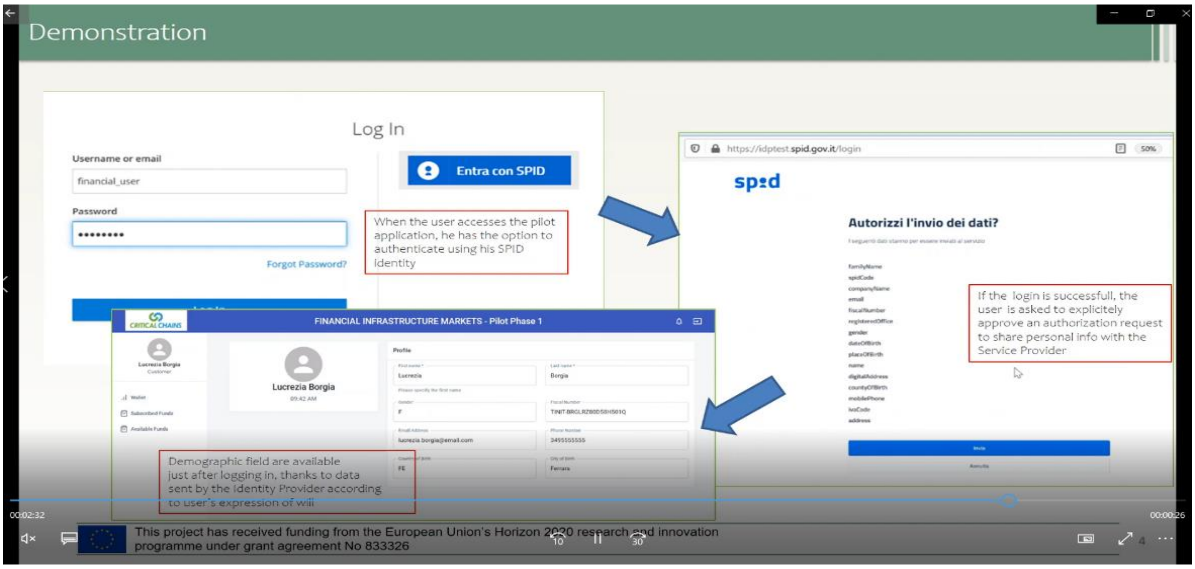
SPID is the Italian Public Digital Identity System, eIDAS compliant, that guarantees all citizens and businesses a single, secure and protected access to the digital services of the Public Administration and Private Service Providers.

SPID integration in CRITICAL-CHAINS' Auth-as-a-Service building block, effectively demonstrates how a qualified digital identity such as SPID can be leveraged to allow easy strong customer identification and simplify both the user experience for the customers and also the processes carried on by financial actors

spid Sistema pubblico di identità digitale	AGID Agenzia per l'Italia digitale (as of June 2021)
SPID Identities issued to date	21.540.028
Active Digital Identity Providers	9
Public Administrations adopting SPID	7.653

INTEGRATION OF SPID IDENTITY IN A PILOT SCENARIO FOR CRITICAL-CHAINS: Subscription of a pension fund

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



Demonstration

Log In

Username or email: financial_user

Password: ••••••••

When the user accesses the pilot application, he has the option to authenticate using his SPID identity

https://idptest.spid.gov.it/login

spid

Autorizzi l'invio dei dati?

familyName
spidCode
companyName
email
fiscalNumber
registeredOffice
gender
dateOfBirth
placeOfBirth
name
digitalAddress
countyOfBirth
mobilePhone
ivaCode
address

If the login is successfull, the user is asked to explicitely approve an authorization request to share personal info with the Service Provider

FINANCIAL INFRASTRUCTURE MARKETS - Pilot Phase 1

Lucrezia Borgia
Customer

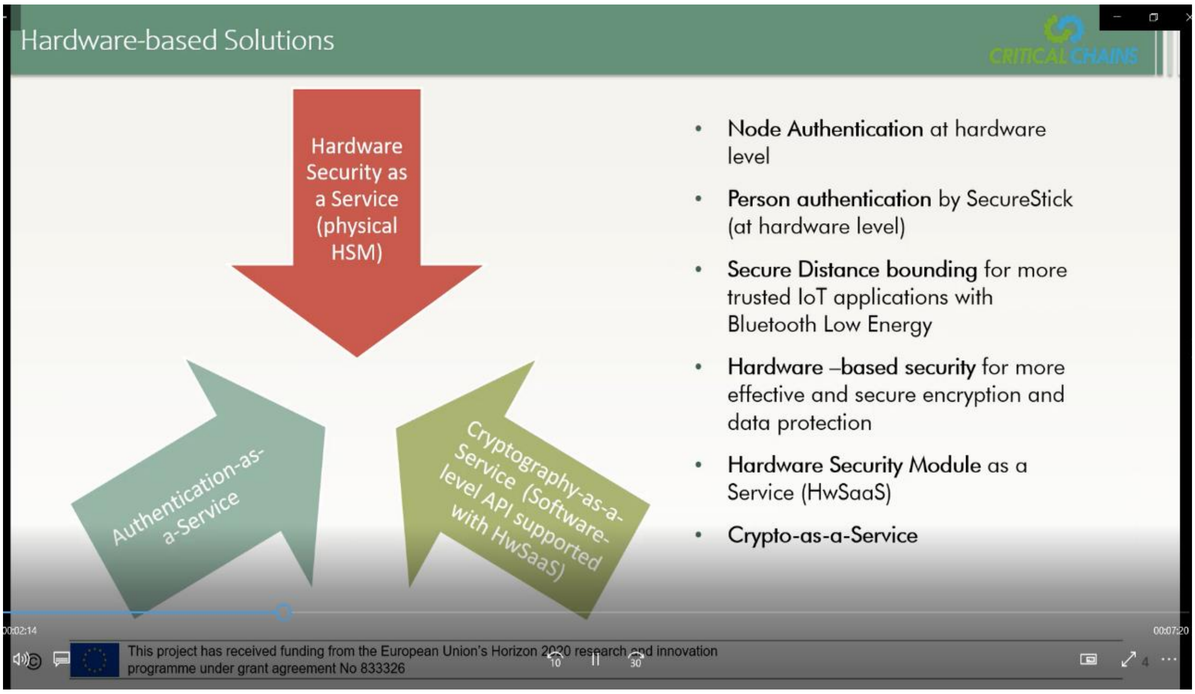
Lucrezia	Borgia
F	TINIT-BRGLRZ80D58H501Q
lucrezia.borgia@email.com	3455555555
FE	Ferrara

Demographic field are available just after logging in, thanks to data sent by the Identity Provider according to user's expression of will

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

- **Hardware based solution and Secure Stick**

The video presents the hardware-based security solution developed in Critical-Chains project with its three main technologies: Authentication as a Service, Hardware Security as a Service and Cryptography as a service. In particular the video explains the authentication with the Secure Stick**.**



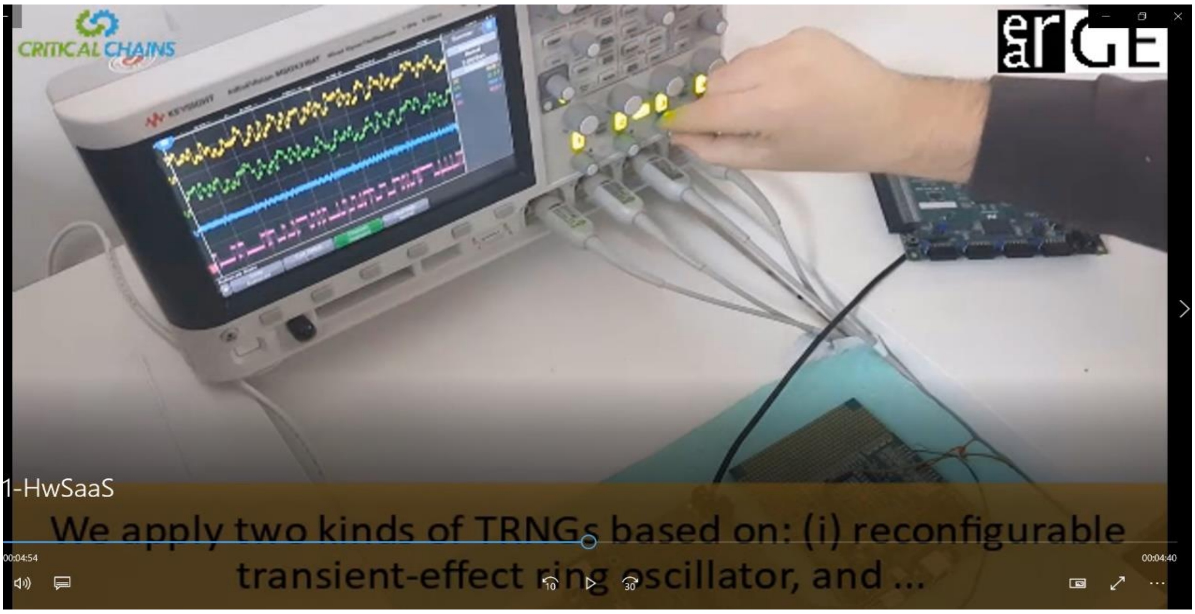
Hardware-based Solutions

CRITICAL CHAINS
Hardware Security as a Service (physical HSM)
Authentication-as-a-Service
Cryptography-as-a-Service (Software-level API supported with HwSaaS)
00:02:14
00:07:20
10
30

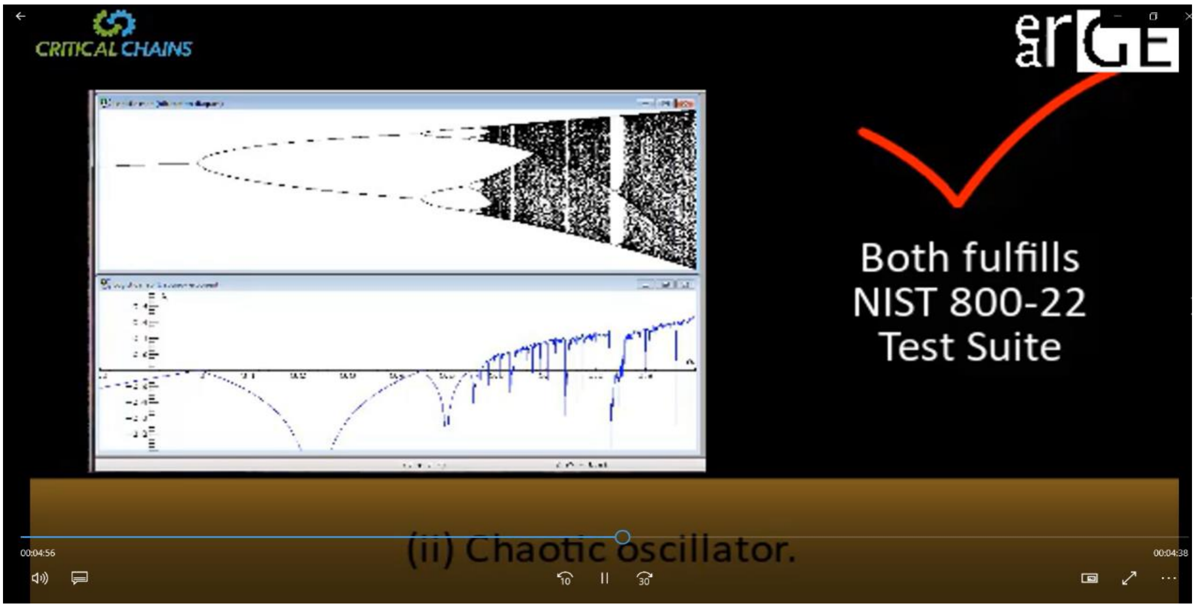
- **Node Authentication** at hardware level
- **Person authentication** by SecureStick (at hardware level)
- **Secure Distance bounding** for more trusted IoT applications with Bluetooth Low Energy
- **Hardware –based security** for more effective and secure encryption and data protection
- **Hardware Security Module** as a Service (HwSaaS)
- **Crypto-as-a-Service**

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

Hardware Security as a Service
Cryptography as a Service

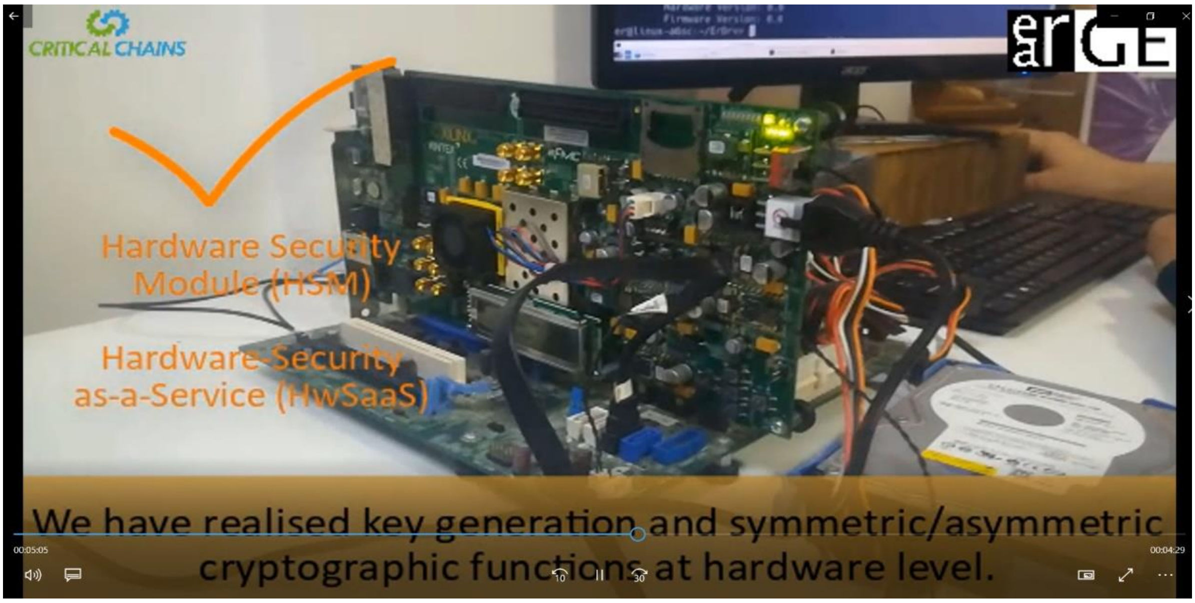


We apply two kinds of TRNGs based on: (i) reconfigurable transient-effect ring oscillator, and ...



Both fulfills NIST 800-22 Test Suite

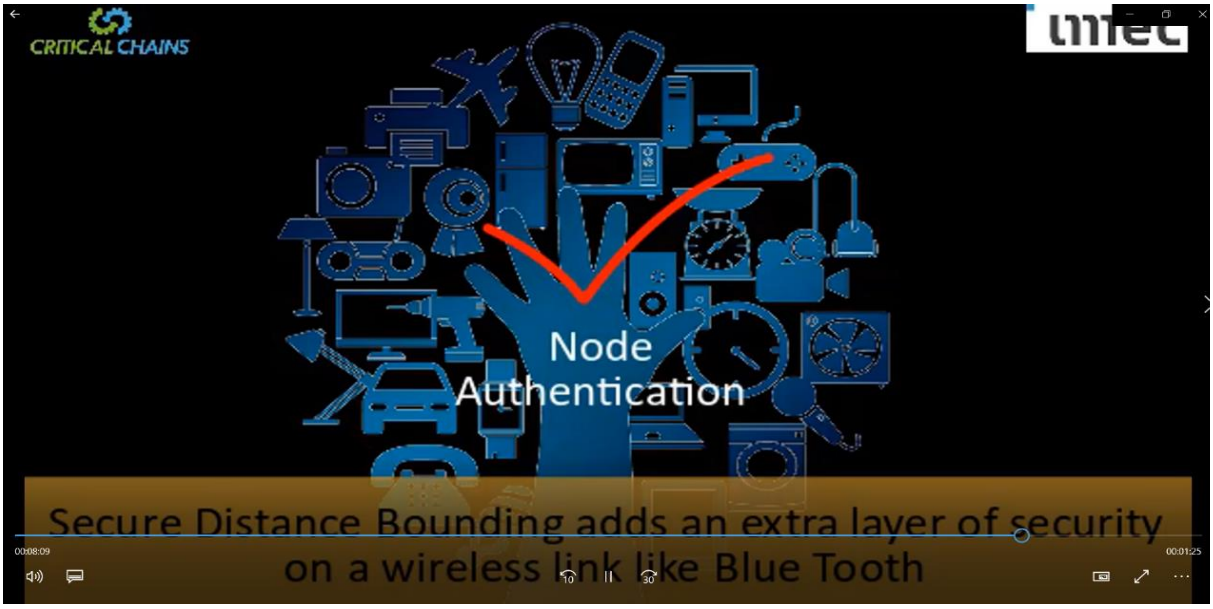
(ii) Chaotic oscillator.



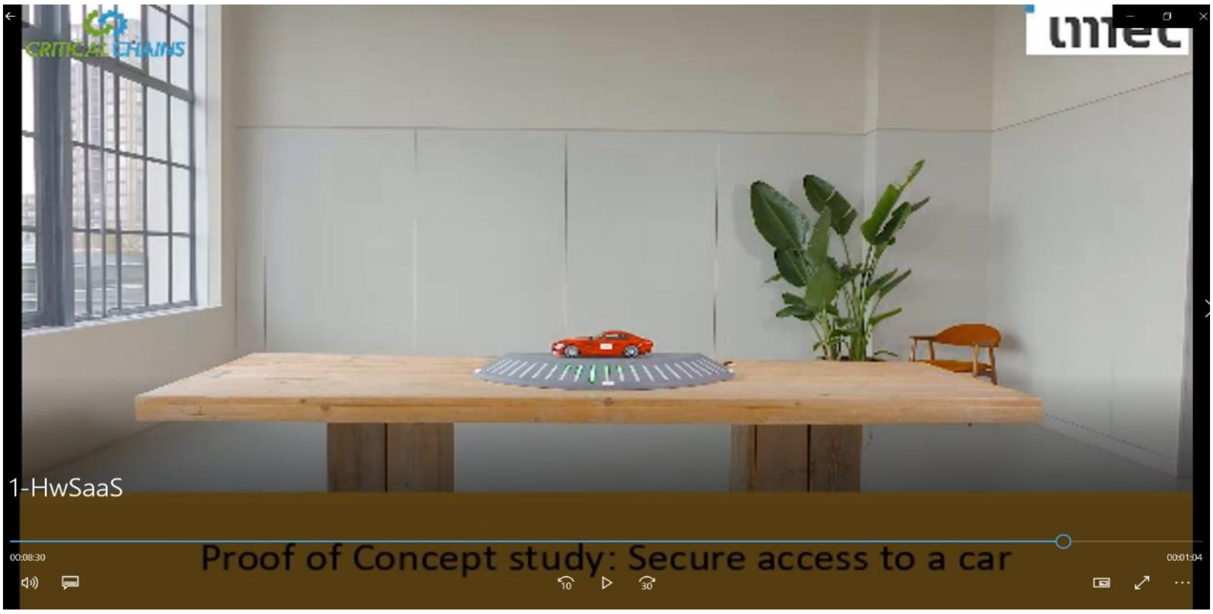
Hardware Security Module (HSM)

Hardware-Security as-a-Service (HwSaaS)

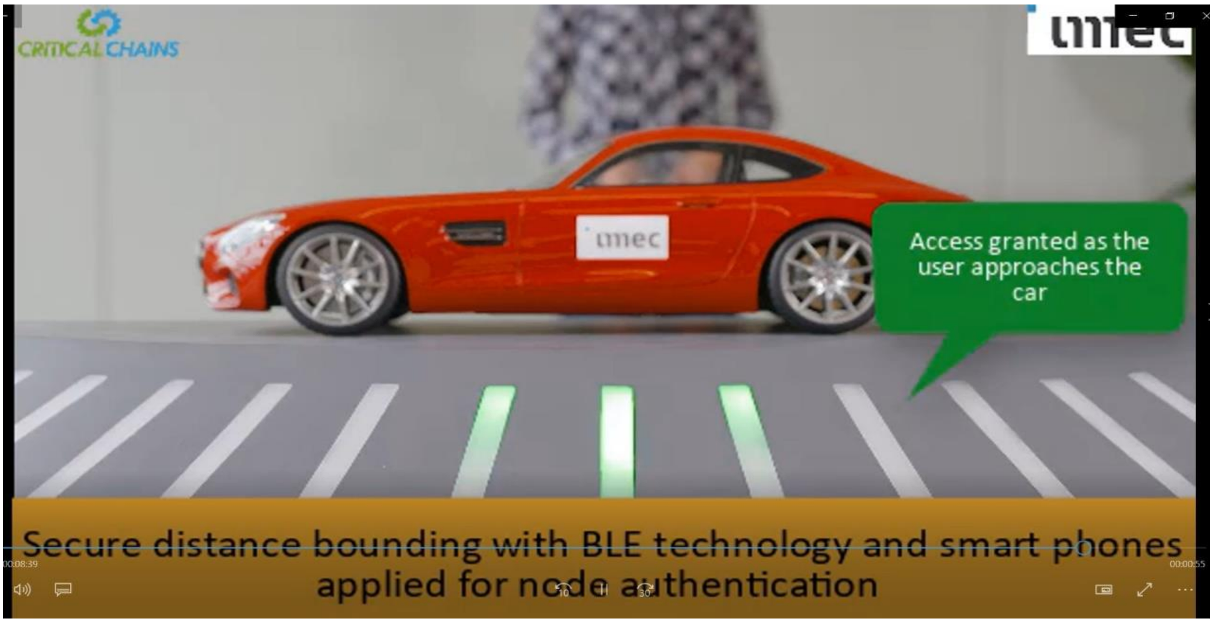
We have realised key generation and symmetric/asymmetric cryptographic functions at hardware level.



Secure Distance Bounding adds an extra layer of security on a wireless link like Blue Tooth



Proof of Concept study: Secure access to a car



Secure distance bounding with BLE technology and smart phones applied for node authentication

9 Events

The Critical-Chains Team performed actions in order to strength the identity of the project and its visibility through several presentations and exhibitions in various events.

A complete of list of events is included in chapter 10 “Table of Performed and Planned Communication & Dissemination Action”.

9.1 Outcome 6: performed events

Main events attended in the period were:

- **Project-to-Policy Workshop**: The Critical-Chains Coordinator Professor Atta Badii represented the Critical-Chains Consortium for the Policy Workshop held at the REA, Brussels and was able to highlight the project objectives and the need to examine the regulatory and certification framework responsive to the evolutionary trends in Fintech and the emergent forms of payment systems and intermediation.
- **The Ethics of Blockchain Workshop**: The workshop considered the ethical issues relating to the large-scale take-up of blockchain technology and viewed the main issues as arising from the challenge to ensure accountability and healthy governance over the blockchain and the need for accountability but also avoiding the longer-term adverse impacts of large-scale blockchain adoption. The workshop was attended by 25 delegates and included 7 presentations on issues relating to the ethical and socio-technical aspects of Blockchain innovation; these were delivered in an informal interactive setting, which invited interventions by the audience and provoked much discussion; this provided an excellent opportunity for exchanges of insight.

The following section presents a detailed description of dissemination events arranged by UREAD:

Responsible Research & Innovation Workshop 1, 11th-12 July 2020

The project kick-off meeting was held on 11th -12 July 2019 and included a workshop style discussion on project research and agenda and implementation objectives and challenges as well a tutorial presentation and discussions.

- Session 1, Ethical, Legal and Societal Impacts, 11th July 2019

This session was led by Dr Julian Stubbe on the ethical challenge of blockchain for responsible research and innovation. This talk addressed the need to consider the social and ethical impact of disruptive technology within a framework approach that encourages ethically and socially reflective innovation and the ethical, legal and social impacts (ELSI). This session concluded with a discussion focused on the ethical and regulatory challenges in adoption of Blockchain technologies.

- Session 2, Stakeholder-Centred Methodological Framework 12th July 2019

Professor Badii presented the principles that motivated the UI-REF framework for integrative user-led Privacy, Security and Accountability by Design. This included a section on the UI-REF ontologically committed interpretivist approach to context-aware prioritisation and conflict resolution of users’ requirements self-expressions and dynamic user-system usability, acceptance, and acceptability evaluation as critical criteria for mainstream ability of the resulting innovation.

Figure 25: Consortium Partners' delegates participating in the Kick-off Research Methodology Workshops

Research Workshop 2: Ethics of Blockchain Date: 17th December 2019

The workshop was organised by the University of Reading and held at the university Park Campus as part of 2-day Project teering meeting and Dissemination activity event. The workshop considered the ethical issues relating to the large-scale take-up of blockchain technology and viewed the main issues as arising from the challenge to ensure accountability and healthy governance over the blockchain and the need for accountability but also avoiding the longer-term adverse impacts of large-scale blockchain adoption.

The workshop was attended by 25 delegates and included 7 presentations on issues relating to the ethical and socio-technical aspects of Blockchain innovation; these were delivered in an informal interactive setting, which invited interventions by the audience and provoked much discussion; this provided an excellent opportunity for exchanges of insight.

Professor Atta Badii chaired the Q & A session and acted as the discussant conducting the final interactive reflective session.

Presentations were from the following contributors and those cleared for publication on the website have been uploaded at the URLs appearing for each presenter as set out below:

- Mr James King, Senior Solutions Consultant, Vizidox Solutions Limited, Oxford, UK - https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/Blockchain-Innovation-Ethical-Challenges-JamesKing.pdf
- Dr Alper Kanak, Director of Research & Development, ERARGE & ERGTECH, Istanbul, Turkey https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/DigitalTwin-Ethics-Blockchain-AlperKanak-ERARGE.pdf
- Mr Bakhtiyor Yokubov PhD Student, Computer Science, Brunel University https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/Blockchain_in_Education-Bakhtiyor_Yokubov.pdf
- Mr Vincent Bryce, University of Nottingham's Horizon Institute for Doctoral Training https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/A-Critical-Chain-Design-Fiction-Vincent-Bryce.pdf
- Mr Kristo Klesment, R&D project manager, Guardtime Tallinn Estonia (Restricted)
- Dr Neil McBride Reader in IT management, Centre for Computing and Social Responsibility, De Montfort University Leicester, UK (Restricted)

Figure 26: Ethics of Blockchain Attendees

Contribution to Project-to-Policy Kick-Off Workshop, Friday 31st January 2020, REA, Brussels Professor Atta Badii represented the Critical-Chains Consortium for the Policy Workshop held at the REA, Brussels and was able to highlight the project objectives and the need for examining theregulatory and certification framework responsive to the evolutionary trends in the Fintech and theemergent forms of payment systems and intermediation. the Critical-Chains project presentation isappended to this deliverable.

Contribution to the FIN-TECH Project Webinar (https://www.fintech-ho2020.eu/) **- 19th May 2020** At the invitation of the FIN-TECH Project Professor Badii delivered a presentation about the Critical-Chains prophecy research and innovation objectives and challenges as a contribution on the part of the Consortium jointly prepared by the Dissemination Manger (RINA-C) and UREAD.

Participation at the 1st ECSCI (European Cluster for Securing Critical Infrastructures) virtual workshop to be held on June 24-25, 2020.

This event was hosted by the FINSEC Project (https://www.finsec-project.eu/. Professor Badii participated in this workshop on behalf of the Consortium as a first step to contributing to the Fintech Security Research Community as an integral of the Critical-Chains clustering and outreach programme.

Clustering Activities Planning with the SOETER Project (https://soterproject.eu/)

Email Communication with representatives from the SOETER project over the period March to June 2020 discussing collaboration towards joint clustering activities culminated in the meeting with 4 members of the SOETER project on the 23rd of June whereby it was agreed that the Critical-Chains Projectand SOETER will organise future webinars for joint dissemination of their innovation results using the RINA-C webinar channel.

Stakeholder Engagement

Stakeholder Group members are invited to our public workshops and can have access to the public deliverables but are also invited to contribute to the requirements revision through special sessions to be held alongside our planned public workshops whereby following presentations of project results to stakeholders they would be invited to express their opinion regarding the various aspects of design and deployment of Critical-Chains services. Accordingly, so far one financial sector company namely (Ub-Technologies NL B.V. https://ubtechnologies.nl/) has been duly approved to join as the first member of the Critical-Chains Stakeholder Group.

Blueprinting (Brown/Green) field Technology Adoption for the Open Banking+ Eco-System Webinar
Critical-Chains project held a webinar on the 28th of June 2021 about the Blueprinting (Brown/Green) field Technology Adoption for the Open Banking+ Eco-System. It has been basically discussed which are the main barriers in fielding new technologies/solutions in the banking/finance sector and how Critical-Chains with its pilots is dealing with it. In this respect, in Session 2, a series of presentations of Critical-Chains demo pilots has been presented by Critical-Chains partners:

- Integrated Secure Authentication and Distance Bounding for Remote Access Control. Demonstration by Dr Alper Kanak (ERARGE), Mr Gert-Jan van Schaik (IMEC).
- Banking Pilot application, Vito Domizio, EY
- Fintech Pilot Application, Marco Avallone, Poste Italiane
- Insurtech Pilot Application, Vito Domizio, EY and Onur Gümüş, NETAŞ
- Highway Toll Collection Pilot Application, Juan Manuel Castro Arias, INDRA
- Critical-Chains Main Framework, Onur Gümüş, NETAŞ

External use-cases has been presented to frame solution provider and stakeholders needs and implementation challenges in finance and banking environment:

- SDX Network use-case
- Ub Technologies use-case

The webinar has been held on the GoToWebinar channel of RINA-C.

9.2 Outcome 7: future events

Clustering Activities Planning with the FIN-TECH Project (https://www.fintech-ho2020.eu/) Following discussions with the FIN-Tech Coordinator, possible collaboration with the Consortiummembers particularly with respect to outreach to the FINTECH stakeholders have been explored and it is planned to involve the FIN-TECH project members in the organisation of our future Critical-Chains webinars with the SOETER project.

Clustering Activities Planning with the FINSEC Project (https://www.finsec-project.eu/)
The Critical-Chains Consortium has also proposed collaboration for joint dissemination activities with the FINSEC project and this is in progress.

10 C&D KPIs

Critical-Chains communication and dissemination strategy effectiveness will be measured on a six-monthly basis in order to track the proper key performance indicators:

- Project awareness: website traffic
- Engagement: social media metrics
- Target loyalty: percentage of content consumed by target groups

11 Table of Performed and Planned Communication & Dissemination Action

11.1 Dissemination Table

Initiating Partner(s)' Name(s)	Type of event	Event Title	Link	Place	Description	Date	Status	Target
UREAD	Participation in a Conference	Ethics of Blockchain	https://research.reading.ac.uk/critical-chains/the-ethics-of-blockchain-workshop-17th-december-2019/	University of Reading	Conference lead by Prof. Badii on the topic of ethical issues relating to large-scale take-up of Blockchain technology. Final reflections also presented by Prof. Badii.	17/12/20	Performed	Scientific Community
UREAD	Participation in a Conference	Project-to-policy workshop	Annex A.2	REA, Brussels	Contribution by Prof. Badii to workshop by highlighting regulatory challenges arising from the rapid transformative evolution of money markets; including mobile money, fintech and Insurtechs.	31/01/20	Performed	Scientific Community
UREAD	Participation in a Conference	Fintech project final conference	Annex A.1	University College London (Webinar)	Presentation by Prof. Badii about new fintech and the mission of the Critical-Chains project in that context, presented to the fintech project final workshop	19/05/20	Performed	Scientific Community
UREAD	Internal Training presentations	Training presentations		Online	Multiple sessions of Awareness and training workshops on various technological and scientific aspects of privacy by co-	11/07/19-30/07/20	Performed	Consortium Members

Initiating Partner(s)' Name(s)	Type of event	Event Title	Link	Place	Description	Date	Status	Target
					design and secure semantic integration of cyber-physical system by Prof. Badii.			
NETAS	Participation in a Conference	Ethics of Blockchain	https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/DigitalTwin-Ethics-Blockchain-AlperKanak-ERARGE.pdf	University of Reading	Presentation by Alper Kanak, PHD, 'Ethical Discussion on Blockchain-based Accountability for Secure and Collaborative Digital Twin Environments – A Case Study on Smart City Transportation'	17/12/20	Performed	Scientific Community
Guardtime	Participation in a Conference	Ethics of Blockchain	(Restricted)	University of Reading	Presentation by Mr Kristo Klesment.	17/12/20	Performed	Scientific Community
NETAS	Website		http://www.netas.com.tr/en/media/blockchain-project-from-netas-to-make-turkey-a-stakeholder-in-securing-eu-s-independent-payment-system/	Online	NETAS website updated for media about Critical-Chains	03/04/2019	Performed	General Public
INDRA	Website			Online	Critical-Chains information added to Indra's website	2020	Performed	General Public
ERARGE	Social Media			Online	Published information about Critical-Chains and conferences related to Critical-Chains to their LinkedIn page.	18/10/2019-19/12/2019	Performed	General Public

Initiating Partner(s)' Name(s)	Type of event	Event Title	Link	Place	Description	Date	Status	Target
Fraunhofer EMI	Participation in a Conference	Fraunhofer-Symposium »Netzwert« 2021	https://www.itwm.fraunhofer.de/en/fairs_events/2021/2021_03_23_Netzwert.html	Munich, Germany	During this digital, two-day event, around 30 current projects from Fraunhofer's preliminary research have been presented. Three parallel session blocks have each bundled several converging topics.	23/03/2021	Performed	Scientific Community
IMEC-NL	Participation in a Webinar	FINANCIAL SECTOR CYBERSECURITY COLLABORATION AND ENGAGEMENT OF STAKEHOLDERS	https://youtu.be/y-S0OudWRqE	online	The webinar focused on best practices, motivational factors, and incentives related to collaboration of financial sector cybersecurity stakeholders, such as efforts to share threat intelligence, design common incident reporting workflows, joint risk assessments and others. It will include demos from H2020 projects.	21/05/2021	Performed	Scientific Community
GT	Participation in a Conference	Extension of ICT Verticals and horizontals for Blockchain Standardisation	Link	Online		24/03/2021	Performed	Industry

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

ERARGE	Participation in a Conference	IEEE 12th Latin American Symposium on Circuits & Systems (LASCAS)	https://lascas2021.pe/	Online	Technical discussion with audience on the use of hardware-based security solutions in IoT-enabled and decentralised payment systems (e.g., with cryptocurrencies, NFC and BLE enabled on-the-fly payment,	23-25/02/2021	Performed	Scientific Community
ERARGE	Participation in a Conference	IEEE International Symposium on Circuits and Systems (ISCAS 2021)	https://www.iscas2021.org/	Daegu-S.Korea/ online	RARGE researchers presented their ongoing work related to hardware-based security and also mentioned Critical-Chains as one of the related projects in this emerging research area.	25-28/05/2021	Performed	Scientific Community
GT	Participation in a Conference	Reference architecture for cross-border and cross-sector energy data exchange	https://global.gotowebinar.com/join/7044870479597143309/481907559&sa=D&source=calendar&ust=1622301542203000&usg=AOvVaw0_WpWL8hDMepr8biX9c92m	GoTo Webinar	Attendance to the event	26/03/2021	Performed	Industry
GT	Participation in a Conference	Decentralised ground segment Authentication using Blockchain Technology	https://meet.lync.com/esa.int/marcus.wallum/TUZPJ65X&sa=D&source=calendar&ust=1622301558059000&usg=AOvVaw03puKxI9y6T3qUyZls6QWn	Lync	Attendance to the event	30/03/2021	Performed	Industry

GT	Participation in a Conference	Extension of ICT Verticals and Horizontals for Blockchain Standardisation // Smart-Contracts Roundtable	Link	MS Teams	Attendance to the event	21/04/2021	Performed	Industry
GT	Participation in a Conference	NECC: Cybersecurity landscape in EU – Challenges, policy and opportunities	Link	Webex	Attendance to the event	18/05/2021	Performed	Industry
GT	Participation in a Conference	Financial Sector Cybersecurity Collaboration and Engagement of Stakeholders	Link	Zoom	Attendance to the event	21/05/2021	Performed	Industry
GT	Participation in a Conference	Extension of ICT Verticals and horizontals for Blockchain	Link	MS Teams	Attendance to the event	02/06/2021	Planned	Industry

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

		Standardisation // AI Roundtable						
JR	website		https://www.joanneum.at/en/digital/latest-developments/news/news-detail/innovative-strategie-fuer-cyber-sicherheit-im-finanzwesen	Online	Published News about the project Critical-chains successful completion of first phase and successful review meeting.	February 2021	Performed	General public
JR	social media		https://www.linkedin.com/posts/joanneum-research_innovative-strategie-f%C3%BCr-cyber-sicherheit-activity-6773513660712202240-_WrS	Online	Published News about the project Critical-chains successful completion of first phase and successful review meeting.	March 2021	Performed	General public

12 Exploitation

This chapter sets out the overall framework plan for the exploitation of innovations resulting from the Critical-Chains project. In particular, a methodology is presented to build the exploitation strategy, which is divided in three main phases. The Consortium objective is to turn innovative ideas and technological progress into marketable products and services, while keeping a competitive advantage by being one of the first to enter the market. Therefore, an exploitation methodology is proposed as shall be supported and informed by appropriately focused dissemination and communication actions to maximise impact mobilisation consistent with IPR management whilst enhancing the potential for the Critical-Chains innovative results to find large scale adoption by the financial sector market.

The exploitation and commercialisation analysis framework (i.e., IPR management, business model, etc.) is being currently developed within the framework of deliverable D7.8 "Report on business modelling, IPR management and innovation modelling" due by month M36.

12.1 Exploitation Strategy building up process

The process for developing the exploitation plan of the Critical-Chains project is devolved into three phases to be implemented mainly within the project lifecycle as follows:

- Phase 1 is aimed at acquiring a first strategic analysis of the project commercialisation opportunities: the possible routes to market are identified as well as the Partners' commercial positioning, which is the pre-requisite to exploitation planning for this Deliverable.

- Phase 2 is aimed at building the business model through which the Critical-Chains Consortium will evaluate potential revenue models from project outcomes during the second phase of the project to be duly investigated under Task 7.5 and reported in D7.8.

- Phase 3 consists of business development planning: the resources needed for commercial development will be evaluated and a concrete action plan will be proposed, after a consolidation of business models developed (M24-M36).

The ultimate goal of this approach is to be in a position to tackle the market with a viable, stable and robust business model as quickly as possible after the project completion.

The Consortium has a strong motivation to support the take-up of its innovations after the project ends. Over the first 5 years, beyond the project funded period, the Consortium will focus on refinement re-engineering and adapting the delivered tools to suit the customers' needs and engaging the market.

For Phase 1, a preliminary identification of project achievements (i.e., exploitable results) is needed to start the commercial positioning, and as such, know the markets to target and frame a unique selling proposition. The following is a representation of the overall methodology.

12.2 Initial identification of project outcomes

The first step to inviting commercial offers is a preliminary identification of project outcomes. The Critical-Chains main framework itself will be offered as a web-based platform on which end-users (either institutions or regular people) should be able to register as subscribers. Each product/service can be delivered in an XaaS model, commercialized and if needed diversified according to the particular needsof stakeholders. The main and initial project outputs are listed below in Table 2.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

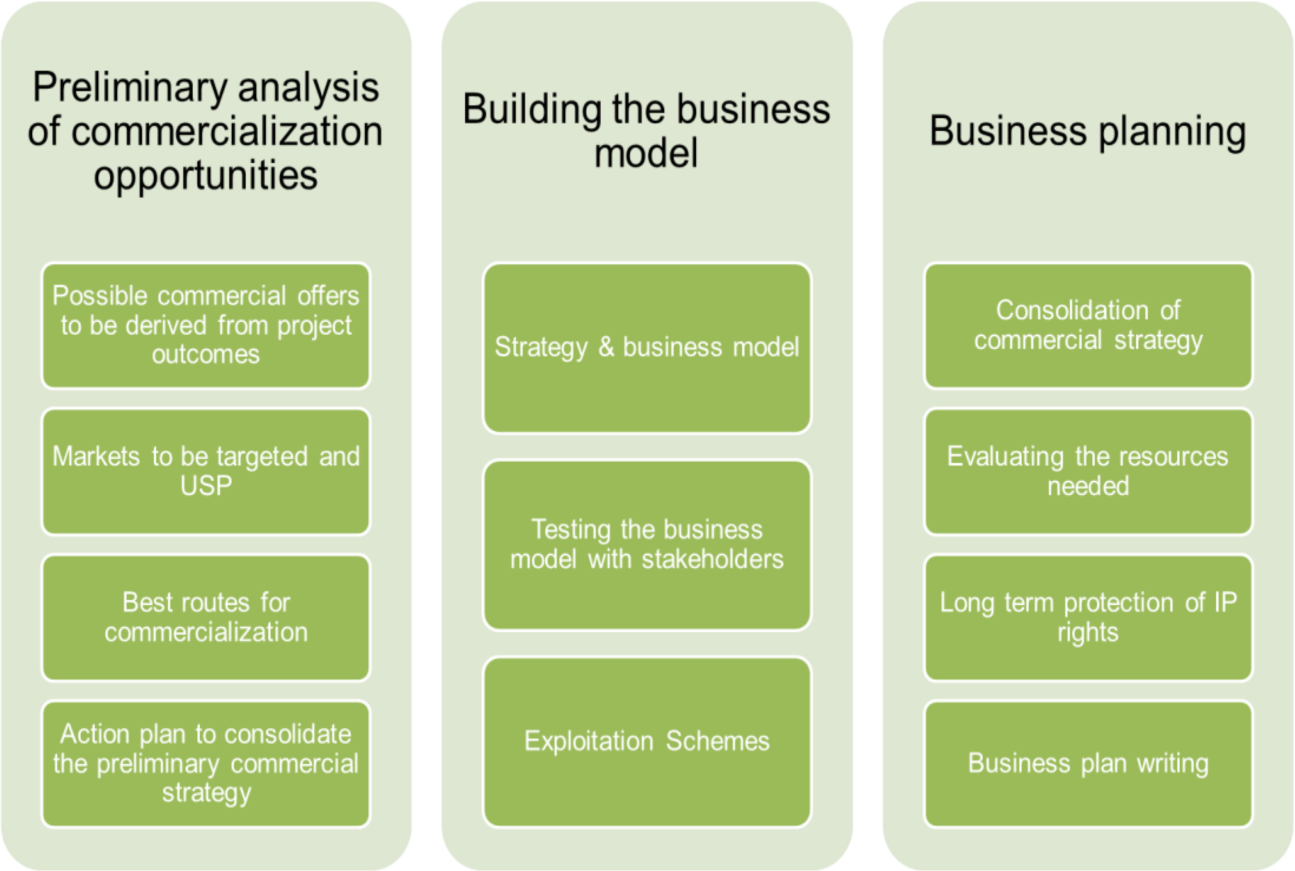

Preliminary analysis of commercialization opportunities
Possible commercial offers to be derived from project outcomes
Markets to be targeted and USP
Best routes for commercialization
Action plan to consolidate the preliminary commercial strategy
Building the business model
Strategy & business model
Testing the business model with stakeholders
Exploitation Schemes
Business planning
Consolidation of commercial strategy
Evaluating the resources needed
Long term protection of IP rights
Business plan writing

Figure 27: Exploitation Strategy Building process

Table 2: ***Main Critical-Chains project outputs***

Critical-Chains Outputs	**The listing follows the originally planned participation of the Partners in WPs -All Partners are listed in alphabetical order**	
Critical-Chain Main Framework	EY, INDRA, NETAS	
Secure Cyber Framework with Resilience Analysis **Intrusion Detection** (for better cyber preparedness)	ERARGE, CEA, FHG, INDRA, JR, NETAS, RINA-C	
Data Flows and Information Modelling (FMaaS), Security-by-Design, Risk Severity and Countermeasures Ranking Framework	ERARGE, FHG, JR, NETAS, POSTEIT, UREAD	
Entire CPSaaS with IoT Functionality	All Partners	
AUTH-as-a-Service- AUTHaaS with Biometric Support and Zero-Knowledge Proof	ERARGE, CEA, EY, FHG, INDRA, POSTEIT, RINA-C, UREAD	
Hardware-Security-as-a-Service	ERARGE, IMEC-NL, FHG, RINA-C	
Blockchain-as-a-Service (BCaaS)	GT, EY, FHG, INDRA, UREAD	
Crypto-as-a-Service (Cryptaas)	ERARGE, FHG	
Triangular Accountability Model with Front-end applications (smart contract, secure transactions, etc.) within specific use-cases	All Partners	
Innovative Business Model that can cope with the pressing financial challenges	ERARGE, EY, FHG, GT, INDRA, POSTE-IT, RINA-C, UREAD	
Technology Acceptance Model	ERARGE, EY, GT, INDRA, NETAS, POSTEIT, RINA-C, UREAD	
Audit & Compliance Tool and set of Models for NIS, GDPR, PSD2 and AML/4 compliance	RINA-C, POSTIET, UREAD	

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

12.3 Partners Exploitation intentions

For a systematic assessment of the commercial potential and positioning of the Critical-Chains exploitable results, a logical starting point is to clarify the individual Partner's positioning in terms of

i) Specific implementation-time contributions to the resulting *foreground* and any elements of their *background* contributed to the project as initial starting point to be further elaborated during the project activities in alignment with project technical development.

ii) Commercial intentions and exploitability consistent with their profile (e.g., enterprise or Research Organisation etc.) and in particular, as background, which is defined as "data, know-how or information that is needed in implementing the action or exploiting the results".

It should be noted that the overall provisor applicable to the Partner statement of exploitation intentions is that all exploitation planning, and rights will need to remain fairly appropriated according to the level of the individual Partners' overall contributions to the results and consistent with the IPR Management Plan that is being developed, and to be finalised by the Consortium, as the basis of D7.8.

1	**The University of Reading (UREAD)**
Exploitation intentions	UREAD Department plans to further its research in the areas of Information Modelling, Machine Learning, Data Mining and Data Science and Embedded Intelligence (including at Cloud, Fog and Edge-Smart) as applied to real-world data intelligence and predictive modelling and as such the results of the project would help in research and innovation capacity building and application of AI techniques to criminal and terrorist networks analytics, behaviour modelling and agent behaviour prediction based on large datasets and agent simulations. This includes exploitation of UREAD innovation in collaboration with its existing and future industrial Partners and other stakeholders including the provision of advance technology adoption and integration.
Background	Contributions by UREAD mainly includes background that is included in the results of work on **i)** Technical and methodological support as needed for the various planned deliverable of Critical- Chains project, **ii)** directly related to: a) Secure Semantic Interoperability and Access Control; **b)** Integrated Context-Aware Privacy and Security Protection by Design, **c)** Ontology-Committed Use-Context-aware Requirements Resolution and Ranking, Use-cases Identification, Prioritisation and Dynamic Usability Evaluation, **d)** FMaaS Hybrid and Ensemble Methods (including hardware acceleration). Subject to limitations, terms and conditions as shall be agreed by the Consortium in the Critical-Chains final version of the exploitation plan.

2	**Commissariat À L'Energie Atomique Et Aux Energies Alternatives (CEA)**
Exploitation intentions	CEA will develop secure data access enablers, with the aim to enrich existing CEA software and then offering it to its customers in the field of data security. CEA will also enhance its network intrusion detection system solutions for cyber-physical security (CPS) systems featuring both signature-based and anomaly-based detection (e.g., with neural networks) and autonomous reconfiguration with cyber- flows blacklisting capability and adaptation to other parameters obtained from Threat Intelligence. CEA promotes technology transfer and encourages innovation. For exploitation of the CEA's Critical-Chains innovations CEA will endeavour to transfer technologies to future industrial Partners in the form of licences.
Background	As to CEA, it is agreed between the Parties, to the best of their knowledge, no data, know-how or information of Party 2 (CEA) shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

4	EY Advisory S.P.A. (EY)
Exploitation intentions	EY intends to exploit project results by using them to enrich its services for Partner organisations in multiple domains. In particular, EY intends to exploit the project results with a focus on the model defined for the implementation of blockchain enabled services for the financial sector. Indeed, the target project results will be exploited in order to define a standard for the evolution of therelationships among operators of the financial sector (banking, insurances, etc.), with high replicability potential at the international level that will be used to provide tailored and innovative services to target clients in the financial sector domain.
Background	As to EY, agreed between the Parties, to the best of their knowledge, no data, know-how or information of Party 4 (EY) shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

5	Fraunhofer-Gesellschaft Zur Förderung Der Angewandten Forschung E.V. (FHG)
Exploitation intentions	Fraunhofer EMI intends to use the further developed technologies from Critical-Chains to apply themas a basis for other security tools and options in the cyber-physical security domain. Furthermore, Fraunhofer EMI plans to present the results and knowledge from Critical-Chains at scientific conferences like the Security IT Summit or the Cyber Security Exchange for Financial Services or in scientific publications in peer-reviewed scientific journals such as the Journal of Cybersecurity.
Background	As to Fraunhofer EMI, it is agreed between the Parties, to the best of their knowledge, no data, know-how or information of Party 5 (FHG) shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

6	Guardtime As (GT)
Exploitation intentions	Critical-Chains will first and foremost enable GT to develop further and create new KSI-based solutions in two interconnected areas: cybersecurity and finance. These domains are also set as priorities in the GT business development strategy. The project will provide marketing opportunitiesand will likely result in expanding services to existing clients in the finance sector. Additionally, the project provides access and sales opportunities with regard to new clients/end-users who are involved in the project. Considering the rapidly growing demand for cybersecurity functionalities, the solutions will be developed with replication in mind, with the aim to establish a basis to support thedevelopment of KSI-based solutions in other domains as well. In addition, the work on the project will enhance the GT R&D capabilities by allowing further research into blockchain-based services together with complementary input from Consortium Partners. This also incentivises cooperation and brings opportunities to build future business or R&D Partnerships to develop blockchain-based solutions together with world leading research organisations, innovative SMEs and end-users.
Background	As to Guardtime AS, it is agreed between the parties that, to the best of their knowledge, no data, know-how or information of Guardtime AS shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or exploitation of that other Party's results (Article 25.3 Grant Agreement). For clarification, in particular, but without limitation, Guardtime AS owns and develops various digital signature and time-stamping technologies and solutions that it refers to by the trademarks "KSI" and"BLT" (referred to here collectively as "Guardtime Proprietary Solutions"). Notwithstanding any interpretation of section 9.8, or of any other provision of the Consortium Agreement, or of any Annex, attachment, or other ancillary agreement thereto, if Guardtime AS makes available to any other Party (including the Party's affiliates) any API, software development kit, or other software that forms an interface with any of the Guardtime Proprietary Solutions (collectively, "interface software"), this shall not cause the interface software itself, or any of the Guardtime Proprietary Solutions, in whole or in part, to be viewed as Background, or as any part of any Result, and shall not give rise to any Access Rights to the Guardtime Proprietary Solutions or interface software, nor to any expressed or implied licence; access to and use of Guardtime Proprietary Solutions and interface software will remain available only on commercial terms.

7	Stichting IMEC Nederland (IMEC)
Exploitation intentions	Stichting IMEC-NL runs open innovation research programmes with the participation of both local and worldwide industrial players that contribute over 55% of its annual budget. In return, these industrial Partners obtain rights to exploit the generated know-how and IP in their products and market offerings. Stichting IMEC-NL actively supports transfer of its expertise and further development through certification requirements (e.g., FDA) for marketing its innovations. The relevant markets within the present scope of their activities are Health and lifestyle, Automotive, and Agri/food, with the Internet-of-Things as an enabler in each of these areas. Insights into the needs of these markets is built through close collaboration with end-users who can articulate the customers' needs. Implementation and use of a large-scale Internet-of-Things infrastructure is supported to test and validate novel hard/software and services. Based on market intelligence, IMEC innovations in Critical-Chains will be used to enlarge and strengthen IMEC open innovation programmes and extend the number and size of their industrial Partnerships through which they end up in the market.
Background	As to IMEC-NL, it is agreed, between the Parties, that to the best of their knowledge, no data, know-how or information of Party 7 (IMEC) shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

8	Indra Sistemas SA (INDRA)
Exploitation intentions	Through this project, INDRA expects to improve its back-office solutions by providing them with newlevels of security, trust and data integrity. Moreover, technologies used, and lessons learnt will be applicable to other solutions that have an embedded financial component, such as multi-modal clearing houses, or other products outside the Transport market, therefore enabling the exploitation of the results beyond the current project scope. As the exploitable results are aligned with the solutions that the company already provides, the existing exploitation channels can be used for distribution. This includes international traffic and transport markets in which INDRA already has a strong presence. INDRA is present in many countries in Europe, Latin America and Middle East. INDRA have a wide knowledge of the requirements of travellers and transport operators in global markets, as well as the ability to develop and adapt the offerings responsive to the needs. This knowledge will be crucial when developing solutions within Critical-Chains, assuring that the results are competitive in the global market. INDRA has offices in 140 countries -an important channel to approach and deliver the identified customer segments in the global transport and traffic market.
Background	As to INDRA, it is agreed between the Parties that, to the best of their knowledge, no data, know-how or information of Party 8 (INDRA) shall be needed by another Party for implementation of the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

9	Joanneum Research Forschungsgesellschaft Mbh (JR)
Exploitation intentions	JR intends to further develop technology building blocks for automatic anomaly detection in data streams as well as formal methods for security verification and specifically adapt them to the requirements of the finance sector, therefore extending its future market presence for its technologyofferings based on research results. This plan is fully in line with the strategy of the JR competencegroup to target the finance sector as an additional market for technology-oriented projects and services by creating synergies and enabling the group to grow over the next 3 years. Subject to the relevant Critical-Chains Partners' agreement and the IPR Management Plan, JR also intends to: **i)** disseminate the results of the projects in both scientific conferences and local or regional events dedicated to cyber security and, **ii)** disseminate information about the project in meetings with the business contacts from industry, SMEs and public authorities.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Background	As to the Party 9 (JR), it is agreed between the Parties that, to the best of their knowledge, no data, know-how or information of Party 9 (JR) shall be needed by another Party for implementation of theProject (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 GrantAgreement).

10	Netas Telekomunikasyon Anonim Şirketi (NETAS)
Exploitation intentions	NETAS plans to exploit the project results in three ways: First, to enhance its know-how and solution bundling on cloud computing with the solutions in Critical-Chains and thus obtaining ready-to-use new cloud architectures in similar future projects. Second, to increase its knowhow and security requirements, solution and test capabilities for blockchain-based critical infrastructure. Third, to extend its customer base in finance sector and provide its current customers access to emerging technologies.
Background	NETAS includes background that is **i)** the result of work done by the team working on the Critical- Chains project, **ii)** directly related to: **a)** Threat intelligence and predictive modelling by performing user and component behaviour analysis; **b)** Analytical rule engine and machine learning techniques for anomaly detection; **c)** Techniques for handling massive concurrent access to cloud servers; **d)** Cachingtechniques in cloud architectures for optimisation of resource allocation and data distribution. Subject to limitations, terms and conditions as shall be agreed by the Consortium in the Critical-Chains final version of the exploitation plan.

11	Poste Italiane - Societa Per Azioni (POSTEIT)
Exploitation intentions	POSTEIT has an interest in the exploitation of the knowledge generated by the project, with specific reference to the cybersecurity framework, the authentication as a service module and the Blockchain-as-a-service module. In particular, POSTEIT will focus on the exploitation of the project results related to the exploratory evaluation of performance of the Multi-Factor Authentication for SPID, using the project solution for authentication. This will be relevant as a baseline for future replication and adaptation to other target services as well as supporting the extension of the financial services provision by POSTEIT. Finally, POSTEIT will be interested in exploiting the project results for knowledge transfer (at company internal and external levels), in particular by organising seminar and workshops aimed at improving the awareness and interest in the domain of cyber security.
Background	As to POSTEIT, it is agreed between the Parties that, to the best of their knowledge, no data, know-how or information of Party 11 (POSTE) shall be needed by another Party for implementation of the Project(Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).

12	Rina Consulting Spa (RINA-C)
Exploitation intentions	RINA-C sees Critical-Chains as a great opportunity for the development of new knowledge and expertise in blockchain, biometric-based authentication and cybersecurity in the context of the financial sector. This enables RINA-C to strengthen its expertise and service offerings to various stakeholders involved also in the insurance sector. In particular RINA-C sees the opportunity to createnew consultancy services using the Audit & Compliance Tool enhancing the existing Risk Assessmentvalue proposition in the following way: **i)** using models created in the project to carry out audit and compliance tasks in accordance with NIS, GDPR, Payment Services (PSD) and e-invoicing EC directives; **ii)** proposing the Critical-Chains services as technical security measures to mitigate security and privacy risks; **iii)** conducting feasibility studies to integrate the existing ICT insurance services of potential Customers with the Critical-Chains Platform.
Background	RINA-C is agreed between the Parties that, to the best of their knowledge the following background is hereby identified and agreed upon for the Project: **i)** Security and Privacy Self-Assessment tool, owned by RINA-C in its Business Unit Industry -Space and Defence; **ii)** Any background created by theBusiness Unit Industry –Space and Defence - and owned by RINA-C and which is directly related to the project, with particular, reference to Software Design and Development, Cyber and Information Security, Product Assurance.

Specific limitations and/or conditions for background **i)** and **ii)** in terms of Exploitation, shall be as mentioned hereunder:

i) RINA-C Background Software Object Code shall be subjected to negotiated licence and/or royaltyfees. They shall not be used for exploitable purposes /sold without prior written agreement. RINA-C furthermore hereby excludes the following Background: All Background generated by employees, agents or representatives of RINA-C, other than the technical team of the Industry unit of RINA, which is directly involved in the Project; All Background generated by employees, agents or representatives of RINA-C that are directly involved in the Project, which is unrelated to the work plan, aims and objectives of the Project; All Background which RINA-C, due to third Party rights, is unable to grant Access Rights to; All Background in patents and current patent applications owned by RINA-C; All RINA-C proprietary materials and software, whether covered by patents or not.

ii) RINA-C hereby excludes from its obligation to grant Access Rights to Background, all Background that has been and/or will be derived outside the Project and/or which RINAC and RINA-S due to third party rights are not able to grant Access Rights to or for which it needs to get permission to grant Access Rights.

12.4 Markets to be targeted and Unique Selling Proposition

Critical-Chains directly targets technological innovation to support the FinTech industry. The targetedcritical sectors are well-defined and focused as Banking, Insurance and Central Counterparties (CCPs) processes. Additionally, Critical-Chains can be commercialised in vertical sectors where e-Payments, eCommerce and eTrade operations take place (i.e., financial audit in a specific sector). In this way, theproject can easily be expanded to other application areas where smart contracting or a financial transaction is executed (such as the retail sector, health, transportation, energy, tourism,manufacturing, trade, investments). The target groups are therefore not only the aforementioned financial authorities, but also companies in the stock market, and actors in financial transactions (i.e., enterprises, individuals).

Different key drivers led to the identification and characterisation of Critical-Chains markets:

- The benefits of blockchain include more accurate reserve calculations based on actual participating contracts and automatic calculation updates once underlying data is updated
- Data gathering process needed to evaluate and process claims is an error-prone process. Permanent audit trails, even in multinational cases should be tracked anytime and anywhere.
- Stakeholders need to align around standards and processes within blockchain technology for reducing the costs and estimating the risks (e.g., aligned with claims in insurance sector)
- Digital certificates have become indispensable for protection against counterfeiting
- Need to increase transparency on banking operations and provide end-users innovative direct (not-mediated) access to data and information concerning such operations
- Need to counter fraud ($57.8 Billion in e-Commerce fraud losses were reported in 2017[1])
- Need Scalable operations (indicatively, total e-Commerce Transaction Value was of the order of $8 trillion in 2020[2] , non-cash transactions in EU only in 2015 were over 100 Billion[3]

The main markets and target customers (stakeholders) for Critical-Chains outcomes are mentioned in Table 3. Below.

Table 3: Critical-Chains markets

Market	Banking Sector
Key features	• Cyber-attacks cause great loss of money and time in banking operations • Existing contracting processes are very cumbersome • Access to banking services is still burdensome; mobile banking needs a wider coverage of portabledevices • The banking system is not ready for the booming blockchain technology; accountability, trust andintegrity are the greatest challenges • Classical blockchain-based infrastructures (i.e., cryptocurrencies) are open to financial crime, money laundering, and illegal money trafficking • Need to enhance interoperability to boost compliance with PSD2 regulation.
Market size	US has approximately 7K banks and 7K credit unions; EU has about 9K banks; worldwide total: 30K
Value proposition	Secure contracts, transactions cyber-physical practices, secure access to data and information.
Customers	• Individuals who have a bank account and make any financial transaction or they are party to any commercial contract, • Banks, as financial authorities, hosting any financial service including transactions and also behaving asthe contractor

Market	Financial Market infrastructures
Key features	• G20 Leaders agreed at the 2009 Pittsburgh Summit that all standardized derivatives contracts shouldbe traded on exchanges or electronic trading platforms • Risk concentration within CCPs will grow, both nationally and internationally • A growing number of banks will participate in key CCPs across the globe • Contracting processes are very cumbersome and not ready for global financial interactions • Ensuring the accountability of CCPs is a major challenge • Clearing, settlement and custody services are open to malicious attacks as related operations/transactions are executed through a multiparty scheme • CCP processes are highly vulnerable to financial crime, (contracts fraud, privacy)
Market size	17 CCPs authorised in the EU, ~200 worldwide; growing number of banks establishing their own CCPs
Value proposition	Secure contracts, secure clearing processing, secure transactions, protection against cyber-physicalattacks
Customers	• Enterprises, firms and companies which are accepted as a contractee or a stakeholder party in any financial transaction or a contract • Central Counter-Party organisations (CCPs) as financial institutions that take on counterparty credit risk between parties to a transaction and provide clearing and settlement services for trade in foreign exchange • Trading venues and Multi-lateral Trading Facilities (MTF) known as alternatives to the traditional stock exchanges where a market is made in securities, typically using electronic systems (especially cryptocurrency stock markets)

- [1] https://www.businesswire.com/news/home/20171026005187/en/New-Study-Reports-57.8-Billion-eCommerce-Fraud
- [2] https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf
- World Payments report – Source: https://www.worldpaymentsreport.com/reports/noncash

Market	Insurance Sector
Key features	• Fraud detection and risk prevention: A decentralised digital repository can independently verify the authenticity of customers, policies and transactions (such as claims) by providing a complete historical record. • Data fragmented and recorded in none- homogeneous formats and not in real-time • Long and costly resolution of complaints • Fraud with fake identities in processes involving digital identities • Unlicensed brokers selling insurance/ pocketing premiums, causing economic loss • IoT and Blockchain enables the re-definition of a dynamic price thanks to new business models suchas PAYL (pay as you live) or PAYD (pay as you drive) • Audit and communication inefficiencies
Market size	~3500 in EU, ~2000 in the US
Value proposition	Secure contracts, transactions, underwriting processes, claim management, policy business services
Customers	• Customers of insurance companies who are a side in any underwriting process or behaving as a contractee (beneficiary) • Insurance companies providing a service of underwriting and claim management where insurance beneficiaries and customers meet in such services

Market	Financial Audit in a specific sector (transport - back office & electronic toll collection)
Key features	• Integrity and traceability of transportation data and financial transactions needed • Highways are often operated following a concession mode, in which a private company enters into an agreement with the government to have the exclusive right to operate, maintain and exploit certain services for a given number of years. • Interoperability agreements are needed (Electronic Toll Collection) in order to enable the clients to pass from one concession to another without signing new contracts. • Concessions exchange transits information and perform clearing process based on detected vehicle transits, in order to distribute the appropriate funds. • Concessions normally need to report to the authorities the correct financing, and are subject to complexaudits, as they need to pay or receive funding depending on the number of transits. • Increasing financial fraud.
Market size	More than 100 million vehicles/day passing electronic tolls across Europe
Value proposition	Secure contracts, secure clearing processing, secure transactions, streamline complex audit processes.
Customers	• Enterprises, firms and companies which are accepted as a contractee or a stakeholder party in any financial transaction or a contract • Central Counter-Party organisations (CCPs) as financial institutions that take on counterparty credit risk between parties to a transaction and provides clearing and settlement services for trade in foreign exchange • Banks, as financial authorities, hosting any financial service including transactions and also behaving as the contractor • Governmental organisations which are to give consent, accredit or monitor financial services such as ministries and other authorities

12.5 Commercialisation roadmaps

Project results can be commercialised in many different ways which are listed below:

- Subscription fee to Critical-Chains framework
- Renting XaaS services
- Commission fees at each transaction or contract
- Promotion areas on main framework
- Selling hardware (secure sticks, HSMs, distance-bounding hardware solution, etc.) and software components (XaaS services) as standalone solutions

- Selling the entire solution to major financial organisations

The commercialisation roadmap is to starts with the second phase of the project and continue into the future (short-/mid- and long-term). In the following Table 4 a preliminary representation of time to market and commercialisation routes is set out.

Table 4: Critical-Chains potential commercialisation route over time to market

Phase	Timeframe	Action towards commercialisation
Project phase	M0-M36	Awareness increasing and promotion ramp-up will be applied to keep thepotential adopters informed. This will be realised through dissemination and communication activities
Short-term	<= 1 year after the project ends	The Consortium will adopt a stakeholder outreach plan to promote the project results sectorally through the relevant Partners e.g., POSTEIT, as a Financial Sector Gateway Partner, or INDRA as a Transport Applications Sectoral Gateway Partner. In this Announcement Phase, project results are emphasised at EU level and a branding process will begin to take hold.
Mid-term	2-4 years after the project ends	The Consortium will extend the scope to a global level aiming to reach the key markets (Europe, Middle East, America, Japan, China, Australia, Arabic countries, etc.). Here, dealership and collaboration opportunities will be discussed. Branding operations will be well-established during this term.
Long-term	>= 4 years	Connection with other critical sectors and application areas will be realised to extend the scope of the project. Creation of spin-off companies in specialised areas around Critical-Chains will be considered in the long term. Additionally, mid-term activities will be sustained.

12.6 Strategy and Business model

This section aims at defining the strategy behind the business model. The Business Model is a concept connected with business strategies and therefore cannot have a unique definition but tends to vary in all its peculiarities depending on the company and sector taken into consideration. The complexity of the goods and services market has, over time, led the right business model having become the critical factor for take-off and sustainable success of any business.

The business model describes the set of elements through which a project or company creates and transfers value to other entities. It identifies the set of characteristics that determine the competitive and economic sustainability of a business project. It is a representative tool of the contents of a business idea, and it analyses the actual ability of a business to create value.

The business model is divided into:

1. Value proposition
2. Key conditions
3. Profit proposition

The value proposition can be divided into:

a) Target end-users
b) The value for the target end-users
c) The methods of disbursement of the value

The end-users target refers to the set of economic players that form the relevant market for the business concerned and to which, in this context, the Critical-Chains solution needs to address its value proposition as a priority. It is necessary for the end-user base to be very homogeneous, at least with respect to the value that the project intends to create for their benefit and the ways in which it intends to provide it, with the aim to create a real market segment.

Provided that the offer is distinguished according to the specific needs of each end-user entity type, differentiated target end-users can be included in such a structured model. In order to have a successful value proposition, it is necessary to understand a multitude of aspects of the business (value-chain) of the target end-users into which the aspiring service provider intends to embed its value proposition, hopefully, to best support such a chain.

Firstly, one must clarify the fundamental needs that the end-users (mainly the financial sector in this context) would wish to satisfy through the use of the services offered by Critical-Chains and the factors that influence their perception of satisfaction of such needs. Secondly, the contents of a distinct offer for which they are willing to pay, for their needs to be met. It is also important to understand the best way to enter into a relationship with the end-users to project direct the value to them and hopefully motivate deep engagement and participation of the end-users in the value-propositioning and its incremental extensions and refinements to best meet end-user's needs and support their sustainably successful competitive strategy.

A pre-requisite to achieving end-user interest is the identification of the most effective communication and distribution channels with respect to the established workflow of the target groups. It is therefore necessary to evaluate the potential profitability of the target groups, especially relevant for the subsequent elaboration of the profitability proposal.

The fundamental needs of the target end-users are met through services which may have tangible, intangible, surface, deep, transient and enduring aspects of value-added. Some examples of such are aesthetic and objective quality, innovativeness, ease of use, price, status, reduction of risks or costs for the user, accessibility, reliability. The methods of providing value are a fundamental component of the value proposition as they affect the strategy for promotion and embedding of the value based on the net benefits determined by the value for the target end-users and the way in which this is actually perceived by them[1]. The goal is therefore to identify:

- The ways in which to make the service offered by Critical-Chains available to the target end-users;
- The methods of communication through which to make target end-users perceive the value elements of the Critical-Chains solutions.

It is important to consider that the *distribution* and *communication* channels of value can themselves represent tools for creating a part of the value supplied. Both these channels must be designed and managed referring to the individual phases into which the interaction process between the value projection and promotion of the Critical-Chains solution and the target end-user can be divided, namely:

- Awareness of the existence of the Critical-Chains solution with certain characteristics
- Evaluation of the value of this solution
- Purchase of the services offered by Critical-Chains by the target end-user
- Effective provision of the services and their value to the target end-user
- Provision of the service(s) to the target end-user after the purchase, aimed at maximising their benefits

In defining the value for the target end-user and the related delivery methods, it is necessary to characterise the type of relationship to be established with the identified target groups. This relationship is relevant in

[1] Osterwalder A., Pigneur Y. (2010), Business Model Generation, Wiley & Sons.

four fundamental areas:

1. Acquisition of the target end-user
2. Maintaining the relationship with the target end-user over time
3. Maximising the value of the target end-user for the project
4. Involvement of the target end-user beyond the commercial sphere

The critical factors form the second reference area of the business model, which is the set of essential conditions necessary to implement the value proposition through which the Critical-Chains solutions aim to achieve a competitive advantage. These are:

- Key resources
- Key activities
- Organisational model

The key resources are the type of resources considered essential for production and delivery of the identified value, recognising this as unique and superior to that provided by competitors.

In developing the business model, it is necessary to verify whether and to what extent these resources are available within the project. If a significant deficit is observed in these resources, a strategy for acquiring or developing the resources or a change in the value proposition must be defined. The key activities, on the other hand, are those that have greater importance in creating the value provided to the target end-user for whose implementation, the provider is to offer its distinctive skills. These therefore represent the core activities, fundamental for the success of the solution offered by the project. They are placed in three possible areas:

- The production process in the broad sense: from the design of the offer to its physical realisation, up to its positioning on the market.
- The creation and management of platforms or networks that optimise the interaction between the solution offered, the target end-user and other subjects possibly relevant in creating value.
- The management of specific problems of the target end-user as deemed relevant to determining the actual value that this derives from the Critical-Chains solution.

The organisational model, on the other hand, identifies the organisational conditions that enable the best implementation of the set of activities, in particular of the key ones, making the most of the available resources. It concerns the organizational structure, the methods of managing human resources, and the dissemination of the values of the project.

A fourth category of crucial influence to the business model and transversal to the three factors outlined above is the model of the relationships amongst the Consortium Partners. This term refers to the fundamental relationships for the availability of critical resources or the implementation of critical activities, i.e., the relationships that the Consortium Partners can establish internally for the projection of the Critical-Chains offering and with their target end-user segments is essential for the best implementation of the value proposition of the Critical-Chains solutions. Hence the envisaged role of the two user Partners (POSTEIT , INDRA) as Sectoral Demonstrator Partners and as such ,naturally also the Sectoral Gateway Partners, is paramount and underpins the strategy for Phase 1 to look to these Partners as uniquely qualified to showcase the thus credible projection of how the brown field adoption of some of the Critical-Chains solutions could provide significant support to existing sectoral value-chains, respectively in financial services and transport sectors, and pave the way for enhanced value-chains in these sectors.

Finally, the Critical-Chains business model is completed by the profitability proposal, divided into revenue stream and cost structure. The profitability proposal makes explicit the way in which economic value is supposed to be obtained from the value proposition made to the target market; it is therefore highly dependent on the expected revenue flows through the provision of value and the cost structure necessary for this purpose.

To identify revenue streams, it is necessary to understand for which aspects and services of the Critical-Chains solution and its value, the target end-users are actually willing to pay and to what extent. Target end-users tend to assign value to many aspects of a service, but not all are actually willing to incur a cost to benefit from them. Revenue flows must also be considered in relation to the channels through which the economic flow and its riskiness occur monetarily. The cost structure identifies the total costs that must be incurred to implement the business model and the possible scenario as the value proposition, or the necessary critical conditions, change. There are two purposes for which the cost structure is determined: on the one hand, it is useful to assess the economic and financial sustainability of the business model on the basis of a comparison with the flow of revenues; on the other hand, it serves to understand the activities that have the greatest impact on the cost structure and on which it is necessary to seek maximum efficiency.

12.6.1 Business Model CANVAS

The Business Model Canvas is a strategic model used for the creation and development of a business models. It represents a visual template that shows the *infrastructure, products, customers, suppliers* and *other elements* that distinguish a business project.

The Business Model Canvas (BMC) is therefore identified as the most suitable business model for a more effective and efficient exploitation of the Critical Chains solution. A structured questionnaire will be devised to seek the views of potential stakeholders and target customers in terms of evaluation of the exploitation relevance of the elements identified for each of the 9 blocks that make up the BMC.

One of the main objectives of this model is the ability to offer an overview of the interconnections present within the model as well as a quick representation of the main elements that make up a business model.
The business model canvas is graphically a scheme divided into 9 blocks: *key Partners, key activities, key resources, value proposition, customer relationship, channels, customer segments, cost structure*, *revenue streams;* defined as follows:

- **Key Partners**: suppliers and Partners who are necessary for the functioning of the company/project business model.
- **Key activities**: the strategic activities that must be performed to create and sustain value propositions, reach customers, maintain relationships with them and generate revenues. It is not necessarily the core business, but all those activities that are in any case indispensable.
- **Key resources**: represent the strategic assets that the company/project must have to support its business model: ranging from intangible aspects such as know-how to machinery or physical premises.
- **Value proposition**: the set of products and services that are offered to customers and that represent value for a specific customer segment.
- **Customer relationship**: the type of relationship that the supplier establishes with the different customer segments; they can have very different modalities and contents.
- **Channels**: the ways in which the supplier reaches a certain customer segment to present and provide it with its value proposition.
- **Customer segments**: the groups of people and/or organisations addressed by the supplier of services.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

- **Cost structure**: defines the costs that the supplier will have to incur to make its business model operational.
- **Revenue streams**: are the revenues that the supplier obtains from the sale of products / services to a specific Customer Segment.

The Business Model Canvas (BMC) is a customer-centric tool with proven innovative effectiveness; it is used by many large companies regularly and successfully. Its main advantage is to facilitate the creation of new business models, of value, and their implementation. The BMC enables the visualisation of the pathways to realisation of value-proposition integration within the customers' value-chains. Furthermore, it is a tool that develops creativity, involves participants, is educational and creates cohesion.

The BMC thus supports efficient structuring of a business plan, it enables all aspects of a business idea to be explored in an exhaustive and orderly manner, enabling the focus to be on the exact value of the proposition. BMC is a simple and intuitive model to understand and therefore helps collaborative development of a portfolio of innovative ideas and supports team, supplier and value-add integration. The tool, used with visualisation, facilitates the understanding of the current business model and its evaluation in the context of changes in the market.

12.6.2 Testing the business model with stakeholders

After indicating the strategy behind the Critical-Chains business model and identifying the Business Model Canvas as the most suitable strategic model for the development of the exploitation pathways, the next step is the testing of the business model with stakeholders. In this regard, a template was produced to support the Consortium in collaborative analysis and exploration of exploitation pathways of the Critical-Chains solutions.

The template consists of two tables to be filled by each project Partner and other stakeholders as required. The Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector.

The first table identified several aspects relating to the exploitation processes and plans as follows:

- Inputs to Critical-Chains
- Targeted assets for exploitation
- Individual or joint exploitation
- Drivers for exploitation
- Plan in relation to core business/institutional mission
- Other types of applicable exploitation
- IPR Ownership
- Internal technology transfer processes
- Internal support for promoting Critical-Chains results
- Potential barriers to exploitation
- Current Plan

Table 5: Partner <NAME> Exploitation Plans

Partner Name: <PARTNER NAME>	**Exploitation Plans and Processes**
Inputs to Critical-Chains	*Insert input given to the project*
Targeted assets for exploitation	*Insert list of Critical-Chains assets*
Individual or joint exploitation	*Please indicate per asset [INDIVIDUAL ONLY / JOINT]*
Drivers for exploitation	*Motivation of exploitation for the Partner*
Plan in relation to core business/institutional mission	*Include, where relevant, reference to toolkit element (early adoption) and/or potential for commercial exploitation (sufficiently mature product/service), including targeted customers or procurement opportunities.*
Other types of applicable exploitation	*Please expand as relevant* • **Scientific exploitation**: Knowledge and technology transfer, e.g., Prototypes that need further work before they are ready for market or that are sustainable through continued research. • **Transfer through standardisation:** Inputs to standards organisations**,** explaining impacts and gaps being filled in the standards landscape. • **Other exploitation opportunities:** Complementary projects or foreseen procurement/tenders that can be leveraged to support the exploitation of a Critical-Chains asset.
IPR Ownership	*Please indicate per asset:* ***What Element: specify the contribution*** (e.g., as a methodology, paradigm, architectural layer (vertical, horizontal), method, component, software, hardware, integration, evaluation, compliance audit. ***To-What-Extent PARTIALLY/WHOLE?*** This claim will need to be underpinned by evidence of contributions to the element specified above in the actual implementation phase of the project.
Internal technology transfer processes	*Please indicate here what kind of support and resources you have*
Internal support for promoting Critical-Chains results	*Please indicate here what kind of support and resources you have*
Potential barriers to exploitation	*If applicable, please specify*
Current Plan (from D7.1_V6)	Text

Critical-Chains has been validated through 4 targeted use-cases aligned with 3 critical horizontal sectors (Banking, Insurance, Finance) and one vertical sector which is closely aligned with the critical sectors mentioned in the NIS directive (Financial Audit in transport in back-office operations & electronic toll collection).

1) Banking sector
   a. #1 contracting and transactions between companies
   b. #2 interoperable account management with zero-knowledge proof and blockchain-enabled integrity and authentication
2) Insurance Sector
3) Central Counter-Parties -CCPs
4) A vertical case study for Financial Audit in specific sector (transport - back-office operations & electronic toll collection)

This validation methodology helped elicit various aspects of system performance such as functional and non-functional capabilities: (e.g., system reliability, usability, user-acceptance and compliance assurance with respect to security and privacy protection, ethical, environmental and legal requirements.

The following table shows the main outputs identified within the project and which can also be exploited as a standalone component or integratively as service bundles through the Critical-Chain main framework.

Table 6: Main Critical-Chains project outputs

Critical-Chains Outputs	**Partners listed in alphabetic order per planned effort, and/or level of contributions to implementation of the tasks.**
Critical-Chains Main Framework	EY, INDRA, **NETAS**
Secure Cyber Framework with Resilience Analysis Intrusion Detection (for better cyber preparedness)	ERARGE, **CEA**, FHG, INDRA, JR, NETAS, RINA-C
Data Flows and Information Modelling (FMaaS), Security-by-Design, Risk Severity and Countermeasures Ranking Framework	ERARGE, FHG, JR, NETAS, POSTEIT, **UREAD**
Entire CPSaaS with IoT Functionality	All Partners
• **AUTH-as-a-Service- AUTHaaS with Biometric Support and Zero-Knowledge Proof**	ERARGE, **CEA**, EY, FHG, INDRA, POSTEIT, RINA-C, UREAD
• **Hardware-Security-as-a-Service**	ERARGE, **IMEC-NL**, FHG, RINA-C
• **Blockchain-as-a-Service (BCaaS)**	**GT**, EY, FHG, INDRA, UREAD
• **Crypto-as-a-Service (Cryptaas)**	**ERARGE**, FHG
Triangular Accountability Model with Front-end applications (smart contract, secure transactions, etc.) within specific use-cases	All Partners
Innovative Business Model that can cope with the pressing financial challenges	ERARGE, EY, FHG, GT, INDRA, POSTE-IT, **RINA-C,** UREAD
Technology Acceptance Model	**ERARGE**, EY, GT, INDRA, NETAS, POSTEIT, RINA-C, UREAD
Audit & Compliance Tool and set of Models for NIS, GDPR, PSD2 and AML/4 compliance	**RINA-C,** POSTIET, UREAD

The Business Model Canvas (BMC) was therefore identified as the most suitable business model for a more effective and efficient exploitation of the Critical-Chains solution. By the end of the project, it is planned to have a questionnaire developed for the Partners to disseminate to potential stakeholders and target customers with the aim to have their evaluation of the elements identified for each of the 9 blocks that make up the BMC. The compilation of the questionnaire will take place online anonymously and will have the purpose of enabling potential stakeholders and target customers to validate whether the elements included in the 9 blocks of the BMC are adequate for the support the commercial exploitation of the solutions resulting from the project.

12.7 Exploitation Schemes

12.7.1 Introduction

The main purpose of this section is to set the scene for Consortium Partners and stakeholders with respect to the overall exploitation strategy and model and the exploitation potential of the tools/solutions identified as project outputs. This will pave the way for the Partners to reach a shared understanding regarding the best way that the exploitation of the project results should proceed.

It will help define for Partners and stakeholders the exploitation models identified and provide the tentative exploitation strategy of the Critical-Chains to sustain project achievements after the project ends, based on the specific intentions and indications provided by the Consortium Partners themselves.
The detailed exploitation strategy and plan will be finalised and included in D7.8 by the end of the project.

12.7.2 Overview

The exploitation strategy of the Critical-Chains project will follow a gradual approach based on the strong motivation of the Consortium to sustain project achievements after the project ends.

Consortium Partners have established a preliminary strategy that can be further expanded and detailed in the final phase of the project to have a clearer vision of the Critical-Chains framework. This is to include the main project output and the additional outputs that could possibly be exploited through direct commercialisation of the Critical-Chains framework and diversifying the XaaS service according to the needs of the stakeholders.

Partners have Identified the exploitation and sustainability aspects to be examined during the project lifetime and the activities to be pursued beyond the project lifetime towards a sustained influence and penetration of the project outputs into the target market; these could include:

1. Identification of innovative exploitable assets, both technological components and services with added value that the Critical-Chains framework could provide to its target users;

2. Market analysis to identify the target market that the Critical-Chains solution could attack, its segmentation, positioning with respect to current competitors and all comparable emerging trends to assess its impact on the target market;

3. Assessment of the sustainability and feasibility of the Business model Canvas for the exploitation of the Critical-Chains solution through the possible services that the Framework will be able to offer to the identified stakeholders and target end-users;

4. IPR protection strategy based on the IPR principles and background outlined in the Consortium Agreement (CA) of the project which will guide the joint and individual degrees of freedom and exploitation capabilities of the project Partners and the management of the knowledge generated.

12.7.3 Definition of exploitation models

Critical-Chains Consortium Partners recognise two main exploitation models for the results achieved by the project:

1. The research exploitation model (non-commercial). This first model is framed within a short-term perspective and is based on enhancement and secure use of the results obtained giving rise to a path of sustainability through EU Cybersecurity resources and platforms already existing to protect financial contracts and transactions against illicit transactions, illegal money trafficking and fraud on FinTech e-operations. This is in order to empower EU cybersecurity and blockchain technology sector development. This implies the possibility of re-using the results of the research know-how acquired during the project for future research activities;

2. The technological exploitation model (commercial), which implies the adoption and application of what is indicated in the IPR protection strategy (***to be elaborated in D7.8***) in order to manage the technological know-how acquired for the development of innovative XaaS services through the Critical-Chains Framework. This was identified as the main project output. In fact, over the 5 years beyond the project lifetime, the Consortium aim is to focus on refinement re-engineering and adapting the delivered tools to suit the customer needs and engage the market. The exploitation plan will be based on a realistic and IPR-protective business plan.

12.7.4 Critical-Chains tools exploitation

For what concerns the technological exploitation model, a template was sent to the Partners to help elicit their position regarding the exploitation potential of each individual tool/solution developed within the Critical-Chains framework. Each Partner has compiled the template according to the tool/solution for which it has most contributed to developing and for which it is the beneficiary.

Table 7: Exploitation Template

Tool/Solution: ***Name of the result***	**Exploitation Potential** **Lead Partners: AAA** **Partners Involved: BBB, CCC**
Tool/Solution Overview	*Insert description of the solution, technological features, innovation, etc.*
Market Delivery Model	Please indicate as relevant per each target customer 1. Assessment Service 2. Advisory Service 3. Capability Set-up Service 4. Solution Delivery Service 5. Licensing 6. Royalty
Targeted stakeholders	*Please indicate the list of target customers* - *Stakeholder 1* - *Stakeholder*
Stakeholder pain point	*to be studied and reported in D7.8*
Critical-Chains value proposition	*to be studied and reported in D7.8*
End-user validation and expected timelines	*Indicate which pilot, how is validated, and the timeline* - *PILOT 1:* - *PILOT 2:*
Technology Readiness Level (TRL)	- *Current TRL:* - *Final Target TRL:*
Market Readiness Level (MRL)	- *Current MRL:* - *Final Target MRL:*
Combined TRL & MRL	*to be finalised in D7.8*
Competitors	*Enumerate here known competitors of your solution (name + link):*
Critical-Chains differentiators	*Summarise here the main differentiators*

In association with the exploitation template, the Partners were provided with a reference scale for the definition of the Technology Readiness Level (TRL) and the Market Readiness Level (MRL) in order to facilitate the compilation of the current TRL and MRL potential and of the TRL and MRL expected.

Finally, a further table was provided to the Partners based on the indications entered within the exploitation template for each identified tool/solution which had as its objective to identify the exploitation potential of each of them. This table was instead developed in order to collect useful elements in terms of possible market delivery models, whereby Partners were asked to indicate, where possible, which of the following delivery modes they would envision as most promising: *Assessment Service, Advisory Service, Capability Set-up Service, Solution Delivery Service, Licensing, Royalty,* in order to be able to implement them in the structuring of the Business Model Canvas.

Please note that any further elaboration of the exploitation related detail would far exceed the planned scope of this section and has to be reserved for the final exploitation plan in D7.8 which shall be based on further stakeholder consultations as planned to be performed in the interim period.

Table 8:Example of market delivery models

Tool	Customer	Market delivery models
X-as-a-Service	**1) CUSTOMER 1**	1) ASSESSMENT SERVICE_PARTNER sells to the CUSTOMER 1 an assessment service: PARTNER uses the TOOL to do the assessment, getting the needed input from the CUSTOMER1.
		2) ADVISORY SERVICE _PARTNER advises CUSTOMER 1 on how to < OPERATION TYPE> and gets a "one shot" compensation for this.
		3) CAPABILITY SET-UP SERVICE_PARTNER helps the CUSTOMER 1 to set-up a capability to <CAPABILITY TYPE>, through training on how to apply the guidelines.
		4) SOLUTION DELIVERY SERVICE_PARTNER installs TOOL on the CUSTOMER 1 workstations or on […].
		5) LICENSING_PARTNER sells a TOOL licence to CUSTOMER 1 and trains CUSTOMER 1 trainers (train the trainer mode) on how to use it; CUSTOMER 1 staff uses the TOOL autonomously; PARTNER provides releases.
		6) ROYALTY_PARTNER gets a royalty for each piece of product sold.
		All the above market delivery models can be combined as follows (example): 7) CAPABILITY SET UP+LICENCE_PARTNER helps the CUSTOMER 1 to set-up a capability to <CAPABILITY TYPE> and sells as support a TOOL licence to CUSTOMER 1 and trains CUSTOMER 1 staff on how to use it; CUSTOMER 1 uses the TOOL autonomously; PARTNER provides releases and content update (e.g. threat catalogues).
	2) CUSTOMER 2	**1)** ASSESSMENT SERVICE_PARTNER sells to the CUSTOMER 2 an assessment service: PARTNER uses the TOOL to do the assessment, getting the needed input from the CUSTOMER 2
		2) (as above but with CUSTOMER 2)

The policy for knowledge management and protection was initially defined in the Consortium Agreement (CA). The CA has handled the specification of IPR framework, including:

- Forms of co-operation among Critical-Chains Partners
- Identification of ownership of results
- Exploitation royalties between the companies
- Solution maintenance and evolution
- Configuration management
- Definition of the education on intellectual assets
- Defining the procedures regulating the layers of technology development and IPR Management
- Definition of the confidentiality and Non-Disclosure Agreement which binds all Consortium Partners
- Detailed description of regarding background, foreground and side-ground information

Further details relating to the IPR protection strategy and how the results will be protected, including details of individual or joint ownership, are to be specified in D7.8. The exploitation models of the Critical-Chains project results will depend on two main parameters:

- The nature and interests of the project Partners and stakeholders in general.

- Ownership and IPRs by the project Partners of the results in terms of algorithms, methods, techniques, software application, tool, etc.

Accordingly, the Partners have each expressed their intention in terms of exploitation of project results. These will be reviewed and elaborated in D7.8, with respect to each of the exploitable results.

12.7.5 Business model connection with Exploitable Results innovation

The business model is indispensable since it has the ability to provide the explanation of how to create, capture and distribute the value proposition. The business model covers two important functions in terms of innovation of exploitable results, which is represented by the value proposition:

- The Business model creates value by accurately defining the elements and activities that will participate in the creation and offer of a Critical-Chain technological product and/or service and which will therefore contribute to the realisation of the value proposition for a market engagement. This function is crucial because in the absence of innovative technological content it would be difficult to attract the interest of potential stakeholders to establish any Partnerships to ensure the long-term sustainability of the outputs produced by the project.

- The Business model captures value by developing and implementing the set of strategic activities through which the Critical-Chains solution acquires a competitive advantage.

The ability of the business model to create and capture value must be carefully balanced to avoid the onset of imbalances that would negatively affect the exploitation activity[2]. The Consortium's ability to generate innovative technological content supports the sustainability of the Critical-Chains solution, but at the same time, stakeholders and end-users may prove reluctant to adopt the solution offered; for various reasons such as the requisite investment threshold (particularly as greenfield development), pricing, purchasing difficulties or specific related services. It is possible that at times, despite the high level of innovative content of the proposed technology that enables the creation of value, the difficulty of demonstrating the high level of the value proposition could increase. Therefore, it is essential that these two factors are properly weighted -in trying to approach and adapt the solution offered to the needs of the target market.

The business model makes the logic of creating, offering and capturing the innovation value of exploitable results immediately and easily understandable. The ability to recognise and communicate the business model identified by the Consortium (Business Model canvas) for the exploitation of the solution will make it possible to clarify the objectives of the Consortium in terms of exploitation in the long term. Thus, a framework will be created to compete more easily with its competitors and to support the sustainability of the solution itself despite frequent market discontinuities.

In order to show the level of innovation of the solution, it is necessary to highlight the importance of imprinting a business model based on clear and approved concepts. The choice of the Business Model Canvas, mentioned several times, embraces this need as it is divided into 9 elementary Building Blocks that enable description of the relevant elements for the management of the exploitation activity, including in the analysis, the four main areas of a business: customers, offer, infrastructures and financial resources.

The value proposition identified within the project through the business model, aims at the exploitation of the solution thanks to the innovative content of the solution itself that provides uniqueness and can offer potential exploitation results in a commercial environment. Accordingly, the Consortium Partners' IPR on

[2] Chesbrough H. (2007), Business model innovation: it's not just about technology anymore, Strategy & Leadership, Vol.35, n.6, pp.12-17.

the individual tool/technological components of the solution developed have to be considered with respect to the potential ability of the Partners to form commercial exploitation initiatives after the end of the project.

13 Conclusions

This deliverable, D7.2, as an update on D7.1, has highlighted the various Period-2 dissemination activities performed, media deployed and preparatory exploitation planning steps undertaken. Accordingly, the results of these efforts have been reported as follows:

- Outcome 1: Project Identity
- Outcome 2: Communication & Dissemination Strategy
- Outcome 3: Channels
- Outcome 4: Editorial Plan
- Outcome 5: Project Promotional Contents
- Outcome 6: Performed Events
- Outcome 7: Exploitation Strategy building up process

An important step in term of exploitation has been the definition and the filling of the exploitation template

to inform the conceptualisation of the Critical-Chains value proposition and business model as pre-requisites to the exploitation strategy phase being undertaken for deliverable D7.8 ''Report on Business Modelling, IPR and Innovation Modelling". In light of experience through the various dissemination activities performed, it has been concluded that Videos and Blogposts should be one of the main channels of dissemination of the results of the project and accordingly these activities will form one of the main areas of activities to be further pursued by the Consortium.

From a business perspective and exploitation point of view, the first phase of preliminary analysis of commercial opportunities has been completed. The next steps to be reported in D7.8 will further advance the analysis to include various relevant factors, including the consideration of:

Strategy & business model

a. **Value for money:** How to monetise Critical-Chains applications developed
b. **Key Partnerships:** Identification of further potential contributors (if any) in order to build strong Partnerships
c. **Revenue sharing:** Network-based Business Model; each business actor (shareholder, supplier, technical or commercial Partner) has to receive some benefit from its participation in the business.

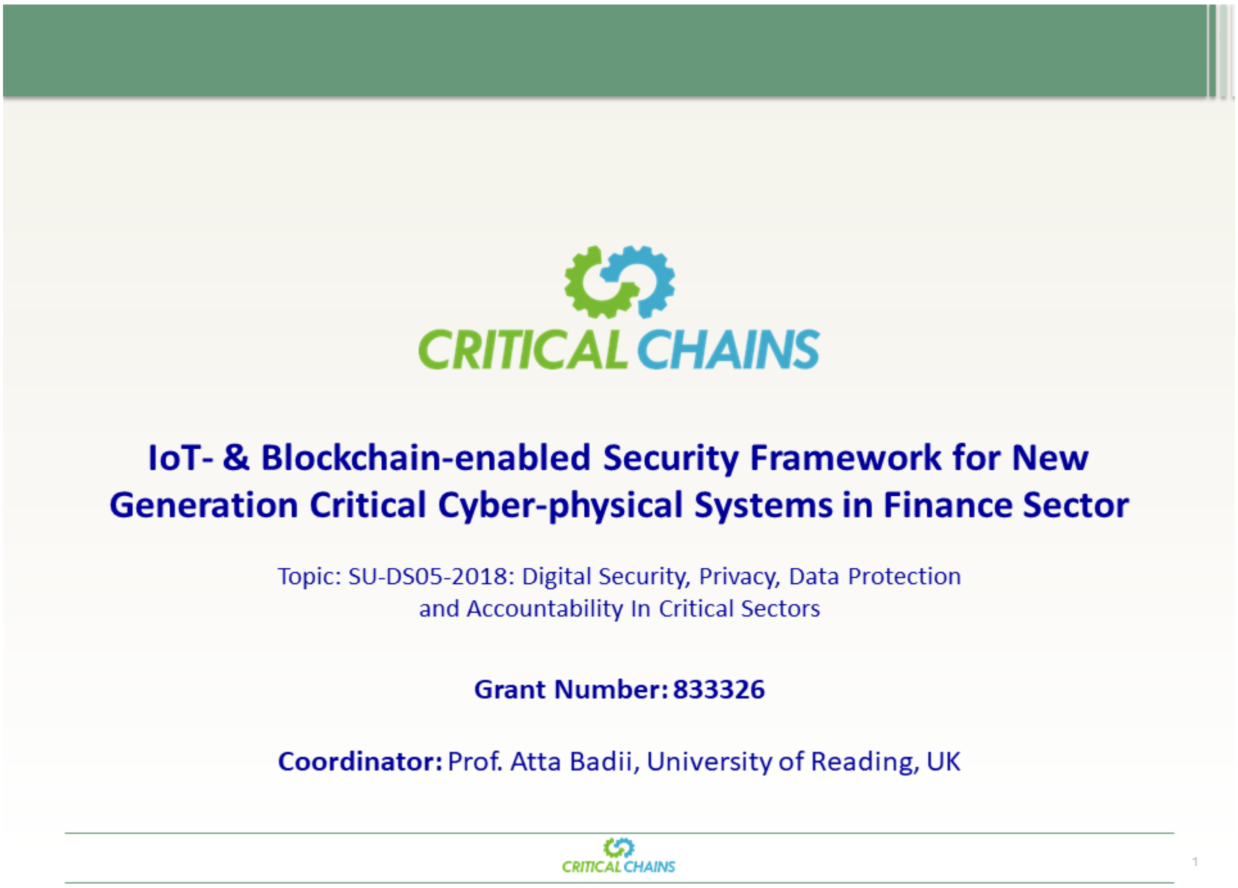
Testing the business model with stakeholders (customers and Partners)

a. **Testing the market:** Product/service and associated pricing scheme will be evaluated. 4P marketing theory (Product, Price, Promotion and Placing) can be applied to conduct the test:
b. **Testing Partnerships:** Agreements and revenue sharing schemes as could be implemented with potential Partners will also be evaluated. The goal is to assess if the different types of Partners are critical and how to manage the risk of sharing knowledge with them.

The overall dissemination, communication and exploitation activities will be performed in the next project period taking into account the above high-level objectives.

13.1 Annex A – Critical-Chains Presentations

A.1 Critical-Chain presentation at the project to policy workshop, Brussels 31st January 2020. Presentation was made by Critical-Chain coordinator Professor Atta Badii, University of Reading.



CRITICAL CHAINS

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

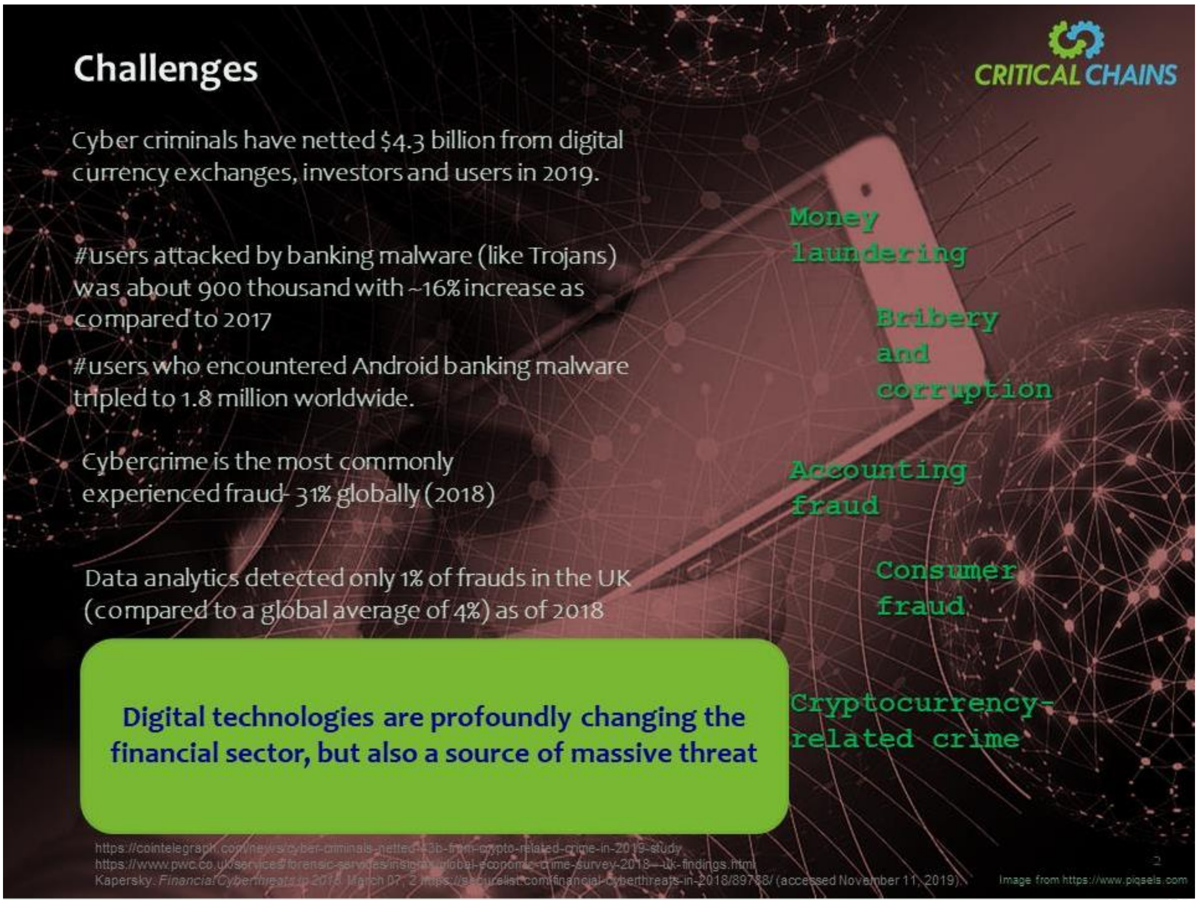
Topic: SU-DS05-2018: Digital Security, Privacy, Data Protection and Accountability In Critical Sectors

Grant Number: 833326

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

CRITICAL CHAINS

1



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

Money laundering

Bribery and corruption

Accounting fraud

Consumer fraud

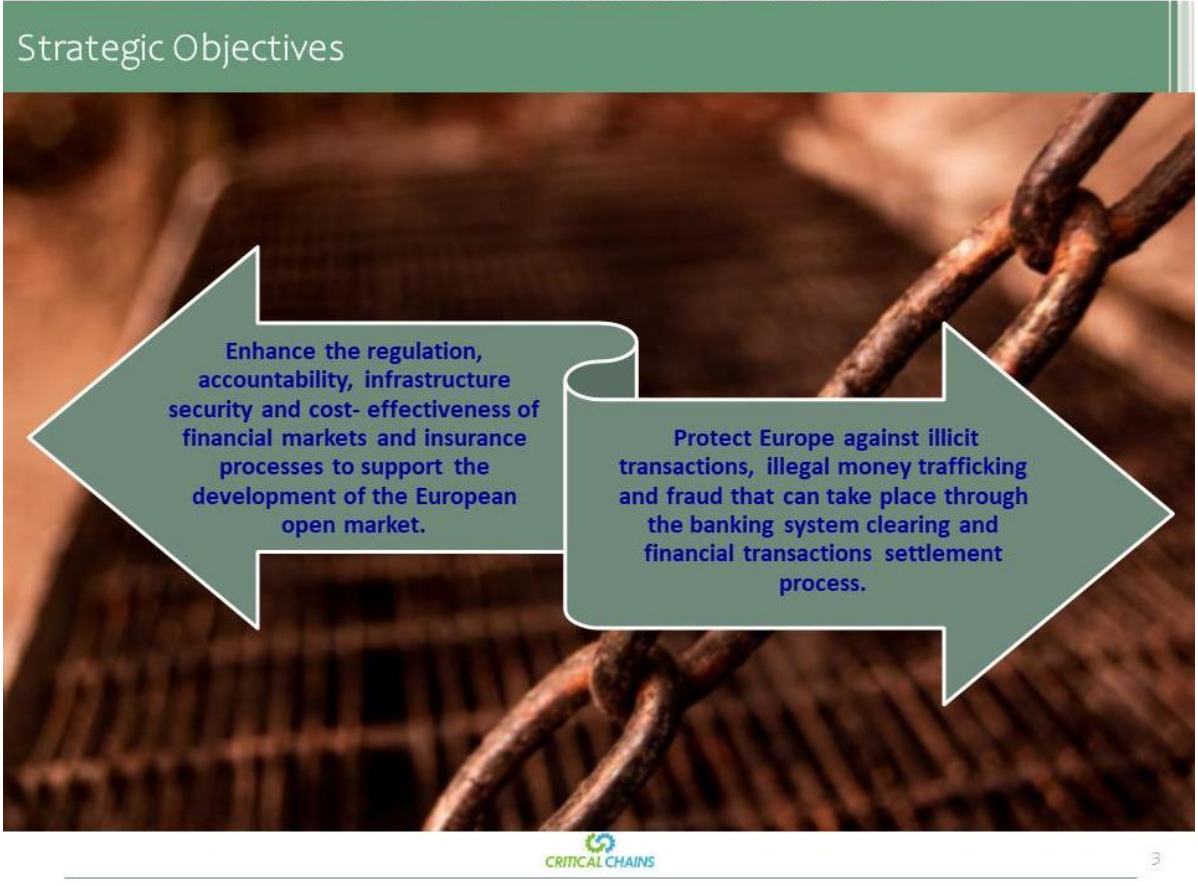
Cryptocurrency-related crime

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 Cyberthreats in 2018*. March 07, 2 https://securelist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019).

Image from https://www.piqsels.com

2



Strategic Objectives

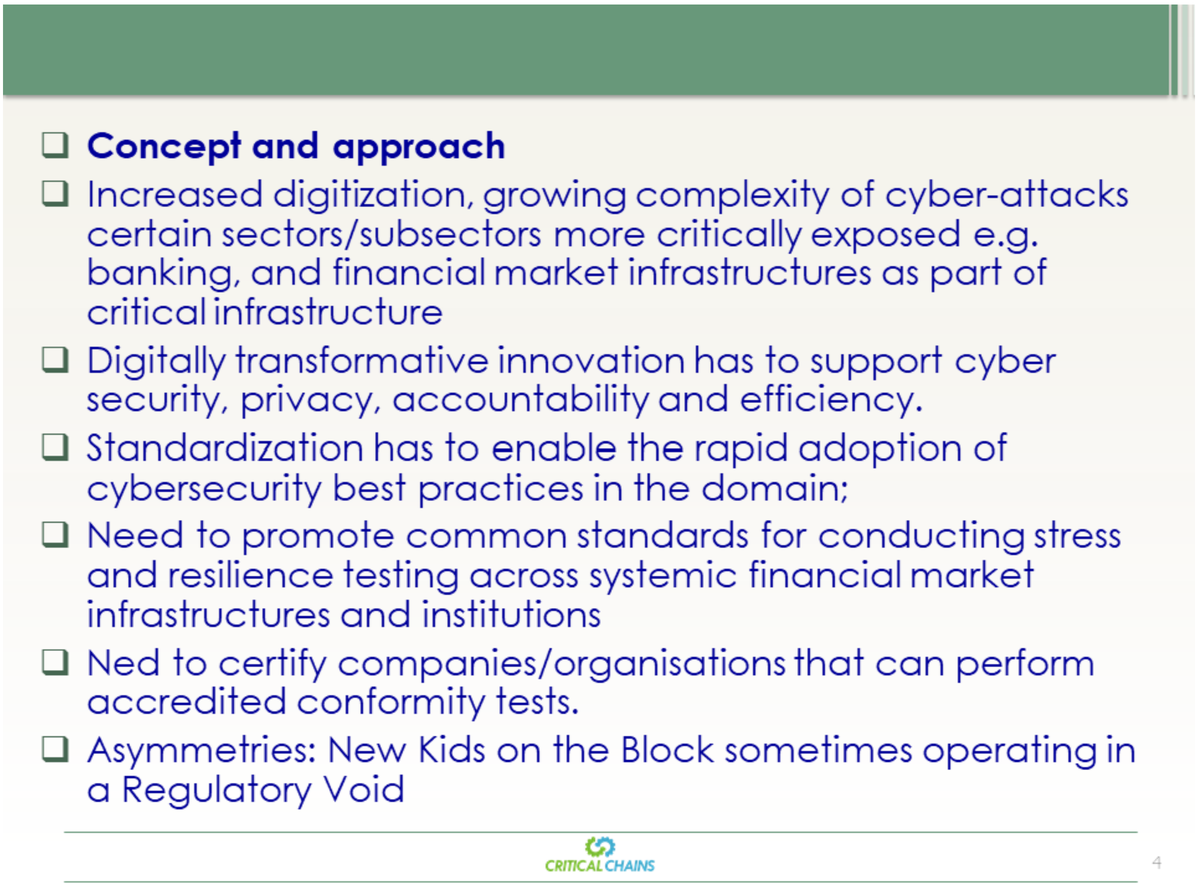
Enhance the regulation, accountability, infrastructure security and cost- effectiveness of financial markets and insurance processes to support the development of the European open market.

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

CRITICAL CHAINS

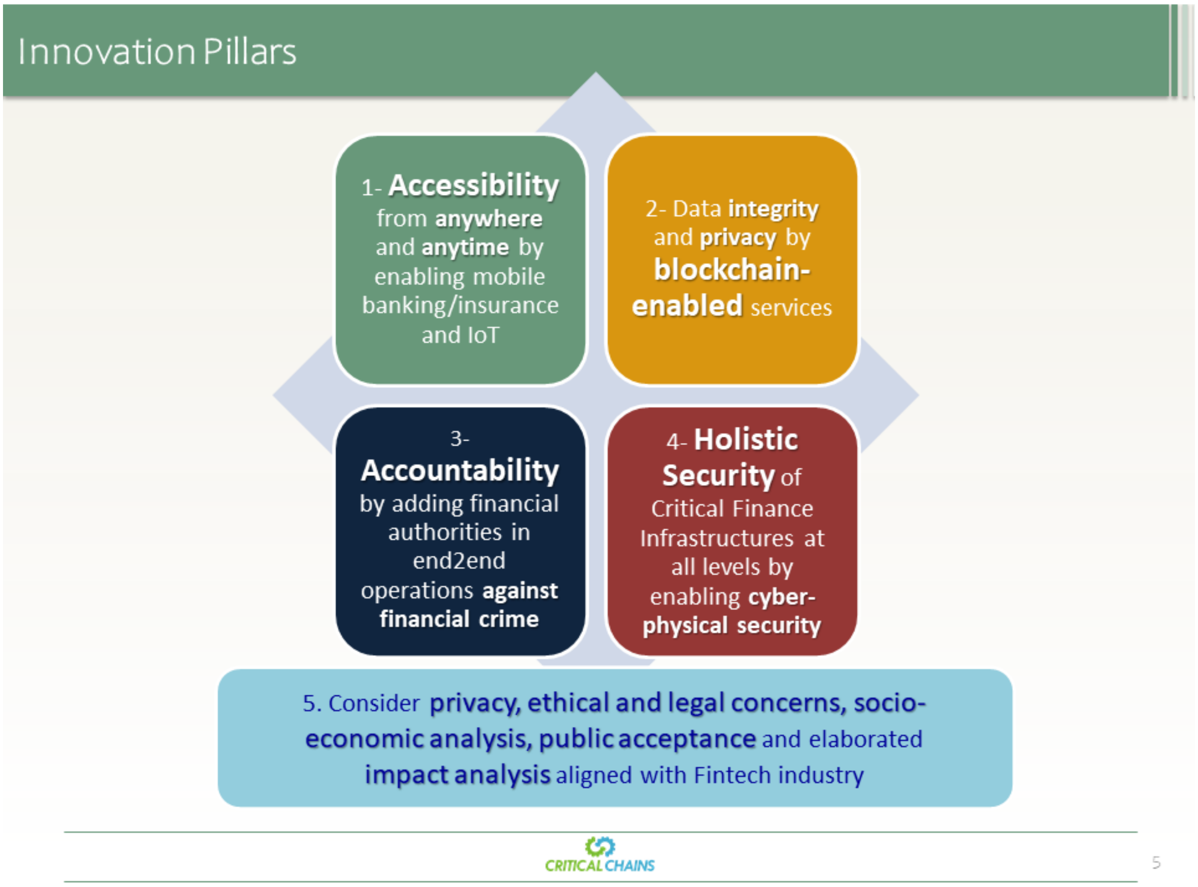
3

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



- ❑ **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
- ❑ Ned to certify companies/organisations that can perform accredited conformity tests.
- ❑ Asymmetries: New Kids on the Block sometimes operating in a Regulatory Void

CRITICAL CHAINS 4



Innovation Pillars

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

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

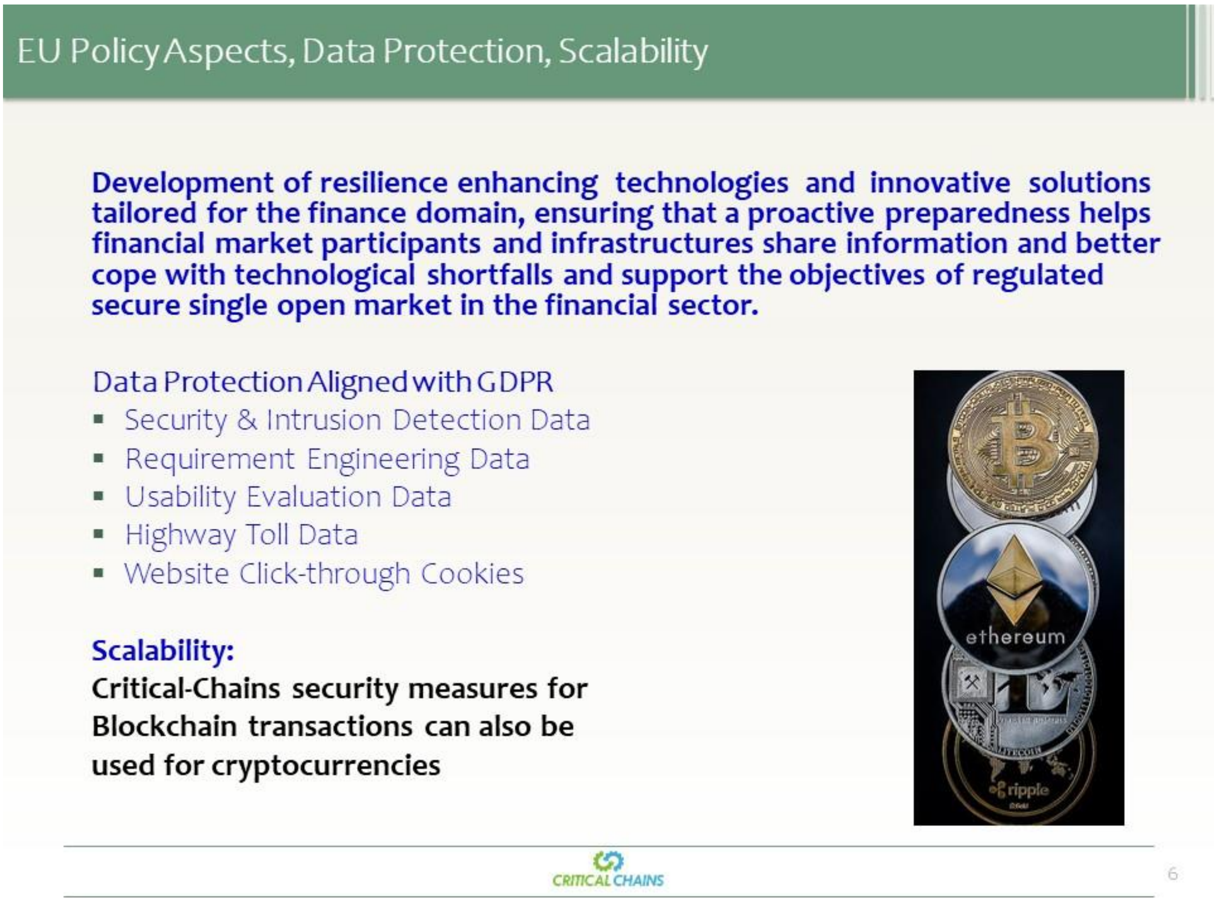
3- **Accountability** by adding financial authorities in end2end operations **against financial crime**

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

CRITICAL CHAINS 5

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



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

CRITICAL CHAINS 6

A.2 Critical-Chain presentation for the fintech project final conference on 19th May 2020. Conference held as a webinar, presentation was made by Critical-Chain coordinator Professor Atta Badii, University of Reading.

CRITICAL CHAINS

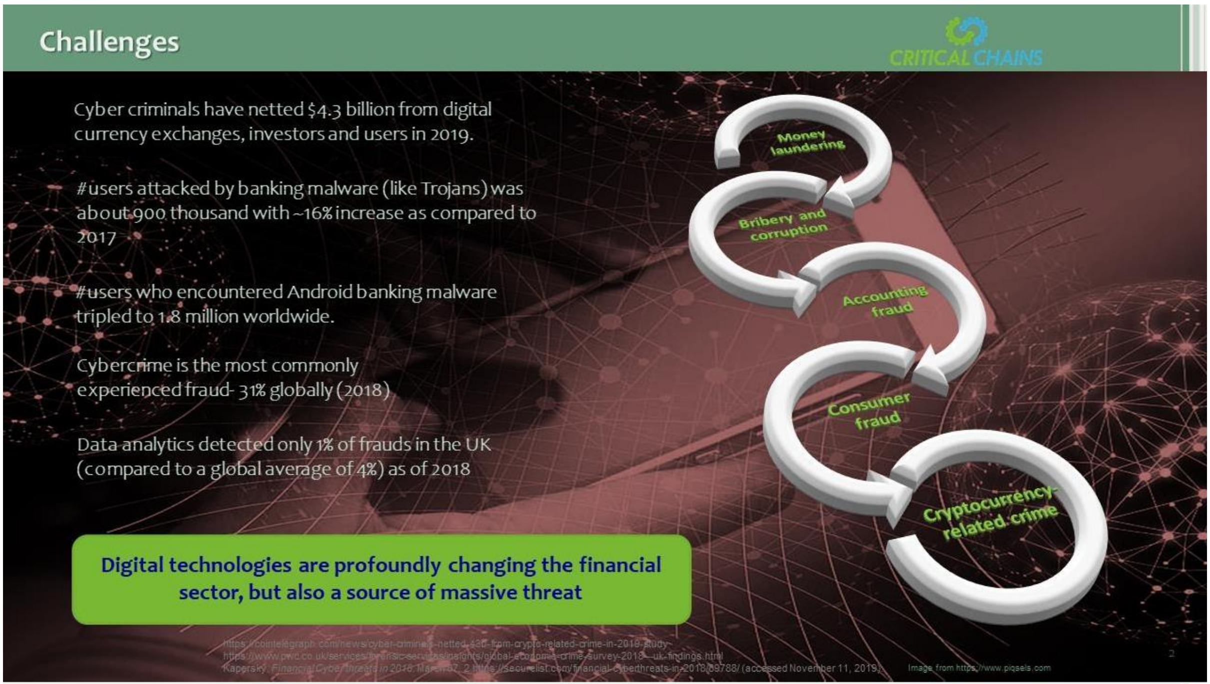
IoT- & Blockchain-enabled Security Framework for New Generation Critical Cyber-physical Systems in Finance Sector

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

CRITICAL CHAINS 1



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)

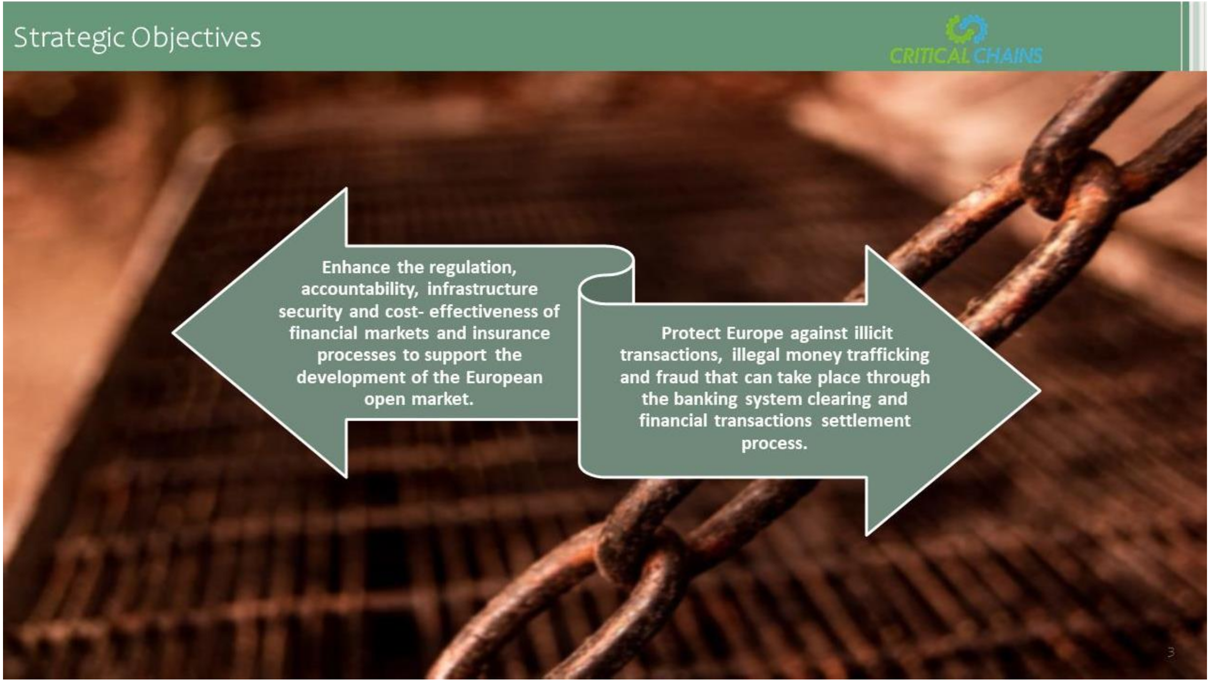
Data analytics detected only 1% of frauds in the UK (compared to a global average of 4%) as of 2018

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

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 Cyberthreats in 2018*, March 07, 2 https://securelist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019).

Image from https://www.piqsels.com

2



Strategic Objectives

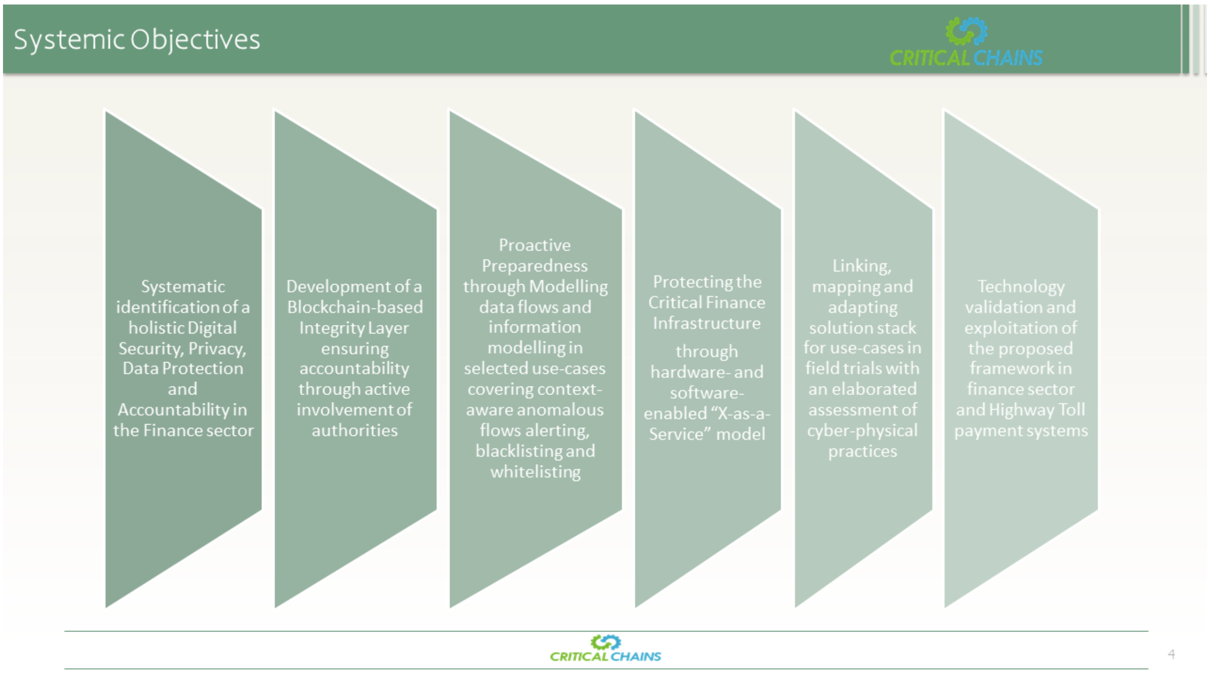
CRITICAL CHAINS

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.

3

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



Systemic Objectives

CRITICAL CHAINS

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

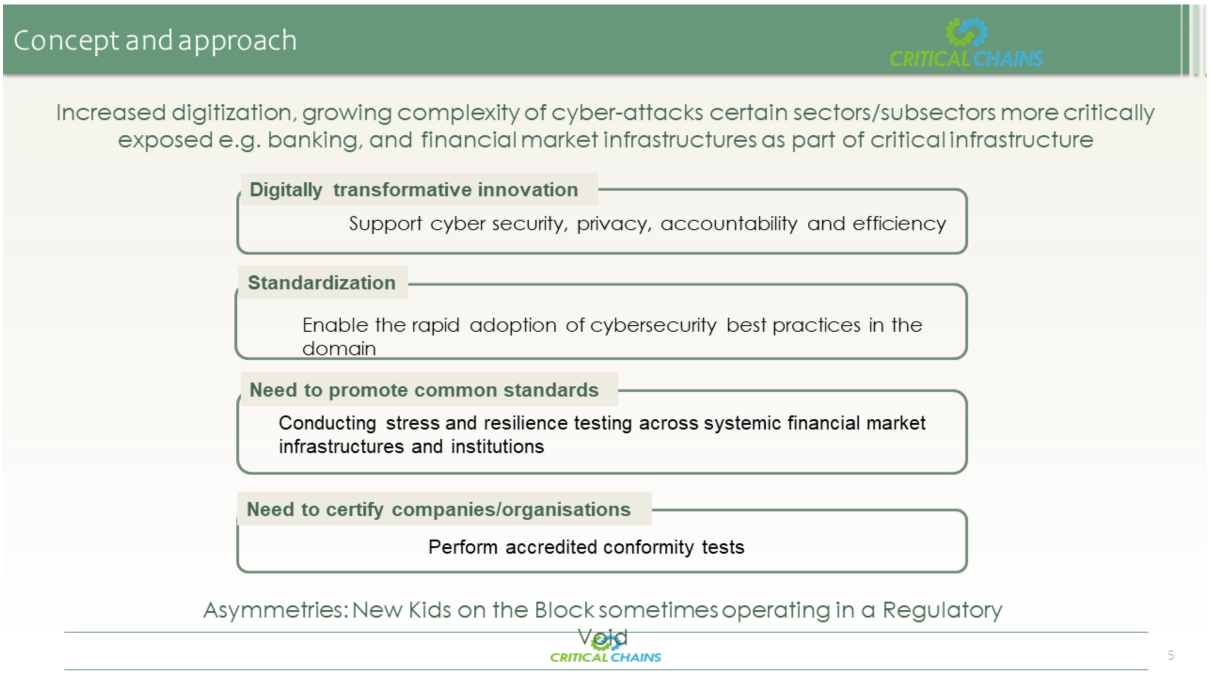
Proactive Preparedness through Modelling data flows and information modelling in selected use-cases covering context-aware anomalous flows alerting, blacklisting and whitelisting

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

CRITICAL CHAINS
4



Concept and approach

CRITICAL CHAINS

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

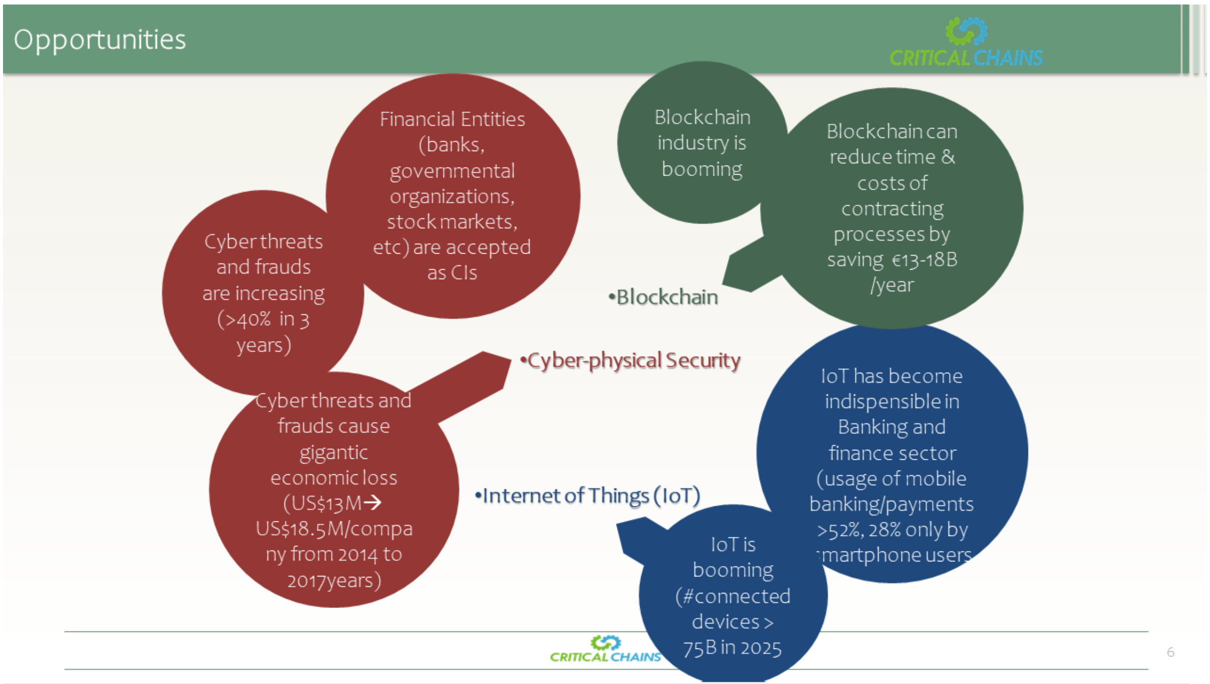
Conducting stress and resilience testing across systemic financial market infrastructures and institutions

Need to certify companies/organisations

Perform accredited conformity tests

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

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



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 2017years)

•Cyber-physical Security

Blockchain industry is booming

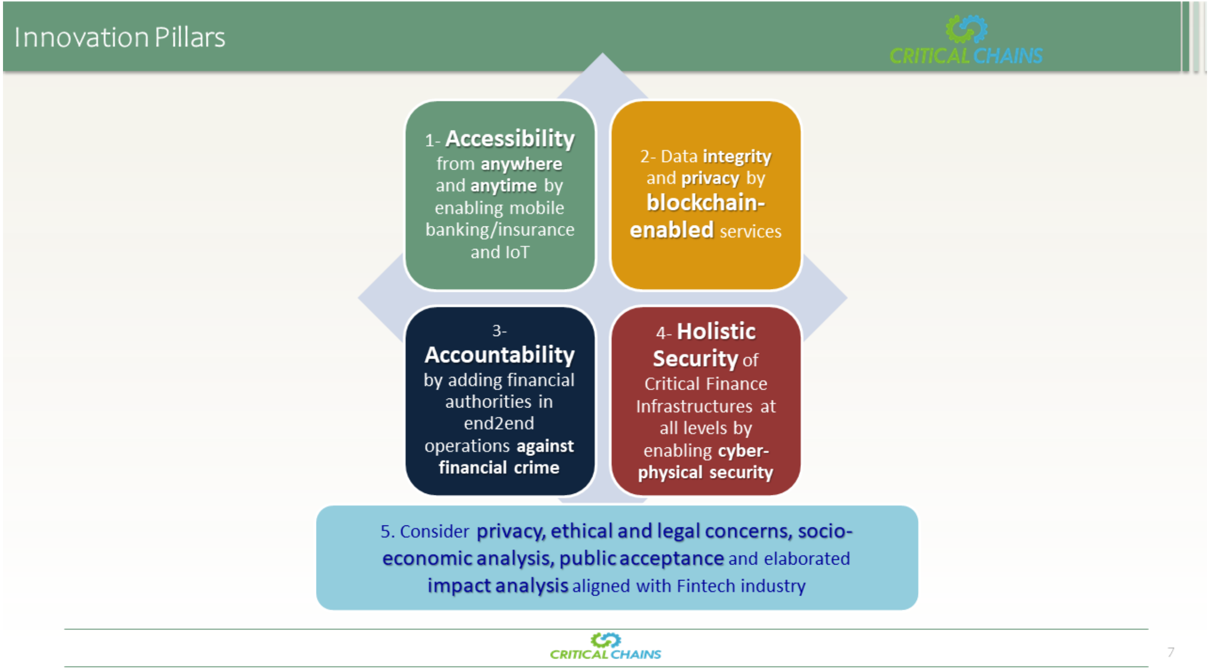
Blockchain can reduce time & costs of contracting processes by saving €13-18B /year

•Blockchain

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

•Internet of Things (IoT)



Innovation Pillars

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

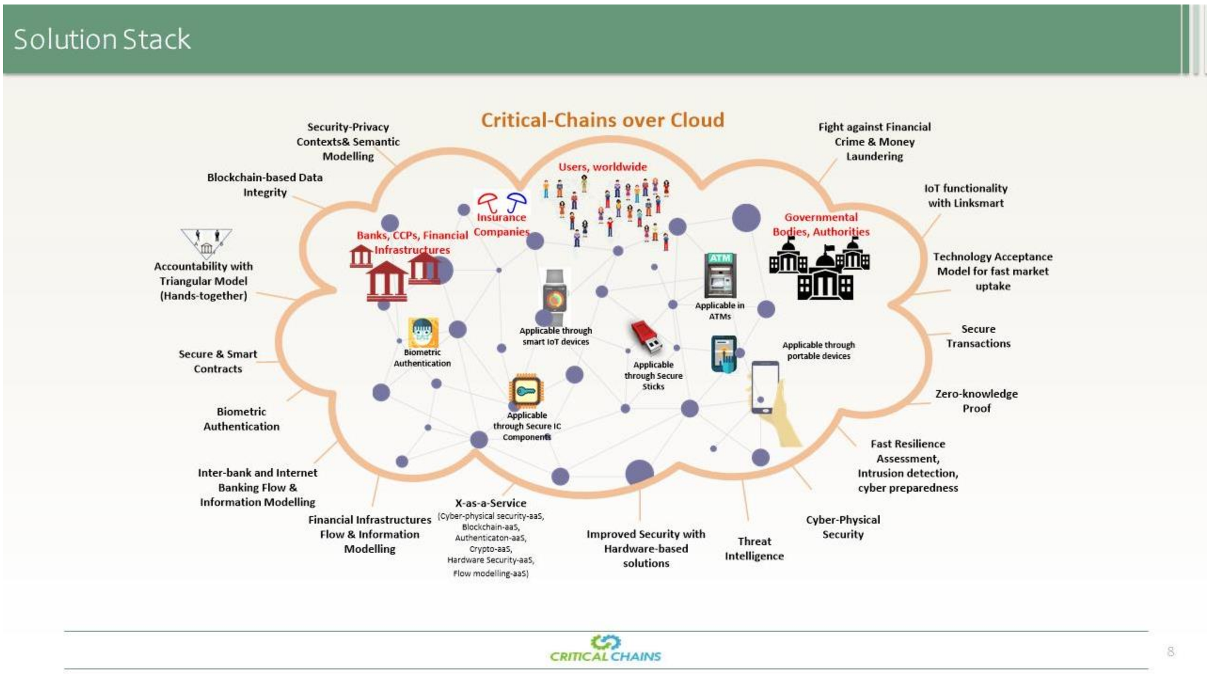
2- Data **integrity** and **privacy** by **blockchain-enabled** services

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

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



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

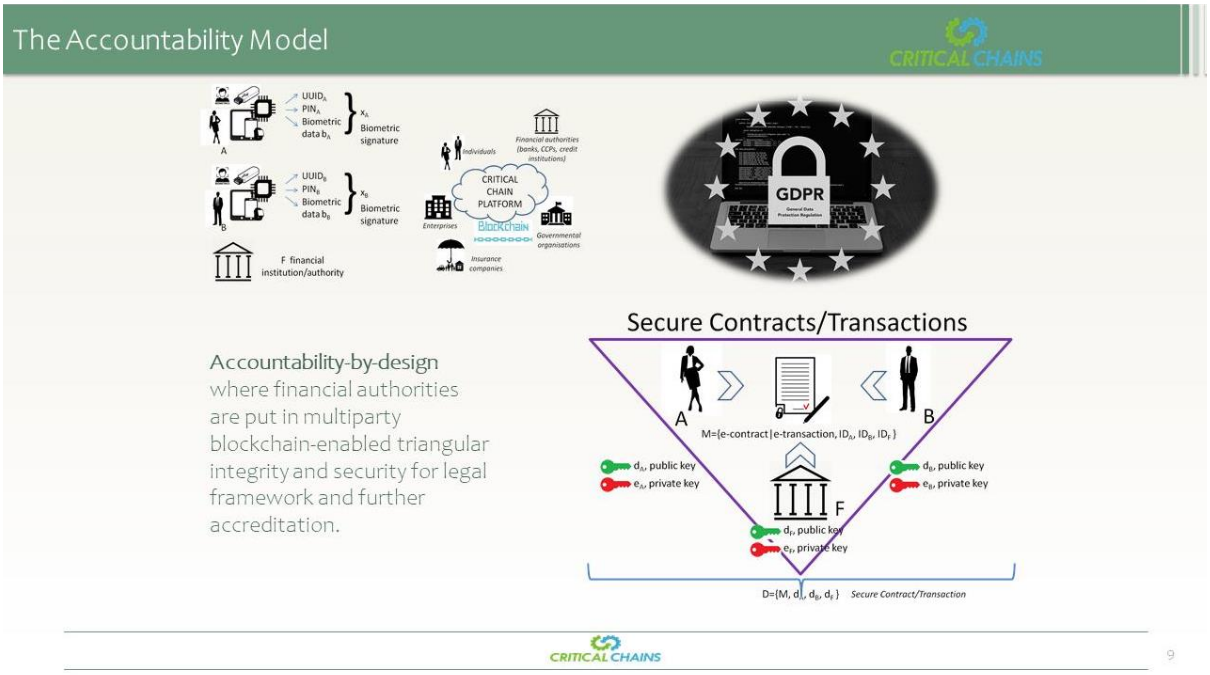
Technology Acceptance Model for fast market uptake

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

8



The Accountability Model

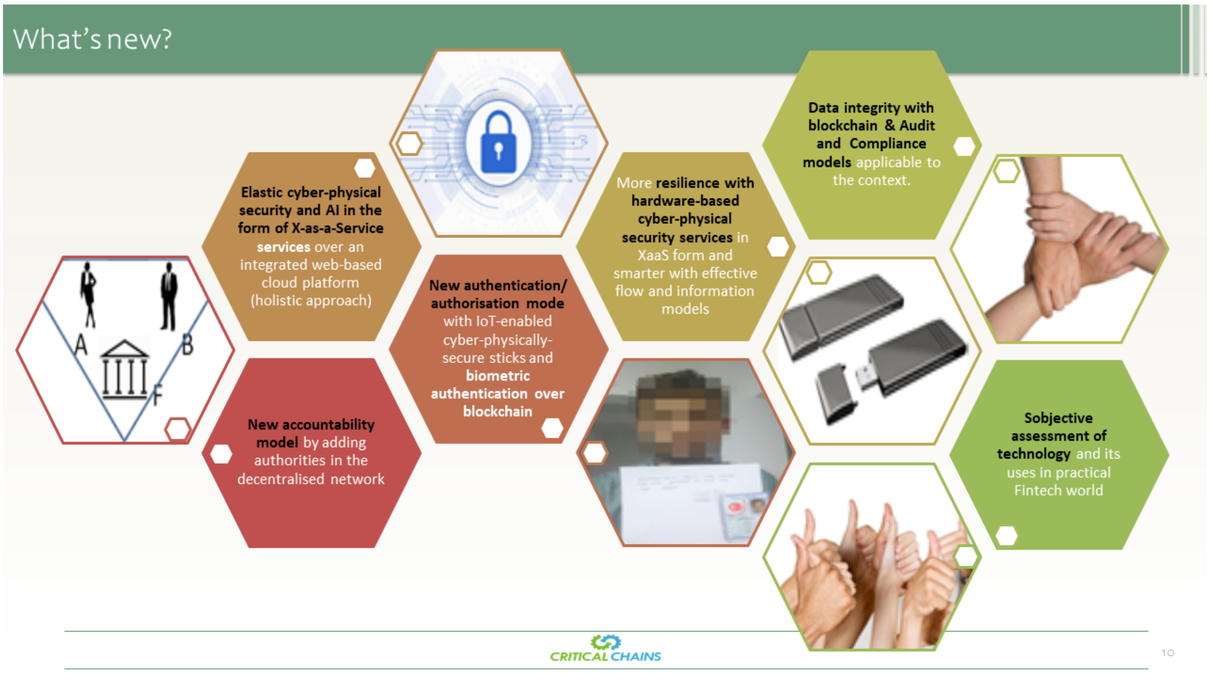
Accountability-by-design where financial authorities are put in multiparty blockchain-enabled triangular integrity and security for legal framework and further accreditation.

Secure Contracts/Transactions

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

9

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



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

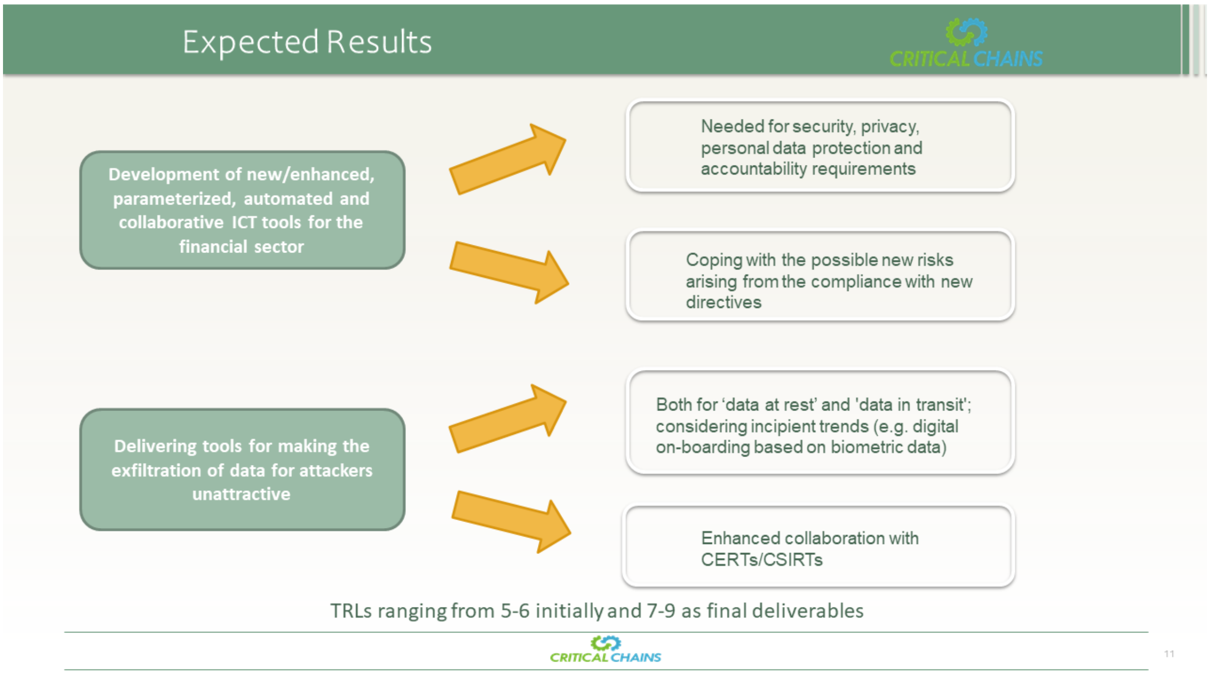
New authentication/ authorisation mode with IoT-enabled cyber-physically-secure sticks and **biometric authentication over blockchain**

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.

Sobjective assessment of technology and its uses in practical Fintech world

10



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

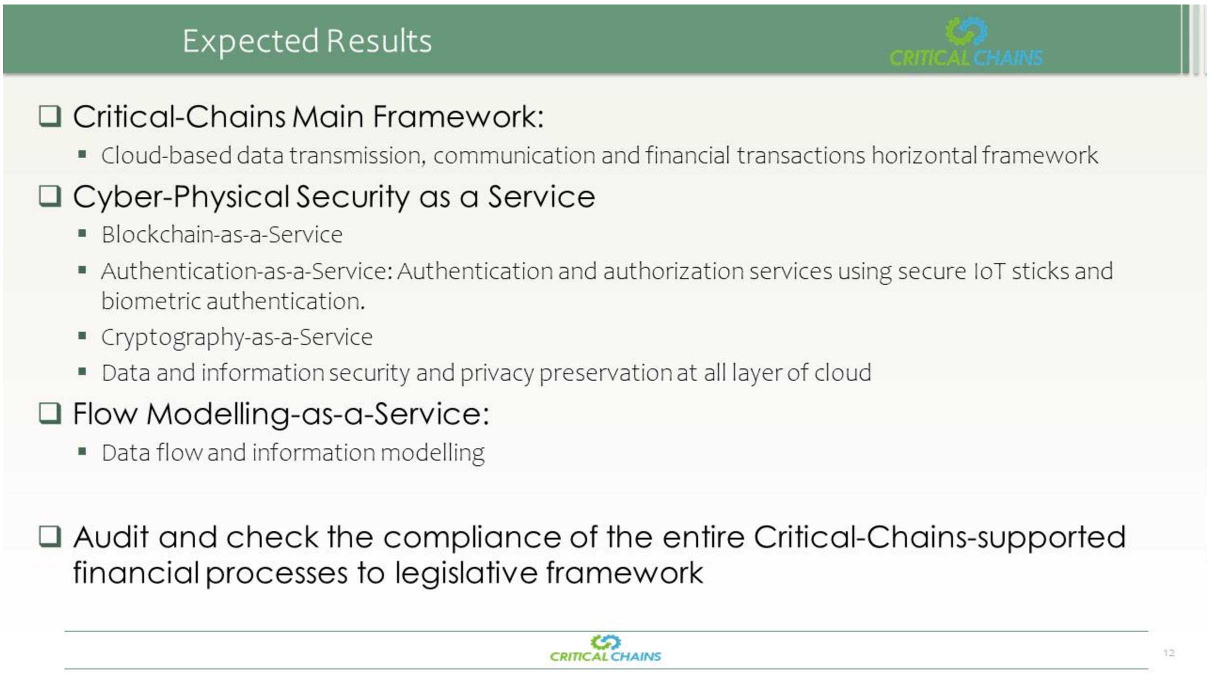
Delivering tools for making the exfiltration of data for attackers unattractive

- 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

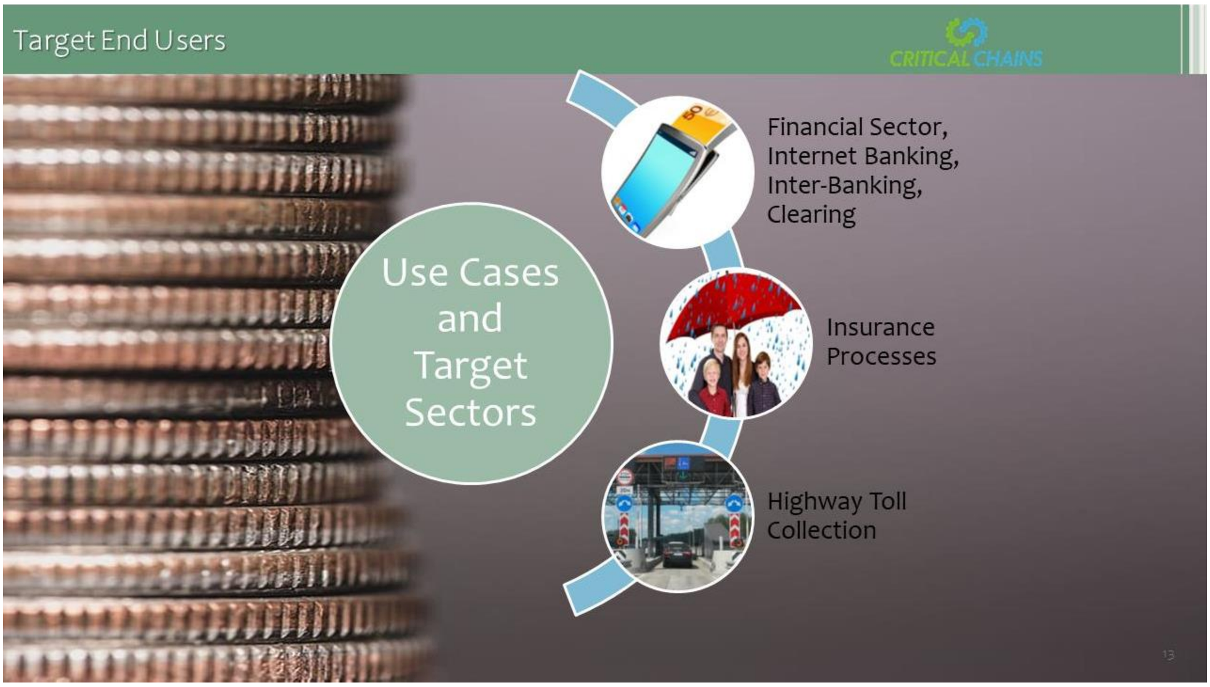
11

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



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

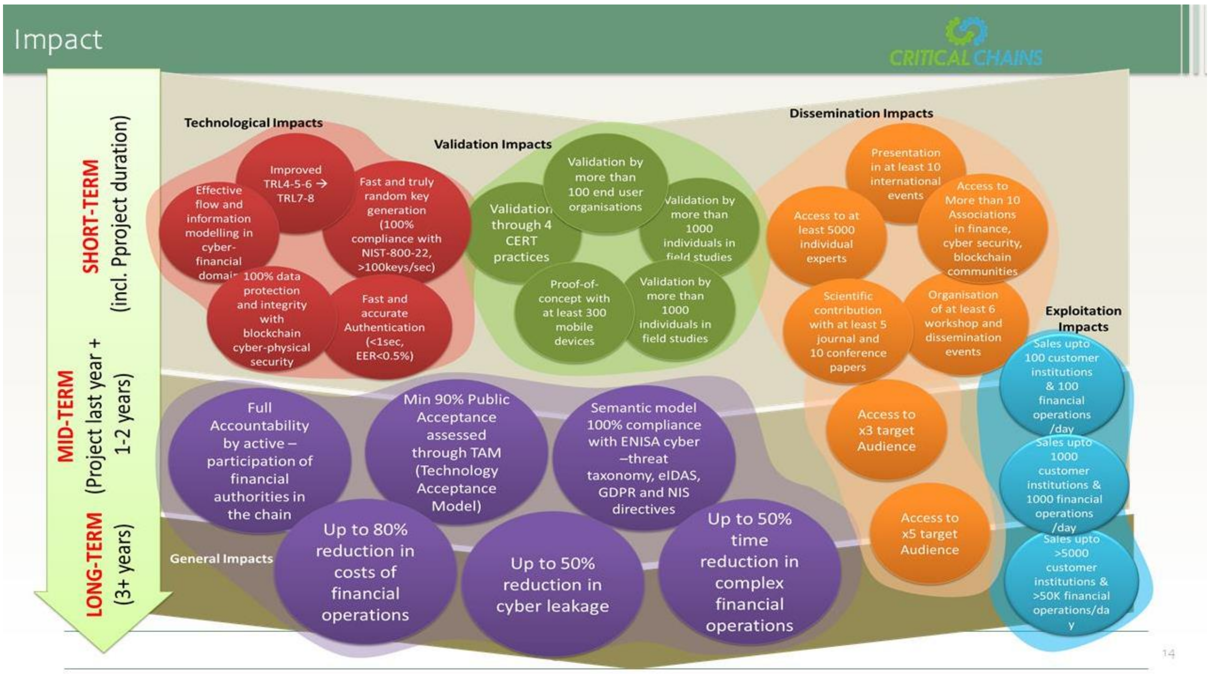
Use Cases and Target Sectors

Financial Sector, Internet Banking, Inter-Banking, Clearing

Insurance Processes

Highway Toll Collection

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



Impact

CRITICAL CHAINS

SHORT-TERM (incl. Pproject duration)

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

LONG-TERM (3+ years)

Technological Impacts

Effective flow and information modelling in cyber-financial domain

Improved TRL4-5-6 → TRL7-8

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

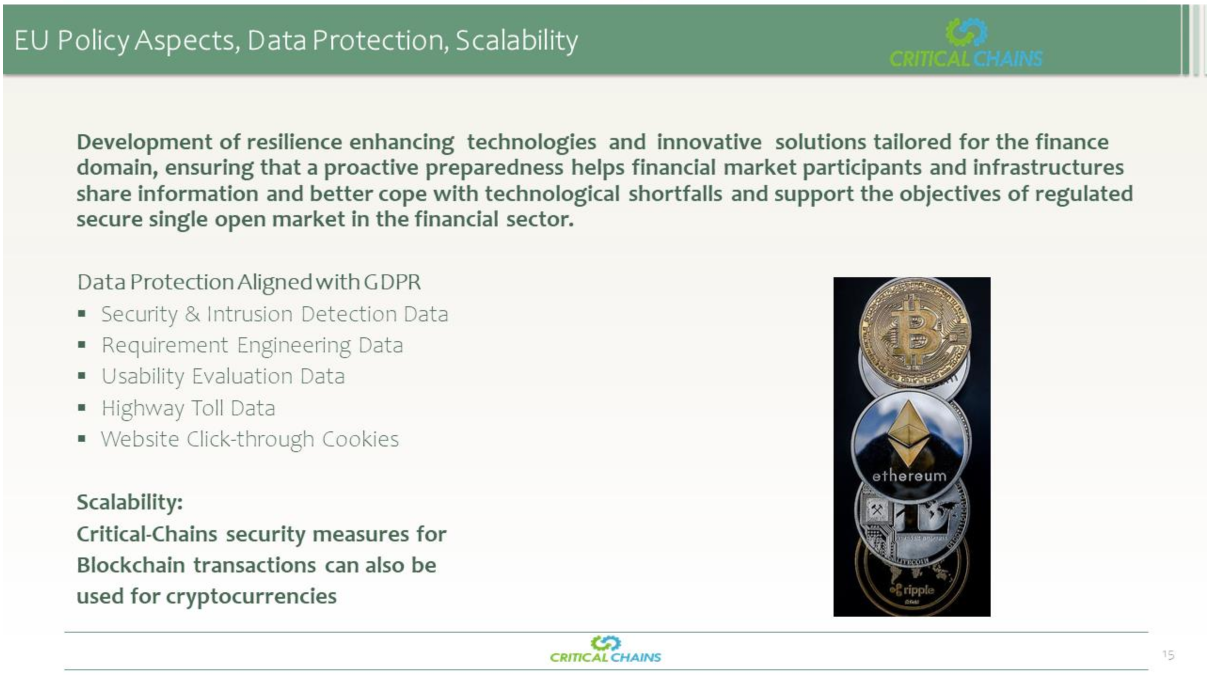
General Impacts

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

14



EU Policy Aspects, Data Protection, Scalability

CRITICAL CHAINS

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

CRITICAL CHAINS

15

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Contact us!

Critical Chains Website: https://research.reading.ac.uk/critical-chains/
Twitter: https://twitter.com/ChainsH2020

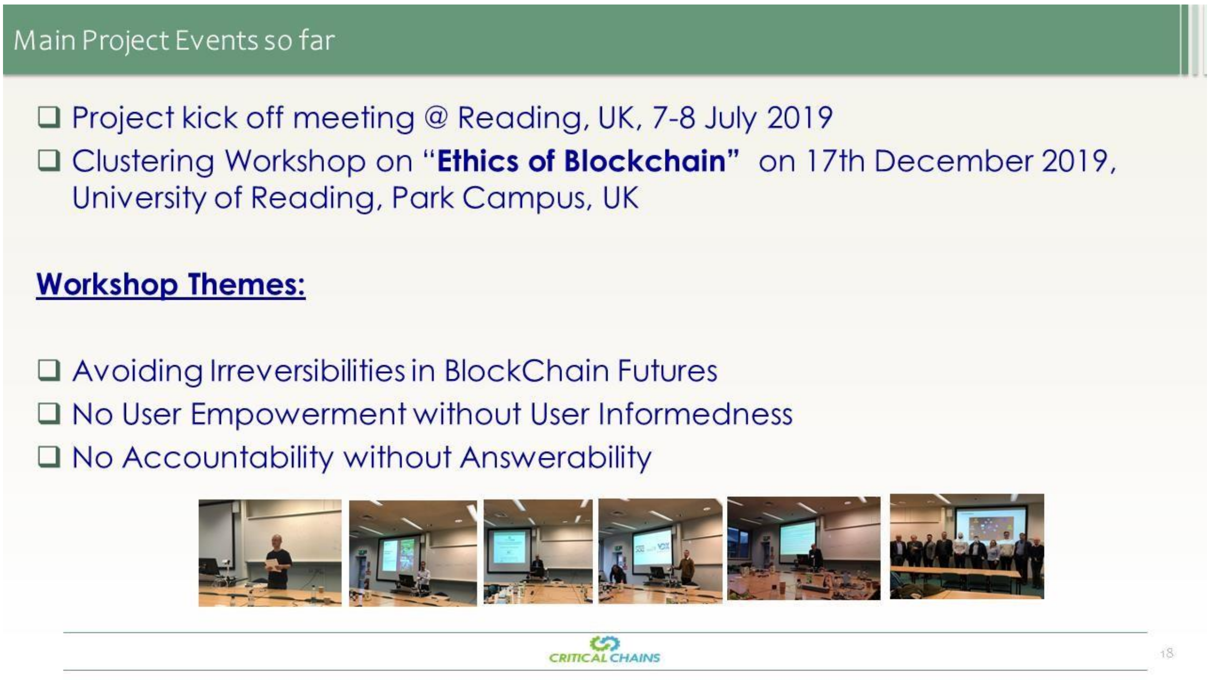
This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

16

Thank you for your kind attention!

Atta Badii – University of Reading
Critical Chains Project Coordinator
atta.badii@reading.ac.uk

17



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

CRITICAL CHAINS
18

13.2 Annex B – Publication Plans

Publications Annual Planning TablePeriod

1: July 2019-June 2020

Initiating Partner(s)' Name(s)	WP/Task Resulting in the innovation	Innovation Area & Specific Topic	Partner Staff Forming the Co-authoring team	Tentative Title of the Targeted Publication	Possible Rank-ordered Target Publications: Workshop/Conference/Journal	Planned Date of Submission of the Pre-final version to the SAB for Security Screening process

****