Critical-Chains

Collaborative Project

Project Start Date 1st July 2019 Duration 36 Months

Deliverable D1.4

Periodic Management Report

Published by the Critical-Chains Consortium

Version 2 Date 30-05-20

Grant Agreement number: 833326
Project acronym: Critical-Chains
Project title: IoT- & Blockchain-Enabled Security Framework for New Generation CRITICAL Cyber-Physical Systems In Finance Sector
Funding Scheme: RIA
Date of latest version of Annex I against which the assessment will be made: 14/03/2019
Draft Periodic report: 1st □ 2nd □ 3rd □ 4th

Period covered: from 1st July 2019, **To**, 31st December 2020

Name, title and organisation of the scientific representative of the project Coordinator
Prof. Atta Badii, University of Reading

Tel: +44 118 378 7842, +44 7484355578
Fax: +44 118 975 1994
E-mail: atta.badii@reading.ac.uk

Project website address: https://research.reading.ac.uk/critical-chains/

Abstract

This document, deliverable D1.4 sets out the Research and Innovation efforts deployed, and results achieved by the Critical-Chains Consortium during the first period running from M1 -M18 (01-07-2019 to 31-12-2020). This is pursuant to the objectives of the Critical-Chains project to be duly realised through the fulfilment of the joint contractual commitments undertaken in respect of the Grant Agreement number 833326. The document sets out the overall achievements, risks update and explanations for deviations and provides a comprehensive account of work-package-specific tasks as performed by each Partner and the resulting achievements at the Task, WP and Project levels and respective resource deployments.

Contents

1. Executive Summary

This deliverable, D1.4, is the draft project management report for the Critical-Chain project for the first reporting period (M1-M18) which extends from 1-July 2019 to 31st-December -2021.
The Deliverable comprises the following sections:

- Project reference tables (Partner-specific work package responsibilities), deliverables listing and milestones);
- Outline of Project-level Objectives and responsive achievements and specific project management challenges
- Tabularised Results of each work Package and respective resources deployed;
- Analysis of the project risks and update of the risk register, review of old risks and addition of new risks;
- Table of overall Partner-specific resource deployment (Planned versus Actual) and accordingly the bar chart of the actual resources deployed compared to the planned levels;
- Tables of Partner-specific task-level contributions and results;
- Tables of Partner-specific staffing, travel and other costs.

2. Introduction

This document, Deliverable, D1.4, is the first periodic project management report for the Critical-Chains project. Critical-Chains is a collaborative project within the H2020 Programme. The project has set out to develop an integrated effective, accessible, fast, secure and privacy-preserving financial contracts and transactions solution stack. This is to protect against illicit transactions, illegal money trafficking and fraud through the banking clearing system and financial transactions settlement process.

The technologies 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 being validated using four case studies aligned with four critical sectors: banking, financial market infrastructures, the insurance sector, and Highway Toll collection. The validation has included evaluating system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance. 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.

3. Reference Tables

WP No	Work Package Title	Lead Participant		Person-Months	Start Month	End month
		No	Short Name			
1	Project Management	1	UREAD	34	1	36
2	Requirements Engineering & Framework Architecture Specification	9	JR	96	1	36
3	Blockchain Core Development & Solution Stack Adaptation for Use-Cases	4	EY	54	3	36
4	Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance	3	ERARGE	94.5	5	35
5	Cyber-Physical Security	2	CEA	159	5	35
6	System Integration & Validation in Various Pilots	8	INDRA	92	1	36
7	Dissemination, Standardisation, Exploitation and Innovation Management	12	RINA-C	47.5	1	36
8	Ethics Requirements	1	UREAD	0	1	36
Total Person-Months				577		

Deliverable (number)	Deliverable name	WP Nr	Participant	Type	Dissem. level	Del. Date (Month)
D1.1	Compliance plan	1	UREAD	R	CO	6
D1.2	White Paper including S&T&I achievements and visionary statements	1	UREAD	R	PU	18
D1.4	Progress report	1	UREAD	R	PU	18
D2.1	Technology & Watch Update	2	JR	R	PU	6
D2.2	Technology & Watch Update	2	JR	R	PU	18
D2.3	Specifications and architectural design	2	JR	R	CO	6
D2.4	Specifications and architectural design	2	JR	R	CO	18
D2.6	Security/Privacy and Threat semantic model	2	UREAD	O	CO	12
D2.7	Regulatory compliance and Accountability-by-Design model	2	RINA-C	R	CO	18
D3.1	Critical-Chains Main Framework	3	NETAS	O	CO	18
D3.3	Blockchain Data Integrity Layer	3	GT	O	CO	18
D3.5	Secure and Smart contracts applications	3	EY	O	CO	18
D3.7	Digital identity and nodes	3	EY	O	CO	18
D3.9	Back-end and front-end applications	3	NETAS	O	CO	18
D4.1	Flow Modelling as-a-Service (FMaaS)	4	UREAD	O	CO	18
D5.1	AUTH-as-a-Service (AUTHaaS)	5	CEA	O	CO	18
D5.3	Secure Cyber Framework	5	CEA	O	CO	18
D5.5	Hardware Security as a Service and regarding HSM and secure IC Stick-in-silicon (HwSaaS)	5	IMEC-NL	O	CO	18
D5.7	Blockchain-as-a-Service (BCaaS)	5	GT	O	CO	18
D5.9	Crypto-as-a-Service (CryptaaS)	5	ERARGE	O	CO	18
D6.1	Methodology and KPI assessment Framework	6	INDRA	R	PU	9
D6.2	Report on integration, deployment and testing for Phase 1 - Phase 2	6	INDRA	R	CO	18
D7.1	Critical-Chains Bulletin: A report on dissemination, exploitation and list of outcomes	7	RINA-C	R	PU	12
D7.4	Contextual and situational description and benchmark of events	7	POSTEIT	R	PU	18
D7.6	Gap analysis of current relevant standards	7	CEA	R	PU	18
D8.1	H - Requirement No. 1	8	UREAD	Ethics	CO	3
D8.2	H - Requirement No. 2	8	UREAD	Ethics	CO	3

Deliverable (number)	Deliverable name	WP Nr	Participant	Type	Dissem. level	Del. Date (Month)
D8.3	POPD - Requirement No. 3	8	UREAD	Ethics	CO	3
D8.4	POPD - Requirement No. 4	8	UREAD	Ethics	CO	3
D8.5	POPD - Requirement No. 5	8	UREAD	Ethics	CO	3
D8.6	POPD - Requirement No. 6	8	UREAD	Ethics	CO	3
D8.7	POPD - Requirement No. 7	8	UREAD	Ethics	CO	3
D8.8	POPD - Requirement No. 8	8	UREAD	Ethics	CO	3
D8.9	POPD - Requirement No. 9	8	UREAD	Ethics	CO	3
D8.10	POPD - Requirement No. 10	8	UREAD	Ethics	CO	3
D8.11	GEN - Requirement No.11	8	UREAD	Ethics	CO	9
D8.12	GEN - Requirement No.12	8	UREAD	Ethics	CO	12

Milestone number	Milestone name	Related WP(s)	Due date (in month)	Means of Verification
MS0	Project Kick-off	WP1	M1	Meeting report with revisited action plan
MS1	Fulfilment of General Design	WP2,8	M6	Publishing requirements, SOTA and market review (D2.1) and system general design and architecture scheme (D2.3) , building the ethics and legal framework (D8.1-10)
MS2	Implementation and Integration of Phase-1 components and dissemination of knowledge	WP3-7	M18	Delivering XaaS services and the deployment of the first-phase software and hardware tools working over the main framework (D3.1,3,5,7,9), (D4.1), (D5.1,3,5), (D6.1-2), (D7.1,3-5)

4. Consortium Achievements in Period 1

The list below provides an outline of the main achievements delivered during the first period (M1-M18) despite the challenging innovation and project management environment:

- Ring oscillator based true random number generator creating unpredictable cryptographic keys with high throughput.
- SecureStick - an authentication token, with 2 versions:
  i) FIDO-compliant and biometric-enabled person authentication;
  ii) BLE secure distance bounding feature for node authentication.
- Biometric authentication includes developing hardware-based secure stick with Secure Distance Bounding solution plus face recognition solution.
- Secure Distance Bounding algorithm preventing man-in-the-middle attack on wireless link provides more robust solution than that of distance measurement algorithms.
- Policy-based authentication solution combines authentication process with the cryptographic enforcement of access policies.
- Multi-Factor Biometric Authentication and Authorisation (login/password, OTP, policy-based authentication and eIDAS-compliant external identity provider authentication) are integrated with AUTHaaS as scheduled for piloting in the 2nd development phase.
- Fast, reliable on-demand and service-oriented Hardware Security Module for Hardware Security-as-a-Service and Cryptography-as-a-Service over cloud.
- Authentication Anomaly Detection module detecting anomalies in the context of any of the seven Critical-Chains scenarios.

- Unique blockchain-based identifier of:
    - source of the anomaly;
    - type of the anomaly.
- Custom event-listening plug-in developed for the Keycloak server.
- Enhanced version of the above plug-in to listen to all events in the Keycloak authentication server.
- Additional events are included in Keycloak server.
- Detection of Anomaly Scenario 005 "Password Login Attempt thru Social Engineering".
- Machine Integrity Defence Awareness solution to monitor platform settings.
- Critical-Chains extensive financial transactions synthesised dataset (SEPA 1.7).
- Systematic feature engineering and benchmarking of an extensive set of Machine Learning approaches for financial transactions anomaly detection with competitive performance.
- Hybrid graph-enhanced ensemble/classic approaches to Flow Modelling and Anomalous Transactions Detection with improved performance.
- Multi-protocol anomaly-based Network Intrusion Detection and Reaction System adapted to Critical-Chains Main Framework to *Detect* and *React* to *Unknown* Attacks.
- Blockchain-based unique identifier proposed for use over the Critical-Chain system as applied in the Authentication Anomaly Detection module.
- Blockchain-based web-applications developed for Insurance and Toll pilot includes verification mechanism and smart-contracting for business logic.
- Solution to integrate Ethereum Quorum and KSI Blockchain.
- To maximise the mobilisation of the dissemination and impact of the results, various outreach activities were targeted through a mutually re-enforcing eco-system of seven gateway channels which essentially wired up Critical-Chain to a network-of-networks with multiplier effects through each touchpoint e.g. clustering workshop through two project hubs (Cyberwatching, and, LSEC), reached over 4500 through participation in 27 workshops; contributed to 10 workshops including 5 (co)-organised by Critical-Chains, contributed to the Project-to-Policy kick-off workshop and to other Project-to-Policy dissemination opportunities responsive to EC invitations exchanging technological, socio-ethical and compliance assurance insights; established the Critical-Chain presence in four social media spaces; started our video series with an introductory video highlighting the project objectives (LinkedIn, Facebook, Twitter, YouTube); published 12 peer-reviewed high quality articles realised; established the Critical-Chains sectoral stakeholder group with two innovative stakeholder SMEs as providers of services to the banking sector and held on-going discussions on collaborations with a further two European banks.
- Established the objective of integrating selected use-cases, validated in 4 pilots with end-user feedback to inform iterative evolutionary platform co-design as successfully validated.
- Submitted 36 deliverables as planned and, in some cases, far exceeding the expected level of attainment.
- Established new technologies and methods underpinning the Critical-Chains X-as-a-Service solution stack:
    - Secure Cyber Hardware;
    - Context-aware Privacy and Security Protection by Design;
    - Integrated Privacy-Security Risk Severity Ranking & Countermeasures Prioritisation;
    - Graph-Enhanced Transaction Anomaly Detection.
- Commended by EAB, for our *integrated and actionable* methodological approach to Privacy Protection and Social Acceptability by Design.

- Have delivered to the ethical requirements to the satisfaction of the EAB who have stated the opinion that the project should continue to proceed as planned.
- Critical-Chains established vision of Accountability Engineering and Integrated Privacy-Security by Design in Clustering Network-of-Networks focused on innovation for Financial Systems and Services Security as part of Infrastructure Security Protection.
- Have demonstrated close collaboration, for sub-system conformance testing, integration and configuration of demonstrator sets facilitated with physically co-located working essential for testing hardware components and user-centred requirements elicitation and usability testing, evaluation and feedback facilitation all despite pandemic-imposed constrains.
- All targeted case studies specified and confirmed -all set for Phase 2 completion and validation of components of the integrated Critical-Chains Framework.

5. Project Level Progress with reference to the Planned Project Objectives

Project Objectives	Consortium Progress to-date
• Transaction and financial data flows analytics and modelling of the financial transactions clearing and claim settlement processes	• Developed innovative graph-enhanced high performance anomalous transaction detectors including hybrid ensemble as well as classic ML methods • Developed and tested the FMaaS and integrated it within the Critical-Chains main framework • Developed new synthetic banking transactions dataset • Developed and benchmarked FMaaS solutions over a dozen machine Learning Algorithms (as specified in the D4.1) • Published the results in a joint publication
• Secure and smart use of Blockchain for data integrity checking, by involving financial institutions in the distributed Blockchain network	• Developed a solution to integrate Ethereum Quorum and KSI Blockchain.
• Cyber security protection of Inter-Banks and Internet Banking, insurance and financial market infrastructures	• Developed the Machine Integrity Defence Awareness solution to monitor the platform operational settings. • Multi-protocol anomaly-based Network Intrusion Detection and Reaction System adapted to Critical-Chains Main Framework to Detect and React to Unknown Attacks
• Privacy protection through secure access supported by embedded systems and Internet-of-Things security	• Developed different authentication factors with different strengths: login/password, OTP, biometric, policy-based authentication, and additionally using an eIDAS-compliant external identity provider • The development of the biometric authentication included developing a hardware-based secure stick with a novel Secure Distance Bounding solution to prevent man-in-the-middle attacks, in addition to the face recognition solution. • Design of an authentication and authorisation XaaS solution, AUTHaaS, that integrates the developed authentication factors and that is built based on standard protocols in order to provide an authenticated and authorised access to the Critical-Chains framework. • During this first development phase, some authentication factors (i.e., login/password, OTP, and eIDAS-compliant authentication) are integrated with AUTHaaS. The

Project Objectives	Consortium Progress to-date
	integration of biometric authentication to AUTHaaS will be carried out in the second development phase.
• 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.	• Case studies specified and confirmed.

6. The Impacts of the Restrictive Project Management Environment

Over the 18 months of period 1 despite the limitations imposed by the global pandemic, this Consortium has established the existence proof of the vision of the Critical-Chains, validated as operationally workable and effective in principle even although more of the components and the big data functionalities could have been more extensively validated at this stage; had the work been unconstrained by the restrictions imposed due to the pandemic leading to entirely unexpected conditions outside the control of the Consortium.

However, the Consortium's achievement in period 1 have included:

- Establishing the primary objective of integrating some of the selected use-cases, carrying out the validation process planned for all four pilots and as a result compiling the end-users' feedback to inform the iterative evolutionary co-design of the platform which has thereby been successfully validated.
- Over the 18 months of period 1, submitting 36 deliverables, that, at the very least, have adequately discharged the responsibility of each deliverable as planned -indeed in some cases have far exceeded the expected level of attainment.
- Have established innovative technologies and methods; for example: Secure Cyber Hardware, the Context-aware Privacy and Security Protection by Design with Integrated Privacy-Security Risk Severity Ranking and Countermeasures prioritisation, Hybrid Graph-Enhanced Transaction Anomaly Detection, etc. that include patent-able innovation.
- Provided high quality publications far exceeding the average number that could be realised in the first period of most projects with such a challenging innovation agenda under a restrictive project management environment.
- Been commended, by the EAB, for the practicality and effectiveness of our integrated and actionable methodological approach to Social Acceptability Engineering.
- Have complied with the ethical requirements to the satisfaction of the EAB who have stated the opinion that the project should continue to proceed as planned. This view has subsequently been supported by the EC Ethics Committee.

The Consortium is confident that the achievements to-date have paved the way for a vigorous follow-through during Phase 2 to culminate in the completion and validation of all components of the integrated Critical-Chains Framework.

Have established Critical-Chains as a leading contributor of the vision of Accountability Engineering and Integrated Privacy-Security by Design within a Clustering Network-of-Networks focused on Infrastructure Security protection and establishing innovation leadership amongst the group of projects engaged in research on Financial Systems and Services Security.

Contributed to the Project-to-Policy arena with technological, Socio-ethical and Compliance Assurance substance and Insight.

The above achievements have been realised whilst coping with the effects of the pandemic-imposed restrictions. Close collaboration, particularly for certain phases of co-development, for example, sub-system conformance testing, and integration and configuration of demonstrator sets which has been implemented despite the difficulties in establishing physically co-located working that would be essential for testing, evaluation and user feedback facilitation.

During the second Requirements Engineering Workshop held at the University of Reading on 16th December 2019 certain follow-on meetings including developers' boot-camp style multi-day meetings were planned for 2020 for interactive test-and debug of subsystems. In the event, none could be arranged due the global pandemic with much of Europe in various phases of lockdown that has lasted through the year and is still on-going. It was also a source of much frustration to find that even the physical testing of the key enabling components (authentication hardware, e.g., Secure Stick) became increasingly constrained.

Each Partner organisation faced project management challenges e.g., some support staff on furlough, lack of the usual level of IT and admin support that would have otherwise been more readily available.

Another factor to consider in terms of unexpected consequences was as follows: At the proposal time it had been understood that some actual financial transaction data, appropriately anonymised at source, would be available facilitating the synthesis of further data for training the Machine Learning models. However, in the event, our risk-aversive approach to data protection meant that the transaction data had to be entirely synthesised. Fortunately, we were able to draw on the considerable experiential knowledge of relevant POSTEIT operational staff working with Partners to develop a SEPA database which we were able to use to develop and test our FMaaS solution. As our data sources were entirely synthetic, it was decided to perform extensive benchmarking to ascertain that our algorithms were able to provide a robust performance which meant developing a greater number of algorithms than had been planned.

7. Work-Package-Specific Resources Deployed and Results Achieved

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
WP1 Leader: UREAD	– Providing administrative, legal, and financial coordination for the project – Promoting and maintain effective communication between the Partners & and the Consortium & EC – Liaising with and support the Advisory Board to facilitate the Board in its ethical scrutiny of the project – Ensuring the responsible, timely and auditable use of all funds, encourage Partners in their work and take all necessary actions including quality, ethical and regulatory compliance in the finance and insurance sector vis-à-vis EU regulations and assurance but also re national laws and international legislation – Ensuring the proper achievement of milestones and deliverables by tracking the scientific and technical objectives and to deal competently in a timely fashion with any management issues		- Provided hands-on methodological, scientific, technical and ethical compliance management, active support, training and follow-through; responsive to the exacting project management demands over and beyond the normally expected levels due to the special circumstances of a restrictive project management environment which affected the last 11 months of the period. Closely supported the development and evolution of every deliverable in terms of methodology, technology, process and final product quality. Closely overseen and completed 36 deliverables (formally responsible for 15 deliverables), all quality assured; delivered 12 substantial ethical deliverables at zero effort allocation. - Prepared and Submitted deliverable D1.1 (Management & Quality Planning). - **D1.1** presented, for all work packages, tasks and deliverables of the Critical-Chains project, the relevant quality metrics which enable the progress verification of each part of the planned work. Furthermore, this deliverable sets out the guidelines for collaborative work on the project deliverables including for the quality assurance process as supported by the internal review process. As such this document constitutes an elaboration of the quality commitments undertaken by the Consortium in the Consortium Agreement. - Prepared and Submitted **D1.2**, This deliverable presents an outline of the innovative results arising from the efforts of the Partners within the Critical-Chains project and situates this in the broader technological, regulatory and social context of the wider innovation horizon and the landscape of emergent systems and services. This is motivated by the vision of the financial sector security and self-audit which the Critical-Chains Triple Accountability Model seeks to serve into the future. - Prepared and submitted the earlier draft version of this document, deliverable **D1.4**. This sets out the R&D efforts deployed, and results achieved by the Critical-Chains Consortium during Period 1; including the achievements, deviations, risks update, and resources deployed.
	Total Effort Planned (M1-M36) **34 Person-Months**	**Total Effort Deployed (M1-M18)** **17.72 Person-Months**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
WP2 Leader: JR	– Presenting the state-of-the art in sustainable, optimised and accountable resilience-enhancing technologies that can protect the targeted critical sectors – Developing the requirements and specifications of the cyber, hardware- and software-based ICT tools that will make the exfiltration of financial and insurance data for attackers unattractive – Though inclusive stakeholder participative engagement and analysis of the stakeholder security-privacy contexts and constructs, deriving and validating a semantic model of the security-privacy, specifications, roles, and predicates – Elaborating and structuring the use-cases and test-cases-specifications by considering the practitioners' and end-users' needs in line with the SWOT analysis ex-ante and ex-post Critical-Chains uptake – Defining and describing the (re)specification of the Critical-Chains Platform by designing the overall architecture and its underlying components responsive to users' requirements		- **D2.1** (Technology & Watch Update) The state-of-the-art was extensively investigated and reported in D2.1 and its update D2.2. The reported work in WP2 is based throughout on the UI-REF Methodological Framework for high-resolution requirements analysis and prioritisation (Badii 2008, 2011). In particular UI-REF-enabled analysis of the State-of-the-Art (SoA), State-of-the-Market (SoM) and State-of-the-Practice (SoP) within FinTech applications and distributed ledger technologies within the targeted critical sectors. **D2.2** also includes new insights related to the impact of the COVID-19 pandemic on cyber-security in the Fintech domain. - WP2 work in the first half of the project included UI-REF-guided analysis of the requirements, use-context and use-cases within 4 targeted domains - banking, insurance, financial market infrastructures and electronic toll collection. This work is reported in two deliverables – D2.3 and D2.4 (Specifications and Architectural Design). Deliverable **D2.3** provides an overview of the Critical-Chains framework architecture that aims to create a holistic and adaptable framework that includes end-users and financial authorities to protect financial infrastructures against illegal money trafficking and fraud on FinTech applications. It reports the ranked requirements set and use-cases definitions. **D2.4** reported the results of the UI-REF-compliant re-ranking of the requirements that have been reviewed in light of: - i) The emerging requirements revision arising from the first round of the system evaluations in the four designated pilots. - ii) The emerging innovation landscape in the fast moving Fintech and mobile money applications landscape and trends as concluded through the updates of SOA, SOM and SOP based on the updated survey and analysis as concluded in D2.2 building on D2.1. - iii) The updated second round of requirements elicitations. - iv) The newly emerging Regulatory deficits and responsive developments if any. - Use-cases had been specified, elaborated and structured in Deliverable D2.3. D2.4 revisited this specification by considering the practitioners' and end-users' needs and trials feedback as elicited through UI-REF-specified usability evaluations and the 2nd iteration of user requirements interviews. Further, it specified the test-cases and configuration requirements for 4 pilots for Phase-1 deployment, and the security test-cases planned for Phase-2 of the project. - Deliverable D2.3 Specifications and Architectural Design provided an overview of the Critical-Chains framework based on a novel “as-a-service” (XaaS) platform, including a specification for an architecture comprising of hardware and software components, mapping of functionality, relationships and inter-connections, internal and external interfaces and configuration and deployment options. D2.4 re-specified the architecture by revisiting previously defined requirements for the Critical-Chains framework. - **D2.6** (Security/Privacy and Threat semantic model), This was led entirely by UREAD, based on the UI-REF-enabled ontologically-committed semantic and threat modelling for which the Coordinator provided several tutorial sessions for the WP Team to ensure consistent analysis for all related aspects within the deliverable. This resolved and ranked privacy and security threats and countermeasures in the Critical-Chains targeted operational contexts. - Thus D2.6 has established a set of criteria and a procedural framework for integrated operational-context-aware, threat-driven, risk-based privacy-security protection by design. This offers a comprehensive analysis base underpinned by the UI-REF as
	Total Effort Planned (M1-M36) **96 Person-Months**	**Total Effort Deployed (M1-M18)** **75.77 Person-Months**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
			extended to privacy-security threat modelling; it is based on a mapping from the fundamental unit-of-analysis of use-contexts and constructs to user-ranked requirements based on high resolution stakeholder-elicited requirements as reported in a series of interviews (D2.3 and D2.4), and security-privacy contexts within the 4 pilots as reported in D2.4 based on the formalisation of evaluation results as presented in D6.2. - **D2.7** This provided an overview of the laws, regulations, standards and best practice relevant to the Critical-Chains Operational Deployment Context (Regulatory Compliance and Accountability-by-Design Model). Here, the responsive compliance-assurance-by-design requirements were examined and resolved in the context of the Critical-Chains architectural commitment to a triple accountability model and evolutionary threat-driven risk-based privacy-security by design. A full set of RACI Accountability-by-Design Audit Check tables have been instantiated to inform the Critical-Chain Accountability Model based Engineering Audit. Accordingly, this deliverable has: - **i)** Performed the analysis of regulatory and standardisation issues with respect to the Critical-Chains Main Framework as a Cloud Infrastructure; - **ii)** the Cyber-Physical Security-as-a-Service (CPSaaS) comprising different critical security services, and - **iii)** Data flows and information modelling. - The deliverable has systematically catalogued the relevant technical requirements arising from the range of relevant regulatory and standardisation instruments, including GDPR, ePD-ePR, PSD2, AML5, NIS, and the mapping from the regulatory requirements to the Critical -Chain technical specification requirements. The deliverable has also addressed the regulatory (dis)harmony issues from a RACI-matrix-based accountable roles analysis viewpoint to explicate the tension across GDPR-AML5-NIS and the tension between PSD2 and GDPR with respect to the legal basis of data processing in particular the interpretation of explicit-consent.
WP3 Leader: EY	– Establishing the Critical-Chains Framework Architecture Specification – Developing the blockchain infrastructural components including: Blockchain Data Integrity Layer, Secure and Smart contracts applications, Digital Identity and nodes, the Backend, Frontend applications, and linking, mapping and synchronization		- Set out the initial requirements analysis in WP2 and contributed to the evaluation. - Designed the first framework architecture draft including components, information and data flows covering aspects including access control, authentication and authorisation management, privacy- preserving user input and logging of data usage. - Formalised the functional and technical design through UMLs and behaviour diagrams. - Updated the general requirements included in WP2 - Analysed the specific requirements and KPIs to review the architecture. - Designed the 2nd architecture and agreed the assignment of the component development responsibilities and ownerships with the respective Partners. - Collected and Analysed new feedbacks, performance requirements and considerations in order to define the final architecture design - Defined the role of Ethereum (Rinkeby) and Quorum blockchain in the Critical-Chains project. - Analysed different cloud solutions and providers in order to identify the best-suited cloud services provider for Critical-Chains development. - Developed software selection analysis to identify the capacity of the infrastructure. - Created cost-analysis related to the different cloud solutions based on official price calculator tools (i.e. https://azure.microsoft.com/it-it/pricing/calculator/).
	Total Effort Planned (M3-M36) **54 Person-Months**	**Total Effort Deployed (M1-M18)** **25.01 Person-Months**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
			- Selected Azure services and products to include for the first deployment. - Started and maintained a provisioned infrastructure to support continuing development. - Developed the initial cloud framework based on Microsoft Azure - Defined components for the first deployment. - Created the environment for the various architectural components - Setup the environment for KSI as part of the Blockchain Integrity Layer that will be developed in the second phase. - Created a set of smart contracts for the first phase pilots and customised this for the updated set of requirements and use-cases - Created front-end and back-end applications to test the first phase pilots to enable third-party access to the relevant data. - Contributed to the dashboard design to provide as much as insight possible. This was to enable link the source of anomaly to the anomaly as identified in the system; as a complementary approach for the further X-as-a-Service approach. - Created identity solutions for the first-phase pilots based on the Metamask wallet. The identities created in the first-phase are not from real users. This was to ensure the testability covering a full set of capabilities of privacy-preserving attribute based credentials to enable users to easily impose a fine-grained access control policy for their data, while respecting multiple security policies. This enabled efficient data sharing and synchronisation among transactional units providing controllable traceability and accountability of the shared data.
WP4 Leader: ERARGE	– Developing the Flow Modelling-as-a-Service (FMaaS) for data flow and information modelling and in conjunction with mining tools (for Inter-banks, Internet Banking and Financial Markets Infrastructure). Profile-based analysis of data flow modelling – Delivering the essential capability for context-aware anomalous flows alerting & blacklisting		- Delivered **D4.1** wherein context-specific requirements have been semantically modelled and specifications have been elaborated to inform feature signature analysis. - FMaaS was designed and positioned within the Critical-Chains main framework in relation to other building blocks. - The existing financial flow data sets have been examined as well as rules deduced based on the experiential knowledge of the transaction flow control practitioners (POSTEIT operational staff) and knowledge engineering expertise from UREAD) to develop a new synthetic funds transfer transaction data set for the most dominant transaction mode as the European Standard (SEPA 1.7) developed by POSTEIT with active support from UREAD for better training of AI algorithms. - Financial flow modelling and AI-based context-aware anomaly detection algorithms by developing, testing and optimising, through feature engineering, each of the following 4 categories of approaches: - Hybrid Graph-enhanced Ensemble methods) - Graph enhanced singular methods - Ensemble methods - Other methods - With the first providing better performance than the 4th category (classic approaches) with all benchmarking datasets including both newly-created synthetic datasets as well as open data sets (e.g. graph and non-graph based feature extraction, applied to *Local Outlier Factor, Isolation Forest, One-class SVM, Elliptic Envelope, Random Forest, Adaboost, Extreme Gradient Boost, Regularised Logistic Regression with Stochastic Gradient Descent learning, KNN, Keras Sequential model*) have been developed and tested with open and newly created datasets. - The Reliability of the AI/ML algorithms has been analysed by layer-wise relevance propagation and feature engineering techniques. - Service-based architecture has been developed and integrated into the main framework.
	Total Effort Planned (M3-M36) **94.5 Person-Months**	**Total Effort Deployed (M1-M18)** **36.05 Person-Months**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
			- Routine weekly meetings, reporting, deliverable preparation (D4.1) and other administrative activities.
WP5 Leader: CEA	– Developing tools for ensuring cyber-physical security to reduce cyber risks and threats at all levels – Presenting new and innovative methods for ensuring integrity, accountability, security, privacy, scalability, and ease-of-use. – Developing a holistic risk and resilience management process for financial infrastructure to include – Risk and resilience analysis – Threat and vulnerability identification and analysis (including cascading effects) – Developing the counter and mitigation measures – Delivering the Cryptographic requirements for access – Limitations and secure communication between participants. – Implementation and evaluation of the use-cases within the pilots (WP6)		- Developing the AUTHaaS component using standard authentication and authorisation protocols (OpenID Connect, UMA) and generic enablers (Keycloak). - Integrating the Italian eIDAS-compliant SPID identity provider with the selected generic enabler (i.e., Keycloak). - Developing multi-factor authentication using new face recognition methods and by developing a FIDO-compliant HwSaaS component built on a secure stick integrated with a Secure Distance Bounding extension solution. - Designing and developing a new policy-based authentication method providing at the same time both authentication and cryptographic enforcement of access policies. - A vulnerability analysis was conducted on the design of the AUTHaaS component. The analysis demonstrated the extent of resilience of the component for instance to insider and DDoS attacks. - A compliance analysis of the developed AUTHaaS component with respect to relevant regulations and directives was also conducted. The analysis showed that the developed AUTHaaS component is fully compliant with NIS, GDPR and AML5 directives, and partially compliant with PSD2 directives. - Security analysis of the Cyber Critical-Chains framework using the STRIDE methodology was presented, in addition to an assessment of cyber-physical threats, vulnerabilities and thus risks on the framework, the authentication information, and the network. - To achieve a secure Cyber Critical-Chains framework, recommendations and best practices using, for instance, pentesting has been provided. - Development of a network intrusion detection and reaction systems based on machine learning and its integration to the Critical-Chains architecture. - As an integrity protection solution for a new blockchain-based financial platform, BCaaS provides specialist KSI signatures used for the signature of root-data-hashes of a calendar blockchain and auxiliary security support to uphold the integrity, signing time and signing entity of processed data. - BCaaS is integrated into the Critical-Chains platform in its current iteration. - Implementation of CryptaaS services: encryption and decryption, cryptographic key generation and techniques used for truly random number generation. During this first phase, the CryptaaS development focused on the laboratory-scale trials and proof-of-concept.
	Total Effort Planned (M3-M36) **159 Person-Months**	**Total Effort Deployed (M1-M18)** **86.97 Person-Months**	
WP6 Leader: INDRA	– Validating the integrated framework developed in the project and its application in real environments to offer accountable, effective, accessible, fast, secure, and privacy-preserving financial contracts and transactions. – Developing four use-cases (3 horizontal and 1 vertical) related to the financial sector, in which cybersecurity and secure and reliable data flows are crucial. – Integrating and validate the solution stacks that have been developed in the previous work packages into useful demonstrations (pilots).		- Critical-Chains-WP6 focuses on the validation of the integrated framework developed in the project and its application in real environments. It carries out the implementation of four pilots related to the financial, insurance and toll collection sectors in which cybersecurity and secure and reliable data flows are crucial. - WP6 has delivered **D6.1** whereby it has established a UI-REF-guided plan for the implementation of the user-experience evaluation in each of the four pilot application domains as designated for the validation of the Critical-Chains system; namely Banking Sector, Insurance Sector, Toll Road Operations, and Financial Market Infrastructures. Based on the UI-REF dynamic usability relationships modelling, the plan includes an extensive set of indicative questionnaire templates and pre/post-experience usability evaluations to support the assessment of the system

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
	– Deployment plan for the identified demonstrators following a two-stage incremental approach – Setting up each demonstrator environment and preparation of the test – Integration of the WP3-WP5 results in a laboratory setting following a use-case description as generated – Adaptation and modifications to deploy the components in a relevant scenario replicating operational conditions – Establishing Best Practices, Synergies and Evaluation of the test results in the different demonstrators, including privacy impact assessment		performance, usability, user-acceptance, accessibility, and impacts. - WP6 has constructed the environment of the use-cases based on the development of the value-added applications according to the scenarios described in D2.4 for the four pilot applications. The environment of the pilots comprises all the developments that are needed to perform the use-cases, including the integration platforms and cloud services. It has also performed test execution in a laboratory setting. The implementations represent running examples that demonstrate the technical research done in WP3-5. WP6 has also carried out the questionnaires for usability evaluations to support the assessment of the system. - Definition of a methodologically guided approach to planning the implementation of the holistic evaluation of the performance and impacts of the adoption of the critical-chains system (related to D6.1). - Integrate the WP3-WP5 results in a laboratory setting following a use-case description as generated (related to D6.2). - Deployment of the demonstrator environments and preparation of the tests in each of the four domains (Financial Infrastructures, Insurance, Banking and Toll Collection) in a laboratory setting (related to D6.2). - Laboratory test specification and execution in a laboratory setting (Phase1) (related to D6.2). - This work has leveraged the use-content-specific user-acceptance, and social-acceptability constructs of UI-REF to plan a methodologically-guided approach to planning the implementation of the holistic evaluation of the performance and impacts of the selected Critical-Chains-enabled use-cases. For this, we established reference questionnaires for UI-REF-guided pre/post/"point-of" experience usability evaluation. - the deliverable includes an extensive set of questionnaires for usability evaluations to support the assessment of the system usability that has informed the UI-REF-guided requirements re-prioritisation in D2.4.
	Total Effort Planned (M3-M36) **92 Person-Months**	**Total Effort Deployed (M1-M18)** **45.65 Person-Months**	
WP7 Leader RINA-C	– Creating and delivering a strategic communications and exploitation campaign across Europe – Creating tailored communication material for specific audiences. – Liaising with relevant projects/initiatives/experts in the field to disseminate project results and facilitate exchange of knowledge in workshops, conferences etc. – Delivering Communication and Dissemination Activities – Gap analysis comparing project results and relevant established standards – Participating in relevant standardisation and communication efforts – Undertaking comprehensive market research to determine a final exploitation model; and – Exploiting: Generate vehicles for the future sustainability of project outcomes and create a 'go to market' strategy		- Critical-Chains project logo has been designed and the project promotional material has been produced: power point project presentation, project single page description sheet, brochure, poster, promotional video. - Development of channel for information and results. dissemination: - Critical Chains website (https://research.reading.ac.uk/critical-chains/) - Twitter (https://twitter.com/ChainsH2020) - and LinkedIn (https://www.linkedin.com/company/critical-chains-h2020-project - project accounts. - A total of 50 posts have been shared through project and Partners social media channels. (21 posts have been shared on abovementioned project accounts/pages). - Analysis of social media activities though specific indicators. approx. 4500 direct contacts within social media only. - Critical-Chains communication and dissemination strategy, based on the creation and distribution of valuable, relevant and consistent content to attract and retain a clearly defined audience, has been developed. - A dissemination implementation strategy., based on the following four objectives, has been produced: - Strengthening the link to other H2020 peer projects. - Increased robustness of Critical-Chains innovations and results. - Strengthening project positioning in the Research Community. - Keeping the project points-of-presence "warmer" by dynamically using communication channels.
	Total Effort Planned (M3-M36)	**Total Effort Deployed (M1-M18)**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
	47.5 Person-Months	**20.53 Person-Months**	- Project consortium Partners participated in 10 workshops (four of which were organized by the Consortium itself); this has enabled the project to widen and deepen its outreach including relevant projects/experts in the field, to disseminate project results and facilitate exchange of knowledge and insights. - New Stakeholders and EU observatory have been engaged: this has included SDX, cyberwatching.eu, UB Technologies, Caixa bank, LS Experts. - In order to reach the wider European FinTech and security community a collaboration with projects within the Cyberwatching hub, notably SOTER project, has been established - Project-to-policy contributions have been made responsive to EC events and questionnaires as well as with the workshop organised and/or been invited to attend. - Eleven scientific and technical publications have been published (two are under revision). The publication types include refereed scientific and technical journal papers or conference papers, and review articles. In order to assess the publications impacts, for each publication, the relevance as number of citations, downloads/views as well as feedback/results have been provided. - Project Partners involved in the definition and development of the Critical Chain solutions have started compiling data regarding Background and Foreground IPR, as well as Exploitable results. - **D7.1** reported on dissemination, exploitation and list of outcomes including: - **D7.4** set out and benchmarked the ecology of the project touchpoints as an integrated mutually re-enforcing events. - **D7.6** “Gap Analysis of Current Relevant Standards” set out the various regulatory and standardisation requirements to support the financial infrastructures and operational layers within the financial sector. - An inventory of current standards relevant to the Critical-Chains domain has been undertaken, including a review of existing standards with reference to the respective standardisation organisation bodies (ISO, IEEE, ETSI, FIDO Alliance, OpenID Foundation, OASIS, NIST) as well as emerging Blockchain and distributed ledger related standards. Assessment of major gaps or alignment between relevant standards in force and Critical-Chains goals and outcome in terms of features impacting the solutions promoted by the project. This motivated the development of regulatory standards to best support the sectoral adoption and operational deployment of the Critical-Chains accountability by design solution stack. This includes Critical-Chains Standards Seeking contributions, including in the area of Multi-factor Authentication and Cryptographic Primitives.
WP8 **Leader** **UREAD**	**Ethical & Data Protection Compliance Assurance Requirements Fulfilment**		- Ethical and legal compliance monitoring and compliance management support has been provided to the Consortium by the Coordinator including with respect to GDPR Data Protection Requirements as stipulated by the Ethical Committee at the GA stage as well as ethically reflective and socially responsible innovation. This process commenced at the kick-off meeting on 11th July 2019 with ethical tutorial workshop integrated with the project kick-off and supported by one of the EAB members (Dr Julian Stubbe) also providing a training session. - Since then all the 12 ethical deliverables have been submitted including EAB reports which have concluded that the Consortium has adequately engaged with the compliance process to ensure ethical and data protection. - indeed, also measures for responsible innovation, as commended by the EAB as being a novel actionable methodology for integrated socio-ethical and privacy and security by design (UI-REF). This has
	Total Effort Planned (M1-Mx) **0 Person-Months**	**Total Effort Deployed (M1-M18)** **Massive, Disproportionate Untold and Utterly Thankless**	

WP-Specific Objectives, & Resources Deployed			Results Achieved (to be listed by each WP Leader)
			been supported by a governance structure for fractally re-enforced adherence to the GDPR principles by ensuring that neither the conduct of the innovation nor its deployment shall adversely impact the fundamental rights and freedoms of citizens and that in particular adherence to the 7 principles of GDPR and the principle of Healthy Explicit Consent is fully ingrained as a routinised process supported by a full pack of consent forms translated in all the languages as required. The risk-aversive approach to data processing has meant that the Consortium has had to Adopt a 100% data synthesis approach e.g. for D4.1 Transaction Flow Modelling although at the proposal stage it had been envisaged that some real data would be available to be supplemented by synthetic data for additional model training. - Total number of deliverables already delivered = 12. - Total number of EAB reports already submitted directly to the EC = 2. - EAB Opinion: Project should be permitted to continue as planned.

8. Updated Risks and Responsive Mitigation Strategies

8.1 General New Risks and Responsive Mitigation due to Pandemic-Imposed Constraints

Travelling restrictions may continue to have an unpredictably limiting effect on the ability of the Partners to hold physical meetings of any sort; for example, Steering Committee meetings, workshops, develop-debug boot camps and attending conferences. For contingency planning the Consortium having already demonstrated that it could readily follow a COVID-adapted dissemination implementation strategy through period 1, will, in period 2 continue to rely on virtual meetings, data repository and folders for document sharing as usual.

Critical-Chains is thus well-placed to take proactive measures to mitigate new threats to the project implementation occurring until the completion of the project as planned.

8.2 Elaboration and Updates of previously identified Risks

Risks 1-5 & Risk 10 Re: Blockchain scalability, integration issues with the Critical-Chains Main Framework and Cloud-based deployment and roll-out

This will mainly focus on the integration of HwSaaS and CryptaaS and the authentication tokens (SecureStick) within AuthaaS. As stated in the DoA, making XaaS service components available over the Internet best supports the integration of the Critical-Chains main framework. ERARGE has implemented the main cryptographic functions available over the Internet through CryptaaS and the software-based HSM functionalities. The one-time-password mechanism was also realised to reduce the authentication-related risks as part of the AuthaaS.
However, as per the implementation plan the HSM (HwSaaS) has to be deployed physically on the server-side and be integrated with the SecureSticks on the client-side. This requires physical site visits and interaction with subjects during or before trials. Given the uncertain level of pandemic-imposed constraints that may be in force, it is planned that the deployment of HSM shall be realised in close collaboration between ERARGE and NETAŞ for practical reasons as NETAŞ and ERARGE are located geographically close to each other.
Thus, a physical deployment will become available over NETAŞ cloud, and this is planned to be opened to the Consortium as planned for the second iteration of the system.
The trials with subjects will also be performed similarly with NETAŞ and ERARGE R&D personnel participating subject to the formal consent seeking procedure consistent with both the national and GDPR requirements. Accordingly, the SecureStick Version-I (for person authentication) is planned to be distributed to up to 50 subjects so that the test and evaluation procedure cand be conducted. The number of subjects can be increased by formatting the SecureStick following the evaluation sessions and requesting new subjects to try the Critical-Chains outputs. The reformatted SecureSticks can be shipped to relevant Partners and support will be provided for the

same test and evaluation procedures to be implemented by interested Partners.

The integration of the SecureStick for node authentication requires a physical setting, e.g. toll collection or a simulation setting resembling such a physical environment. In order to minimise the integration risks, IMEC and ERARGE will work on lab-scale integration initially to ensure that all components operate coherently without any problem. This will then be extended to a use-case in the field (e.g. toll collection).

According to INDRA availabilities, a parallel use-case will be applied which is supposed to have the highest similarity to INDRA's current toll collection applications. The technical discussions are still ongoing.

Risk 6-10 Re: Data Availability For Developing X-as-a-Service particularly relating to Transaction Flow Modelling & Intrusion Detection

The Authentication anomaly detection uses the traffic data generator script to enhance its detection mechanism according to the previously generated anomaly scenarios. Therefore for successful deployment, in a real-world setting, the system would need refinements in the real user-environment.

Moreover, in the second phase, an ML-based additional anomaly detection mechanism is planned to be implemented to fuse the inputs of AuthAD, NIDS and FMaaS (dashboarded-XaaS). For the proposed dashboarded-XaaS, more realistic data should be used in the same real world environment, in order for the outputs of these systems to be semantically integrated and the decisions to be produced. Finally, all systems should use the blockchain-based identifier for the fused outputs of the XaaS.

The network intrusion detection system (NIDS) is being implemented and tested on a local CEA demonstrator server using public network datasets. Therefore, any risk of data unavailability is unlikely to hinder the development of NIDS. However during the 2nd phase, NIDS will be integrated into the Azure Cloud infrastructure, and will use the Azure Network Watcher for data collection. The NIDS solution will thus run on the Critical-Chains framework with encrypted data since all communications are SSL/TLS protected. This means that during use-case evaluation results, NIDS will have to be tested and validated using use-case-specific data.

The extent of any risks here would depend on the possibility to update the models for the FMaaS, NIS and AuthAD with data from the target operating environment to enable model refinement. This is mitigated by the deployment of the components to the cloud-infrastructure and data generation over the same environment using well-known tools such as Selenium Webdriver (or equivalent).

RISKS 11-12 Re: Deviations, Performance Issues and Partner Conflicts

During phase 1 there was a deviation in WP4 in connection with the deployment of the CAESAR tool as had been planned but in the event this proved technically infeasible and the Fraunhofer team supported by the Coordinator and WP Leader were able to devise an appropriate research and innovation plan to develop a Reliability Checker Tool as thematically convergent with the overall objectives of their planned contribution to WP4 which was to support secure and reliable algorithms for modelling the financial transaction flows.

Concomitantly the contribution of other Partners has to be re-assessed and if necessary, re-planned for WP4 to deliver the planned objective as per the DoA.

This is to be re-confirmed early in Phase II to ensure full adherence to the planned efforts and expected results as per the DoA whilst maintaining the complementarity of effort as had been planned and avoiding duplication/repetition of effort intra/inter Partner/Task/WP.

Discussions have been on-going to ascertain any limitations that may affect the delivery of the results as had been planned and once definitive statements re the scope and extent of the expected delivery of results as planned in the DoA are available from the respective Partners, the WP leader and the Coordinator will seek to compile a plan of work incorporating substantive alternative efforts on the part of each Partner and take advice from the Project Officer as to the way forward re the need for any amendment.

Risks 14-15; Re: Special-Purpose Hardware Design, Fabrication and Testing

ERARGE has presented significant progress in HSM design as a part of the HwSaaS and CryptaaS and its adaptation to the Critical-Chains framework. However, ERARGE engineers could not find an opportunity to deploy the HSM on a physical server because of the COVID-19 lockdown. The ERARGE team has been working from home since March 2020 and the prototyping studies have been managed by taking into consideration the precautions which needed to be taken against COVID-19.

Nevertheless, as a recovery and mitigation strategy, ERARGE and the demonstrator Partners have agreed to first deploy the CryptaaS and HwSaaS at the software level. The software-based CryptaaS is capable of realising all the functionalities of a physical HSM (HwSaaS) which had been seen as sufficient for the first integration purposes. HwSaaS, CryptaaS, and AuthaaS had been integrated at a laboratory scale and made ready for the first integration within Period 1.

For the second iteration, ERARGE and NETAŞ created an action plan to deploy the HSM first in NETAŞ premises in the first half of 2021. Then, the final integration phase is to be conducted with EY and other Partners in close coordination with WP6 activities. There is no significant risk foreseen for the hardware implementation of the HSM.

For the SecureStick Version-I (person authentication), the foreseen hardware prototype design and fabrication plan have been followed without any significant delay. ERARGE has planned to produce 10 samples at the first stage (within 2021) and aims to increase this number to 50 by the end of the project. No significant risk is foreseen related to the production of sufficient number of SecureStick Version-I. The actual demonstration is planned to be held in Turkey in order to avoid any GDPR concern over data transfer (to/from third country Turkey) and for the sake of practicality, as NETAŞ and ERARGE will be able hopefully to recruit up to 50 volunteering staff to participate in the trials subject to consent seeking process compliant with both GDPR and the equivalent Turkish Data Protection Law requirements. The reformatted SecureSticks can be shipped to relevant Partners and support will be provided for the same test and evaluation procedures to be implemented by interested Partners.

For the SecureStick Version-II (with the IMEC secure distance bounding), no significant risk is foreseen to prototype the solution. However, its actual use in a specific demonstrator (e.g. toll collection) may require technical visits to and collaboration in Spain which may subject to travel restrictions. In such a case, a proof-of-concept trial can be organised at the IMEC premises where secure distance bounding can be tried within the context of Critical-Chains. Technical discussions among IMEC, INDRA, ERARGE, and WP3/5 contributors are still ongoing to solidify and elaborate this mitigation strategy.

Risks concomitant to T7.2 and the Declaration of IPR Ownership and Exploitation Plans

At this stage where innovation rights to exploitation are to be formally specified it is possible that some differences of opinion may occur re the relative ownership of particular results arising from shared tasks. To minimise the risk of any conflicts arising Partners have been advised to identify fact-based ownership of innovation results with the maximum possible level of specificity (e.g. at the algorithm, method, tool/tool component, design element) level based on the background and track record of leading contributions to any particular element and not by reference to an X-as-a-Service layer as a whole. Should any conflicts occur, these shall be resolved based on the provisions of the Consortium Agreement.

8.3 Risks Register Update

The above-mentioned risks are related to the risks as highlighted in dark green in the updated Table 3.2b below.

Updated Critical risks for implementation (All Partners)

Description of risk	Level	WP	Proposed risk-mitigation measures
Notarisation requirements-related issues: surplus and redundancy of information expected to be notarised with the Blockchain, which makes the actual development burdensome.	L	3	Setting up requirements-revision loops, allowing Partners to review requirements according to development needs, and reducing the complexity of the overall information structure and of the smart contract transaction rules.
Issues concerning the number of nodes implemented within Critical-Chains, potentially detracting from the overall system security.	M	3	Appropriate definition of security requirements (within WP2), supervision and validation of security requirements (concerning the number of nodes) by WP3 leader, flexibility of the architecture for marginal adaptation during the development phase (minor adjustments in the number of nodes); additionally use of monitoring tools on critical components where feasible.

Description of risk	Level	WP	Proposed risk-mitigation measures
Issues concerning rules defined within the consensus mechanism (e.g. risk of allowing cartel mechanisms).	M	3	Implementation of consensus mechanisms using probabilistic functions (e.g. zero-knowledge proof) and involvement of all Partners in the definition of a scalable and unbiased consensus mechanism.
Issues concerning the configuration and communication among the nodes of the blockchain.	L	3	Use of the same communication language (e.g. UDP) among all the nodes of the chain, to be defined at WP2 stage.
Because of the complexity of protocols there might be only small parts of them suitable for formal verification.	M	2	Start with only a few protocols with reduced complexity to generate quick-wins and gradually add more complexity.
Too little or insufficient data available for machine learning methods.	L	4	Seek the support of user Partners to get access to necessary data. Use benchmark datasets as far as possible.
Too little annotated/verified data available.	M	4	Plan sufficient resources for annotation/verification of data.
Legal restrictions or companies' policies do not allow usage of data for development and testing.	L	4	Check beforehand as much as possible to see if there are any legal or company policy restrictions over dataset availability; try to use other data sources in case of problems.
Reservation of companies to use "as-a-service" solutions, because they are not hosted in house under their control but in the cloud.	L	General	General attitude towards cloud services is changing because more and more services are hosted in Europe and are providing adequate SLAs and privacy policies. More tools available that enable better control over cloud assets.
Underperforming Partners .	L	All	Close contact between WP leaders and Coordinator, short feedback loops and personal contacts (regular Strategic Direction telcos, physical meetings, etc.) - continuous internal quality/progress control.
Conflicts between Partners (technically and administrative).	L	All	Conflict management through close and good contacts, frequent meeting (regular Strategic Direction telcos/meetings, General Assembly meeting, etc.).
RTD efforts are not reaching technical targets.	L	3,4,5	WP leaders are present in all technical meetings and hold the expertise, involvement of additional experts if necessary. Continuous internal quality/progress control.
Distance measurement stability insufficient	L	5	De-risk through early benchmark.
Compatibility of all components for full demonstrator integration.	M	5	System design with project Partners maintaining a strong focus on the specification and development of semantically interoperable interfaces. Continuous integration testing and evaluation.
Integration issues: difficulties in ensuring interactions between the blockchain and the APIs, with potential impacts in terms of endpoint vulnerabilities.	M	3 & 6	Early collaborative efforts by all Partners involved in the development of APIs, in order to design requirements and set the development path so as to prevent integration issues with the blockchain; Implement security features on the overall process concerning the credential requirements to activate an endpoint as-a-service; implement cryptographic solutions to protect private keys.
Training datasets used for NIDS in the first phase may differ from the data flows of the real network of the Azure environment that is to be deployed in the final demonstrator.	M	3	In this case, we will have to adapt the NIDS solution in order to process the new data flows of the final demonstrator network.
Deviations, Performance Issues and Partner Conflicts.	M	3,4,5, 7	Deviations re-planning has already been resolved with one Partner and mitigation plans are in hand to deal with any further re-planning as necessary to ensure full delivery of the results as per DoA and Amendments shall be requested as necessary.
Partner conflicts over IPR ownership boundaries relating to the new innovations.	M	3,4,5	Any IPR related conflicts as may arise in Phase 2 shall be resolved through the provisions of the CA.

9. Deviation Statements

This section sets out the clarifications provided by the partners regarding their respective resource deployments within period 1.

9.1 Partner 2 CEA

CEA PM claims are justified by the significant progress having been made in parallel on both the Network Intrusion Detection and Reaction Systems, in addition to the Policy-Based Authentication Solution. To be able to obtain advanced phase 1-results more quickly than expected, we had to put more resources into the project.

9.2 Partner 5 Fraunhofer EMI

WP	Planned PMs	Actual PMs	Rationale
2	0.5	0.81	WP2 required more contributions from all Partners in the beginning of the project than expected. The efforts can be re-adjusted in the same WP in the next iteration.
4	9.5	7.73	A new method for data flow analysis had to be used, because a re-evaluation of the proposed method showed an inapplicability for the needs of Critical-Chains. Therefore, the working plan for this WP had to be modified.
5	12	9.60	The resilience analysis concept could not be adapted to the cyber-physical domain as fast and as comprehensively as anticipated. This prevented the engagement of more staff members into the task. With the resulting further developed tool, more staff members could participate in the second iteration, without the need to upgrade the tool themselves.
7	2	1.64	Lower than planned effort also it is expected that more scientific publication will arise in the second period.

9.3 Partner 6 GT

For period 1 of the project Guardtime planned and actual staff deployment figures were 21 and 11.94 man-months respectively. The under-deployment was due to the fact that the original implementation plan for this period was based on the assumption that the cloud environment would be ready for components to be delivered by Guardtime being installation by October 2020 but as the cloud provider selection and procurement took longer than had been anticipated, fewer installation tasks could be implemented before the end of period 1 and hence less resources were deployed during period 1. However, this will naturally self-correct as per the work scheduled with the cloud environment now having been made fully operational.

9.4 Partner 8 INDRA

(Deviation Statemen for WP6- as a whole)

Due to the integration problems as faced in Phase 1, during the period 2, WP6 is expected to require higher effort compared to the level expected per a linear distribution between period 1 and 2. WP6 Partners will integrate the different components to be developed and carry out internal testing for some of the tests carried over from Phase 1. The main objective is to conduct a debugging phase for the integration before the implementation of Phase 2. This deviation was determined before the end of period 1 as even although we achieved the main objectives of Phase 1, some work still had to be completed in Phase 2.

9.5 Partner 9 JR

JR, as the leader of the WP2 Requirements Engineering and Framework Architecture Specification was focused extensively on the work within this work package in the first half of the project. WP2 tasks, including requirements definition and technology watch, are enabling tasks for the work in the other work packages, and as such require higher workload in the first half of the project. An additional consideration would be the number of submitted deliverables in period 1 (six out of seven deliverables were submitted) versus the one final deliverable to be delivered in period 2 by the end of the project. This is reflected in the higher number of PMs as needed and deployed during the first period of the project.

9.5 Partner 12 RINA-C

WP2 – RINA-C has used 86% of total PMs foreseen for WP2 because in the first project phase RINA-C has been more highly involved due to the new system releases developments by the Partners.

WP5-RINA-C has used 79% of total PMs foreseen for WP5 because in the first project phase RINA-C has been more highly involved in the specification phase.
WP6 - RINA-C has used 72% of PMs planned for WP6 to set up the DPIA (Task 6.4) and to analyse the use-cases.

In some activities RINA-C has involved junior staff, not originally foreseen, to collaborate with more senior resources. This has resulted in the use of more man-months compared to the planning time arrangements. Despite this over-spending in terms of resources, the activities are being carried out within the original budget and will continue to be remain within the budget for the remaining part of the project.

10. Project Level Resource Deployment Reporting

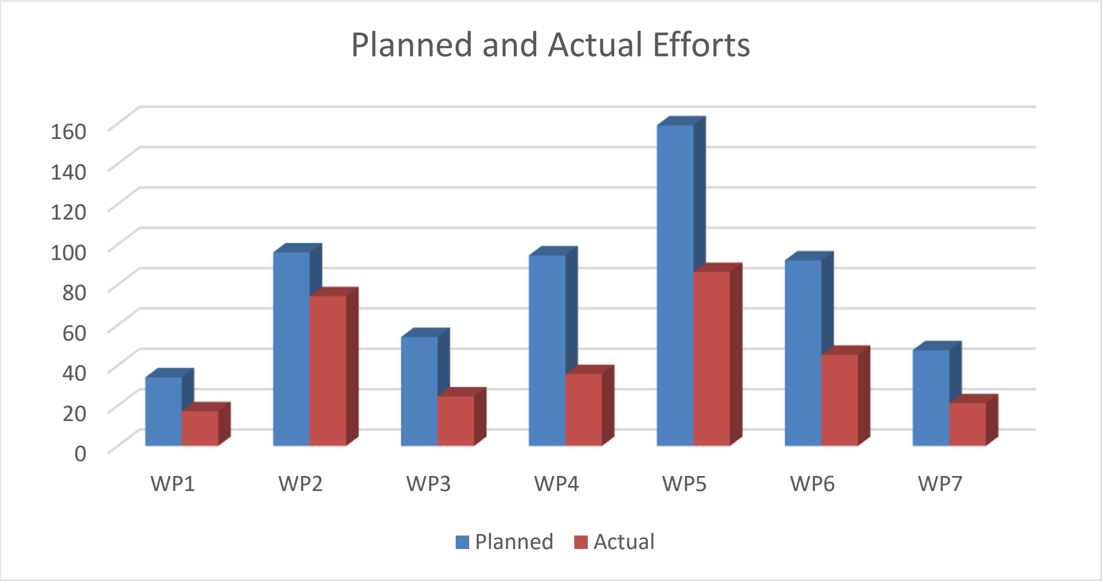
10.1 Partner Specific Staffing Resources Deployed versus that Planned

Partner number	Partner organisation name	Short Name	Total Person-Months PLANNED	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	Total
			ACTUAL									
1	The University of Reading	**UREAD**	**Planned:**	20	12	0	24	8	5	3	0	72
			Actual:	10.69	7.6	0	7.68	2.11	1.92	1.65	0	31.65
2	Commissariat À L'Energie Atomique Et Aux Energies Alternatives	**CEA**	**Planned:**	1	4	0	0	22	4	2	0	33
			Actual:	0.61	3.16	0	0	18.46	1.96	0.94	0	25.13
3	Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik Su Urunleri Sanayi ve Ticaret Limited STI.	**ERARGE**	**Planned:**	4	6	0	24	26	5	4	0	69
			Actual:	1.5	7	0	6.5	17	2	2	0	36
4	EY Advisory S.P.A.	**EY**	**Planned:**	1	8	14	5.5	8	2	7.5	0	46
			Actual:	1	6	8.5	2	4.5	4	2	0	28
5	Fraunhofer-Gesellschaft Zur Förderung Der Angewandten Forschung e.V.	**FHG**	**Planned:**	1	1	2	19	24	5	4	0	56
			Actual:	0.45	0.81	0.95	7.73	9.6	2.16	1.64	0	23.34
6	Guardtime As	**GT**	**Planned:**	1	3	14	0	16	8	0	0	42
			Actual:	0.59	2.85	3.36	0	3.93	1.21	0	0	11.94
7	Stichting Imec Nederland	**IMEC-NL**	**Planned:**	1	0	0	0	20	0	4	0	25
			Actual:	0.5	0	0	0	11	0	2	0	13.5
8	Indra Sistemas SA	**INDRA**	**Planned:**	1	7	6	0	5	24	4	0	47
			Actual:	0.51	3.72	0.74	0	0.25	9.97	0.79	0	15.98
9	Joanneum Research Forschungsgesellschaft Mbh	**JR**	**Planned:**	1	23	0	14	2	4	2	0	46
			Actual:	0.61	17.24	0	6.17	1.69	1.58	1.54	0	28.83
10	Netas Telekomunikasyon Annonim Şirketi	**NETAS**	**Planned:**	1	9	12	5	13	17	4	0	61
			Actual:	0.5	7.2	8	2.55	8.5	9.4	1.45	0	37.6
11	Poste Italiane - Societa Per Azioni	POSTEIT	**Planned:**	1	14	6	3	9	7	5	0	45
			Actual:	0.11	12.49	3.46	3.42	5.19	3.44	2	0	30.11
12	RINA Consulting Spa	RINA-C	**Planned:**	1	9	0	0	6	11	8	0	35
			Actual:	0.65	7.7	0	0	4.74	8.01	4.92	0	26.02

10.2 Proportion of Resources Deployed

Proportion of Resources Deployed	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	Total
Total of planned resources per WP for Periods 1 & 2	34	96	54	94.5	159	92	47.5	0	577
Total of deployed resources per WP for Period 1	17.72	75.77	25.01	36.05	86.97	45.65	20.93	0	308.1
Percentage of resources remaining for Period 2	52.12	78.93	46.31	38.15	54.70	49.62	44.06	0	53.39

10.3 Graphical representation of the planned versus actual resources deployed



11. Consortium Meetings

Project Meetings Date	Venue	Meeting Title & Reason
11th July 2019	Univ.	Kick-off Plenary, Technical & Ethical Training Meeting
16th December 2019	Univ.	Requirements Engineering Deliverables Development
17th December 2019	Univ.	Ethics of Blockchain Workshop
3rd February 2020	Virtual	Steering Committee Meeting Re Financial Data Assets Sourcing
28th May 2020	Virtual	Steering Committee Meeting Re INDRA Linked Third Party Amendment
31st August 2020	Virtual	Steering Committee Meeting Re EY Infrastructure Burden Sharing
10th September 2020	Virtual	Steering Committee Meeting Re EY Infrastructure Burden Sharing
Bi-Weekly	Virtual	All-WPs Progress Verification Meetings
Weekly or Bi-Weekly as	Virtual	WP-Specific Teams Meetings
7th May & 23rd June	Virtual	Collaboration Meetings with the SOETER & Fintech project core teams
Fintech meeting Meetings	Virtual	Collaboration Meetings

12. Partners' Description of their Task-Level Contributions

Task Number	Task Title	List of Contributors	Description of Results Delivered
12.1 Partner 1: UREAD			
WP1: Project Management			
T1.1	**Consortium management**	(M1-36) [TL: UREAD]	Established the protocols for weekly and fortnightly consortium meetings for process verification at the work package and overall project levels. Provided active leadership and hands on support to help with planning and structuring deliverables and the mapping across from definition of scope to a methodologically guided design of the work and the technical reporting of it in order to ensure high quality deliverables are achieved.
T1.2	**Quality, Data, Ethical & Regulatory Compliance Planning & Assurance**	(M1-36) [TL:UREAD,	Providing the quality guidelines and templates for collaborative deliverables development addressing the end-to-end process including deliverable scope and KPI analysis and consistent structuring, subsection responsibility assignment and version control etc. Held discussions to clarify quality management guidelines for the Consortium. Circulated various templates and example work. Provided regular mentoring and support for ethical and data protection compliance including consent form constructor kit translated into different languages as required.
T1.3	**Scientific & Technical & Innovation management & reporting**	(M1-36) [TL:UREAD, ERARGE]	Provided scientific technical and methodological leadership and support at various levels and stages of the development of various deliverables.
T1.4	**Project administration & financial reporting**	(M1-36) [TL:UREAD, Contributors: All Partners]	Organisation of protocols for collaborative document authoring and reporting established the project shared working site on Teams and its structure and advised on management and financial reporting. Developed the structure of the periodic management report and advised on how Partners should be contributing content to it.
WP2: Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	Provided the first deliverable structure for D2.1 and D2.3. Carried out the initial domain knowledge analysis for the financial services sector in particular Fintech and crypto currencies to provide the knowledge basis for the Consortium in order to prepare for the ontological analysis of the domain and the adoption of UI-REF as the methodology for requirements reprioritisation. Provided various tutorials and advice on knowledge engineering, and context-aware requirements elicitation, prioritisation and dynamic usability relationships-based re-prioritisation(system adaptation).
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA,, FHG, GT, INDRA]	Established a framework approach for the analysis of context aware privacy and security requirements analysis and elicitation and continued to provide training and active support to help with the requirements engineering from a privacy and security preferences elicitation standpoint and the use-context eco-system as the universal reference of analysis.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	Introduced the mapping from use-context to use-scenarios and workflows, security context, policy context, and information theoretic considerations in the design of role-based access control policy to ensure zero knowledge.
T2.1.3	**Regulatory compliance and Accountability-by-Design requirements**	(M1-M27) [Contributors: UREAD, NETAS, GT, INDRA, POSTEIT]	Established the deliverable structure for D2.7 and provided guidance and active support to help contributors contribute to the deliverable in particular in relation to the regulatory and standardisation requirements to support accountability engineering and vice versa the accountability by design features to support regulatory compliance in particular developed the analysis in relation to GDPR, ePD/PR, and contributed to the analysis relating to regulatory tensions between GDPR and PSD2.
T2.1.4:	**Technology and market watch updating**	(**M**1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS] UREAD	Introduced the analysis of market forces as a framework for emergent trends analysis including Porter's Competitive Strategy Model and Boston Matrix. Contributed to the literature with analysis of trends and helped shape and complete the deliverable D2.1.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	Led the deliverable D2.6 throughout, provided a series of tutorials to familiarise the Consortium with the concepts underpinning integrated context-aware privacy, modelling. This included the use-context-indexed privacy-security requirements, policy and access control context, privacy threat modelling tool and threat severity modelling and ranking to inform countermeasures prioritisation.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	Supported the use-cases and test-cases with reference to the Flow Modelling as a Service (FMaaS) requirements mapping to use-cases and test-cases. Added a system for requirements indexing and tracking and templates for use-cases and test - cases definition.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.1	**Inter-banks data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, EY, NETAS)	Led the structuring and preparatory analysis to support the roadmap for this deliverable including the two key areas of effort namely data synthesis and algorithmic innovation. In particular introduced the knowledge graph-based approach leading to the graph-enhanced solution set and ensemble solution sets both of which out-performed all the other approaches. Added the design for integration of the resulting FMaaS into the main Critical-Chain framework and contributed a formal specification for implementation within Deliverable D3.1. Also provided tutorials on LinkSmart and provided active knowledge engineering based support for the development of the synthetic database for SEPA transactions by POSTEIT (SEPA 1.7). This included sustained effort over several iterations.
T4.2	**Internet banking data flow & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	Internet banking focus - Continued to develop the analysis base with reference to use-context modelling to inform the information-theoretic feature signature analysis to optimise the trade-off between algorithmic efficiency and complexity in dataflow modelling.
T4.3	**Financial markets infrastructure flow modelling**	(M5-M35) [TL: FHG, Contributors: ERARGE, UREAD, EY, NETAS,]	Fintech focus - Continued to develop the analysis base with reference to use-context modelling to inform the information theoretic feature signature analysis to optimise the trade-off between algorithmic efficiency and complexity in dataflow modelling.
T4.4	**Profile-based dynamic context-aware flow mining & modelling**	(M5-M35) [TL: ERARGE, Contributors: FHG, UREAD, NETAS]	KYC focus - Continued to develop the analysis base with reference to use context modelling to inform the information theoretic feature signature analysis to optimise the trade-off between algorithmic efficiency and complexity in dataflow modelling.
T4.5	**Context-aware anomalous flows alerting & blacklisting**	(M5-M35) [TL: JR, Contributors: UREAD, FHG, NETAS, UREAD]	Hardware acceleration focus - Continued to develop the analysis base with reference to use context modelling to inform the information theoretic feature signature analysis to optimise the trade-off between algorithmic efficiency and complexity in dataflow modelling.
WP5: Cyber-Physical Security			
T5.4	**Blockchain-as-a-Service (BCaaS) integrity checking**	(M5-M35) [TL:GT, Contributors: UREAD, EY, FHG, INDRA]	Smart contract security by design performed analysis of smart contract threat, vulnerabilities and exploits conclusive observations with respect to security by design requirements and possible solutions for smart contracting.
WP6: System Integration & Validation in Various Pilots			
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	Supported the structuring and methodological design of the framework for evaluation planning including use scenario selection and UI-REF enabled dynamic usability and acceptability evaluation and responsive resolution of requirements re-ranking to inform the evolutionary, iterative design. Supported the design and restructuring of the questionnaires for pre- post- point-of experience usability evaluation and feedback elicitation to be used for all the pilots.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	Supported the selection of the use-cases for piloting implementation; in particular in devising a use-scenario to be able to integrate the IMEC chip with respect to anti-tampering and distance bounding capabilities. Contributed to the revision of requirements engineering and usability evaluation questionnaires consistent with UI-REF in order to support Acceptability-by-Design.

Task Number	Task Title	List of Contributors	Description of Results Delivered
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	Helped set up the project touch-points and branding as an ecosystem of dissemination channels including website, LinkedIn, and membership of clustering groups and network of networks such as cyber-watching and LSEC. Formulated workshops agendas and (co)organised several workshops and contributed to other workshops starting from the first workshop at the kick-off on the 11th of July 2019 and the second on 17th December 2019 (Ethics of Blockchain) and so on to end Period 1 with the last of the ten workshops which was organised and hosted by Critical-Chains on Financial Systems and Services Cyber-Security and Regulatory and Standardisation held on 14th December 2019. Additionally provided major contributions and revisions and co-led for the publications with JR and FHG in the area of FMaaS and Fintech Security by Design as well as to other dissemination efforts. Also contributed to the Project-to-Policy Kick-Off Workshop and subsequently made detailed responses to the EC questionnaire re the regulatory and standardisation requirements. Contributed to D7.4 structuring and content throughout. Contributed to D7.6 structuring and content in particular in relation to GDPR and PSD2, ePD/ePR requirements for Accountability-by-Design.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	Structured Deliverable D7.8 with an integration of the UI-REF enabled framework for innovation management: *Beyond the Chasm and towards Mainstreaming.*
WP8: Ethics Requirements			
T8.1 **D8.1**	**Recruitment Criteria specified** **Deliverable D8.1** Requirement No. 1	M3), Type: Ethics	**Delivered:** procedures and criteria that will be used identify/recruit research participants.
T8.2 **D8.2**	**Informed Consent Procedures specified** **Deliverable D8.2** H - Requirement No. 2	M3), Type: Ethics; CO	**Delivered:** The informed consent procedures that will implemented for the participation of humans.
T8.3 **D8.3**	**Informed Consent Form & Written Clarifications Information Pack -all translated to relevant languages** **Deliverable D8.3** POPD - Requirement No. 3	(M3), Type: Ethics, CO	**Delivered:** Templates of the informed consent/assent forms information sheets (in language and terms intelligible to participants).
T8.4 **D8.4**	**Compliance with GDPR and National Laws re processing of data in special categories (e.g. biometric data)** **Deliverable D8.4** Requirement No. 4	(M3), Type: Ethics, CO	**Delivered:** examination of any special derogations applicable pertaining to the rights of data subjects or the processing genetic, biometric and compliance assurance.
T8.5 **D8.5**	**Detailed Partner & Consortium Level Data Protection Policy & Governance Structures** **Deliverable D8.5** POPD - Requirement No. 5	(M3), Type: Ethics, CO	**Delivered**: set out the data processing, the compliance strat and its legal basis as well as a description of the complian Assurance governance structure.
T8.6 **D8.6**	**Special Category Data Compliance Detailed** Requirements No 6	(M3), Type: Ethics, CO	**Delivered**: Provided justification for the processing of spe categories of personal data.
T8.7 **D8.7**	**Confirmation of data transfer compliance with the law in source country & with GDPR** **Deliverable D8.7:** Requirement No. 7	(M3), Type: Ethics, CO	**Delivered:** provided confirmation that any data transfers comply with both GDPR and the laws of the country in which data was collected.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T8.8 **D8.8**	**Ethics risks analysis and opinion as to whether Data Protection Risk Assessment should be performed.** **Deliverable D8.8:** Requirement No. 8	(M3), Type: Ethics, CO	**Delivered**: provided elaboration on the position of the project any profiling and how in any case ethical and legal compliance be assured.
T8.9 **D8.9**	**Ethics risks analysis and opinion as to whether Data Protection Risk Assessment should be performed.** **Deliverable D8.9** Requirement No. 9	(M3), Type: Ethics, CO	**Delivered:** provided a comprehensive risk analysis for all purposes and contexts of the data processing planned.
T8.10 **D8.10**	Justification of scale of data collection and proof of compliance with the Data Minimisation Principle **Deliverable D8.10** Requirement No. 10	(M3), Type: Ethics, CO	**Delivered**: elaborated the approach to ensuring full adherence to the 7 principles of GDPR in particular to data minimisation and purpose limitation appertaining to all data processing purposes and contexts.
T8.11 **D8.11**	**Data Anonymisation Techniques** GEN - Requirement No.11	(M3), Type: Ethics, CO	**Delivered:** Elaborated on the approaches pursued anonymisation and pseudonymisation as required.
T8.12 **D8.12**	**Annual Ethical Report 1** GEN - Requirement No.12	(M12), Type: Ethics, CO	**Delivered:** submitted the annual ethical compliance report which also included the second report by the EAB detailing their opinion of the ethical conduct, and legal and social responsibility compliance of the project.

12.2 Partner 2: CEA

Task Number	Task Title	List of Contributors	Description of Results Delivered
WP1: Project Management			
T1.4	**Project administration & financial reporting**	(M1-36) [TL:UREAD, Contributors: All Partners]	Management of CEA contributions in the project Leading WP5 (organisation of WP5 meetings, writing progress reports on WP5 activities, etc.).
WP2: Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	Contributions to the identification of security and privacy requirements related to authentication and network security, their analysis and prioritisation.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA,, FHG, GT, INDRA]	Identification of functional and non-functional requirements associated with authentication and network security and related to the AUTHaaS component and the secure Cyber framework (more precisely, the intrusion detection system).
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	Definition of the AUTHaaS workflows: authentication & authorisation.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	Contribution to the identification of relationships between security and privacy requirements. Contribution to classes of objects and object properties for the reference ontology, in addition to the IoT taxonomy extended middleware.
T2.4	**Critical-Chains framework architecture & integration (re)-specification**	(M1-M36) [TL: EY, Contributors: JR, UREAD, POSTEIT, ERARGE, CEA, GT, INDRA, NETAS]	Participation to the definition of the Critical-Chains architecture: integration of the AUTHaaS component and the network intrusion detection system within the Critical-Chains architecture.
WP3: Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.1	**Developing the Critical-Chains framework architecture**	(M3-M36) [TL:EY, Contributors: INDRA, NETAS]	Specification of the integrated Intrusion Detection System architecture in relation to the Cloud infrastructure defined in the project (using VMs and Azure infrastructure) and of the standalone version already deployed. Definition of technical requirements related to the development of the IDS driven by the project requirements. Identification of technical requirements related to the AUTHaaS development driven by the project requirements. Update of the AUTHaaS component workflows (authentication & authorisation) using the selected generic enabler and standard protocols.

Task Number	**Task Title**	**List of Contributors**	**Description of Results Delivered**
WP5: Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	Leading activities in WP5 and T5.1. Definition of the AUTHaaS architecture and its constituted sub-systems. Setting up a local demonstrator hosted at CEA of the AUTHaaS component that is used for integration testing and evaluation. Editing D5.1.
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	Design and development of the policy-based authentication factor that provides authentication and access control and is built on a federated identity protocol (i.e., OpenID Connect). In the second phase, this authentication factor will be integrated to the selected generic enabler and into the Critical-Chains architecture.
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	Defining check lists for the AUTHaaS component and network security that are used for pentesting.
T5.2.2	**Threat intelligence, mining, predictive modelling and white-listing**	(M5-M35) [Contributors: CEA, NETAS, FHG, ERARGE RINA-C]	General information on relevant and accessible network logs Analysis of network threats related to the Critical-Chains architecture. Full Intrusion Detection System (IDS) specification (pre-processing, detection, post-processing, reaction suggestion) and detailed explanations of design choices. Presentation of results on the well-known CICIDS2017 dataset Presentation of the first version of the IDS dashboard. Development and validation of pre-processing, intrusion detection process and post-processing functions. Development and testing of a suggested reaction function currently considered in beta version. Development of version 1 of the dashboard and its API. Integration of the IDS into the local server hosted by CEA with pre-processing, intrusion detection process and post-processing functions (i.e. the mechanism described in D5.3 to reduce the number of false positives). Integration of version 1 of the Critical-Chains dashboard for viewing IDS result. Version 1 communicates with the IDS APIs.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	Specification of the AUTHaaS expected behaviours (authentication initiated by either IDP or SP, authorisation) and provision of the corresponding ESEA analysis.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	Participation to the specification of interfaces notably with the AUTHaaS component. Integration of the developed network intrusion detection system to the local server hosted at CEA.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	Participation to the compilation of an inventory on standards and regulations relevant to the Critical-Chains domain and related to the design of the AUTHaaS component. Editing D7.6.

12.3 Partner 3: ERARGE

WP1:Project Management			
T1.3	**Scientific & Technical & Innovation management & reporting**	(M1-36) [TL:UREAD, ERARGE]	ERARGE has assisted the Coordinator in monitoring the progress, assessing the quality of technical works, identifying the technical risks and revisiting the mitigation plans mainly re WPs 3, 5, 6.
WP2: Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	ERARGE focused on the functional and non-functional requirements related to overall authentication and cryptographic needs, and the service-based architecture. ERARGE contributed to the implementation of the UI-REF Requirements prioritisation methodology as led by the Coordinator and conducted the requirement engineering studies in collaboration with other Partners.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	ERARGE focused on the GDPR needs and the security-privacy requirements by explicating the relevant compliance requirements according to the Turkish Data Protection Requirements (KVKK) in relation to Fintech-context stakeholder approach.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	ERARGE focused on the FIDO standards and their alignment with eIDAS and project-specific needs. ERARGE also focused on node security requirements needed for IoT security.
T2.1.4:	**Technology and market watch updating**	(M1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS]	ERARGE applied the BCG matrix methodology on hardware and software-based authentication and cryptology products, their market analysis and the SOTA updates in line with the project scope as motivated by the Coordinator as an analytical tool twinned with Porter's Models as incorporated in D2.1 for analysis of Market Forces in Fintech.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	ERARGE contributed to the preparation of the IoT-based communication and authentication ontology, overall system specification and requirements prioritisation.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	ERARGE has monitored the studies related to the use-cases and identified the system specification for authentication, cryptographic tools and their service-based architectures.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.1	**Inter-banks data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, NETAS)	ERARGE (WP Leader) has managed the technical studies jointly with the Coordinator, focused on the semantic understanding of the inter-banks data flows and the deliverable preparation.
T4.2	**Internet banking data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	ERARGE (WP Leader) has managed the technical studies jointly with the Coordinator, focused on the semantic understanding of the internet banking data flows and the deliverable preparation.
T4.3	**Financial markets infrastructure flows modelling**	(M5-M35) [TL: FHG, Contributors: ERARGE, UREAD, EY, NETAS, UREAD]	ERARGE (WP Leader) has managed the technical studies jointly with the Coordinator, focused on the semantic understanding of the financial market infrastructures data flows and the deliverable preparation.
T4.4	**Profile-based dynamic context-aware flows mining & modelling**	(M5-M35) [TL: ERARGE, Contributors: FHG, UREAD, NETAS]	ERARGE (WP Leader) has managed the technical studies jointly with the Coordinator and focused on the identification of roles and profiles within the semantic context of financial flows. ERARGE has assessed the quality of technical works developed within the task and led the deliverable (D4.1) preparation jointly with the Coordinator.
WP5: Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	ERARGE contributed to the high level architecture, revisiting the token-based authentication and authentication mechanisms, and the development of the multifactor authentication with SecureSticks and biometrics. ERARGE has contributed to the development of D5.1.
T5.1.1	**Multi-lateral biometrics-based access control**	(M5-M35) [Contributors: ERARGE, EY, FHG, POSTEIT]	ERARGE has developed a face verification solution experimented with open data sets. The developed algorithms are based on new advancements in recursive and convolutional neural networks enabling fast and efficient face tracking and recognition. The obtained results are below 1% equal error rate, and the solution was tested in the form XaaS that will be deployed in the main framework (Phase 2).
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	ERARGE focused on the development of the SecureStick and its use for the token-based authentication. SecureStick is a hardware token which is orchestrated and initiated by the HwSaaS. All hardware design, assembly of electronic components and lab-scale verifications have been accomplished.
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	ERARGE focused on the authentication related cyber-attacks classified by NETAŞ and CEA. ERARGE contributed to the preparation of D5.3.
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	ERARGE focused on the authentication-based vulnerabilities. The logging mechanism of the HwSaaS and the authentication workflows have been shared with relevant Partners to identify

Task Number	Task Title	List of Contributors	Description of Results Delivered
			more than 20 different types of cyber-attacks caused by authentication-based failures.
T5.2.2	**Threat intelligence, mining, predictive modelling and white-listing**	(M5-M35) [Contributors: CEA, NETAS, FHG, ERARGE RINA-C]	ERARGE focused on the cryptanalysis of true random number generators which are used as key subcomponents of the HwSaaS. ERARGE has identified potential threats that might be originated from the cryptographic key generation schemes and reported them in conjunction with T5.3.
T5.3	**Hardware-Security-as-a-Service**	(M5-M35) [TL: IMEC-NL, Contributors: ERARGE, FHG, INDRA]	ERARGE HSM, known as PRIGM, was developed, and adapted to the scope of this task. HSM is positioned as the HwSaaS that performs cryptographic logical operations in the Critical-Chains framework. ERARGE contributed to the preparation of D5.5.
T5.3.1	**Embedded-systems secure inter-operation framework (LinkSmart) integration**	(M5-M35) [Contributors: ERARGE, FHG]	ERARGE focused on the LinkSmart and Keycloak specifications and its adaptation to cryptographic schemes as-design. The integration studies will continue in Phase 2.
T5.3.2	**Tamper–Proofing self-reset**	(M5-M35) [Contributors: IMEC-NL, ERARGE]	The HSM secure key storage is developed at the hardware level which is protected against tampering attacks. ERARGE HSM is enclosed in a tamper-proof enclosure which was tested in ERARGE's private cloud.
T5.3.3	**Secure IC Stick-in-Silicon**	(M5-M35) [Contributors: IMEC-NL, ERARGE]	SecureStick version 1 design was completed. The first prototype was produced and tested. IMEC distance measurement technology with BLE was modularly integrated with SecureStick.
T5.3.4	**Security Module (HSM)**	(M5-M35) [Contributors: ERARGE, FHG, INDRA]	Hardware Security Module (HSM) or HwSaaS is developed as a physical device that is capable of carrying out major cryptographic operations such as true random number generation, prime number generation, key generation and management, secure key storage and exchange, symmetric encryption (AES, 3DES), asymmetric encryption (RSA, ECDSA), and hashing (SHA). It has three different interface peripherals (PCIe, USB, Ethernet).
T5.5	**Crypto-as-a-Service (Cryptaas)**	(M5-M35) [TL:ERARGE, Contributors: FHG]	ERARGE has implemented the lab-scale software-level integration of cryptographic functions, fully compliant with the PKCS#11 standards, and assisted the Blockchain-as-a-Service and Authentication-as-a-Service. ERARGE prepared the D5.9.
T5.5.1	**Symmetric-Asymmetric Cryptography**	(M5-M35) [Contributors: ERARGE, FHG]	3DES, AES symmetric, and RSA asymmetric encryption algorithms were improved over ERARGE HSM at FPGA level adjustments. Moreover, ERARGE SecureStick is adapted as a complementary token working with ECDSA algorithm compliant with FIDO.
T5.5.2	**Key generation based on truly random number generator**	(M5-M35) [Contributors: ERARGE, FHG]	Comparison and pre-normative development of various benchmarking TRNGs and their security analyses have been implemented. Development of the high throughput and low-cost TRNG was completed. TRNG and the key generation scheme were implemented on HSM at FPGA level. The key exchange protocol was developed by HSM at software level. Scientific papers were prepared and published.
WP6: System Integration & Validation in Various Pilots			
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	ERARGE has contributed to the review of the studies related to the use-cases and identified the integration strategy of authentication and cryptographic services (XaaS) within the Critical-Chains ecosystem.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	ERARGE focused on the GDPR and KVKK (Turkish law similar to GDPR) comparison and the privacy preservation techniques, especially related to the biometric data protection. ERARGE started to work on biometric data encryption and hashing techniques, as well as match-on-device (SecureStick) to comply with GDPR and KVKK.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			

Task Number	Task Title	List of Contributors	Description of Results Delivered
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	ERARGE focused on the FIDO standards and their alignment with eIDAS. ERARGE contributed to D7.6 in the fields of audit/certification for cybersecurity and privacy aspects, authentication schemes and cryptography.
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	ERARGE published 7 scientific papers in the top conferences. The published papers are the direct outputs of T5.3 covering the advanced topics of true random number generation and cryptographic key generation techniques aligned with the accountability models. ERARGE contributed D7.1 and D7.4.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	ERARGE has identified the background, foreground and side-ground knowledge that can be benefited throughout the project and potential joint studies mainly with IMEC, UREAD, NETAŞ, EY and JR.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	ERARGE has contributed to the identification of communication channels with potential national and international Partners, other EU projects and customers. The company-specific commercialisation plans have been revisited and joint actions with other Partners have been discussed.

12.4 Partner 4: EY

WP2 Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	EY focused and contributed to the definition of functional and technical requirements related to architecture and infrastructure, concerning performance, throughput, utilisation, scalability, capacity, availability, reliability, recoverability, maintainability, security, privacy, manageability, environmental sustainability, data integrity, usability, interoperability, accountability.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	EY focused on regulatory needs and security-privacy requirements in relation with Fintech environment and blockchain technology.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	EY developed a set of use-cases for banking and insurance selecting two of them for the first phase development. In addition, EY contributed to the definition of the financial infrastructure use-case. Overall, EY monitored the studies related the use-cases and identified the system specification of Fintech cases, blockchain tools, cloud services and their service-based architectures. After the definition, EY contributed with relevant Partners to the test-cases.
T2.4	**Critical-Chains framework architecture & integration (re)-specification**	(M1-M36) [TL:EY,	EY led the overall design of the Critical-Chains architecture interpreting the results of the requirements and specifications determined within T2.1-3, T2.4. EY gathered different feedbacks and KPIs in order to determine the best solution for the project considering tools and software. In addition, EY created an evaluation report for the comparison of cloud solutions and providers selecting, in accordance with other Partners, “Azure” for the Critical-Chains Framework architecture with respective cost-analysis related to the different cloud solutions based on official price calculator tools (i.e. https://azure.microsoft.com/it-it/pricing/calculator/).
WP3 Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.1	**Developing the Critical-Chains framework architecture**	(M3-M36) [TL:EY(6), Contributors: INDRA(4), NETAS(3)]	After gathering and contributing to final requirements, feedbacks, KPIs and other analysis, EY designed Critical-Chains components in order to create a fully integrative, holistic and scalable infrastructure. In the first phase EY led the selection of the components to develop and created the environment for their integration.
T3.2	**Blockchain Integrity Layer**	(M3-M36) [TL: GT, Contributors: NETAS, EY, FHG, INDRA]	EY has contributed to the identification, design and integration of the Integrity layer provided by GT with KSI with a deep study of the technology and related considerations focusing on the integration with Quorum blockchain, the network selected by EY in accordance with other Partners. During the first phase, EY created the environment to integrate KSI in the next development stages.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T3.3	**Secure & Smart contracts development**	(M3-M36) [TL: EY (4), Contributors: GT, FHG, INDRA]	EY led the task providing requirements and insights on the technology and developing the full set of smart contracts for all the pilots released for the first phase. Before the development EY analysed different smart contracts frameworks and environments.
T3.4	**Digital identities and node development**	(M4-M36) [TL: POSTEIT, Contributors: EY, GT]	EY has contributed to the creation of identity solutions implemented during the first phase pilots EIDAS compliant.
T3.5	**Back-end and Front-end applications**	(M4-M36) [TL: NETAS, Contributors: POSTEIT, EY, GT]	EY has contributed to the realisation of a common framework for the use-case development. For this first phase, EY developed and deployed the web-application for the banking pilot and contributed to the development of the insurance pilot.
T3.6	**Conformance testing**	(M5-M36) [TL: NETAS, Contributors: EY, GT]	EY completed and co-created initial functionally tests over the 2 developed pilots web-applications where the overall usability was approved and verified.
T3.7	**Linking, mapping and synchronisation**	(M5-M36) [TL: NETAS, Contributors: GT, EY]	EY has contributed to the linking, mapping and synchronisation of the different components namely "Authentication-as-a Service" and "Blockchain as-a-Service" in which the overall sequence was studied and calculated over the first phase.
WP4 Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.1	**Inter-banks data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, EY, NETAS)	EY has contributed to the technical studies focusing on the modelling of inter-banks data flows and information with the BCaaS and the Critical-Chains Main Framework.
T4.2	**Internet banking data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	EY has contributed to the technical studies focusing on the modelling of internet banking data flows and information with the BCaaS and the Critical-Chains Main Framework.
T4.3	**Financial markets infrastructure flows modelling**	(M5-M35) [TL: FHG, Contributors: ERARGE, UREAD, EY, NETAS, UREAD]	EY has contributed to the technical studies focusing on the modelling of financial markets data flows with the BCaaS and the Critical-Chains Main Framework.
WP5 Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	EY has contributed to the definition of the token-based authentication and authentication mechanisms, and the development of the multifactor authentication with SecureSticks and biometrics. In addition, EY created the environment for this component.
T5.1.1	**Multi-lateral biometrics-based access control**	(M5-M35) [Contributors: ERARGE, EY, FHG, POSTEIT]	
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	EY has contributed to the definition of security access policies to configure them on the AUTH-as-a-Service component.
T5.4	**Blockchain-as-a-Service (BCaaS) integrity checking**	(M5-M35) [TL: GT, Contributors: UREAD, EY, FHG, INDRA]	EY has contributed to the deliverable and activities related data-integrity checking part of the GT KSI Blockchain and MIDA technologies and integrated into the BCaaS component led by EY.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	EY has contributed to this task analysing KPIs, user needs and Critical-Chains solutions to develop for the first phase. EY also conducted different questionnaires in order to adapt the strategy to the user needs.
T6.5	**Technology acceptance and best practices**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	EY conducted analysis based on lesson learnt, recommendation and best practices for the application of the Critical-Chains framework in financial contexts. The focus was on framework and components to offer reliability, usability, accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	EY has contributed to the studies and related activities focusing on blockchain, cryptocurrencies and smart contracts standards as well on e-banking, mobile money and insurtech.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	EY has identified the background, foreground and side-ground knowledge that can be benefited throughout the project and potential joint studies mainly with ERARGE, IMEC, UREAD, NETAŞ and JR.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY,	EY has contributed to the identification of communication channels with potential national and international Partners, other EU projects and customers. The company-specific

Task Number	Task Title	List of Contributors	Description of Results Delivered
		ERARGE, FHG, IMEC-NL, INDRA, UREAD]	commercialisation plans have been revisited and joint actions with other Partners have been discussed.

12.5 Partner 5: FHG

WP2: Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	Support of the requirements elicitation and prioritisation. Elicitation of prevention strategies according to the resilience cycle for enhancing the functionality of the Critical-Chains framework.
WP3: Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.2	**Blockchain Integrity Layer**	(M3-M36) [TL: GT, Contributors: NETAS, EY, FHG, INDRA]	The blockchain-as-a-service components have been analysed regarding their impact on the resilience of the whole Critical-Chains network with respect to an initial model.
T3.3	**Secure & Smart contracts development**	(M3-M36) [TL: EY(4), Contributors: GT, FHG, INDRA]	The technical details of safety measures such as passwords have not yet been discussed by the consortium.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.1	**Inter-banks data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, EY, NETAS)	Provision of a Reliability assessment functionality for machine learning-based predictions for detecting anomalous transactions.
T4.2	**Internet banking data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	Provision of a Reliability assessment functionality for machine learning-based predictions for detecting anomalous transactions.
T4.3	**Financial markets infrastructure flows modelling**	(M5-M35) [TL: FHG, Contributors: ERARGE, UREAD, EY, NETAS, UREAD]	Provision of a Reliability assessment functionality for machine learning-based predictions for detecting anomalous transactions.
T4.4	**Profile-based dynamic context-aware flows mining & modelling**	(M5-M35) [TL: ERARGE, Contributors: FHG, UREAD, NETAS]	Provision of a Reliability assessment functionality for machine learning-based predictions for detecting anomalous transactions.
T4.5	**Context-aware anomalous flows alerting & blacklisting**	(M5-M35) [TL: JR, Contributors: UREAD, FHG, NETAS, UREAD]	Deployment of a dense neural network for detecting fraudulent transactions.
WP5: Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	Further development of the simulation tool CaESAR. This was necessary to apply the results of EU project SNOWBALL and this process is planned to be continued throughout the project.
T5.1.1	**Multi-lateral biometrics-based access control**	(M5-M35) [Contributors: ERARGE, EY, FHG, POSTE]	The access control module was analysed regarding its impact on the resilience of the whole Critical-Chains network with respect to an initial model.
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	The authentication and access control module have been analysed regarding their impact on the resilience of the whole Critical-Chains network with respect to an initial model.
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	Vulnerability analysis of the Critical-Chains framework and subcomponents based on its graph structure as well as simulating various attack strategies and formulating mitigation strategies.
T5.2.2	**Threat intelligence, mining, predictive modelling and white-listing**	(M5-M35) [Contributors: CEA, NETAS, FHG, ERARGE RINA-C]	Deployment of a dense neural network for detecting fraudulent transactions.
T5.3	**Hardware-Security-as-a-Service**	(M5-M35) [TL: IMEC-NL, Contributors: ERARGE, FHG, INDRA]	
T5.3.1	**Embedded-systems secure inter-operation framework (LinkSmart) integration**	(M5-M35) [Contributors: ERARGE, FHG]	The contributions were postponed to the second half of the project due to delays in the integration of the components.
T5.3.4	**Security Module (HSM)**	(M5-M35) [Contributors: ERARGE, FHG, INDRA]	Vulnerability analysis of the HSM with reference to its dependencies on the whole Critical-Chains framework.
T5.4	**Blockchain-as-a-Service (BCaaS) integrity checking**	(M5-M35) [TL:GT, Contributors: UREAD, EY, FHG, INDRA]	Vulnerability analysis of the BCaaS regarding its impact on the resilience of the whole Critical-Chains framework.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T5.5	**Crypto-as-a-Service (Cryptaas)**	(M5-M35) [TL:ERARGE, Contributors: FHG]	
T5.5.1	**Symmetric-Asymmetric Cryptography**	(M5-M35) [Contributors: ERARGE, FHG]	The contributions were postponed to the second half of the project due to delays in the integration of the components.
T5.5.2	**Key generation based on truly random number generator**	(M5-M35) [Contributors: ERARGE, FHG]	The contributions were postponed to the second half of the project due to delays in the integration of the components.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	FHG contributed to the evaluation methodology of the secure cyber-framework by performing an ESEA analysis regarding side- and cross-effects of requirements.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA(8), Contributors: ERARGE, CEA, FHG, GT, NETAS, JR, POSTE, RINA-C, UREAD]	FHG supported the review of the studies related to system integration, testing and security.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	Promoting the Critical-Chains project on the Fraunhofer LinkedIn account. Contribution to a scientific publication with JR and UREAD.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	Further enhancement of the FHG simulation tool and analysis regarding the reliability of machine learning-based predictions were used for further proposals and customer activities. The latter is part of a submitted joint publication with JR and UREAD.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	FHG started to use the developed technologies to apply them as a basis for a versatile and robust reliability analysis tool.

12.6 Partner 6: GT

WP3: Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.2	**Blockchain Integrity Layer**	(M3-M36) [TL: GT, Contributors: NETAS, EY, FHG, INDRA]	D3.3. The document describes several technologies that can enhance the Critical-Chains framework to provide secure data-integrity checking. The solution takes the form of a Blockchain-as-a-Service platform component, which will be underpinned by Guardtime Keyless Signature Infrastructure Blockchain technologies. The BCaaS will also receive authentication and access control support from the Authentication-as-a-Service component which is also briefly described in this document. Document input coordination with Partners.
T3.3	**Secure & Smart contracts development**	(M3-M36) [TL: EY(4), Contributors: GT, FHG, INDRA]	GT took part in discussions, finding the optimal solution for integration. Preparing for deployment.
T3.4	**Digital identities and node development**	(M4-M36) [TL: POSTEIT, Contributors: EY, GT]	EIDAS related identity management and integration for token-based identity linking on the platform. Explanations how GT technologies can benefit the system.
T3.5	**Back-end and Front-end applications**	(M4-M36) [TL: NETAS, Contributors: POSTEIT, EY, GT]	Avoiding double front end interfaces, synchronisation of plans.
T3.6	**Conformance testing**	(M5-M36) [TL: NETAS, Contributors: EY, GT]	Test planning, integrity testing cases.
T3.7	**Linking, mapping and synchronisation**	(M5-M36) [TL: NETAS, Contributors: GT, EY]	GT is involved in the integrity protection and have to give needed input to discussions. GT supported the review of the studies related to system blockchain integration and security.
WP5: Cyber-Physical Security			
T5.4	**Blockchain-as-a-Service (BCaaS) integrity checking**	(M5-M35) [TL:GT, Contributors: UREAD, EY, FHG, INDRA]	D5.7. The document describes the technologies that can be used to support the Critical-Chains framework to provide secure, data-integrity checking. This facility is enabled by the incorporation of BCaaS into the Critical-Chains framework, which itself is supported by the Guardtime KSI Blockchain and MIDA technologies. Document input coordination with Partners.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG,	Requirements and pilot's check. Validation scenarios.

Task Number	Task Title	List of Contributors	Description of Results Delivered
		RINA-C, GT, CEA, EY, POSTEIT]	
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	Integration validation. Options for cloud infrastructure analysed. DDOS protection options.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	Analysis of the Azure environment. Preparations for KSI gateway and MIDA installation.
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	Blockchain related privacy aspects explained to Partners. Importance of privacy impact understood.
T6.5	**Technology acceptance and best practice**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	Discussions regarding technology mix and blockchain best practises with Coordinator and Partners.

12.7 Partner 7: IMEC-NL

WP5: Cyber-Physical Security			
T5.3	**Hardware-Security-as-a-Service**	(M5-M35) [TL:IMEC-NL, Contributors: ERARGE, FHG, INDRA]	As task leader and contributor of Task 5.3, we contributed with the development of Secure Distance Bounding based on Time of Flight and contributed to the deliverable D5.5.
T5.3.2	**Tamper–Proofing self-reset**	(M5-M35) [Contributors: IMEC-NL, ERARGE]	For this task IMEC-NL examined Tamper Proofing for the BLE link needed for the Critical-Chains project. For the Critical-Chains project we chose the Secure Distance Bounding based on time of flight mechanism, which prevents for a 'Man in the middle attack'.
T5.3.3	**Secure IC Stick-in-Silicon**	(M5-M35) [Contributors: IMEC-NL, ERARGE]	For this task IMEC-NL integrated our secure Ranging algorithm on an NXP chip/development platform instead of an IMEC BLE chip and is being integrated into the Critical Chains system to prevent a 'man in the middle attack'.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	IMEC actively participating in industry consortia and standardisation bodies such as Bluetooth SIG, IEEE and Car Connectivity Consortium (CCC).
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	IMEC is actively contributing to A-level conferences in wireless communications and circuit design. As part of that we published a paper about our secure distance bounding IP, stated in D7.4.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	IMEC is always looking into the possibility of patenting or publishing our new innovations. As part of that we published a paper about our secure distance bounding IP, stated in D7.4.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	IMEC is planning to investigate options to disseminate results via the typical IMEC business models such as open innovation technology research programs as well as licensing.

12.8 Partner 8: INDRA

WP2: Requirements Engineering & Framework Architecture Specification			
			Management of Indra contributions in the project Attend to project's meetings Lead WP6
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	Contributions to the identification of requirements related to Toll Collection Pilot, their analysis and prioritisation.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	Indra participated in defining use-contexts and defining and prioritising requirements in the targeted Toll Collection domain.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	Indra has contributed with the necessary pilot specific roles for Toll Collection and defined of the Toll Collection system workflows.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T2.1.3	**Regulatory compliance and Accountability-by-Design requirements**	(M1-M27) [Contributors: UREAD, NETAS, GT, INDRA, POSTEIT]	Indra has contributed to the consortium discussions, it has provided feedback and participated in deliverable D2.7.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	Indra led the task and developed a set of use-cases for Toll Collection for the first phase developments. Overall, Indra monitored the studies related the use-cases and Indra defined the test-cases for the Toll Pilot in connection T6.2. Indra interviewed stakeholders related to Toll Collection.
WP3: Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.1	**Developing the Critical-Chains framework architecture**	(M3-M36) [TL:EY, Contributors: INDRA, NETAS]	Indra has contributed to with requirements and feedback to the overall design of the infrastructure models taking into account the specific needs of the Toll Collection Pilot .
T3.2	**Blockchain Integrity Layer**	(M3-M36) [TL: GT, Contributors: NETAS, EY, FHG, INDRA]	Indra has supported Partners in this task by providing feedback and reviewing the documentation.
T3.3	**Secure & Smart contracts development**	(M3-M36) [TL: EY(4), Contributors: GT, FHG, INDRA]	Indra has supported Partners in this task by providing feedback and reviewing the documentation.
WP5: Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view.
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view.
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view.
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view.
T5.3	**Hardware-Security-as-a-Service**	(M5-M35) [TL:IMEC-NL, Contributors: ERARGE, FHG, INDRA]	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view and analysed the possibility to integrate to the Toll Collection Pilot.
T5.3.4	**Security Module (HSM)**	(M5-M35) [Contributors: ERARGE, FHG, INDRA]	Indra was part of the discussions and provided feedback from Toll Collection Pilot points of view.
T5.4	**Blockchain-as-a-Service (BCaaS) integrity checking**	(M5-M35) [TL:GT, Contributors: UREAD, EY, FHG, INDRA]	Indra was part of the consortium discussions and provided feedback from Toll Collection Pilot points of view.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	Indra has led the D6.1 and it has contributed to this task analysing KPIs, users' needs, and Critical-Chains solutions as informed by the WP2 results based on the UI-REF methodology. In addition, Indra has also conducted different questionnaires in order to adapt the strategy to the user needs.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	Indra has led the task and deliverable D6.2. Indra has prepared the Toll Collection Pilot, executed the Tests Cases to validate Phase 1 and carried out the interviews during the pilot.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	Indra has led this task and has stared the analysis to implement the Critical Chains developments in a relevant environment
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	The Indra contribution has been delayed until RP2.
T6.5	**Technology acceptance and best practices**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.1	**Project website and awareness raising material development and updates**	(M1-M36) [TL: NETAS, Contributors: INDRA, RINA-C, POSTEIT]	Indra has promoted Critical –Chains project on the Indra's website.
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	

Task Number	Task Title	List of Contributors	Description of Results Delivered
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	

12.9 Partner 9: JR

T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	JR led two iterations of requirements compilation, analysis & (re)prioritisation, based on UI-REF methodology as reported in D2.3 (Specifications and Architectural Design) and in its update D2.4. JR led content definition and compiling of these two deliverables with domain knowledge based modelling, structuring and requirements indexing guidance from the Coordinator supported by the UI-REF methodological framework. Accordingly JR actively participated in defining use-contexts and defining and prioritising requirements for banking and financial infrastructures pilots. JR led the technology & market watch update reported in D2.1 (Technology & Watch Update) incorporating the competitive strategy models as introduced by the Coordinator; D2.1 has been followed by its update as D2.2. incorporating the updates from 4 channels of stakeholder preferences elicitation to inform the UI-REF-enabled requirements ranking and re-prioritisation as advised by the Coordinator.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	JR contributed to defining of the context-specific security & privacy requirements for the banking and financial infrastructures pilots. JR participated in identifying the relevant domain entities, actors and objects, their characteristics, and the establishing of usage-contexts consistent with the UI-REF methodology. JR participated in prioritising of the requirements, according to UI-REF as advised by the Coordinator. Output of this work is reported in D2.3 and D2.4 4 in the form of a detailed textual description and prioritisation lists.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	JR actively contributed to the definition of the necessary requirements for a secure role-based access mechanism for the Critical-Chains framework, in order to facilitate audit mechanisms with a focus on a banking and financial infrastructures pilot. Outputs of this work are presented in D2.3 and D2.4 in the form of a detailed textual description and prioritisation list.
T2.1.4:	**Technology and market watch updating**	(**M**1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS]	JR led two iterations of technology and market watch updating, as reported in D2.1 (Technology & Watch Update) and in its update, supported by the UI-REF domain knowledge analysis, and competitive strategy modelling as advised by the Coordinator. JR led content definition and compiling of these two deliverables. JR contributed to monitoring and reporting the State-of-the-Art/Market/Practice for cyber-attacks on financial infrastructures and best cyber practices. JR contributed to monitoring and reporting the State-of-the-Art/Market/Practice for AI, machine learning technologies, blacklisting, anomaly detection, flow modelling.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	JR contributed to security-privacy contexts specification and semantic modelling as led by the deliverable responsible (UREAD) and reported in D2.6 (Security/Privacy and Threat semantic model).

Task Number	Task Title	List of Contributors	Description of Results Delivered
			JR contributed to the initial compilation of deliverable D2.6. and subsequently contributed to the review of the UREAD-led interim and final versions. JR contributed with analysis and description of legacy systems in the financial sector. JR contributed to the definition of the cyber-physical security threats ontology as led by UREAD. JR defined the cyber-attacks taxonomy of financial infrastructures. JR contributed to the cyber security threat assumptions and contributed to the adoption of the threat model and risk-severity-ranking of threat sets for two pilots as devised and led by UREAD including the UI-REF-based risks and countermeasures prioritisation calculus and respective templates for threat prioritising, mitigation and result analysis. JR contributed to the specification of the general and Critical-Chains ranked cyber-security threats responsive mitigation techniques and countermeasures needed. JR contributed to the mapping of security countermeasures to Critical-Chains building blocks and requirements within the UI-REF-enabled risks-countermeasures classification framework as devised and led by UREAD. JR investigated the applicability of model-based formal verification tools for parts of the security/privacy specification within the authentication procedure.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	JR contributed to the use-case specification in banking and financial infrastructure domains. JR defined security test-cases for the whole Critical-Chains architecture, based on D6.1 and in connection with the work provided for T6.2; this work is reported in D2.4 and planned for deployment in Phase-2. This is implemented in accordance with all the UI-REF-prioritised use-cases as specified in D6.1.
T2.4	**Critical-Chains framework architecture & integration (re)-specification**	(M1-M36) [TL: EY, Contributors: JR, UREAD, POSTEIT, ERARGE, CEA, GT, INDRA, NETAS]	JR contributed to the system architecture for Critical-Chains for different levels of detail - high-level overview, non-functional overview, functional overview, by working on the initial requirements and use-cases, as a baseline for architecture, reported in D2.4. JR extended this work and its findings in contributing to threat modelling of two pilots' architectures – banking and financial infrastructures reported in D2.6.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.5	**Context-aware anomalous flows alerting & blacklisting**	(M5-M35) [TL: JR, Contributors: UREAD, FHG, NETAS, UREAD]	JR provided contributions to this task as per road map established by UREAD. JR did an extensive literature survey on APT attacks in Fintech domain aspect; this work is published as a review paper in a prestigious journal Computers & Security, Volume 92, May 2020, 101734 (IF=3.579). JR compiled an extensive literature survey on machine learning application for fraud detection in the Fintech domain; this work is reported in D4.1 and is part of a submitted joint journal paper. JR investigated in detail publicly available datasets for Fintech fraud detection and tested three different outlier detection methods on these datasets, resulting in a promising performance scores; additional contributions in collaboration with UREAD were the research and testing of different feature engineering techniques on available datasets, in order to determine influence of features on detection performance, achieving promising results; this

Task Number	Task Title	List of Contributors	Description of Results Delivered
			work is reported in D4.1, and is part of a submitted joint journal paper. JR tested feature engineering and outlier detection methods on the Critical-Chains SEPA transactions dataset; this work is reported in D4.1. JR provided inputs for the Phase-1 FMaaS dashboard.
WP5: Cyber-Physical Security			
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	JR contributed with the Threat Model of the Critical-Chains architecture with regards to the Azure Cloud, the Critical-Chains framework and pilots; this work is reported in D5.3 (Secure Cyber Framework). JR contributed with reporting security recommendations for cloud environment, including network security and vulnerability management and security testing, in D5.3. JR contributed to security and penetration testing with defining platform interaction tests, reported in D5.3. JR carried out an internal review for D5.1 AUTH-as-a-Service (AUTHaaS). JR carried out an internal review for D5.3 Secure Cyber Framework. JR carried out an internal review for D5.7 Blockchain-as-a-Service (BCaaS).
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	JR contributed to this subtask with definition of threat actors. JR contributed to validation and prioritisation of threats with regards to the results of the threat model. JR also contributed to the evaluation of mitigation strategies for the respective threats within the cloud architecture and the Critical-Chains framework. JR work on this subtask is reported in D5.3 (Secure Cyber Framework).
WP6: System Integration & Validation in Various Pilots			
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	JR contributed to this task with the evaluation of the current Critical-Chains framework. JR contributed to D6.2 with description of the Critical-Chains platform. JR defined security test-cases for deployment in Phase-2 in connection with the work provided for T2.3; this work is reported in D2.4
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	JR promoted Critical-Chains in numerous physical and online events, through targeted presentations about project and work performed in the project. JR was also extensively engaged in clustering activities, talks and meetings with stakeholders from industry, academia and policy makers. JR organised a joint online event with the Austrian members (Joanneum Research, Rise, WU - Vienna University of Economics and Business, UNI Graz, Silicon Alps Cluster) of ongoing Fintech projects (Critical-Chains, SOTER, Fintech) on November 27th, 2020, and presented work from WP2. JR promoted Critical-Chains on its electronic channels, including LinkedIn, Twitter and JR web site, on several occasions, including Critical-Chains promotional video and news and announcements of events organised/co-organised by Critical-Chains. JR promoted Critical-Chains by displaying a project rollup poster at one physical event and several online events as background. JR carried out an internal review for D7.6 Gap analysis of current relevant standards.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	JR published work from WP2 in a review paper in a prestigious journal Computers & Security, Volume 92, May 2020, 101734 (IF=3.579) - *APT datasets and attack modelling for automated detection methods: A review*. JR submitted work and results from WP4 in a joint journal paper with UREAD and FHG - *Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications*. JR published a preprint and plans submission of a joint journal paper with UREAD with results from WP2 - *Cyber-Attack Taxonomy of Distributed Ledger- and Legacy Systems-based Financial Infrastructures*.
12.10 Partner 10: NETAS			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	NETAS focused on the technical requirements related to overall cloud infrastructure, security of the infrastructure and the service-based architecture. NETAS contributed to prioritisation methodology offered by the Coordinator and conducted the requirement engineering studies in collaboration with other Partners.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	NETAS focused on the GDPR requirements and the security-privacy requirements by explicating the relevant compliance requirements according to the Turkish Data Protection Requirements(KVKK) in relation with Fintech-context user-intimate approach in the sense of planned technologies. Especially focused on the blockchain technology.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	NETAS focused on the Secure Cyber Framework and Flow modelling-as-a-Service points to define overall audit mechanism in the X-as-a-Service specific needs. NETAS also focused on blockchain node security requirements needed for the overall infrastructure security.
T2.1.3	**Regulatory compliance and Accountability-by-Design requirements**	(M1-M27) [Contributors: UREAD, NETAS, GT, INDRA, POSTEIT]	NETAS focused on the regulatory aspects of the Blockchain technology, and user tracking in the system which further allowed NETAS to create the design requirements of the Secure Cyber Framework and Main Framework. The technical ground established considering the overall compliance.
T2.1.4:	**Technology and market watch updating**	**(M**1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS]	NETAS focused on the Fintech market Pull-Push forces in terms of the compliant globalisation and scalable environments for the financial industry. Moreover, NETAS focused on the Cloud and Blockchain related products, their market analysis and the SOTA updates in line with the project scope.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	NETAS contributed to the preparation of the Cyber-Physical security and privacy and threats ontologies, overall system specification and requirements prioritisation.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	NETAS has monitored the studies related to the use-cases and identified the system specification of Fintech cases, blockchain tools, cloud services and their service-based architectures.
T2.4	**Critical-Chains framework architecture & integration (re)-specification**	(M1-M36) TL: EY(4), Contributors: ERARGE(1), CEA(1), GT(1), JR(7), INDRA(1), NETAS(1), POSTE (2), UREAD(2)]	NETAS contributed to the overall design of the Critical-Chains architecture by interpreting the results of the requirements and specifications determined within T2.1-3, T2.4. Moreover, NETAS created an evaluation report for the comparison between on house infrastructure and Cloud Service Provider "Azure" for the Critical-Chains Framework architecture.
WP3: Blockchain Core Development & Solution Stack			
Adaptation for Use- Cases			
T3.1	**Developing the Critical-Chains framework architecture**	(M3-M36) [TL: EY, Contributors: INDRA, NETAS]	NETAS has interpreted Critical-Chains components in order to create a fully integrative and scalable infrastructure. The overall design respected the state-of-the-art infrastructure models in which it supports the micro-service and container-based applications and modules to be run with high availability. Therefore, the related elements and serverless services have been adapted into the Main Framework and entry-level deployment of the components was started. Moreover, NETAS contributed to the deployment of the

Task Number	Task Title	List of Contributors	Description of Results Delivered
			Critical-Chains standalone Main Framework. Finally, NETAS established and led the deliverable for this particular task.
T3.2	**Blockchain Integrity Layer**	(M3-M36) [TL: GT, Contributors: NETAS, EY, FHG, INDRA]	NETAS has contributed to the overall integration matters of the Integrity layer and specifically studied the integration and harmonisation of the selected Blockchain Network "Quorum" and GTs "KSI" blockchain in the cloud infrastructure.
T3.5	**Back-end and Front-end applications**	(M4-M36) [TL: NETAS, Contributors: POSTEIT, EY, GT]	NETAS has monitored the overall use-case development and the requirements closely to create the Critical-Chains blockchain based web-applications. For this first phase, NETAS developed and deployed two different web-applications as a standalone with the components required for the overall usage context. NETAS led the successful deployment of the blockchain-based Critical-Chains pilots' first phase functionality. Moreover, NETAS contributed to shifting the conventional backend to blockchain-based smart-contracted business logics. Finally, NETAS established and led the deliverable for this particular task.
T3.6	**Conformance testing**	(M5-M36) [TL: NETAS, Contributors: EY, GT]	NETAS has complete initial functionally tests over the 4 developed pilots web-applications. Therefore, the overall usability was approved and verified. Moreover, NETAS started to record the outputs of user-intimate usability tests over the web-applications.
T3.7	**Linking, mapping and synchronisation**	(M5-M36) [TL: NETAS, Contributors: GT, EY]	NETAS has contributed to the linking, mapping and synchronisation of the different components namely "Authentication-as-a Service" and "Blockchain as-a-Service" in which the overall sequence was studied and calculated over the first phase. Moreover, the initial linking and synchronisation was completed in the standalone cloud environment of NETAS for the Critical-Chains pilot applications.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.1	**Inter-banks data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, EY, NETAS)	NETAS has contributed to the technical studies and focused on the understanding of the inter-banks data flows and harmonization of the data flow with the Blockchain-as-a-Service and Main Framework for the future integration.
T4.2	**Internet banking data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	NETAS has contributed to the technical studies and focused on the understanding of the Internet banking data flows and harmonisation of the data flow with the blockchain-as-a-Service and Main Framework for the future integration.
T4.3	**Financial markets infrastructure flows modelling**	(M5-M35) [TL: FHG, Contributors: ERARGE, UREAD, EY, NETAS, UREAD]	NETAS has contributed to the technical studies and focused on the understanding of the Financial markets data flows and harmonisation of the data flow with the blockchain-as-a-Service and Main Framework for the future integration.
T4.4	**Profile-based dynamic context-aware flows mining & modelling**	(M5-M35) [TL: ERARGE, Contributors: FHG, UREAD, NETAS]	NETAS has worked on the detection of the anomalies in the Authentication-as-a-Service layer within the context of Task 5.2. In this task NETAS has contributed to the studies related to the malicious user identification in the various the data flows. Moreover, NETAS has introduced a holistic mechanism for the detection of the Anomalies in Authentication layer and identification of the Anomalies occurring in that layer in the sense of this task. On the other hand, NETAS has provided the Blockchain-based unique identifier model for the Critical-Chains usage context to further support the privacy preserving system.
T4.5	**Context-aware anomalous flows alerting & blacklisting**	(M5-M35) [TL: JR, Contributors: UREAD, FHG, NETAS, UREAD]	NETAS has proposed a X-as-a-Service-enabled dash-boarded platform for the harmonisation of the various detection algorithms (over data flows) consistent with the functionality of malicious user identification and blacklisting and whitelisting mechanisms to be integrated with the Authentication-as-a-Service. Accordingly NETAS created some initial dashboards for the Flow Modelling-as-a-Service and Authentication Anomaly Detection module to support the above objectives.
WP5: Cyber-Physical Security			

Task Number	Task Title	List of Contributors	Description of Results Delivered
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	NETAS focused on the "risk-based approach" for the overall cyber security of the Critical-Chains framework. This task is led by NETAS and is made up of two subtasks. Moreover, NETAS has led the deliverable of this task in general.
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	NETAS has introduced the overall "risk-based approach" and list of identification methods for assessment of the threats, vulnerability and risks for the cloud environment, authentication layer, blockchain layer and network layer. Then, NETAS led to the identification of the possible measures to protect against the identified vulnerabilities, threats and risk. Moreover, NETAS set out the structure of the deliverable to result from this particular task. On the other hand, NETAS established a penetration and security checklist to be followed in the second phase of the Critical-Chains project.
T5.2.2	**Threat intelligence, mining, predictive modelling and whitelisting**	(M5-M35) [Contributors: CEA, NETAS, FHG, ERARGE RINA-C]	In this task, NETAS has led the way to establish threat intelligence and predictive modelling in two important infrastructure layers; Network and Application layers of the cloud environments. Accordingly, NETAS successfully deployed the Authentication Anomaly Detection module with a very high detection ratio in a secured environment as a standalone module. The module development aligned with the actual Authentication provider of the Critical-Chains (T5.1 Keycloak) in which this progress made the integration preparations much faster than anticipated. Moreover, two important plug-ins were developed for the Keycloak, namely: 1) The custom listening plug-in to further support the integration to the other ICT projects. 2) Additional events to listen over the Keycloak server. These were achievements in which these two could be publicly disseminated as a contribution of the Critical-Chains consortium to the open-source world. Moreover, NETAS has contributed to Task 4.4 and Task 4.5 in line with this task.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	NETAS has led this task in which, NETAS firstly adapted the UI-REF methodology (Methodology used in Critical-Chains) with the support of the project Coordinator. Afterwards NETAS introduced the use-case interpretation strategy to better understand the user needs in line with the Critical-Chains technical and practical needs. Afterwards, NETAS led in creating the Component Behaviour diagram to analyse the effects, side-effect, cross-effects and effects of the components to humans. Accordingly, NETAS has established the KPIs of the project with the support of the other contributors and then further analysed in the usage-scenarios. Finally, NETAS developed the deliverable structure.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, NETAS, UREAD, GT, POSTEIT, RINA-C, ERARGE]	NETAS contributed to the review of the studies related to the use-cases and identified the integration strategy of services (Web Services) and components (Web-Applications & AuthaaS & BCaaS for the first phase) within the Critical-Chains ecosystem.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	NETAS has demonstrated the functionality of the Critical-Chains Pilot web-applications, the Main Framework functionality, and Authentication Anomaly Detection module as standalone applications which have been readied for phase 2 early integration.
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	NETAS focused on the GDPR and KVKK (Turkish law similar to GDPR) comparison and the privacy preservation techniques, especially related to the user traceability in the framework. Moreover, proposed a blockchain-based unique user identifier model for Critical-Chains.
T6.5	**Technology acceptance and best practices**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	The user stories and the stakeholder reviews have been elaborated as a preparatory work to identify the hypotheses of the Technology Acceptance Model with the contributions of the other Partners.

Task Number	Task Title	List of Contributors	Description of Results Delivered
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.1	**Project website and awareness raising material development and updates**	(M1-M36) [TL: NETAS, Contributors: INDRA, RINA-C, POSTEIT]	NETAS has led this task with the support of the Dissemination manager (RINA) who contributed to the e-material preparation for the dissemination of the Critical-Chains project over the web. Moreover, NETAS encouraged other consortium Partners to share the prepared materials in their channels to maximise the impact.
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	NETAS has contributed to the task with the constant support the dissemination manager (RINA) by establishing project poster, creating news about the public deliverables, publishing Critical-Chains achievements in the NETAS social media channels and internal network in Turkey. Moreover, NETAS supported the project Coordinator in the establishment of the joint paper.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	NETAS has identified the background, foreground and side-ground knowledge that can be of benefit throughout the project and potential joint studies mainly with IMEC, UREAD, ERARGE, EY and JR.

12.11 Partner 11: POSTEIT

WP2: Requirements Engineering & Framework Architecture Specification			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	POSTEIT actively participated in defining use-contexts and defining and prioritising requirements for banking and financial infrastructure pilots as a practitioner. POSTEIT actively contributed to the technology & market watch update reported in D2.1 (Technology & Watch Update) and in its update D2.2.
T2.1.1	**Context-specific security-privacy protection requirements elicitation**	(M1-M18) [Contributors: JR, UREAD, EY, NETAS, POSTEIT, ERARGE, CEA, FHG, GT, INDRA]	POSTEIT actively participated in defining use-contexts and defining and prioritising security-privacy protection requirements in the targeted Financial Infrastructure and Banking domain in consideration of the main European regulations (e.g. NIS directive and CI protection). Outputs of this work are presented in D2.3 and D2.4.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	POSTEIT actively contributed to definition of necessary pilot specific roles for the Financial Infrastructure and Banking Pilot. Outputs of this work are presented in D2.3 and D2.4.
T2.1.3	**Regulatory compliance and Accountability-by-Design requirements**	(M1-M27) [Contributors: UREAD, NETAS, GT, INDRA, POSTEIT]	POSTEIT actively contributed to the definition of regulatory context by describing existing and emerging regulations (e.g. PSD2, PCI/DSS) on national and European levels that can affect systems which will be equipped with Critical Chains Technology. Outputs of this work are presented in D2.7.
T2.1.4:	**Technology and market watch updating**	(M1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS]	POSTEIT contributed to update the reporting of the State-of-the-Art/Market/Practice on financial and banking domain. Outputs of this work are presented in D2.1 and D2.2.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	POSTEIT contributed to the definition of semantic models for all Banking and Financial Infrastructures use-cases. POSTEIT contributed to the definition of ontology and taxonomy for Financial and Banking domain. POSTEIT defined the threat modelling for financial and insurance domain and contributed for the banking one including adapted threat template, threat prioritising, mitigation and result analysis. POSTEIT contributed to the privacy threat analysis for banking domain. POSTEIT defined a threat catalogue for financial and insurance domain.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	POSTEIT contributed to the use-case specification in banking and financial infrastructure domains. POSTEIT defined security test-cases for Financial Infrastructure and Banking pilot, in connection with the work provided for T6.2; this work is reported in D2.4 and planned for deployment in Phase-2. POSTEIT interviewed stakeholders related to financial and banking domain.
WP3: Blockchain Core Development & Solution Stack Adaptation for Use- Cases			
T3.4	**Digital identities and node development**	(M4-M36) [TL: POSTEIT, Contributors: EY, GT]	POSTEIT led this task in which a first set of Smart Contracts (e.g. Ethereum Smart Contracts) were developed. Outputs of this work are presented in D3.7.
T3.5	**Back-end and Front-end applications**	(M4-M36) [TL: NETAS, Contributors: POSTEIT, EY, GT]	POSTEIT developed a front-end and back-end application for the Financial Infrastructure pilot and contributed to the design of back-end and front-end applications for the Banking pilot. Outputs of this work are presented in D3.9.
WP4: Data Streams Transmission Security-Privacy Protection Inter & Internet Banking and Insurance			
T4.2	**Internet banking data flows & information modelling**	(M5-M35) [TL: UREAD, Contributors: ERARGE, FHG, POSTEIT, EY NETAS]	POSTEIT performed a state-of-the-art of synthetic data generation and open dataset survey in order to identify existing financial datasets and tools for generate synthetic data. POSTEIT developed a tool based on the Trumania framework in order to generate an extended dataset of banking transactions simulating the activity of 10,000 banking users for one year. Additionally POSTEIT generated a separated dataset of anomalous transactions based on set of rules and predefined distribution (SEPA 1.7). This was delivered with the active data modelling and knowledge engineering based advice as provided by UREAD. To summarise: - a set of 10 different scenarios well developed in order to manage different types of financial transactions (see annex I – D4.1); - a set of two populations (users and defrauders) and three different activity profiles were defined; - finally, a set of timer profiles were implemented in order to define activities of populations according to some plausible logics; Outputs of this work are presented in D4.1.
WP5: Cyber-Physical Security5 Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	POSTEIT actively contributed to the definition of the technological architecture of the AUTH-as-a-Service component and developed an extension for the integration into the Italian digital identity provider (SPID). POSTEIT contributed to define the security access policies and configure them on the AUTH-as-a-Service component. Outputs of this work are presented in D5.1.
T5.1.1	**Multi-lateral biometrics-based access control**	(M5-M35) [Contributors: ERARGE, EY, FHG, POSTEIT]	
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	POSTEIT contributed to define the security access policies and configure them on the AUTH-as-a-Service component. Outputs of this work are presented in D5.1.
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA,	POSTEIT performed a list of security recommendations related to threats due to the use of cloud environments.

Task Number	Task Title	List of Contributors	Description of Results Delivered
		POSTEIT ERARGE, RINA-C, INDRA, JR]	POSTEIT contributed to the review of the document D5.3. Outputs of this work are presented in D5.3.
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	POSTEIT performed a list of security recommendations related to threats due to the use of cloud environments. POSTEIT contributed to the review of the document D5.3. Outputs of this work are presented in D5.3.
WP6: System Integration & Validation in Various Pilots			
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	POSTEIT contributed to set up the Critical-Chains assessment framework, which satisfies a set of basic needs for the banking and financial sector intending to investigate the adoption of Critical-Chains solutions. POSTEIT contributed to define a baseline for a KPI assessment framework and methodology. POSTEIT conducted a set of interviews with target stakeholders of financial domain. Outputs of this work are presented in D6.1.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	POSTEIT defined and realised Phase 1 of the Financial Infrastructure Pilot and contributed to the definition of Phase 1 of the Banking Pilot. Outputs of this work are presented in D6.1.
T6.3	**Demonstration in relevant environment configuration, maintenance and evaluation of trials**	(M10-M36) [TL: INDRA, Contributors: NETAS, POSTEIT, UREAD, ERARGE, GT]	POSTEIT defined and executed test-case for the Phase 1 of the Financial Infrastructure Pilot and gathered feedbacks from testers through questionnaires. Outputs of this work are presented in D6.1.
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	Contributed to this deliverable from the perspective of the Financial Services operational Delivery Context.
T6.5	**Technology acceptance and best practices**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	Contributed to this deliverable from the perspective of the Financial Services operational Delivery Context.
WP7: Dissemination, Standardisation, Exploitation and Innovation Management			
T7.1	Project website and awareness raising material development and updates	(M1-M36) [TL:NETAS, Contributors: INDRA, RINA-C, POSTEIT]	POSTEIT contributed to the implementation of the communication strategy described in D7.1 through the use of its website and participation in workshops. Outputs of this work are presented in D7.1.
T7.3	**User awareness raising and scientific & technical disseminations**	(M1-M36) [TL: UREAD, Contributors: FHG, POSTEIT, ERARGE, IMEC-NL, JR, NETAS]	POSTEIT led contributions to D7.4 by coordinating the activities of collection of material provided by the Partners to be included for the analysis relating to: - logo design and branding messaging; - social media activities; - clustering efforts; - stakeholder awareness; - stakeholder group forming; - scientific and technical publications; - project-to-policy engagement. Outputs of this work are presented in D7.4.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	POSTEIT actively contributed to the definition of the table of content for D7.8. POSTEIT attended regular meeting related to WP7 and prepared constant updates with respect to the task.

Task Number	Task Title	List of Contributors	Description of Results Delivered
12.12 Partner 12: RINA-C			
T2.1	**Overall requirements compilation, analysis & (re)prioritisation**	(M1-M27) [TL: JR, Contributors: RINA-C, POSTEIT, NETAS, UREAD, ERARGE, INDRA, CEA, EY, GT, FHG]	Conducted stakeholder interview for requirements identification. For auditing tasks, RINA-C implemented a methodology to map, trace and manage regulatory aspects on engineering requirements.
T2.1.2	**Workflow embedded secure role-based access & audit requirements**	(M1-M27) [Contributors: JR, RINA-C, POSTEIT, UREAD, ERARGE, CEA, INDRA, NETAS, POSTEIT]	Design and first implementation of audit templates inside RINA-C solution to be used in the design of the audit log.
T2.1.3	**Regulatory compliance and Accountability-by-Design requirements**	(M1-M27) [Contributors: UREAD, NETAS, GT, INDRA, POSTEIT]	As leader of the D2.7 *Regulatory compliance and Accountability-by-*Design model, RINA-C proposed the contents, the topics and built the methodology to be followed including the Coordinator's contributions. Two main aspects were tackled: the identification of technical requirements responsive to applicable regulatory frameworks, and the implied accountabilities (responsibilities and roles) with respect to each such legislation and highlighting commonalities. RINA-C has contributed by dealing with GDPR and NIS regulations (in terms of both technical requirements and implied accountabilities), and regulatory requirements for cloud security. Moreover, on the basis of the principles about the accountability analysed in the deliverable, RINA-C has elaborated the RACI matrix where each phase of a project (involving the definition of processes, the design, implementation, testing, and other phases of product development) is the responsibility of specific entities.
T2.1.4	**Technology and market watch updating**	(M1-M27) [Contributors: RINA-C, POSTEIT, ERARGE, JR, NETAS]	RINA-C contributed to D2.1 and D2.2 describing what an audit process is and its relationship to the Deming cycle (based on PDCA - Plan Do Check Act). In addition, the focus was placed on compliance audits and the importance of performing audit in the financial field where it is necessary to comply with various standards and regulations was highlighted. RINA-C also contributed to outline the state of the art for technological solutions that support the audit and compliance assessment. Critical and technical review of D2.1 and D2.2.
T2.2	**Security-Privacy contexts specification and semantic modelling**	(M1-M18) [TL: JR, Contributors: POSTEIT, UREAD, ERARGE, CEA, NETAS, RINA-C]	In the context of D2.6 RINA-C revised the structure of Privacy-Context Ontology ePrivacy Protection Compliance Ontology. Then an audit of the developed ontology (based on security-privacy contexts specification) was undertaken by way of a specific checklist.
T2.3	**Use-cases and test-cases specification**	(M1-M36) [TL: INDRA, Contributors: JR, EY, POSTEIT, ERARGE, NETAS, RINA-C, UREAD]	In alignment with T2.1 and T6.1, RINA-C built a methodology to correlate requirements with the test-cases in order to evaluate its coverage in relation to regulatory and compliance aspects.
WP5 Cyber-Physical Security			
T5.1	**AUTH-as-a-Service (AUTHaaS)**	(M5-M35) [TL: CEA, Contributors: FHG, ERARGE, EY, POSTEIT, RINA-C, INDRA]	RINA-C has analysed the development activities of the AUTHaaS component in terms of compliance with relevant directives, namely NIS, GDPR, PSD2, and AML5.
T5.1.2	**Role-based access control and authentication device integration**	(M5-M35) [Contributors: CEA, RINA-C, FHG, ERARGE, EY, POSTEIT, INDRA)	Based on the performed analysis, design recommendations that could be addressed during the first development phase of the component were given.
T5.2	**Secure Cyber Framework**	(M5-M35) [TL: NETAS, Contributors: FHG, CEA, POSTEIT ERARGE, RINA-C, INDRA, JR]	RINA-C reviewed the initial stage of the cyber framework, reflected in the D5.3 structure and in the final stage, by undertaking a technical review of the entire document.

Task Number	Task Title	List of Contributors	Description of Results Delivered
T5.2.1	**Threats, vulnerability and risks assessment**	(M5-M35) [Contributors: FHG, POSTEIT, NETAS, ERARGE, INDRA, JR, RINA-C]	RINA-C reviewed the coverage of threats, vulnerability and risk assessment and provided recommendations to solution providers as to how to properly position the Critical-Chains perimeter with respect to the external (security) environment.
T5.2.2	**Threat intelligence, mining, predictive modelling and white-listing**	(M5-M35) [Contributors: CEA, NETAS, FHG, ERARGE RINA-C]	RINA-C reviewed the methodologies and solutions dealt with Threat intelligence, mining, predictive modelling and white-listing and provided recommendations to solution providers as to how to better address them.
T6.1	**Evaluation methodology and validation scenarios specification**	(M1-M9) [TL: NETAS, Contributors: INDRA, FHG, RINA-C, GTCEA, EY, POSTEIT]	RINA-C gave support in the definition of Behaviour Diagrams and advised the consortium on how to create them and the project framework to be used. RINA-C made an analysis of the use-cases and the definition of metrics and key performance indicators. RINA -C provided a guideline regarding the KPI Evaluation Process and example of KPI evaluation. RINA-C carefully revised and re-elaborated the table of contents D6.1. RINA-C has described in D6.1 the Audit and Compliance Assessment Process to determine the level of compliance with certain regulations of the Critical Chains Framework and its components in the design and development phase.
T6.2	**System integration, testing and security examination**	(M10-M36) [TL: INDRA, Contributors: JR, CEA, UREAD, GT, POSTEIT, RINA-C, ERARGE]	RINA-C provided an independent evaluation and support to project solution provider to properly address the design of Critical-Chains building blocks in guaranteeing compliance with NIS, GDPR, PSD2 and AML/4 EU directives.
T6.4	**Privacy impact assessment**	(M13-M33) [TL: RINA-C, Contributors: NETAS, ERARGE, GT, INDRA, POSTEIT]	RINA-C worked on the Data Protection and Privacy Impact Assessment (DPIA), by analysing the project target scenarios and use-cases.
T6.5	**Technology acceptance and best practices**	(M28-M34) [TL: ERARGE, Contributors: POSTEIT, EY, GT, INDRA, NETAS, RINA-C]	Not applicable in the current period.
T7.1	**Project website and awareness raising material development and updates**	(M1-M36) [TL:NETAS, Contributors: INDRA, RINA-C, POSTEIT]	RINA-C is managing the Critical-Chains social media accounts (Twitter and LinkedIn) and sharing news/updates. RINA-C produced the promotional material as the brochure, poster, promotional video and a power point project presentation. RINA-C uses RINA company social media accounts and website for sharing Critical-Chains promotional video and other news in order to raise awareness and visibility about project. RINA-C is assisting the Coordinator and other Partners in preparing presentation for events/conferences/workshop.
T7.2	**Sector engagement, outreach, clustering and standardisation activities**	(M1-M36) [TL: RINA-C, Contributors: CEA, EY, ERARGE, IMEC-NL, INDRA, JR]	RINA-C has developed the Critical-Chains communication, dissemination and engagement strategy, that is based on the creation and distribution of valuable, relevant and consistent content to attract and retain a clearly defined audience, as built and reported in D7.1. A dissemination implementation strategy was produced, based on the below four objectives: - Strengthening the link to other H2020 peer projects; - Increased robustness of Critical-Chains innovations and results; - Strengthening project positioning in the Research Community; - Making the project "warmer" by dynamically using communication channels; In this sense, RINA-C engaged new stakeholders from industry and R&D EU network (i.e. SDX, cyberwatching.eu, Ub Technology, etc.).

Task Number	Task Title	List of Contributors	Description of Results Delivered
			RINA-C co-organised together with UREAD and hosted the collaborative webinar *"Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop"* as a series of joint workshop in the financial domain. RINA C keeps tracking all the performed communication and dissemination activities through elaborated specific communication and dissemination tracking file for the project. RINA-C elaborated the D7.4 and contributed to the report. In particular RINA-C took built the methodology and cared the assessment of the social media activity carried out by evaluating proper key performance indicators. RINA-C made an inventory of existing standards and regulations relevant to the Critical-Chains project in the Audit/certification for cybersecurity and privacy field and analysed the lack of standards for Blockchain and AI. RNA – C reviewed and organized the structure of D7.6 and ensured the alignment among regulatory and compliance aspects dealt in the project with gap analysis of current standards.
T7.4	**IPR & innovation management**	(M1-M36) [TL: EY, Contributors: RINA-C, NETAS, ERARGE, FHG, IMEC-NL, POSTEIT]	RINA C built and proposed a methodology to deal with business modelling, IPR and innovation models and identified the key aspects reflected in D7.8 structure.
T7.5	**Business modelling for X-as-a-Service and exploitation planning**	(M1-M36) [TL: RINA-C, Contributors: POSTEIT, EY, ERARGE, FHG, IMEC-NL, INDRA, UREAD]	RINA C built and proposed a methodology to structure exploitation topic reflected in D7.8 structure.

13. Partner-Specific Financial Statements: Staffing & Travel Costs

13.1 UREAD Financial Statement Tables

13.1.1 UREAD Person-Months Deployed

Staff Name	PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
BADII Atta	9.38	5.65	1.20	0	1.15	0.31	0.42	.65	8
Elliot Jordan	15	2.50	6.40	0	2.10	1.80	1.50	.70	0
Maheshkumar Sundaram	4	0	0	0	3.70	0	0	.30	0
Giuseppe Di Fatta	2.54	2.54	0	0	0	0	0	0	0
Joel Runevic	0.73	0	0	0	0.73	0	0	0	0
Total	**31.65**	**10.69**	**7.60**	**0**	**7.68**	**2.11**	**1.92**	**1.5**	**0**

13.1.2 UREAD Travel & Events Costs

Contributor's Name of Participant(s)	Engagement Events Date and Location	Reason & Contribution actually made	Costs(€)
Dr Julian Stubbe Member of the EAB	Travel (Berlin-Reading) to attend the Kick-off meeting at the University of Reading 10-11/07/2019.	Provided a tutorial on the ethical compliance aspects of the project as a whole and social acceptability criteria in technology innovation, tickets.	374.41
Prof. Atta Badii	Travel to (Reading-Istanbul) to attend Horizon 2020 Security innovation event 04/07/2019.	Dissemination of Critical Chain project objectives and sharing insights, tickets.	183.77
Prof. Atta Badii	Travel (Reading -Brussels) Security Research Info Day and Project-to-Policy kick-off meeting.	Dissemination of Critical Chain project objectives and sharing early findings re Financial sector security and regulatory requirements, tickets.	616.15

Contributor's Name of Participant(s)	Engagement Events Date and Location	Reason & Contribution actually made	Costs(€)
Critical-Chains Consortium	Two-day Project Kick-off Meeting & Ethics Workshop 10-11/07/2019.	WP tasks discussion and implementation planning pls Ethics and requirements Engineering Tutorials (Stubbe, Badii), catering for the meeting (tea /coffee and buffet lunch) over two days; 18 delegates.	567.23
Dr Julian Stubbe, Professor Badii, Dr Giuseppe DI-Fatta, Mr Daniel Szabo	Working dinner to plan and the Ethics Tutorial.	Discussed and finalised the content of the workshop presentations, dinner cost.	109.58
Critical-Chains Consortium	Project management meeting, University of Reading 16/12/2019.	WP-specific progress verification and deliverables make-ready consolidation planning, catering costs.	392.32
Critical-Chains Consortium	Project management meeting, University of Reading 16/12/2019.	WP-specific Progress verification and deliverables make-ready consolidation planning, catering costs.	490.40
Total			**2733.86**

13.1.3 UREAD Other Costs

Date	Items	Costs (€)
02/10/2019	Bank charges for Partner payment transfers.	174.74
05/03/2020	Laptop and extended storage for data synthesis.	1831.72
Total		**2006.46**

13.2 CEA Financial Statement Tables

13.2.1 CEA Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Nouha Oualha	10.06	0.23	0.62	0	0	8.21	1	0	0
Baptiste Polve	10.09	0	0.67	0	0	8.46	0.96	0	0
Romain Farel	2.96	0	1.05	0	0	0.97	0	0.94	0
Antoine Vialle	1.33	0.18	0.62	0	0	0.53	0	0	0
Christophe Janneteau	0.69	0.2	0.2	0	0	0.29	0	0	0
Total	**25.13**	**0.61**	**3.16**	**0**	**0**	**18.46**	**1.96**	**0.94**	**0**

13.2.2 CEA Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
Nouha Oualha	Kick-off meeting 11 -12 July 2019.	Presentation of CEA contributions in the project and WP5 objectives.	419.45
Nouha Oualha	Project Steering Meeting 16th December 2019.	Presentation of WP5 activities.	679.18
Nouha Oualha	Ethics of Blockchain Workshop 17th December 2019.	Participation to the workshop as CEA representative.	
Total			**1098.63**

13.3 ERARGE Financial Statement Tables

13.3.1 ERARGE Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Salih ERGÜN	12		2			8	1	1	0

Salih Halit ERGÜN	16		3		3	8	1	1	0
Alper KANAK	6	0.5	2		3.5				0
Ünal Ergün	2	1				1			0
Total	**36**	**1.5**	**7**		**6.5**	**17**	**2**	**2**	**0**

13.3.2 ERARGE Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
ERARGE (Alper Kanak)	Kick-off meeting 11 -12 July 2019.	Project kick-off, revisiting of project objectives, KPIs and action re-planning.	835.83
ERARGE (Alper Kanak)	Project Steering Meeting 16th December 2019.	Project progress monitoring. Presentation of "Ethical Discussion on Blockchain-based Accountability for Secure and Collaborative Digital Twin Environments – Case Studies".	1228.54
ERARGE (Alper Kanak)	Ethics of Blockchain Workshop 17th December 2017.		
ERARGE (Alper Kanak)	3rd Webinar 'Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop'.	Joint Presentation of "Authentication & Accountability Models in Financial Flows" with UREAD with a specific focus on hardware-based security achievements within the first phase of Critical-Chains.	0.00
ERARGE (Salih Ergün)	ISICAS 29-30 August 2020 (International Symposium on Integrated Circuits and Systems).	Conference paper presentation. One of the RNG designs of the HwSaaS module developed for Critical-Chains was presented at this conference. A Reconfigurable Random Number Generator Based on the Transient Effects of Ring Oscillator was demonstrated. The relationship between the project and the publication was explained to the participants.	315.11
ERARGE (Salih Ergün)	ICHMS 7-9 September 2020 (IEEE International Conference on Human-Machine Systems).	Conference paper presentation. Raised strong attention on the hardware-based security schemes in IoT and blockchain environments. Critical-Chains project was introduced. Potential uses for the Fintech industry were explained.	445.95
ERARGE (Salih Ergün)	MWSCAS 4-7 August 2019 (Midwest Symposium on Circuits and Systems)	Conference paper presentation. Raised strong attention on the use truly random number generation, cryptographic solutions and their applications in Fintech. Critical-Chains project was introduced. Potential uses for the Fintech industry was explained.	2674.62
ERARGE (Salih Ergün)	ISICAS 29-30 August 2019 (International Symposium on Integrated Circuits and Systems).	Conference paper presentation. One of the RNG designs of the HwSaaS module developed for Critical-Chains was presented in this conference. Random Number Generators Based on Irregular Sampling and Fibonacci–Galois Ring Oscillators were demonstrated. The relationship between the project and the publication was explained to the participants.	1411.48
ERARGE (Salih Ergün)	APPCAS 11-14 November 2019 (IEEE Asia-Pacific Conference on Circuits and Systems).	[2100,98 €] Conference paper presentation. A paper comparing the candidate RNGs for the use of HwSaaS was presented. Critical-Chains project was introduced.	2100.98
ERARGE (Salih Ergün)	AsianHOST 16-17 December 2019 (Asian Hardware Oriented Security and Trust Symposium).	Conference paper presentation. Raised strong attention on the microcomputer-based RNG's vulnerabilities. Critical-Chains project was introduced.	453.43
ERARGE (Salih Ergün)	SMC 2019 6-9 October (EEE International Conference on Systems, Man and Cybernetics).	Conference paper presentation. Raised strong attention on block-chain based accountability modes and its usage on digital twin concept. Critical-Chains project was introduced.	1458.76
ERARGE (Salih Ergün)	Blackhat 2019 3-8 August.	Presentation of Critical-Chains project to BlackHat participants was the reason. Cyber (software) security issues were generally on the agenda at the BlackHat event. By attending this event, the importance of cyber-	500.72

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
		physical security was emphasised. As ERARGE, the work to be done within the scope of the project in terms of cyber physical security was shared with the participants.	
ERARGE (Salih Ergün)	APPCAS 8-9 December 2020 (IEEE Asia-Pacific Conference on Circuits and Systems).	Conference paper presentation. The paper proposes skew-tent map and its chaotic sampling as candidate RNGs for the use of HwSaaS was presented. Critical-Chains project was introduced.	168.32
Total			**11593.74**

13.3.3 ERARGE Other Costs

Description and supplier name if applicable	Costs(€)
PCB design, circuit elements, FPGA boards, circuitry consumables	8600.98
Total	**8600.98**

13.4 EY Financial Statement Tables

13.4.1 EY Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Volpone, Gerardo Gabriele	6.67		1.47	3.60		1.35	0.25		
Domizio, Vito	5.28		1.40	0.71	0.68	0.47	2.02		
Cozzolino, Andrea	1.14			0.60		0.54			
De Rose, Pasquale	0.90			0.90					
Di Stefano, Davide	0.46			0.46					
Malaman, Michael	0.19			0.19					
De Poli, Federico	1.64		0.60	1.04					
Perrone, Giuseppe	1.62			0.65	0.52	0.45			
Guzzetta, Mariano	1.08				0.43	0.15	0.50		
De Angelis, Iacopo	2.45	1.00	0.35	0.35		0.35	0.35	0.15	
Volpe, Margherita	1.65		0.90		0.37	0.28			
Boanelli, Gianluca	1.79		0.50			0.52	0.27	0.50	
Fuganti Casagrande, Julia	0.39		0.39						
Avigliano, Giuseppe	0.03							0.03	
Mercuri, Giorgio	0.31						0.31		
Di Gennaro, Giacomo	0.05							0.05	
Meucci, Claudio	0.67		0.06			0.05	0.29	0.27	
Spagnoli, Francesca	1.68		0.34			0.34		1.00	
Total	**28**	**1.00**	**6**	**8.5**	**2**	**4.5**	**4**	**2**	**0**

13.4.2 EY Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
Gerardo Volpone	Kick-off meeting 11 -12 July 2019.	Presentation of EY and WP3 objectives.	758.06
Margherita Volpe	Kick-off meeting 11 -12 July 2019.	Presentation of EY and WP3 objectives.	487.77
Gerardo Volpone	Project Steering Meeting 16th December 2019.	Presentation of WP3 activities.	247.26

Contributor’s Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
Gerardo Volpone	Ethics of Blockchain Workshop 17th December 2019.	Participation in the workshop – EY representative.	134.49
Vito Domizio	Ethics of Blockchain Workshop 17th December 2019.	Participation in the workshop – EY representative.	187.32
Total			**1814.9**

13.4.3 EY Other Costs

Description	Date	Costs (€)
Azure Sandbox	November 2020	146.33
Azure Sandbox	December 2020	221.26
Total		**367.59**

13.5 FHG Financial Statement Tables

13.5.1 FHG Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Katharina Roß	4.14	0.45	0.59	0.63	0.84			1.65	
Christoph Brockt	10.23			0.17	5.01	3.59	1.46		
Andreas Weber	7.06		0.22	0.17	1.29	4.92	0.45		
Andreas Frorath	1.9				0.59	1.09	0.25		
Total	**23.34**	**0.45**	**0.81**	**0.96**	**7.73**	**9.6**	**2.16**	**1.65**	**0**

13.5.2 FHG Travel & Events Costs

Contributor’s Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs (€)
Katharina Ross	Kick-off meeting 11 -12 July 2019.	Official project start, preparation of a presentation about Fraunhofer’s contributions in Critical-Chains WP1.	632.55
	Data Security for different applications, Bonn, 28 October 2019.	Input as Security Officer (WP1).	346.28
	SMIG, Brussels, 28 January 2020.	Dissemination of Critical-Chains project ideas.	731.18
Christoph Brockt, Andreas Frorath	Project Steering Meeting 16th December 2019.	Project Progress Monitoring, Representation of the Critical-Chains Security Officer Katharina Roß.	-
Christoph Brockt, Andreas Frorath	Ethics of Blockchain Workshop 17th December 2017.	Participation in the project workshop.	-
Total			**1710.01**

13.6 GT Financial Statement Tables

13.6.1 GT Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Tuuli Lõhmus	0.74	0.28	0.36	0.1					
Kristo Klesment	4.04	0.07	0.46	1.28		1.57	0.66		
Rando Kulla	0.34		0.34						
Henry Rõigas	1.53		1.05	0.24			0.24		
Andres Ojamaa	2.24		0.63	0.89		0.72			
Liis Livin	0.06	0.06							
Margo Raja	0.98			0.25		0.73			
Karmen Kadakas	0.17	0.17							
Paul James Gardner	1.18			0.31		0.87			
Luukas Kristjan Ilves	0.65			0.28		0.05	0.32		
Ahto Truu	0.01	0.01							
Total	**11.94**	**0.59**	**2.85**	**3.36**	**0**	**3.93**	**1.21**	**0**	**0**

13.6.2 GT Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs(€)
Tuuli Lõhmus	Kick-off meeting 11 -12 July 2019.	Flight tickets, accommodation, daily allowance, train tickets.	747.70
Kristo Klesment	Project Steering Meeting 16th December 2019.	Flight tickets, accommodation, daily allowance, bus tickets.	734.43
Kristo Klesment	Ethics of Blockchain Workshop 17th December 2017.	Steering Meeting and Workshop were organized at the same location.	
Total			**1482.13**

13.7 IMEC-NL Financial Statement Tables

13.7.1 IMEC-NL Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Boer, Pepijn	3.96					3.96			
Breeschoten, Arjan	1.04							1.04	
Schaafsma, Siebren	0.01	0.01							
Schaik, Gert-Jan	7.09	0.56				5.43		1.1	
Zand, Pouria	1.14					1.14			
Total	**13.24**	**0,56**	**0**	**0**	**0**	**10.53**	**0**	**2.14**	**0**

13.7.2 IMEC-NL Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Costs (€)
Schaik, Gert-Jan van	Kick-off meeting 11 -12 July 2019.	102.05
Schaik, Gert-Jan van	Project Steering Meeting, 16th December 2019.	141.04
Total		**243.09**

13.8 INDRA Financial Statement Tables

13.8.1 INDRA Person-Months Deployed

Staff Name (employee identification)*	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
401812	1.35	0.00	0.00	0.00	0.00	0.00	1.35	0.00	
415279	3.12	0.00	2.50	0.05	0.00	0.00	0.57	0.00	
434915	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.19	
475314	3.39	0.51	0.85	0.67	0.00	0.00	1.35	0.00	
452539	0.56	0.00	0.00	0.00	0.00	0.00	0.56	0.00	
361463	0.05	0.00	0.00	0.00	0.00	0.00	0.05	0.00	
422937	2.00	0.00	0.00	0.00	0.00	0.00	1.40	0.60	
468640	0.17	0.00	0.17	0.00	0.00	0.00	0.00	0.00	
458902	0.20	0.00	0.20	0.00	0.00	0.00	0.00	0.00	
406013	0.02	0.00	0.00	0.0	0.00	0.00	0.00	0.00	
361508	0.25	0.00	0.00	0.00	0.00	0.25	0.00	0.00	
404980	1.08	0.00	0.00	0.00	0.00	0.00	1.08	0.00	
426709	3.02	0.00	0.00	0.00	0.00	0.00	3.02	0.00	
485263	0.59	0.00	0.00	0.00	0.00	0.00	0.59	0.00	
Total	**15.98**	**0.51**	**3.72**	**0.74**	**0.0**	**0.25**	**9.97**	**0.79**	**0**

*Indra normally prefers not to include personal information in the reports; therefore the employee number has been included instead of employee's full name. The employee number is unique and allows to identify univocally each employee within the company. However, Indra will provide complete names if it is requested by the European Commission. Figures include both main beneficiary and LTP.

13.8.2 INDRA Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Cost (€)
Ana Cabrera	Kick-off meeting 11 -12 July 2019.	Official project start. preparation of a presentation about Indra's contributions in Critical-Chains.	1041.86
Juan Castro	Kick-off meeting 11 -12 July 2019.	Official project start. preparation of a presentation about Indra's contributions in Critical-Chains.	803.56
Leyre Merle	Kick-off meeting 11 -12 July 2019.	Official project start. preparation of a presentation about Indra's contributions in Critical-Chains.	895.35
Juan Castro	Project Steering Meeting 16th December 2019.	Project Progress Monitoring. Representation of the Critical-Chains.	848.53
Total			**3589.3**

13.9 JR Financial Statement Tables

13.9.1 JR Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Ankele Ralph	6.54	0.18	5.68		0.01	0.15	0.01	0.51	
Bozic Josip	0.94		0.00		0.22	0.00	0.44	0.28	
Derler Christian	2.51		1.28		0.85	0.00		0.38	
Hasenauer Helen	0.43	0.43	0.00		0.00	0.00		0.00	
Hofer-Schmitz Katharina	2.48		1.54		0.92	0.00		0.02	
Jandl-Scherf Bernhard	0.13		0.00		0.04	0.09		0.00	
Lernbeiß Harald	0.78		0.13		0.65	0.00		0.00	
Nahrgang Kai	6.77		4.09		0.00	1.45	1.14	0.10	
Stojanovic Branka	8.25		4.52		3.48	1.69		0.25	

Total	**28.83**	**0.61**	**17.24**	**0**	**6.17**	**1.69**	**1.58**	**1.54**	**0**

13.9.2 JR Travel & Events Costs

Contributor’s Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs(€)
Derler Christian	04.07.2019; Raaba, Austria.	Dissemination Critical-Chains - RRZ Event, , discussions with stakeholders, promoting Critical-Chains.	11.80
Derler Christian	10.07.2019 to 12.07.2019; Reading, UK - Brussels, Belgium.	Critical-Chains Kick-off and EARTO SDRG Meeting.	1146.97
Ankele Ralph	11.07.2019 to 12.07.2019; Reading, UK.	Critical-Chains Kick-off meeting.	832.98
Ankele Ralph	14.12.2019 to 17.12.2019; Reading, UK.	Project Steering Committee Meeting 16th December 2019.	629.96
Ankele Ralph	19.11.2019; Vienna, Austria.	FinTechWeek19, discussions with stakeholders, promoting Critical-Chains.	401.06
Derler Christian	19.11.2019; Vienna, Austria.	FinTechWeek19, discussions with stakeholders, promoting Critical-Chains.	110.28
Ankele Ralph	10.02.2020 to 13.02.2020; Haifa, Israel.	Biometric Winter School – Workshop, discussions with stakeholders, promoting Critical-Chains.	712.40
Derler Christian	24.09.2020; Vienna, Austria.	Critical Chains Speech at FinTechWeek20, Critical-Chains project presentation and poster exhibition to Austrian blockchain community, discussions with stakeholders, promoting Critical-Chains.	58.75
Stojanovic Branka	24.09.2020; Vienna, Austria.	Critical Chains Speech at FinTechWeek20, Critical-Chains project presentation and poster exhibition to Austrian blockchain community, discussions with stakeholders, promoting Critical-Chains.	51.24
Total			**3955.44**

13.9.3 JR Other Costs

Description and supplier name if applicable	Costs(€
Roll-up DIG / Critical Chains - Repro Team.	278.00
Total	**278.00**

13.10 NETAS Financial Statement Tables

13.10.1 NETAS Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Onur Gümüş	0.5	0.5							
Osman Kumaş	11.6		6	2.5	1.15		0.5	1.45	
Mehmet Nuri Demirel	3		0.7	2.3					
Orhan Başar Evren	7.3		0.5	0.5			6.3		
Atilla Kara	2.7			2.7					
Mehmet Hakkı Ersoy	1.8				1.4		0.4		
İbrahim Doğru	6.2					5.5	0.7		
Sezin Tunaboylu	3					3			
Nagehan Çakır	1.5						1.5		
Total	**37.6**	**0.5**	**7.2**	**8**	**2.55**	**8.5**	**9.4**	**1.45**	**0**

13.10.2 NETAS Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution made	Cost (€)
İbrahim Doğru	Kick-off meeting 11 -12 July 2019.	Project kick-off, revisiting of project objectives, KPIs and action re-planning.	1247.77
Onur Gümüş	Kick-off meeting 11 -12 July 2019.	Project kick-off, revisiting of project objectives, KPIs and action re-planning.	1249.39
Onur Gümüş	Project Steering Meeting 16thDecember 2019. and Ethics of Blockchain Workshop 17thDecember 2017.	Project progress monitoring and participation to the workshop.	1210.23
Osman Kumaş	Project Steering Meeting 16thDecember 2019 and Ethics of Blockchain Workshop and 17thDecember 2017.	Project progress monitoring and participation to the workshop.	1521.57
Nagehan Çakır	Project Steering Meeting 16thDecember 2019 and Ethics of Blockchain Workshop and 17thDecember 2017.	Project progress monitoring and participation to the workshop.	1309.07
Total			**6538.03**

13.11 POSTEIT Financial Statement Tables

13.11.1 POSTEIT Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Avallone, Marco	4.53	0.04	0.74	1.56	-	1.57	0.62	-	
Hocevar, Massimliano	8.79	0.04	3.79	0.76	2.22	0.62	1.36	-	
Giacalone, Matteo	4.06	-	2.22	0.34	-	0.78	0.72	-	
Lapa, Francesco	3.17	-	1.45	-	0.74	0.78	0.20	-	
Paolone Beatrice	2.38	-	0.98	-	-	0.64	-	0.76	
Aschi, Massimiliano	0.95	0.04	-	-	-	-	-	0.91	
Farfaglia, Maurizio	6.25	-	3.31	0.80	0.46	0.80	0.55	0.33	
Total	**30.12**	**0.11**	**12.49**	**3.46**	**3.42**	**5.19**	**3.44**	**2.00**	**0**

13.10.2 POSTEIT Travel & Events Costs

No travel costs declared by POSTEIT.

13.12 RINA-C Financial Statement Tables

13.12.1 RINA-C Person-Months Deployed

Staff Name	Total PMs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8
Engineer	18.40	0.45	5.77			2.47	5.90	3.82	
Project Manager	5.51	0.20	1.08			1.98	1.14	1.10	
Manager	2.11	0.00	0.85			0.29	0.97	0.00	
Total	**26.02**	**0.65**	**7.7**			**4.74**	**8.01**	**4.92**	**0**

13.12.2 RINA-C Travel & Events Costs

Contributor's Name	Engagement Events Date and Location	Reason & Contribution actually made	Costs(€)
Martina Miro, Manuele Barbieri	Kick-off meeting 11 -12 July 2019	Project kick-off, revisiting of project objectives, KPIs and action re-planning.	1350.26
Ivan Tesfai, Davide Martini	Project Steering Meeting 16th December 2019	Project progress monitoring.	1193.04
Ivan Tesfai, Davide Martini	Ethics of Blockchain Workshop 17th December 2017	Participation to the overall discussions	
Total			**2543.30**

****