



Critical-Chains

Collaborative Project

Project Start Date 1st July 2019
Duration 36 Months

Deliverable D7.1 (Public)

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

Published by the Critical-Chains Consortium

Version 6.0

Date: 30/06/2020

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP7

Document Responsible: RINA-C

Contributors: All

Status: Final

Abstract

D7.1 “Critical-Chains Bulletin: A report on dissemination, exploitation and list of outcomes (a)” 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
- Show all the content created to promote the Critical-Chains project
- Make 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.
- List all the communication and dissemination activities performed to promote the project
- Present the exploitation strategy building process and the activities aimed at analysing Critical-Chains outcomes for commercial evaluation.

Deliverable D7.1 Document History

Versioning			
Version Number	Date	Contributors' name and organisation	Changes
V0	30/05/2020	RINA-C	ToC Elaboration
V1	18/05/2020	RINA-C, NETAS	1 st Draft - Contribution to communication
V2	25/06/2020	RINA-C, All	2 nd Draft - Contribution to dissemination
V3	29/06/2020	RINA-C	Contribution to main events and exploitation report consolidation
V4	30/06/2020	RINA-C, UREAD	Contributions to C& D tables
V5 -V6	30/07/2020- 30-09-2020	UREAD-RINA-C	Finalisation of the C& D Tables Final edits and formatting

Internal Review History

Internal Reviewers	Date	Comments
Ivan Tesfai	29/06/2020	Quality Check
Atta Badii	29/06/2020	C&D table needs to be finalised

Table of Contents

Abstract	2
Executive Summary	7
1 Introduction.....	8
1.1 Scope of the Deliverable	8
2 Outcome 1: Project Identity	9
2.1 Logo	9
2.2 Promotional Payoff.....	9
3 Outcome 2: Communication & Dissemination Strategy	9
4 Objectives.....	10
5 Target	11
6 Outcome 3: Project Channels.....	12
6.1 Website	12
6.2 Social Media (UREAD).....	15
7 Outcome 4: Editorial Plan.....	18
7.1 Promotion through Partner’s channels.....	18
7.2 Communication & Dissemination Tracking File.....	20
8 Outcome 5: Project Promotional Contents	21
8.1 Video.....	21
8.2 Presentation	22
8.3 Brochure	24
8.4 Posters.....	26
9 Events	27
9.1 Outcome 6: performed events	27
9.2 Outcome 7: future events	30
10 C&D KPIs	31
11 Table of Performed and Planned Communication & Dissemination Action	32
11.1 Dissemination Table	32
12 Exploitation.....	34
12.1 Exploitation Strategy building up process.....	34
12.2 Initial identification of project outcomes.....	35
12.3 Partners Exploitation intentions.....	36
12.4 Markets to be targeted and Unique Selling Proposition.....	40
12.5 Commercialisation roadmaps.....	42
13 Conclusions.....	44

Annex A – Critical-Chains Presentations 45

Table of Figures

Figure 1: Critical-Chains Project Logo.....	9
Figure 2: Time per day spent using the internet	10
Figure 3: Critical-Chains Website Homepage.....	14
Figure 4: Critical-Chains social media banner	15
Figure 5: Example of Promotional Tweet.....	17
Figure 6: Example of Promotional Tweet.....	17
Figure 7: Critical-Chains YouTube Channel.....	18
Figure 8: Critical-Chains project on RINA website.....	20
Figure 9: Critical-Chains C&D Tracking File.....	20
Figure 10: Critical-Chains Promotional Video.....	21
Figure 11: Critical-Chains Promotional Video.....	22
Figure 12: Critical-Chains Promotional Video.....	22
Figure 13: Critical-Chains project presentation.....	23
Figure 14. Critical-Chains project presentation.....	23
Figure 15: Critical-Chains project presentation.....	24
Figure 16: Critical-Chains project brochure.....	25
Figure 17:Critical-Chains project poster-2 (NETAS).....	26
Figure 18: Critical-Chains project poster-3 (RINA)	27
Figure 19: Consortium Partners’ delegates participating in the Kickoff Research Methodology Workshops.....	28
Figure 20: Ethics of Blockchain Attendees	29
Figure 21: Exploitation Strategy Building process.....	35

List of Tables

Table 1: Critical-Chains Target Groups	11
Table 2: Main Critical-Chains project outputs.....	35
Table 3:Critical-Chains markets.....	41
Table 4:Critical-Chains potential commercialisation route over time to market.....	43

Executive Summary

D7.1 aims at explaining the communication, dissemination and exploitation strategy of Critical-Chains; highlighting all the outcomes achieved from M1 to M12.

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 year 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 shall be 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.

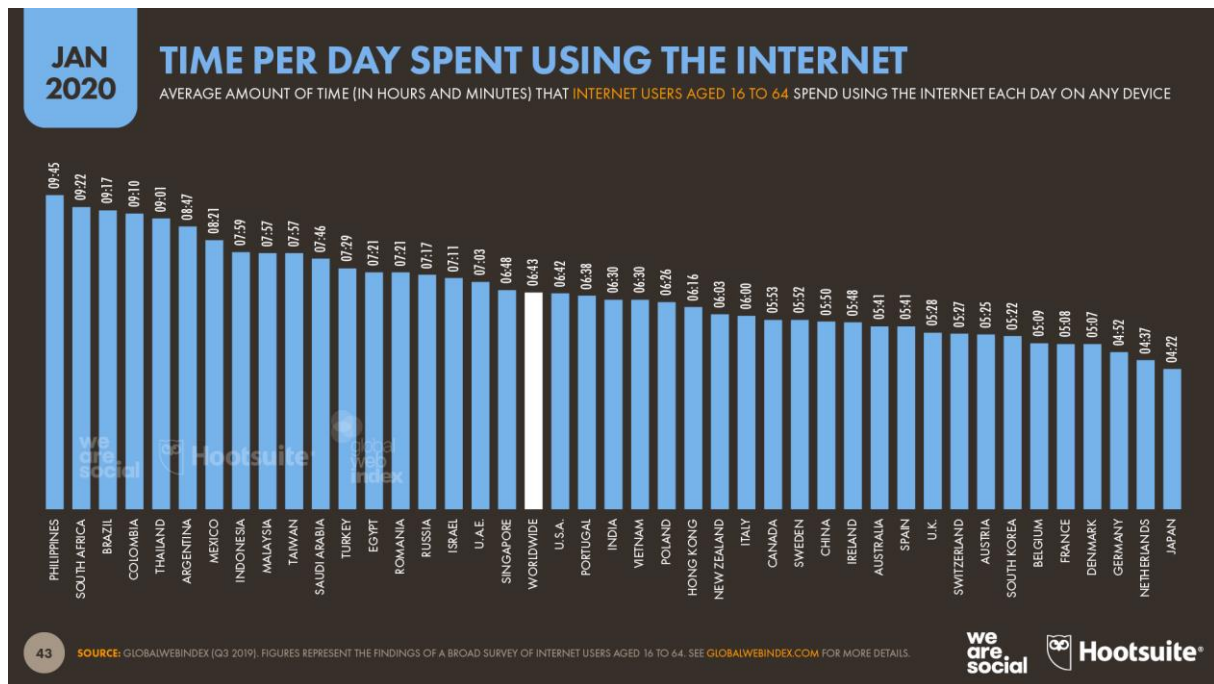


Figure 2: Time per day spent using the internet

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 updated with new content ideas and customised according to target audiences).

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 maximise 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**

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:

- 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.)	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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
Direct customers, enterprises	<ul style="list-style-type: none"> include banks, insurance companies, financial organisations (mid-parties in triangular accountability model) 	<ul style="list-style-type: none"> Send them regular newsletters, Direct and personal contacts to the financial IT managers; Discussion group meetings with partners
	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Promotional activities over media (including social media) Activate practitioners' existing customer portfolio to increase their awareness Business relations, own events/summits
Solution partners	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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; 	<ul style="list-style-type: none"> Online dissemination (e.g. posts/news on project website) Dissemination through social media, media, news Share videos and animations over Internet
Company internal stakeholders	<ul style="list-style-type: none"> Knowledge transfer & awareness raising Transfer project generated knowledge towards security practitioners, professionals working in the banking divisions, professionals working in the trust services' departments 	<ul style="list-style-type: none"> 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 visibility and impact, especially towards the wider FinTech community and also to the security community and general 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 also serves 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 Agreement No 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/>
- Critical-Chains Innovation: <https://research.reading.ac.uk/critical-chains/innovation/>
- Critical-Chains Validation: <https://research.reading.ac.uk/critical-chains/innovation/>
- News and Events: <https://research.reading.ac.uk/critical-chains/news-and-events/>
- Publications: <https://research.reading.ac.uk/critical-chains/publications/>
- Advisory Boards: <https://research.reading.ac.uk/critical-chains/advisory-boards/>

University of Reading Home Mission Innovation Validation Advisory Boards News and Events Publications Deliverables Consortium

CRITICAL CHAINS

Welcome to Critical-Chains

Critical-Chains is a 3-year research and innovation programme funded with the support of the European Commission Horizon 2020 Programme with a focus on IOT & Blockchain-Enabled Security Framework for Fintech Integrated New Generation Cyber-Physical Systems to support the Financial Sector. The Critical-Chains 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.

This project has received funding from the European Union Horizon 2020 Research and Innovation Programme under Grant Agreement No 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.

that presents a novel XaaS platform based on Blockchain-as-a-Service...

<p>MISSION The Critical-Chains Mission is to deliver: A novel triangular accountability model and integrated framework supporting accountable, effective.</p>	<p>INNOVATION Critical-Chains Stakeholders and Roles Critical-Chains primary stakeholders are as follows: Citizens and Companies as Bank Account Holders Citizens and</p>	<p>VALIDATION Validation Critical-Chains is to be validated within 4 case studies aligned with 3 critical sectors as follows: Banking Financial market...</p>
<p>ADVISORY BOARDS Advisory Boards The Critical-Chains Advisory Boards benefits from the knowledge and experience of members of two Advisory Boards as follows...</p>	<p>PUBLICATIONS Publications Publications Annual Planning Tables</p>	<p>NEWS AND EVENTS</p>

CONTACT US
 +44 118 378 7842
 atta.badli@reading.ac.uk
 Professor Atta Badli
 Department of Computer Science
 School of Mathematical, Physical and Computational Sciences (SMPCS)
 University of Reading
 Park Campus
 Reading RG6 6AH
 United Kingdom

UNIVERSITY OF READING
 Research
 News and events
 Research blog

© Copyright University of Reading

Figure 3: Critical-Chains Website Homepage

6.2 Social Media (UREAD)

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



Figure 4: 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 Twitter account, 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.

LinkedIn
People ▼ Critical-Chains Project
Join now [Sign in](#)

Critical-Chains Project

Secure Societies Project at EC-Funded H2020 Programme

Reading, United Kingdom · 0 connections

Connect with Critical-Chains

About

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 illicit 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

People also viewed

- Profile Name**
Secure Societies Project at EC-Funded H2020 Programme
- Profile Name**
Secure Societies Project at EC-Funded H2020 Programme
- Profile Name**
Secure Societies Project at EC-Funded H2020 Programme
- Profile Name**
Secure Societies Project at EC-Funded H2020 Programme

About

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 illicit 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

Critical-Chains' public profile badge

Include this LinkedIn profile on other websites

[View profile](#)

[View profile badges](#)

16



Figure 5: Example of Promotional Tweet



Figure 6: Example of Promotional Tweet

Youtube Channel

<https://www.youtube.com/channel/UCa3QA5cOLRMR8bPeGlvsVWg>

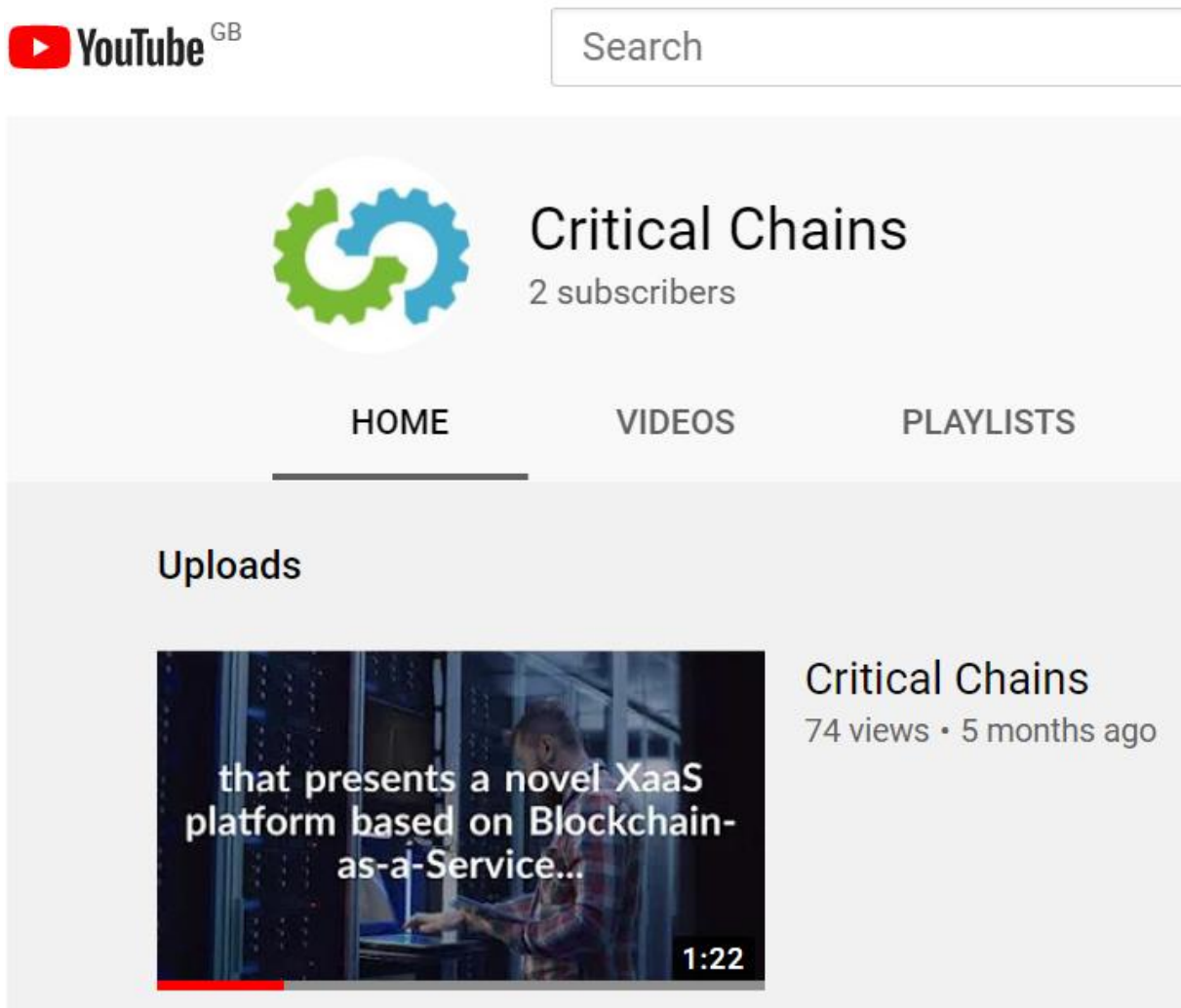


Figure 7: Critical-Chains YouTube Channel

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.

RINA What we do About us Media Careers Contacts

Home / Media / Case Studies / Critical Chains

Ivan Tsefal
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

Map Satellite

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 Horizon 2020 research and innovation programme

Contact us ▾

RINA. Excellence Behind Excellence.

© 2017 RINA S.p.A. VAT number: 03724021038

Figure 8: Critical-Chains project on RINA website

The same was made 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

	A	B	C	D	E	F	G	H	I	J
1										
2	CRITICAL CHAINS									
3										
4										
5	Type of event	Event Title	Link	Date	Place	Partner Contribution (project presentation, brochure, stand...)	Countries addressed	Target	Responsible partner	Status
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										

Figure 9: 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”
- 29.2 - 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 because:

- 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=7NUI djFHMhI>) 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.

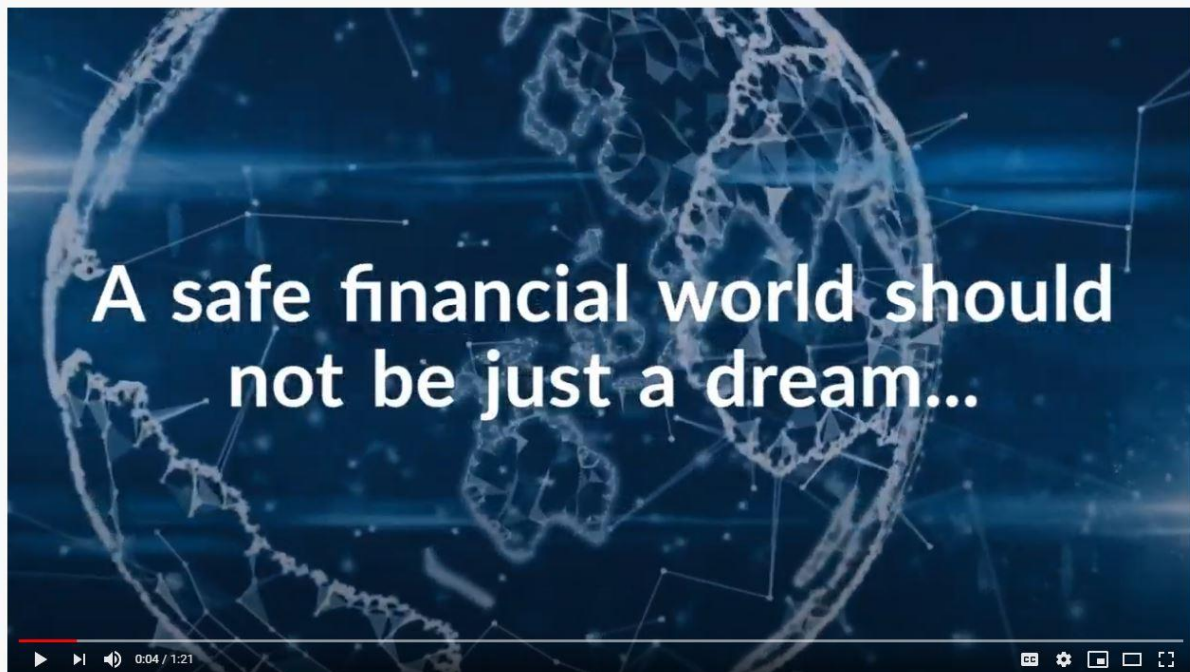


Figure 10: Critical-Chains Promotional Video



Figure 11: Critical-Chains Promotional Video



Figure 12: 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.

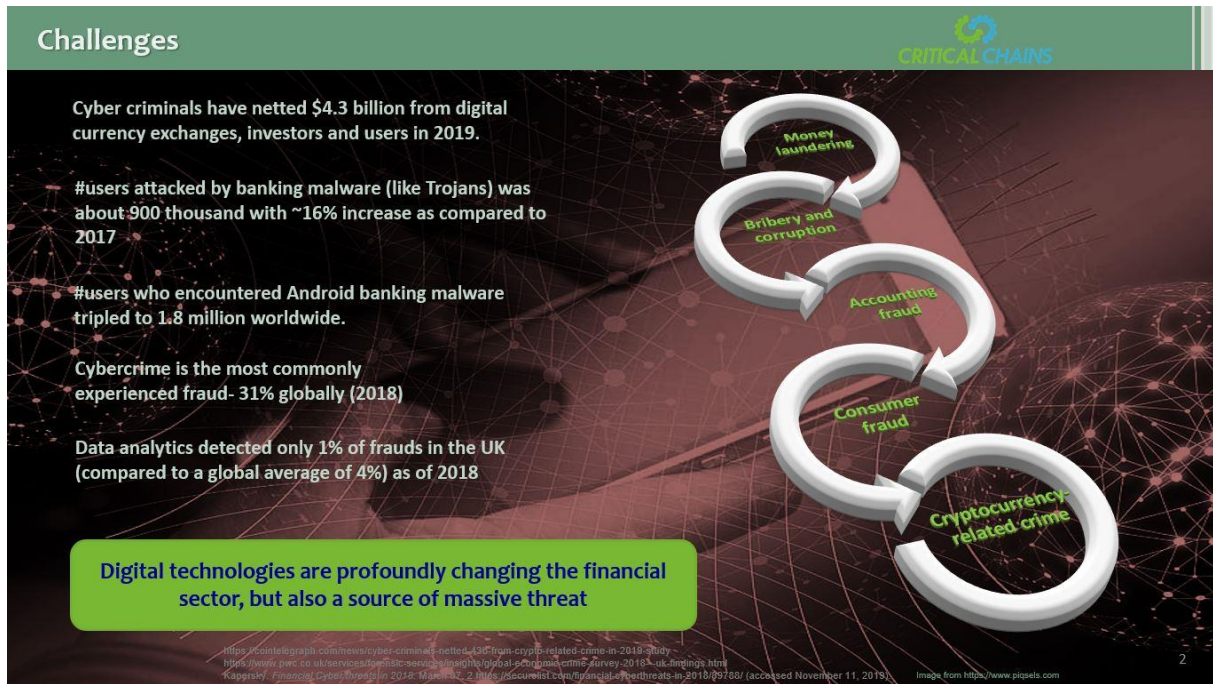


Figure 13: Critical-Chains project presentation

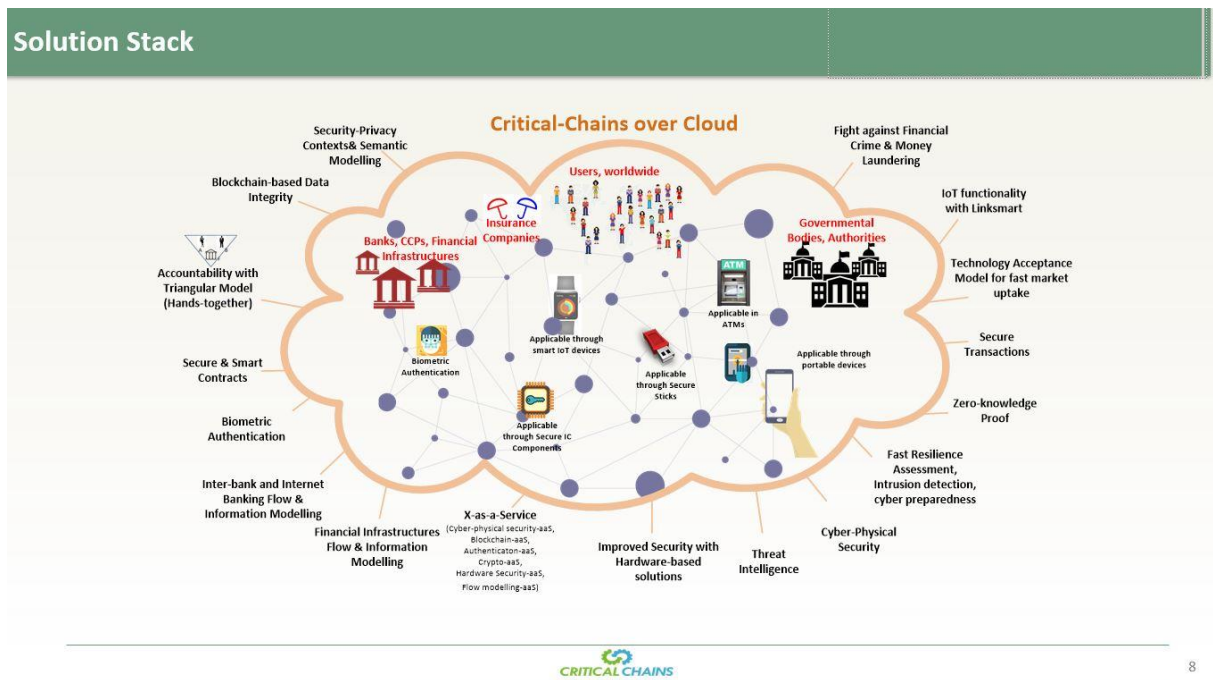


Figure 14. Critical-Chains project presentation

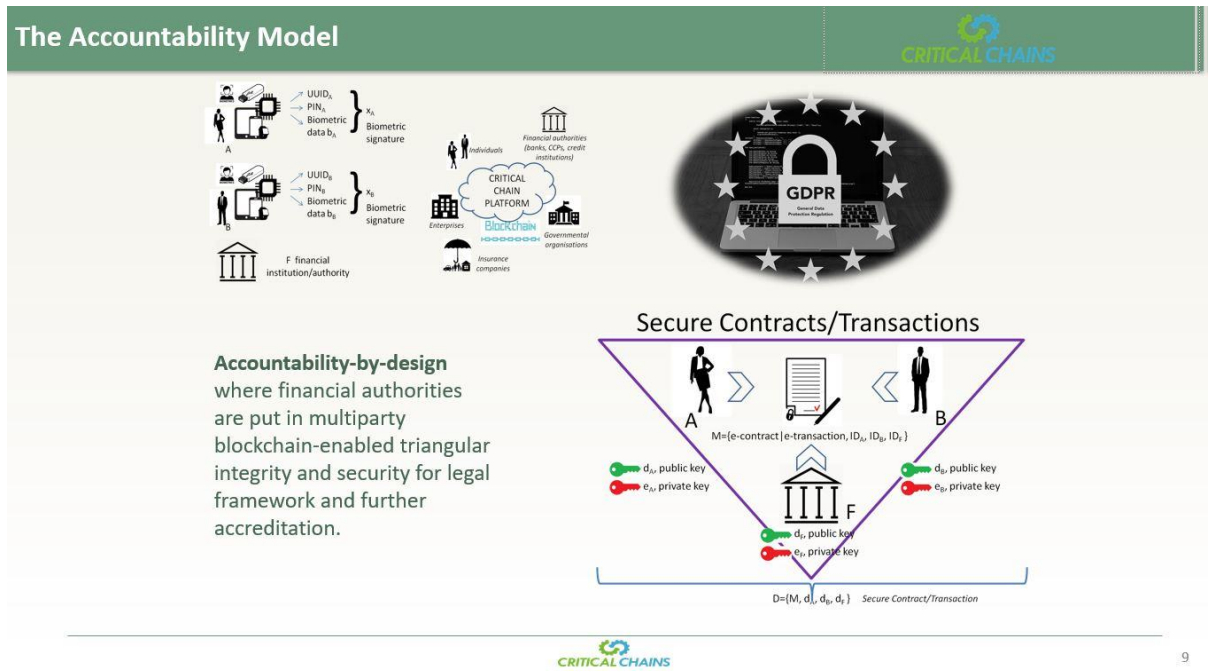
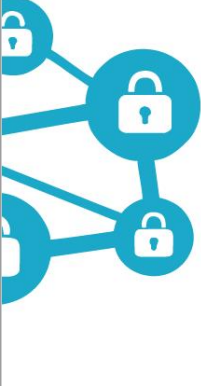


Figure 15: Critical-Chains project presentation

8.3 Brochure

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






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 voluptur am int arum nihicius et, ent alitis quidite mpeleti iatendi doluptam nosandi temod volori tem estiam, ut verferia omni simus, num fugiate mi.

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

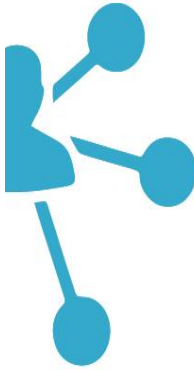


CRITICAL-CHAINS

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 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 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 16: 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

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

- 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 Infrastructures
- 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

Critical Chains over Cloud

Main Building Blocks

Critical-Chains Website: <http://research.rdg.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 17: Critical-Chains project poster-2 (NETAS)

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

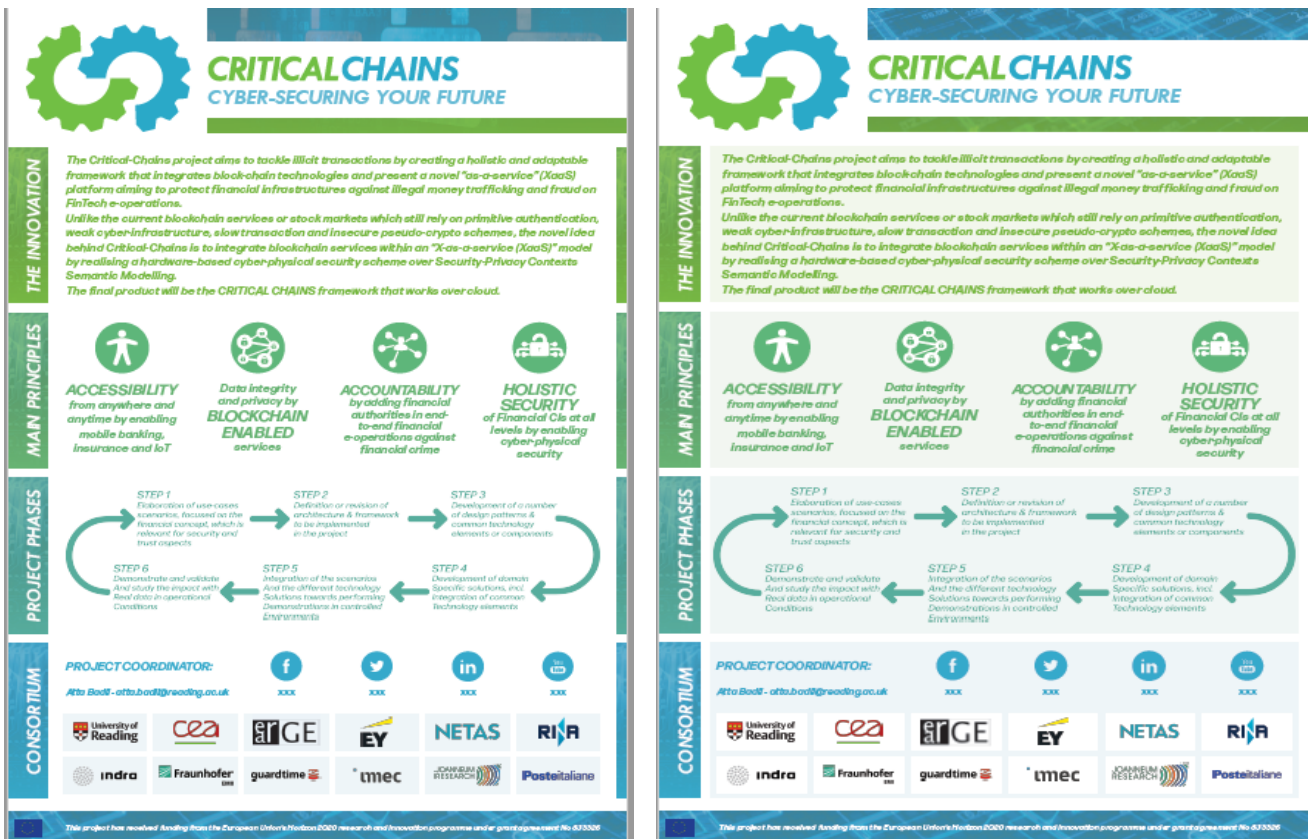


Figure 18: Critical-Chains project poster-3 (RINA)

9 Events

The Critical-Chains Team performed actions in order to strengthen 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 19: Consortium Partners' delegates participating in the Kickoff 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 20: 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 the regulatory and certification framework responsive to the evolutionary trends in the Fintech and the emergent forms of payment systems and intermediation. The Critical-Chains project presentation is appended 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 Manager (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 June whereby it was agreed that the Critical-Chains Project and 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.

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 Consortium members 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 insurtech.	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

12 Exploitation

This chapter shows the overall plan of the exploitation and sustainability activities for the Critical-Chains project, which can be considered as actions to sustain a process towards commercialisation of the project outcomes. In particular, a methodology is presented to build the exploitation strategy, which is divided in three main phases.

It is critical for the enterprises to turn innovative ideas and technological progress into marketable products and services, while keeping a competitive advantage by being one of the first to penetrate the market. Therefore, a solid methodology and driven dissemination and communication actions are essential for a sustained influence and penetration of the project outcomes into the marketplace.

The exploitation and commercialisation analysis (i.e. IPR, business model, etc.) will be carried out in the framework of deliverable D7.8 “Report on business modelling, IPR and innovation modelling” due to month M36.

12.1 Exploitation Strategy building up process

The process for the building up of the exploitation plan of Critical-Chains project is three-fold, to be implemented mainly within the timeframe of the project itself.

- Phase 1 is aimed at acquiring a first strategic analysis of the project commercialisation opportunities: the possible routes to get to the market are identified as well as the partners’ commercial positioning, which is the main focus of the current project stage (M1-M12);
- 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 (M12-M24) duly investigated in the frame of 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 the position to penetrate the market with a viable, trustworthy, stable and robust business model as quickly as possible after the project completion.

The Consortium has a strong motivation to sustain project achievement after the project ends. Over 5 years beyond the project funded period, the Consortium will focus on refinement re-engineering and adapting the delivered tools to suit the customer needs and engage the market.

For Phase 1 in this early stage of the project (M1-M12), 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.

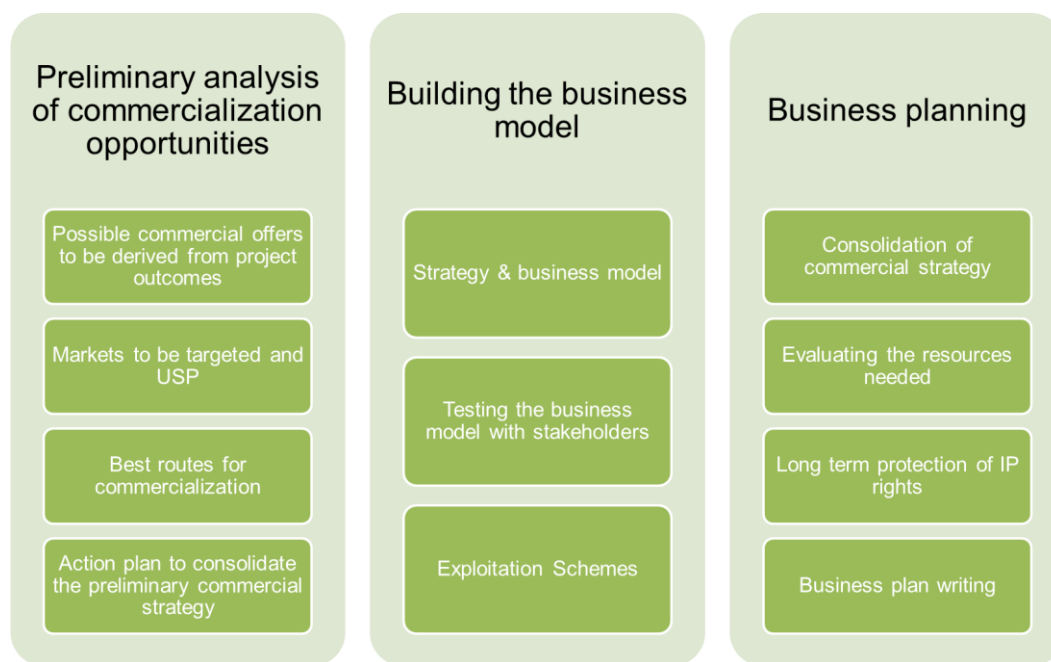


Figure 21: Exploitation Strategy Building process

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 a web-based platform on which end users (either institutions or regular people) should be able to register and subscribe. Each product/service can be delivered in an XaaS model, commercialised and if needed diversified according to the particular needs of stakeholders. The hardware-based solutions enhanced with IoT and blockchain are solid outcomes of the project that can be commercialised either as single devices or a part of an XaaS. The main and initial project outputs are listed in Table 2.

Table 2: Main Critical-Chains project outputs

Critical-Chains Outputs	Main Beneficiaries
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) with Security-privacy context and semantic modelling	ERARGE, EY, FHG, JR, NETAS, POSTEIT, UREAD
Entire CPSaaS with IoT Functionality	All partners
<ul style="list-style-type: none"> AUTH-as-a-Service- AUTHaaS with biometric support and zero-knowledge proof 	ERARGE, CEA, EY, FHG, INDRA, POSTEIT, RINA-C, UREAD
<ul style="list-style-type: none"> Hardware-Security-as-a-Service 	ERARGE, IMEC-NL, FHG, RINA-C
<ul style="list-style-type: none"> Blockchain-as-a-Service (BCaaS) 	GT, EY, FHG, INDRA
<ul style="list-style-type: none"> Crypto-as-a-Service (Cryptaas) 	ERARGE, FHG
Proof of triangular accountability model with Frontend applications (smart contract, secure transactions, etc.) within regarding use-cases	All partners
Innovative business model that can cope with the pressing financial challenges	ERARGE, EY, FHG, GT, INDRA, POSTEIT, RINA-C
Technology acceptance model	ERARGE, EY, GT, INDRA, NETAS, POSTEIT, RINAC
Audit & Compliance Tool and set of Models for NIS, GDPR, PSD2 and AML/4 compliance	RINA-C

12.3 Partners Exploitation intentions

To have a comprehensive view of the commercial understanding regarding the project outcomes, it is worth considering the partner positioning in terms of commercial intentions, and exploitability aligned with their profile (i.e. enterprise, research entity, etc.) and to their background as initial starting point to be further elaborated during the project activities in alignment with project technical development. In particular, as background is defined as “data, know-how or information that is needed to implement the action or exploit the results”.

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 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 and modelling, behaviour modelling and agent behaviour prediction based on large datasets and agent simulations.
Background	UREAD includes background that is i) the result of work done by the team working on the Critical-Chains project, ii) directly related to: a) Secure Access; b) Context-Aware Privacy Protection Requirements Engineering & Evaluation. 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'Énergie Atomique Et Aux Énergies 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 flow blacklisting capability and adaptation to other parameters obtained from Threat Intelligence. CEA promotes technology transfer and encourages innovation. In the project, CEA will endeavour to transfer technologies to future industrial partners in the form of licences.
Background	CEA is agreed between the Parties that, 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).
3 Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik Su Urunleri Sanayi ve Ticaret Limited STI (ERARGE)	
Exploitation intentions	This project is a perfect opportunity for ERARGE to demonstrate its hardware-based security product family, PRIGM-Stick and PRIGM-HSM, in a blockchain-enabled FinTech application. ERARGE has a geographical / market relevance presence in Switzerland, Central Europe and an active network in Turkey, Turkish countries, Pakistan, and Qatar. ERARGE plans to promote project results to related stakeholders in these countries, initiate demonstration activities, and focus on selling PRIGM in the context of Critical-Chains. Since it has key PCT patents in cryptography, ERARGE will also seek ways to promote these patents and sell know-how deepened in this project.
Background	ERARGE includes background that is i) the result of work done by the team working on the Critical-Chains project, ii) directly related to: a) Decentralised Triangular Accountability Model utilising blockchain and cryptographic solution stack; b) Hardware security components and secure access tools; c) Security-Aware Requirements Engineering and Evaluation. Subject to limitations, terms and conditions as shall be agreed by the Consortium in the Critical-Chains final version of the exploitation plan.

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 the relationships among operators of the financial sector (banking, insurances, etc.), with high replicability potential at international level that will be used to provide tailored and innovative services to target clients in the financial sector domain.
Background	EY is agreed between the Parties that, 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 them as 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	FHG it is agreed between the Parties that, 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 opportunities and 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 that are involved in the project. Considering the exploding demand for cybersecurity functionalities, the solutions will be developed with replication in mind, with the aim to provide a basis and support the development of KSI-based solutions in other domains as well. In addition, the project will increase 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	<p>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 offering. Stichting IMEC-NL actively supports transfer of its expertise and further development through certification requirements (e.g. FDA) to market introduction. Markets within the present scope of their activities are Health and lifestyle, Automotive, and Agro/food, with the Internet of Things as an enabler in each of these areas. Insight into the needs of these markets is built through close collaboration with end-users that provide voice-of-the-customer. Implementation and use of a large-scale Internet of Things infrastructure is supported to test and validate novel hard/software and services.</p> <p>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.</p>
Background	IMEC 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	<p>Through this project, INDRA expects to improve its back-office solutions by providing them with new levels of security, trust and data integrity. Moreover, technologies used and lessons learnt will be applicable to other solutions that have a deep financial component, such as multimodal clearing houses, or other products outside the Transport market, therefore enabling the exploitation of the results beyond the current project scope. Being aligned with the solutions that the company already provides; 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 a large number of countries in Europe, LATAM and MEA, having a wide knowledge of the requirements of travellers and transport operators in global markets, as well as the ability to develop and adapt the offering according to these needs. This knowledge will be crucial when developing solutions within this proposal, assuring that the results are competitive in the global market. INDRA has offices in 140 countries which represent an important channel to approach and deliver the identified customer's segments world-wide in the transport and traffic market.</p>
Background	INDRA 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	<p>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 technology offerings coming from research results. This plan is fully in line with the strategy of the JR competence group 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. JR also intends to disseminate the results of the projects in both scientific conferences and local or regional events dedicated to cyber security and will disseminate information about the project in meetings with business contacts from industry, SME and public authorities.</p>

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 the Project (Article 25.2 Grant Agreement) or Exploitation of that other Party's Results (Article 25.3 Grant Agreement).
-------------------	---

10	Netas Telekomunikasyon Anonim Şirketi (NETAS)
-----------	--

Exploitation intentions	NETAS is planning to exploit the project outcomes in three ways: First, to increase its know-how and solution bundle in cloud computing with the requirements and solutions in Critical-Chains and thus obtain 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 expand its role in finance sector and provide its current customers with technology of the near-future.
--------------------------------	---

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) Caching techniques 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 experimentation of the multifactor authentication for SPID, using the project solution for authentication. This experience will be relevant as a baseline for future replication and adaptation to other target services; moreover, this experimentation will be functional to the extension of the financial services' provision by POSTEIT. Finally, POSTEIT will be interested in exploiting project results for knowledge transfer (at company internal and external level), in particular by organising seminar and workshops aimed at improving the awareness and interest in the domain of cyber security.
--------------------------------	---

Background	POSTEIT 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 conceptualised in the financial sector. This enables RINA-C to strengthen the expertise and service offering to various stakeholders involved also in the insurance sector. In particular RINA-C sees the opportunity to create new consultancy services using the Audit & Compliance Tool enhancing the existing Risk Assessment value proposition in the following way: 1) 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; 2) proposing the Critical-Chains services as technical security measures to mitigate security and privacy risks; 3) 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 the Business 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 royalty fees. 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, who 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 is 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 targeted critical sectors are well-defined and focused as banking, insurance and central counterparty (CCPs) processes. Additionally, Critical-Chains can be commercialised in vertical sectors where ePayments, eCommerce and eTrade operations take place (i.e. financial audit in a specific sector). In this way, the project 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 (i.e. aligned with claims in insurance sector)
- Digital certificates have become indispensable 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
- \$57.8 Billion in e-Commerce fraud losses are reported in 2017¹
- Total e-Commerce Transaction Value is expected to reach \$8,000 Billion by 2020²
- Non-cash transactions EU (2015): 101,5 Billion³

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

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>

³ World Payments report – Source: <https://www.worldpaymentsreport.com/reports/noncash>

Table 3: Critical-Chains markets

Market	Banking Sector
Key features	<ul style="list-style-type: none"> • 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 portable devices • The banking system is not ready for the booming blockchain technology; accountability, trust and integrity 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	<ul style="list-style-type: none"> • 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 as the contractor

Market	Financial Market infrastructures
Key features	<ul style="list-style-type: none"> • G20 Leaders agreed at the 2009 Pittsburgh Summit that all standardized derivatives contracts should be 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 • Accountability of CCP is a big 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-physical Attacks
Customers	<ul style="list-style-type: none"> • 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 • Trading venues and Multilateral 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)

Market	Insurance Sector
Key features	<ul style="list-style-type: none"> • 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 on 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 cause economic loss • IoT and Blockchain enables the redefinition of a dynamic price thanks to new business models such as 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
Customers	<ul style="list-style-type: none"> • Customers of insurance companies who are a side in any underwriting process or behaving as a contractee (beneficiary),

Market	Insurance Sector
	<ul style="list-style-type: none"> • Insurance companies giving 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	<ul style="list-style-type: none"> • 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 it 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 complex audits, 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	<ul style="list-style-type: none"> • 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 give any 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 (i.e. secure sticks, HSMs) and software components (XaaS services) as standalone solutions
- Selling the entire solution to big financial organisations

The commercialisation roadmap starts from the second phase of the project and continues in the short-, mid- and long-term. In the following Table 4 a preliminary representation of time to market and commercialisation routes.

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 the potential adopters informed. This will be realised through dissemination and communication activities.
Short-term	<= 1 year after the project ends	The Consortium will select a proactive SME (within the Consortium) to promote project results by visiting top customers and influential companies. This will be the announcement phase where the project results are emphasised at EU level. In the short-term the branding process will start.
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 (EMEA, America, Japan, China, Australia, Arabic countries, etc.). Here, dealership and collaboration opportunities will be discussed. Branding operations will be finished 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.

13 Conclusions

The report D7.1 is the first version of the deliverable, in fact the deliverables D7.2 and D7.3 are two versions of the same report "Critical-Chains Bulletin: a report on dissemination, exploitation and list of outcomes".

The D7.2 and D7.3 will correspond to the second (M12-M24) and third (M24-M36) phases both of the communication & dissemination strategy and of the exploitation strategy.

Moreover, the exploitation field will be further explored in the dedicated deliverable D7.8 "Report on business modelling, IPR and innovation modelling" together with the business models.

Considering the dissemination and communication activities the main actions aimed at identifying the project identity and at disseminating the project scope have been undertaken.

It is still essential to keep sharing the project video on different channels, divulgating the promotional material and to maintain the project website, for example by sharing news periodically.

From a business perspective and exploitation point of view, the first phase of preliminary analysis of commercial opportunities has been complete. Now planning for the next steps can begin which are:

Strategy & business model

- a. Value for money: how to monetise Critical-Chains applications developed
- b. Key partnership: identification of further potential contributors (if any) in order to build strong partnerships
- c. Revenue sharing: Business model Network-based. Each business actor (shareholder, supplier, technical or commercial partner) has to retrieve some benefit from its participation to the business.

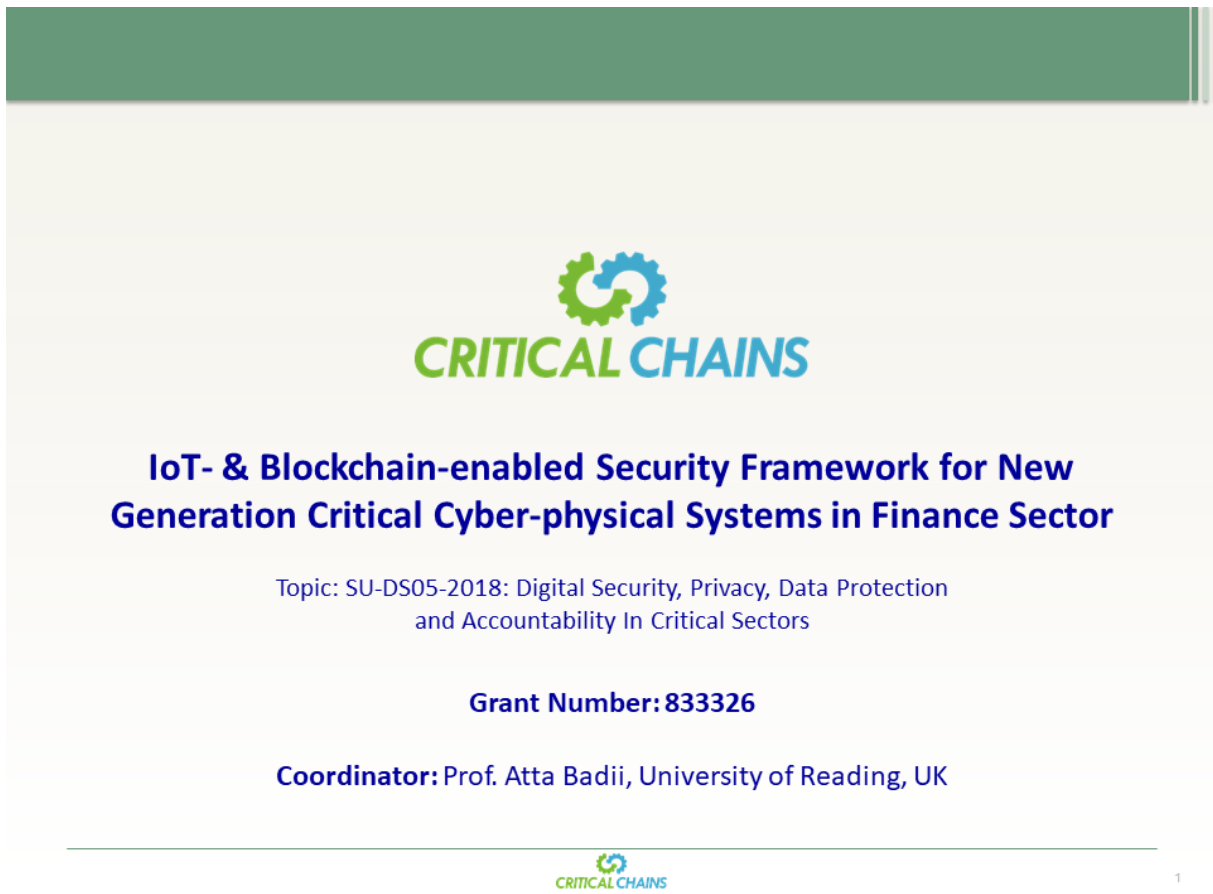
Testing the business model with stakeholders (customers and partners)

- a. Testing the market: product/service and associated pricing scheme will be evaluated. 4P marketing theory can be applied to conduct the test: Product, Price, Promotion and Place.
- b. Testing partnerships: agreements and revenue sharing schemes to 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 to share knowledge with them.

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

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.



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

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://cointellegent.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study
 https://www.pwc.co.uk/services/forensic-services/instant/global-economic-crime-survey-2018-uk-findings.html
 Kaspersky. FinancialCyberthreats.ip.2018. March 07. 2 https://securitylist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019). Image from https://www.pexels.com

Strategic Objectives

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

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

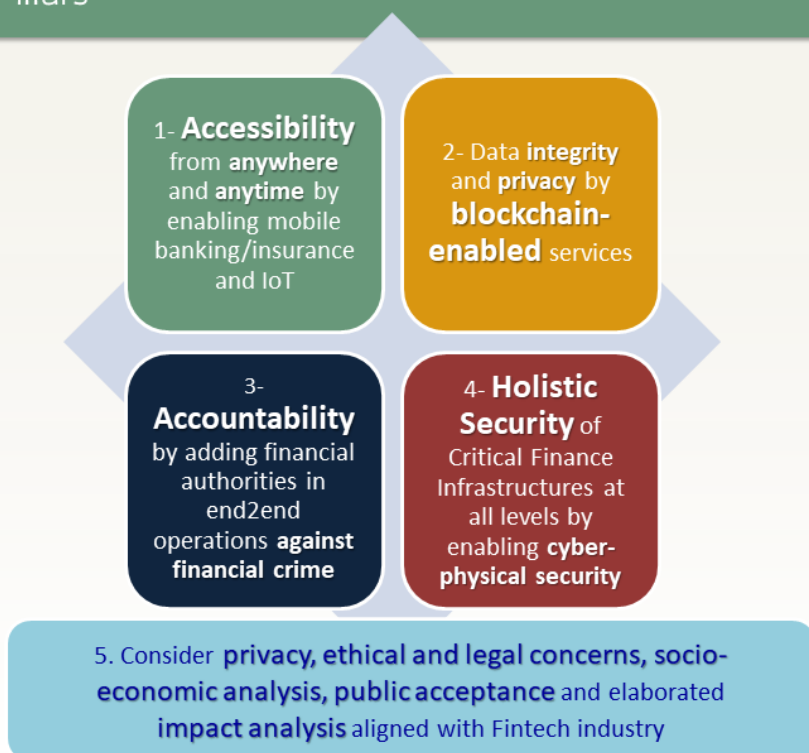
❑ Concept and approach

- ❑ 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



4

Innovation Pillars



5

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



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.



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



1

Challenges



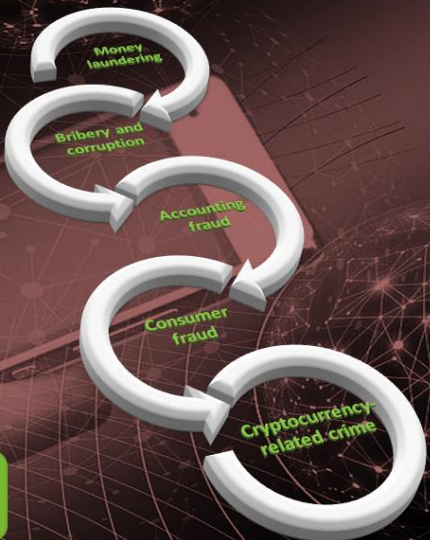
Cyber criminals have netted \$4.3 billion from digital currency exchanges, investors and users in 2019.

- #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

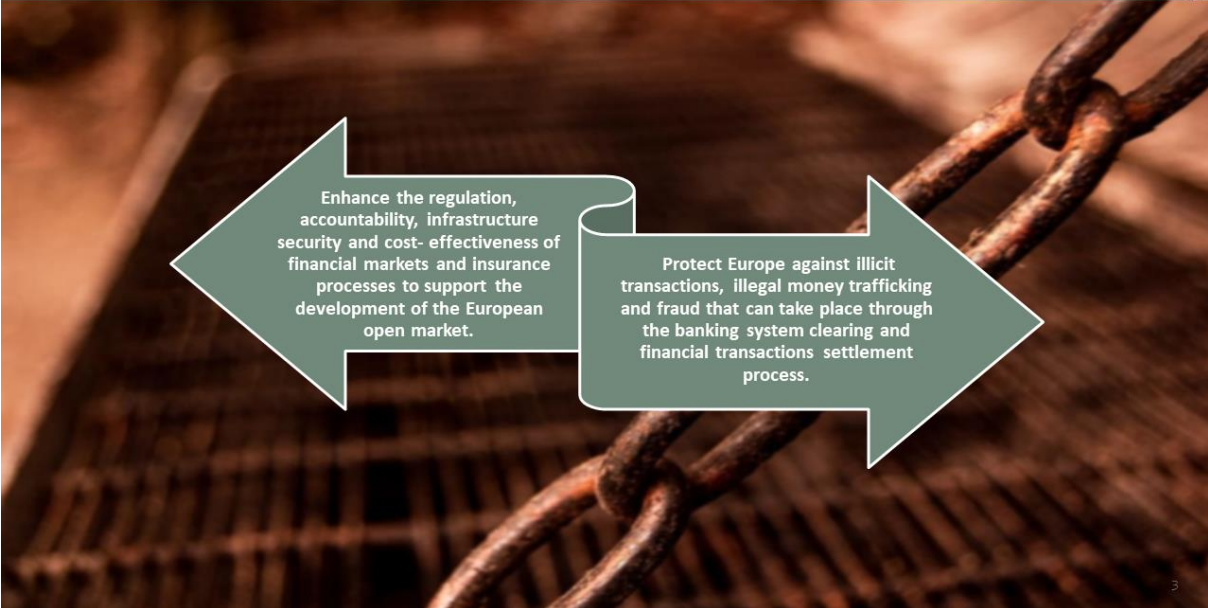
Digital technologies are profoundly changing the financial sector, but also a source of massive threat



<https://online.governancenews.com/cyber-crime-netted-43-billion-cyber-criminals-gained-2019-0107>
<https://www.pwc.co.uk/assets/pdfs/press-releases/2019/04/04-cyber-crime-survey-2019-uk-english.html>
[Kappers M. Financial Cyber threats in 2018: 11 facts and 2 data sources | www.financial-cyberthreats-in-2018-09768/ \(accessed November 11, 2019\)](https://www.pwc.co.uk/assets/pdfs/press-releases/2019/04/04-cyber-crime-survey-2019-uk-english.html)
Image from <https://www.pexels.com>

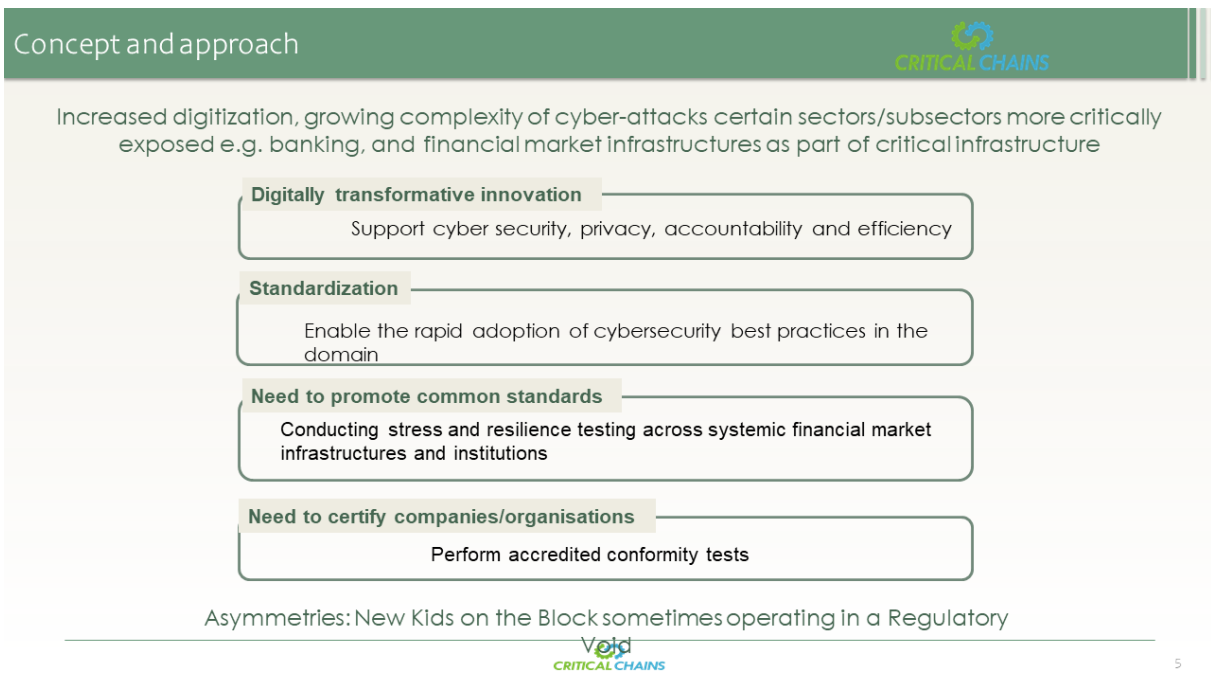
Strategic Objectives

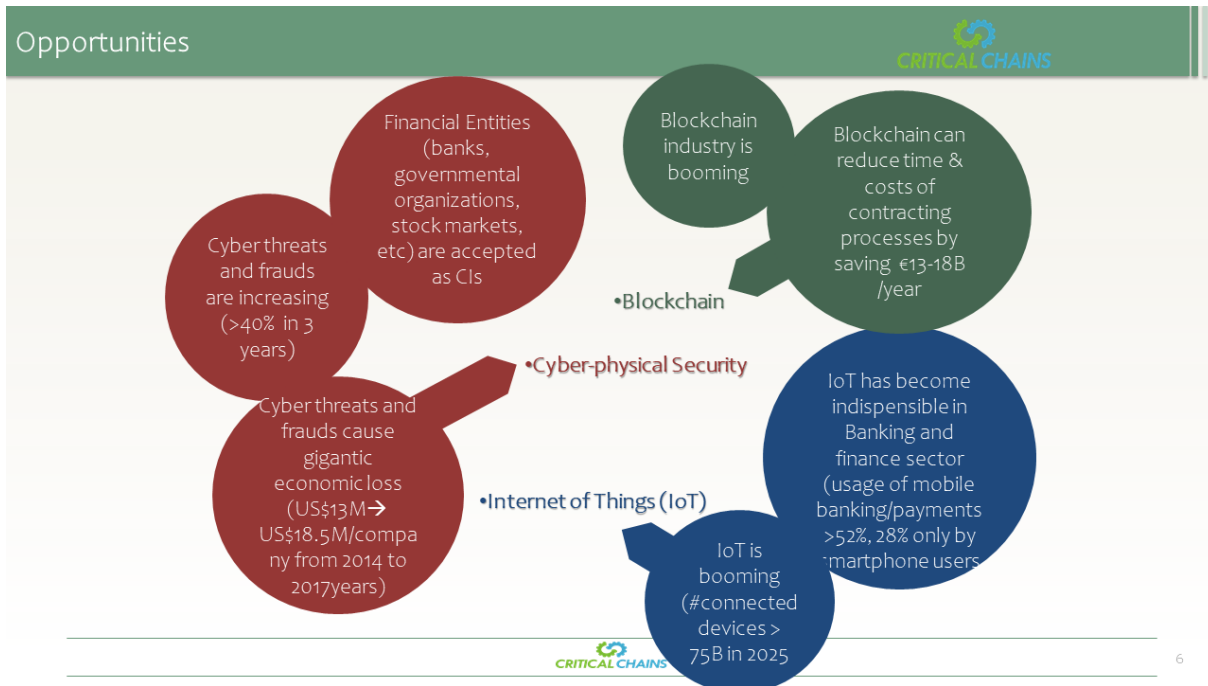




Enhance the regulation, accountability, infrastructure security and cost- effectiveness of financial markets and insurance processes to support the development of the European open market.

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



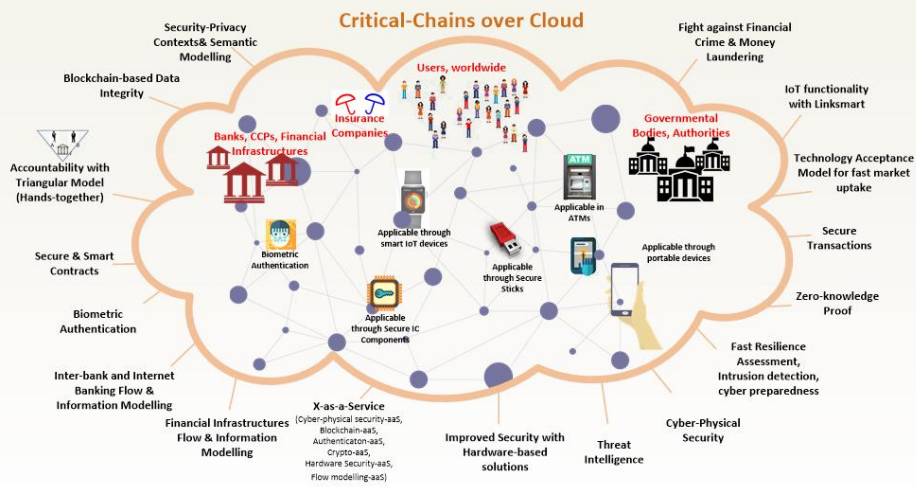


6



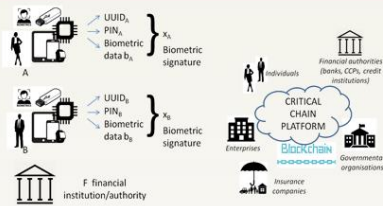
7

Solution Stack



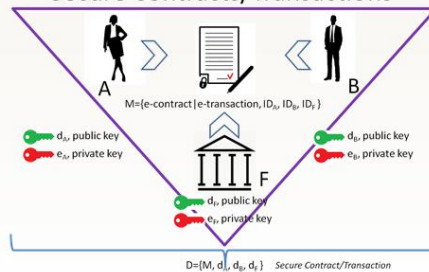
8

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



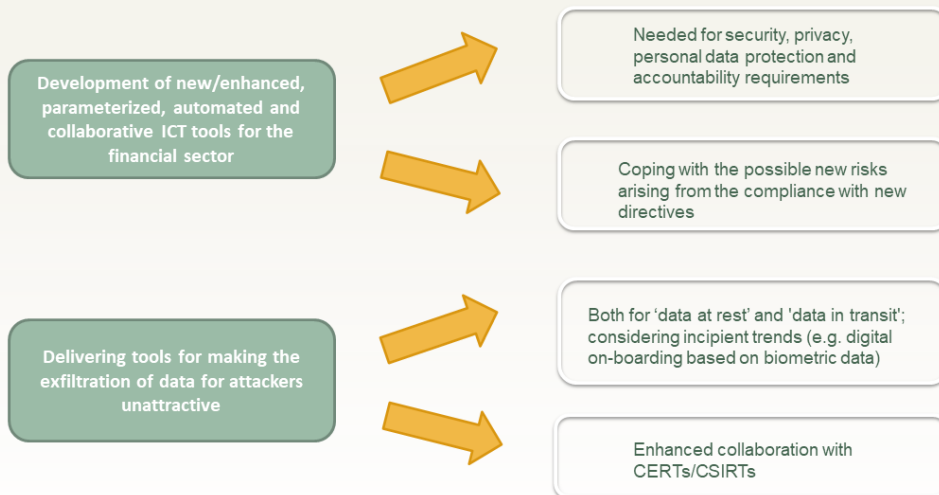
9

What's new?



10

Expected Results




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




11

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**



12

Target End Users

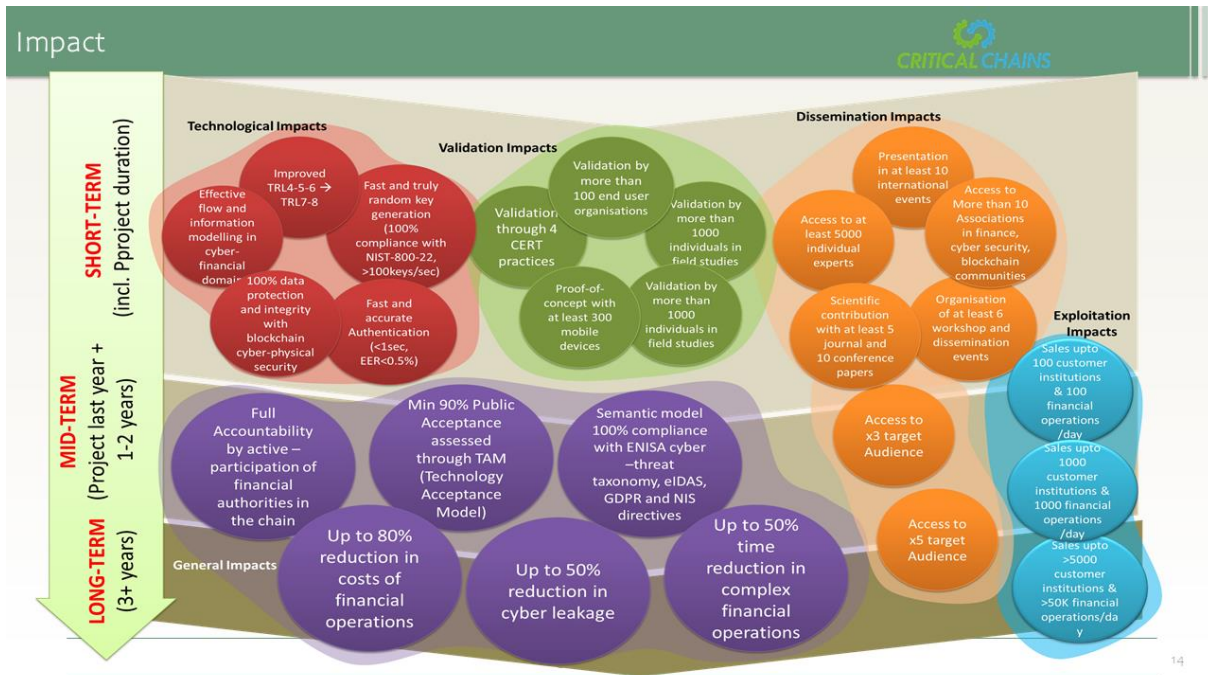




Use Cases and Target Sectors

- Financial Sector, Internet Banking, Inter-Banking, Clearing
- Insurance Processes
- Highway Toll Collection

13



EU Policy Aspects, Data Protection, Scalability

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

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

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



Contact us!



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



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



Annex B – Publication Plans

Publications Annual Planning Table

Period 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
