Critical-Chains

Collaborative Project

Project Start Date 1st July 2019 Duration 36 Months

Deliverable D6.1

Methodology and KPI Assessment Framework

Published by the Critical-Chains Consortium

Version 4.0 Date 30-04-2020

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP6

Document Responsible: NETAS

Contributors: NETAS, INDRA, UREAD, EY, POSTE, RINA-C, CEA, GT, FHG

Status: Final

Abstract

The deliverable sets out a methodologically-guided evaluation framework for the stakeholders adopting the Critical-Chains to explicate and assess the impacts of using the system. Such evaluation of the system performance is facilitated by the UI-REF methodological framework (Badii 2008). This is an ontologically committed, psycho-cognitively based and user-experience centred methodology for identifying the metrics for a holistic set of use-context-specific socio-technical Key Performance Indicators (KPIs). These include all the direct and indirect impacts of the operational deployment of the system (usability-acceptance and acceptability). The deliverable explicates a range of UI-REF-derived holistic KPI metrics and accordingly establishes a plan for the implementation of the user-experience evaluation in each of the four pilot application domains as planned for the validation of the Critical-Chains system; namely Banking Sector, Insurance Sector, Toll Road Operations, and Financial Market Infrastructures. The deliverable conlcudes with an extensive set of indicative questionnaire templates pre/post-exeperience usability evaluation to support the assessment of the system performance, usability, user-acceptance, accessibilty and impacts.

Acknowledgement

The Critical-Chains Consortium acknowledges the project funding received from the European Union Horizon 2020 Programme under Grant Agreement number 833326 H2020-SU-DS-2018.

Deliverable D6.1 Document Development History

Versioning			
Version Number	**Date**	**Contributors' name and organisation**	**Contributions**
V1.0	07-02-2020	NETAS	Initial Draft
V2.0	15-02-2020	UREAD	Privided two tutoriual sessions and documentation on methdology and led the rational structuring of the deliverable
V2.0	23-03-2020	UREAD, EY, POSTE, NETAS, INDRA, FHG, GT, RINA-C	Advanced Version
V3.0	3-03-2020	UREAD	Contributions and edits to arrive at pre-final status
V4.0	Thru-04-2020	UREAD	Extensive corrections and re-writes were implemented throughout. Incomplete references were completed Referencing style and Reference List had to be uniformalised to standard. Reference Questionnaires had to be amended extensively to ensure consistency.
V4.0	30-04-2020	ERARGE	Formatting check-and-fix as required.

Internal Review History

Internal Reviewers	**Date**	**Comments**
ERARGE	30-03-2020	Minor changes and amendments
UREAD	31-03-2020	Various corrections and re-writes proved necessary throughout to ensure quality.

Abbreviations

AI	Artificial Intelligence
AML/4	Anti-Money Laundering / 4
ATM	Automated Teller Machine
BCG Matrix	Boston Consulting Group Matrix
BIS	Bank for International Settlements
BRSA	Banking Regulation and Supervision Agency
CAVE	Computer-Aided Virtual Environment
CCP	Central Counterparties
CEMLA	Centre for Latin American Monetary Studies
CPMI	Committee on Payments and Market Infrastructures
CSD	Central Securities Depositories
CSP	Cloud Service Provider
DURE	Dynamic Usability Relationships Evaluation
ELSI	Ethical, Legal, and Social Impacts
ESCAI	Effects-SideEffects-CrossEffects-Affects-Impacts
ESEA	Effects, Side-Effects and (human) Affects
ETC	Electronic Toll Collection
FMI	Financial Market Infrastructures
GDPR	General Data Protection Regulation
HI	Heuristic Inspection
HE	Heuristic Evaluation
HSM	Hardware Security Module
HTC	Highway Toll Collection application domain
ICT	Information and Communication Technologies
IOSCO	International Organisation of Securities Commissions
IoT	Internet of Things
JDM	Judgement and Decision Making
KPI	Key Performance Indicators
KYC	Know Your Customer
LAC	Latin American and Caribbean
M&A	Merger and Acquisitions
MMREA	Multimedia Requirements Engineering Assistant
NGO	Non-Governmental Organisation

NIS	Network and Information Systems
PFMI	Principal Financial Market Infrastructures
PoE	Point-of-Experience (PoE)
PPR	Pleasure-Pain-Recall
PSD2	Payments Services Directive 2
PSS	Payment Settlement Systems
QoE	Quality of Experience
SSS	Securities Settlement Systems
SWOT	Strengths, Weakness, Opportunities and Threats
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TR	Trade Repositories
UI-REF	User-Intimate Requirements hierarchy resolution and Evaluation Framework
UTAUT	Unified Theory of Acceptance and Use of Technology

Table of Contents

Abstract 2

Acknowledgement 2

Deliverable D6.1 Document Development History 3

Abbreviations 4

Executive Summary 9

1. Introduction 11

1.1. Background 11

1.2. Scope of this Deliverable 11

2. Methodologically-Guided System Evaluation Framework 12

2.1. User-Intimate Evaluation Methodology 12

2.1.1 System Evaluation Typology 12

2.1.2 The Evaluation Methodology 13

2.1.3 Technology Appropriation 14

2.1.4 Appropriation Trajectories 14

2.1.5 Dynamic Usability Relationship Evaluation (DURE) 17

2.1.6 Usability Data Capture Support Environment 18

2.1.7 Evaluation of User Acceptance, Acceptability and Use of Technology 19

2.2. Evaluation Plan Phases 21

2.3. Key Performance Indicator Identification 23

2.4. Key Performance Indicator Evaluation 23

2.5. Audit and Compliance Assessment Process 24

3. Ontological Domain Knowledge Analysis 25

3.1. Analysis of the Emerging Needs of the Fintech Sector 25

3.1.1 Stakeholder Gaps 25

3.1.2 Consumer Gaps 28

3.1.3 Fintech Metrics 28

3.2. Stakeholders Interviews Questionnaires 29

3.2.1 Toll Collection Pilot Interviews 29

3.2.2 Insurance Pilot Interviews 30

3.2.3 Banking Pilot Interviews 30

3.2.4 Financial Market Infrastructure Interviews 30

3.3. Stakeholder Requirements 31

3.4. Introduction to the Pilot Validation Domains 32

3.4.1. Banking Sector 32

3.4.1.1 Introduction to the Banking Pilot....32
3.4.1.2 Use-Cases....33
3.4.1.3 Key Performance Indicators....36
3.4.2. Insurance Secto....38
3.4.2.1 Introduction to the Insurance Pilot....38
3.4.2.2 Use-Cases....40
3.4.2.3 Key Performance Indicators....41
3.4.3. Toll Road Operations....43
3.4.3.1 Introduction to the Toll Road Operations Pilot....43
3.4.3.2 Use-Cases....43
3.4.3.3 Key Performance Indicators....44
3.4.4. Financial Infrastructures....46
3.4.4.1 Introduction to the Financial Infrastructures Pilot....46
3.4.4.2 Use-Cases....47
3.4.4.3 Key Performance Indicators....48
4. Expected Behaviour of Critical-Chain Components....50
4.1. Critical-Chains Main Framework....50
4.2. The Secure Cyber Framework....52
4.3. Flow Modelling-as-a-Service....54
4.4. Cyber-Physical Security-as-a-Service....56
4.4.1 Blockchain-as-a-Service....56
4.4.2 Cryptography as-a-Service/Hardware Security-as-a-Service....58
4.4.3 Authentication/Authorisation as-a-Service....60
4.5. ATM Integration....64
4.6. Toll Collection System....66
5. Evaluation Process....69
5.1. Use Scenarios Specification in the Banking Sector and KPI Evaluation....69
5.2. Use Scenarios Specification in the Insurance Sector & KPI Evaluation....72
5.3. Use Scenarios Specification for Toll Road Operations & KPI Evaluation....76
5.4. Use Scenarios Specification for Financial Infrastructures & KPI Evaluation....78
6. Use-Cases-to-Requirement Mapping....79
7. Conclusions....84
8. References....85
9. Annex1: Indicative Questionnaires for the Financial Sector....87
Indicative Pre-Experience Questionnaire - Fintech Applications Domain....87
Indicative Post-Experience Questionnaire - Fintech Applications Domain....91

10. Annex 2: Indicative Questionnaires for the Toll Collection Domain 95

Indicative Pre-Experience Questionnaire – Highway Toll Collection Domain 95

Indicative Post-Experience Questionnaire – Highway Toll Collection Domain 98

List of Figures

FIGURE 1: THE TECHNOLOGY ACCEPTANCE, REJECTION AND (MIS)APPROPRIATION CYCLES 15
FIGURE 2: TECHNOLOGY ACCEPTANCE MODEL, DAVIS (1989) 20
FIGURE 3: UNIFIED THEORY OF ACCEPTANCE AND USE TECHNOLOGY, VANKATESH (2003) 20
FIGURE 4: COMPLIANCE ASSESSMENT PROCESS 25
FIGURE 5: SWOT ANALYSIS FOR THE FINTECH DOMAIN 29
FIGURE 6: BOSTON MATRIX ANALYSIS 29
FIGURE 7: INSURANCE CASHFLOW MODELS 38
FIGURE 8: CRITICAL-CHAINS MAIN FRAMEWORK BEHAVIOURS 51
FIGURE 9: SECURE CYBER FRAMEWORK BEHAVIOURS 53
FIGURE 10: FLOW MODELLING AS A SERVICE BEHAVIOURS 55
FIGURE 11: BLOCKCHAIN-AS-A-SERVICE-BEHAVIOURS 57
FIGURE 12: CRYPTOGRAPHY AS A SERVICE/HARDWARE-SECURITY-AS-A-SERVICE 59
FIGURE 13: AUTHENTICATION/AUTHORISATION-AS-A-SERVICE BEHAVIOURS: IDENTITY PROVIDER INITIATED AUTHENTICATION 61
FIGURE 14: AUTHENTICATION/AUTHORISATION-AS-A-SERVICE-BEHAVIOURS: SERVICE PROVIDER INITIATED AUTHENTICATION 62
FIGURE 15: AUTHENTICATION/AUTHORISATION-AS-A-SERVICE BEHAVIOURS: AUTHORISATION 62
FIGURE 16: ATM INTEGRATION BEHAVIOURS 64
FIGURE 17: TOLL COLLECTION SYSTEM BEHAVIOURS 67
FIGURE 18: TRADITIONAL IMPLEMENTATION 73
FIGURE 19: THE SMART CONTRACT APPROACH 74

List of Tables

TABLE 1: KPI EXAMPLE 23
TABLE 2: COMPANY FINANCIAL AUDIT ADVISORY USE-CASE 31
TABLE 3: CHECK FINANCIAL SERVICES IN ONE CHANNEL USE-CASE 31
TABLE 4: KPIS FOR THE BANKING PILOT 37
TABLE 5: KPIS FOR THE INSURANCE PILOT 42
TABLE 6: KPIS FOR THE TOLL COLLECTION PILOT 45
TABLE 7: KPIS FOR THE FINANCIAL INFRASTRUCTURES PILOT 49
TABLE 8: ESEA METRICS FOR THE EVALUATION OF THE MAIN FRAMEWORK 51
TABLE 9: ESEA METRICS FOR THE CYBER-PHYSICAL SECURITY FRAMEWORK 53
TABLE 10: ESEA METRICS FOR FLOW MODELLING-AS-A-SERVICE 55
TABLE 11: ESEA METRICS FOR BLOCKCHAIN-AS-A-SERVICE 57
TABLE 12: ESEA METRICS FOR CRYPTOGRAPHY AS-A-SERVICE/HARDWARE AS-A-SERVICE 60
TABLE 13: ESEA METRICS FOR AUTHENTICATION/AUTHORISATION AS-A-SERVICE 63
TABLE 14: ESEA METRICS FOR THE ATM INTEGRATION 65
TABLE 15: ESEA METRICS FOR THE TOLL COLLECTION SYSTEM 67
TABLE 16: COMPARISON OF EXISTING AND FUTURE REINSURANCE 72
TABLE 17: USE-CASES-TO-REQUIREMENTS MAPPING 80

Executive Summary

This Deliverable, D6.1, sets out the methodologically-guided implementation plan for the validation of the Critical-Chains platform. It follows the ontologically-committed and psycho-cognitively based UI-REF Requirements Elicitation and Usability Evaluation Framework (Badii 2008) for user-centred co-design, as already adopted for requirements prioritisation in Deliverable D2.3 of WP2. Deliverable D6.1 sets out the preparatory and subsequent trialling process to elicit the users' Quality-of-Experience (QoE) arising from the deployment of the system.

The methodologically perspective is that usability depends not so much on a single point or instance of usage but on the overall perceived QoE of a user in interacting with a system over a number of instances. This involves perceived QoE over a sequence of experiences with usability evaluated both instantaneously and longitudinally. As such the user's perceived comfort with, or usability of the system, is their overall impression of the system effects, side-effects, cross-effects, and (latent) affects (including the Ethical, Legal and Social Impacts -ELSI- and Socio-economic Impacts) as *perceived* and valued (*remembered)* by the user. Some of these *effects* are more deeply-valued and so more intensely perceived by a particular user and thus may prove *more memorable* for them. A primary experience can pre-dispose a user to the perception of more or less (dis)satisfaction and (dis)affection, therefore usability evaluation, in reality, is the evaluation of the user's evolving (usability) relationship with the system. The human memory system is affected by Recall Biases due to Pleasure-Pain-Recall (PPR)-theoretic bias, or, relative perception of Saliency-Recency-Primacy ("End Effects", "Duration Neglect") or other factors affecting Human Judgement and Decision Making (JDM). The main purpose of the evaluation is "formulating a judgment" (Hurteau, 2009). The JDM mediated bias in turn influences the user-expressed usability evaluation. Such influence operates at all levels and with all relationships of which the user-system relationship is but one example. Another instance of this is shown in the human voter's (users) judgement (voting pattern) changeability after watching each single debate or after watching the last of a series of debates amongst the candidates etc. (Badii 2000).

It follows that, in an online world of increasingly *click-happy and fickle* users with changeable lifestyles, it is important to get to the *stable determinants* of usability (dis)satisfaction in order to detect, assess and remedy any usability problems effectively. Thus, it is important to ensure that usability evaluation follows a well-established JDM-theoretic framework as incorporated in Dynamic Usability relationships (DUR) Modelling which is the foundational concept motivating UI-REF as an integrative Requirements Prioritisation and Usability Evaluation framework.

This framework enables the traceability from the users' usability assessment statements about the system to specific usability flaws of the sub-systems and the relative significance of such flaws in shaping the overall usability assessments of the users. This takes into account the effect of the user's serial experiences of the system (serial points-of-click, points-of-experience, Badii 2000) and their recursively self-reinforcing usability relationship consequences in the context of their JDM-theoretically more memorable affects over time (i.e. perceived as more usability-sensitive/critical).

The deliverable is divided into six main chapters that follow the above methodology to derive a holistic set of Key Performance Indicator (KPI) metrics to evaluate the usability, acceptability and social acceptance of the system plus a plan and reference templates for the assessment of the Side/Cross Effects and (Latent) Affects to be used at the implementation stage of the evaluation of the system in each of the four pilot application domains of Critical-Chains; as described below:

Chapter 1: This sets out the background highlighting the objectives of the Critical-Chains system and clarifying the scope of the analysis for this deliverable.

Chapter 2: This presents the approach adopted in this deliverable consistent with a methodologically-guided framework for evaluation supporting the explication of the holistic metrics for the KPIs to prioritise the evaluation of the holistic socio-technical KPIs of Critical-Chains. This is to underpin the

iterative, user-centred evaluation process to support the adopted evolutionary system design methodology.

Chapter 3: This provides the use-contexts, user-scenarios and associated KPIs and their user-centred metrics and expected levels to be evaluated as appropriately planned under this deliverable.

Chapter 4: This sets out an analysis of the expected outcomes arising from the deployment of the Critical-Chains-enabled applications in the financial sectors and other domains including the Highway Toll Collection application as an exemplar. This examines the affordances resulting directly from the Critical-Chains-enabled use-cases to support the targeted workflows plus the likely indirect effects Effects, Side-Effects, Cross-Effects and (human) Affects) identified for the before, after and current points of use of the system (pre/post and at-the-point-of users' experience of using the system).

Chapter 5: This presents the implementation plans for the methodologically-guided holistic evaluation of the performance and impacts of the adopted methodology.

Chapter 6: This Sets out the evaluation matrices to be used for each Use-Case responsive to each of the user-centred requirements as derived and prioritised and as are to be revised in light of the evaluation results following the iterative evolutionary methodology as adopted for the Requirements Prioritisation and usability, acceptance and acceptability Evaluation of the Critical-Chains solution. .

Chapter 7: This chapter highlights the conclusions of the deliverable and is followed by the References section which includes the detail referencing of sources consulted.

Annex 1 & 2 : The Annexes provide indicative questionniare temolates to support the evaluation of system performance, usability user-accepatnce, accesptability and impacts; this process will also incude semi-structured interviews.

1. Introduction

1.1. Background

The aim of the project is to develop an integrated effective, accessible, fast, secure and privacy-preserving financial contracts and transactions solution. A solution that can protect against illicit transactions, illegal money trafficking and fraud. Thus, the objective of the project is in the public interest. The planned Research and Innovation agenda involves the use of the following data types of participants for respective purposes as outlined in this section:

- Anonymised Inter-bank data related to fund transfers as required for clearing funds
- Anonymised funds transfers from sender to receiver accounts
- Anonymised Highway Toll Collection (HTC) Data for the trialling in the HTC domain Anonymised user-expressed system requirements and usability evaluation data
- Minimal profiling data as essential for anonymised users' requirements and usability clustering analysis, or, anonymised transactor's transactions clustering and aggregated analysis
- Facial Images encrypted and stored for authentication and identity management. This is needed to support authentication, auditability and accountability. The Critical-Chains system will not have any access to the encrypted images but will receive the results of the success or failure of the authentication process.
- The technologies to be deployed consist of:
- Transaction and financial data flow 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
- Cybersecurity 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 will be validated using four case studies aligned with three critical sectors: banking, financial market infrastructures, the insurance sector and Highway Toll Collection. The validation will include evaluating the system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy with the rest of the world. The Consortium represents strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector.

1.2. Scope of this Deliverable

The scope of this deliverable is to create a methodologically-guided evaluation framework for the stakeholders who are intending to adopt the Critical-Chains to present models that explicate the Critical-Chains' impact on critical sectors. Afterwards, the preparation proposes 4 pilots in the area of Banking Sector, Insurance Sector, Toll Road Operations, and Financial Market Infrastructures. The aim is to evaluate the Critical-Chains Framework in various aspects and assess the improvement that Critical-Chains could make to the current Fintech operations.

2. Methodologically-Guided System Evaluation Framework

The direct and indirect impacts of ICT innovation deployment are multi-faceted and would require a system-of-systems ontologically-committed framework of analysis of the cascaded and mutual interplay of the various effects of the system on people and the socio-econo-political and ethical and legal context impacted by its operational deployment and routinisation (Badii, Rolfe 1996, Eva, Badii 1997). The Consortium has adopted the UI-REF methodology (Badii 2008, Badii, Fuschi, et al. 2009) for the planning and implementation of the usability evaluation of the Critical-Chains prototype in each of its four pilots application domains. The overall aim of this task and therefore of this document is to establish the methodological analysis framework and preparatory planning steps for the holistic assessment of the usability-acceptance and societal acceptability of the operational deployment of the Critical-Chains system in the Banking Sector, Insurance Sector, Toll Road Operations and Financial Market Infrastructure.

2.1. User-Intimate Evaluation Methodology

2.1.1 System Evaluation Typology

Just as system functionalities, also referred to as affordances, have to be both useful and senseful so the evaluations are also subjected to scrutiny for senseful-ness and cost-effectiveness. As a process, the evaluation itself has to be designed to be user-centred and non-stressful, at-appropriate-scale, and, efficient. The evaluation process is expected to result in actionable and generalise-able insights to contribute to the evolutionary user-centred co-design of systems.

From the viewpoint of the scope, scale and timing/phasing-in of the evaluation processes, these can be classified into any one of the following four categories:

i. **Formative Evaluation:** to help improve the design of the target system.

ii. **Summative Evaluation:** to help users appropriate an adaptation of the system to a particular usage-context.

iii. **Illuminative Evaluation:** to discover any latent influential factors that pervade over a usage-context and influence usability; i.e. find out over the course of the evaluation some hitherto unknown patterns of user reaction or other influences which could not have been foreseen but which could play a significant influence on the usability relationship.

iv. **Integrative Evaluation**: This is an evaluation that uses all available channels of usability evaluation to maximise benefit realisation from the target system in the targeted usage-contexts.

From the viewpoint of the situated environment and modalities involved in the evaluation (laboratory, field virtual, physical), the process can be seen as comprised of the following categories:

- **Heuristic Inspection** (HI): also referred to as Heuristic Evaluation (HE) is often used as a relatively inexpensive means of discovering and eliminating foresee-able usability bugs prior to the user trials. Thus, this process involves a minimum of five expert usability evaluators (i.e. rule-based) evaluation method. It includes a range of evaluations to foresee possible usability problems that may occur in the subsequent field evaluations to be conducted by the end-users. The experts independently examine the degree of system compliance against the general usability guidelines and inspect the functionalities of the system as they deem appropriate. For example, using a cognitive and interactive walk-through of the system use-cases, applying test-cases as they see fit and scoring and thus ranking the usability bugs according to criteria of their relative saliency (i.e. usability sensitivity, performance -criticality). This process amounts to a cost-effective first screening of the system which could be a natural sequel to the first test stage of the system (i.e. the conformance testing).

- **Virtual User Systems:** This is a usability co-design approach that can take place at any time during the lifecycle of the prototyping and completion of the design of the first prototype as well as beyond that to aid cost-effective testing and usability evaluation of the various configurations of the system for user adaptation. Virtual user systems often deploy a Computer-Aided Virtual Environment (CAVE) or a "Digital-Twin" simulation platform, to simulate alternative system configurations and adaptations interacting with target users in a (partly) simulated and thus cost-effective fashion. Such approaches can provide lifecycle formative, summative and instructive evaluation to inform the iterative user-centred co-design process.
- **Pilot/focus-group-based evaluation:** This is an evaluation process involving a group of users selected on the basis of certain criteria so as to ensure that the evaluation process results include answers to some specific questions.

2.1.2 The Evaluation Methodology

The procedure for all the trials in this set, as reported here, is based on UI-REF [Badii, Atta 2008] which is the integrated requirements prioritisation and usability evaluation methodological framework. This framework is systematically deployed for all Critical-Chains evaluations as well as at the outset of the project for requirements engineering and framework architecture specification. This section sets out the principles of the UI-REF methodology and concludes with the outline of the UI-REF-based evaluation as planned for Critical-Chains as elaborated in the subsequent sections of this document.

UI-REF supports dynamic user-system relationship-based evaluation of system performance at points-of-interaction plus post-experience reflections, which are captured and context-layered to inform the designers of the user-specified and prioritised requirements and usability flaws of the system. This is so that iterative design improvements could be most effectively and efficiently made to ensure the system is best matched to the user's priority needs and preferences, likes, dislikes, lifestyle, workstyle, and dispositions. Thus, UI-REF supports a set of three integrated usability evaluation stages in order to elicit both instantaneous and overall assessment of user-perceived usability of the system; as follows:

i. **Pre-Experience:** Users' experience working unaided by the system, users' prior dispositions as may have evolved through using a legacy system or work-around in absence of the new system to be trialled by them; users' prior disposition towards an existing solution and their expressed priority needs for enhanced support.

ii. **Point-of-Experience:** User impressions, experiences and observations re system performance and usability evaluation of user interactions with the system at the end of a single session/trial day.

iii. **Overall-Post-Experience:** Overall impressions, experiences and observations re system performance and usability evaluation after users' interactions with the Critical-Chains system at the end of all the trials i.e. at the end of each phase of evaluation for each release of the system prototype.

UI-REF represents a pioneering user-centred co-design methodology consistent with the psycho-cognitive operation of the human perceptual and memory-recall system. It is a methodology for relationship-based context-layered persona-specific user requirements ranking. The usability evaluation informs the iterative requirements ranking based on an integrative assessment of usability, Quality-of-Experience (QoE), user-acceptance, social acceptability, safety-security-privacy safeguards and societal impact. In UI-REF all the above functional and non-functional aspects of the performance of the system are evaluated within a 4-tier measurement framework comprising the evaluation of the situated Effects, Side-Effects, Cross-Effects, and, Affects associated with each use-case in each "use-context" as the fundamental "situated unit-of-analysis; as follows:

i. **EFFECTS** which are the intended affordances or features to be delivered by each functionality of the system i.e. the goal of the use-case being evaluated as provided by the system.

ii. **SIDE-EFFECTS** which are the secondary intended/unintended, good/bad, and direct/indirect effects of the system functionality and deployment, for example, constraints or new degrees of freedom that the user can experience when opting to use the use-case, impacts on users' lifestyle, workstyle.

iii. **CROSS-EFFECTS** which are the intended/unintended, good/bad effects of the system functionality and deployment, indirectly impacting the wider societal and environmental arena etc.

iv. **AFFECTS** which are the psychological, emotional, and sentimental consequences of the user's experience of the effects, side-effects and cross-effects of a use-case in a given use-context;

Further, UI-REF incorporates a number of instruments (i.e. protocols and techniques) for implementing the Requirements Elicitation and Prioritisation; these include Cultural Probes and Filters (e.g. Online self-report, card-sorts, laddering, nested-video interviews/cognitive-walk-throughs, Noah's Ark, Ablation, Frequency-Purpose-Hurry, nested video and virtualisation techniques). These can help overcome articulation-theoretic barriers to deep interpretivist elicitation of the roots of, and, routes to usability (dis)satisfactions, so as to most accurately resolve user's real sentiments, sensitivities, sensibilities, and preferences.

2.1.3 Technology Appropriation

Badii (2002, 2004, 2008) refers to appropriation as it relates to patterns of technology adoption or rejection. In other words, the way a user may integrate or reject a particular system artefact or a sub-set of the affordances that such an artefact was designed to provide in the context of that user's prevailing patterns of usage. Appropriation is implicit in the assumption of requirements negotiation and consensus-seeking in co-design of systems.

Users' appropriation of a system, as it unfolds, can result either in completion of the design to tune it to a well-appropriated deployment or its mis/dis appropriation or instant/eventual rejection of the system by the user (2008).

The Dynamic Usability Relationships (DUR) modelling approach (Badii 2000) as takes place under UI-REF, enables insights to emerge that would help provide answers to the questions relating to lifecycle usability-relationship evaluation of the target systems as deployed by the targeted users. For example, attempting to elicit answers to the following types of questions:

i. What are the various ways, modes and means by which "usage value" for the system may be viewed by the users?

ii. What are the various ways, modes and means by which "benefit realisation" of the system may be pursued by the various stakeholders?

iii. What will emerge as the Conflict Sets between the answers to (i) and (ii) above including prioritisation conflicts between end-user types and stakeholder layers?

iv. How could various stakeholders resolve the above Conflict Sets?

v. What are the side-effects of any appropriation patterns of the system by any of the users involved? -including the mis-usage possibilities that may expose some users or other citizens to risks of any loss of safety, security, privacy and dignity and/or being otherwise treated unfairly and unethically?

vi. How would the disposition of any users with respect to any of the above change with serial exposures by the users to the system over time?

2.1.4 Appropriation Trajectories

The *roots-of* and *routes-to* appropriation is the evolutionary trajectory of the user-system usability relationship that evolves depending on the interplay between a user's needs and expectations, and, the

functionalities provided by the system, their effects/side-effects/cross-effects in practice in the usage-contexts of the user's life-style and/or work-style.

Badii (2008) concluded that the dynamic balance of influences of the above factors determines the evolutionary path of the usability relationship from the user's first–exposure-point, i.e. the user's first Point-of-Experience (PoE) with the system to eventual acceptance and appropriation, seen as mediating integration of the system in, or exclusion from, user's routinised processes, leading to one of the following outcomes:

- **Acceptance:** Using the system as it was intended and designed for (well-appropriated design and usage).
- **Non-Acceptance:** (non-appropriation): Rejection of the system by the user (outright or later).
- **Dis-appropriation:** Adoption of the system in whole or part BUT for the pattern(s)/mode(s) of usage other than that intended by the designers, e.g. using the mobile phone solely for texting, or for locating people or as a fashion accessory rather than as a phone.
- **Mis-Appropriation/Mis-Use:** Such modes of adoption for usages that are intended to subvert the system affordances for perverse or anti-social/criminal activity such as the use of a mobile phone to deliver and/or trigger bombs, as a weapon to locate and destroy people, etc. or using twitter/email for hate crime –any form of appropriation amounting to a means of harm/hurt of any kind including blatant weaponisation.

Appropriation is analogous to a "personal construction" of an attitude towards the system. This attitude is rooted, on the one hand, in the cross-elasticity between personal constructs and developmental aspirations of the user and, on the other hand, dependent on the adaptabilities of the system affordances as may evolve in the course of their evolving usability relationship (Badii 2000). Figure 1, below, illustrates the dynamic usability evolution process and the possible outcomes.

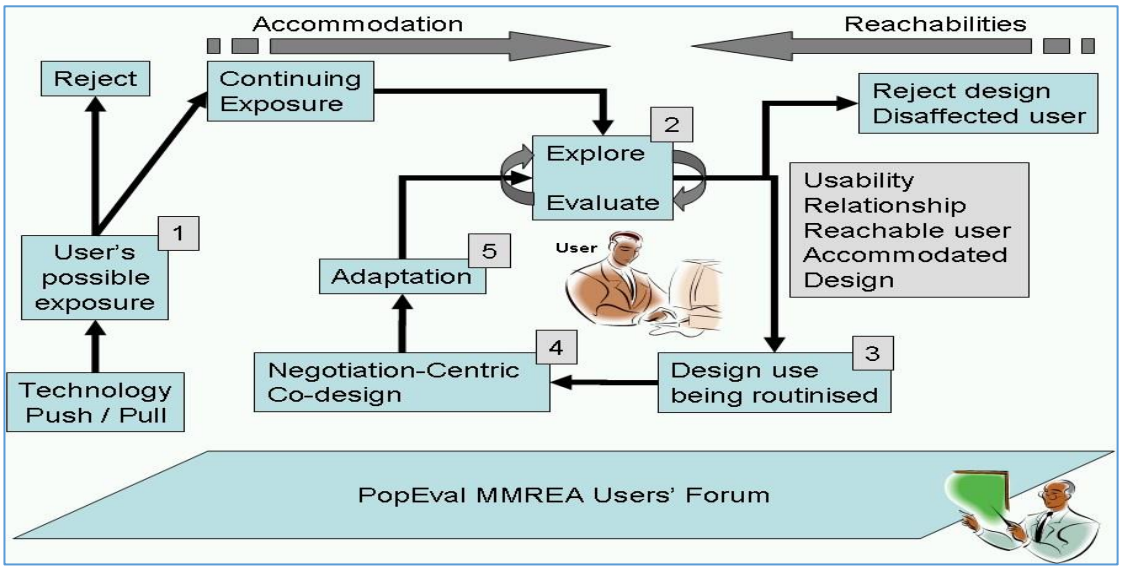

Figure 1: The Technology Acceptance, Rejection and (mis)Appropriation Cycles

This personal construction is informed by the *perceived and remembered* (dis)satisfaction episodes arising from the user-system interaction. The user's impressions of the system are largely modulated by the effects of the inherent human memory re-call biases as these shape the pleasure-pain-theoretic influences on the evolving perceived usability of a particular system by a particular user as illustrated in Figure 1Figure 1, above. Thus, the outcome of the usability relationship is influenced by:

- The level of sustainable adaptability of the system to the users' important and deeply-valued needs afforded by the new system through its design features (accommodation by the system)
- The expected level of co-adaptation potential of a user group to such features as may be affordable through the evolving system – trainability of the users to co-work with the adapted system without them suffering intolerable cognitive, cultural, financial stress/distress (Users' Reachabilities).

The above two properties of the usability relationship are due to the influence arising from the following well-established psycho-cognitive effects that affect the user's perception and recall of their experiences:

- Human Judgement & Decision Making (JDM) as affected by Pleasure-Pain-Recall (PPR) theoretic bias and Primacy-Recency-Saliency
- Many psycho-physiological research results relating to human Judgement and Decision Making Theory (JDM), Pleasure and Pain Theory, and, Learning Theory (e.g. as reported e.g. in Badii 2000) have established facts relating to human memory biases that underpin the above important methodological approach; justified for example by the following observations:

  a) A user's view on the usability of a device is not frozen but its subject dynamically evolves, changes depending on the users' experiences over sequential instances of usage of the system or even during a series of interactions with the system during the execution of a task.

  b) A user's view of the usability of a device has a trajectory that includes bi-furcation, transient and steady-state regions depending on the sequences of instantaneous usability impressions from the beginning of exposure of a user to a device right up to the moment of usability measurement (as illustrated in Figure 1, above).

  c) A user's view of the usability of a device is influenced by the inherent human memory re-call biases in a recall of sequential experiences in a way that is not necessarily linearly or monotonically influenced by a simple aggregate of the user's perceived usability at individual Points-of-Exposure in serial exposures.

  d) Users are most likely to have been most affected by their latest exposure to the system functionality i.e. depending on what went wrong or right just before the interview, their assessment of the system performance at earlier times may be affected.

  e) Users are most likely to remember, and thus allow their usability evaluation to be affected by, any usability incidents that caused the most pleasure, pain, surprise, disaster, rather than remembering lots of little usability bugs (whose evaluations are typically easily miss-able by the evaluation process if no evaluation occurs at PoE; hence the importance of item (a) above). However, users themselves may be unaware of the significance of the influence that such un-reported usability bugs may have played in forming the users' impression of the system over time (i.e. in shaping their current overall usability relationship with the system).

The above distinguishing features of the framework are deployed within a system-of-systems analysis perspective whereby the system-of-systems includes the user's human perception, cognition and memory system co-working with the ICT system as one integrated system, factoring in Human Memory Recall-Bias-Effects, Pleasure-Pain-Recall Effects, and Man-Machine-Mutuality of the relationship - transiently and over time. As such UI-REF has been applied for socio-technical design and evaluation in a range of domains including decision support systems, and, user-led security-privacy-preserving systems co-design.

UI-REF, cost-effective but holistic co-design and impact assessment for both short and longitudinal user studies, lends itself particularly well to supporting "open innovation-open evaluation" of technology e.g. support for living laboratory-based strategies for progressing innovation from concept to commercialisation. This is a highly competitive value proposition to underpin the mainstreaming of socially responsible and responsive technology – particularly of disruptive and transformative innovation as in Critical-Chains.

The UI-REF approach will enable the identification of those usability features of the system that are relatively more critical to the users' overall perceived satisfaction and the final outcome of the usability relationship based on the cumulative recall of perceived transitional usability (from user's instantaneous sentiments to transitional usability and over time to steady state usability).

The assessment of pre-and-post-experience and point-of-experience usability as planned for the Critical-Chains project will thus inform the identification of those features of the system which affect the overall perceived user-experience significantly. This will in turn enable the ensure responsive re-prioritisation of the requirements and thus the refinements to arrive at a user-led co-designed system optimally adapted to the users' needs.

Such relationship-centric evaluation of the system acceptability includes both the evaluation of system usability and, the senseful-ness of its longer-term deployment from an individual user's perspective as well as from an organisational and societal standpoint.

A system might be highly useful, but such use might be sense-less, harmful (e.g. open to mis-use), cost-inefficient, unsustainable, unscalable or in some other way have side-effects that defeat a higher personal or societal objective. For example, a system will have a low senseful-ness evaluation if it provides such high usability features that it encourages over-dependency thus detracting from the higher level objective of keeping the users appropriately engaged in the right decision loops in order for them to remain maximally informed, capable and creative in other ways. A system that is too interventionist and attempts to do everything for the user, over time, will stifle both its own potential and reliability as well as that of the user-and-system as a co-working team. This comes about as the system misses out on some opportunities to learn from the users and maintain its reliability e.g. through learning by reinforcement by involving the users in some decision points. The users will miss out on the opportunity to exercise their judgement and creativity as they are not adequately in the loop for the more challenging decision points.

2.1.5 Dynamic Usability Relationship Evaluation (DURE)

This is an approach which privileges a memory-bias-aware relationship-centric and usage-context-based evaluation of the most usability-sensitive *effects, side-effects, cross-effects, (latent) affects* and *impacts* of the usage of the system, on the user and on the wider social/sectorial stakeholders. Usability evaluation results, in essence, are the perceived cumulative impressions re-called by a user. Thus, the users' usability verdict on the system hinges on what is more significant and thus more memorable usability moments of a user's lived experience with the system.

This means that as the patterns or causes of user dissatisfaction can be variable and ever changing, single overall evaluation of usability based on any fixed criteria will be inadequate in revealing the roots-and-routes of a user's perceived (dis)satisfaction. Thus, it is more effective from a remedial co-design viewpoint to be able to trace the precise causes of usability bugs/issues that a user experienced as perceived, and remembered, and, thus was affected by. This valuable usability data intelligence can only be obtained with careful measurement of point-of-experience usability through users' self-expressions at any pain/joy points during serial episodes of interaction with the system or immediately afterwards.

To have the best hope of both detecting and locating the root causes of usability bugs, a system must:

- Perform evaluations that are human-memory-biases-aware.

- Capture the users' perceived evaluations at both the Point-of-Experience and later.
- Prioritise the evaluation of the functionalities of the system according to the latest user-specified order of priorities; given the three broad ranking of the system requirements as distinguished by UI-REF as being **i)** Mandatory, **ii)** Desirable and **iii)** Optional (as defined in D2.6 and elsewhere (Badii 2008)) start from the use-cases that use the higher ranking Mandatory functionalities of the system as routinely deployed in practice and then move down the rankings to evaluate the use-cases integrating lower functionalities and eventually to the ones less frequently deployed.
- Factor in the evaluation, the additional influence of the recursively reinforcing human memory-recall-bias in shaping the users' usability relationship trajectory over time, reflecting the feedback loop affecting the usability relationship as depicted in Figure 1above.
- Conduct Effects-SideEffects-CrossEffects-Affects-Impacts (ESCAI) analysis re the users' highest priority needs based on both instantaneous and longitudinal evaluations. The ESCAI analytics can enable pattern discovery not just of the explicitly articulated usability concerns but also of any latent links between certain usability views of the same user or across various users. An example of this is the latent parametric of certain usability bugs that may be thus discovered to have been responsible for the most user disaffection and should, therefore, be prioritised for remedying. It follows that this leads to a reliable actionable insight to inform the requirements refinement and reengineering of the next prototype. The ESCAI analytics can thus enable a mapping of the *Affordances-vs-Resonances i.e. system functionalities vs. personal-usage-context-priority-needs* for each user or user sub-group. This supports the evaluation of the impact of relevant changes involving actors, processes and situated contexts as experienced by all stakeholders and by particular sub-groups, thus enabling the resolution of any re-prioritisation of the requirements for particular versions (releases) of the prototype customised for particular user sub-groups.
- For the usability data intelligence, a shared evaluation reporting ontology has to be agreed with all concerned before embarking on the evaluation process i.e. the same evaluation expression language used by users and evaluator and semantically linked to the same usage-context, user's preferences and prioritisation. This will include an established scale of qualitative measures e.g. a 5-to-7(max)-point interval-based (Likert) scale with appropriate granularity, selectivity and sensitivity to ensure shared differentiation of the meaning of the semantic qualifier points on the Likert-scale e.g. one user's expression of "very good" and the same user's "quite good" in another place must not relate to essentially the same intended evaluation score re that user's perceived quality of experience. In any event, the evaluation expression language should not include words such as "quite", "nice", "depends" etc. which tend to add nothing to the evaluation information but can make statements ambiguous or misleading. If a user tends to use such words thereby being unable to adhere to an agreed small set of qualifiers, then the researchers must on each occasion ascertain the relative meaning of the words meant by the user related to the interval based qualifiers deployed in the language. To ensure that the user's evaluation expressions remain as explicit as possible, the protocol should be as simplified as possible, using a very small vocabulary of qualifying words illustrated by means of an online gallery if possible. This will help the users to articulate their usability evaluation as may be supported by an online self-report tool to serve Dynamic Point-of-Experience Usability Relationship Evaluation as in PopEval (Badii 2000).

2.1.6 Usability Data Capture Support Environment

As UI-REF provides for Dynamic Usability Relationships modelling to inform co-design which requires pre-experience, point-of-experience, and post-experience usability evaluation, this process requires a

(digital/physical) note-pad to support the users in providing pre/post-experience and point-of-experience usability feedback as to their input to the co-design input process.

Accordingly, UI-REF maintains that user-preferred support has to be in place to enable users to provide timely usability feedback. Previous work has deployed tools such as a Multimedia Requirements Engineering Assistant (MMREA) or PopEval for online dynamic usability evaluation and co-design instruments as well as nested video and virtualisation techniques (Badii 2000). Care has to be taken that usability evaluation facilitation is conducted in such a way as to avoid unintended side-effects such as it becoming a source of user irritation, usability complexity and user frustration. Accordingly to support the implementation of the UI-REF user-centred methodology and thus to enable the users' to articulate their perceived instantaneous and cumulative usability evaluation of the Critical-Chains system a managed mix of evaluation support will be adopted such as a pre-experience questionnaire and interviews, usability messaging using whatever note-pad mechanism is preferred by the user (e.g. digital diary file, spoken messaging /texting using a mobile phone) during every day of the usability evaluation process followed by a post-experience questionnaire and interview. This is to ensure the accurate rapid assessment of the authentic Point-of-Experience usability perception as well as the overall usability perceptions plus the societal impacts of the deployment of the system as a whole for verifying the degree to which a system delivers the expected functionalities according to its design specifications. A range of escalated tests will be performed at components, sub-system and system level and the application of test-cases will check the delivery of each use-case, including conformance testing to establish the degree to which the system is (mal)functioning and to ensure that the system delivers its functional requirements based on the identified requirements, described in detail in D2.3.

2.1.7 Evaluation of User Acceptance, Acceptability and Use of Technology

The well-established Technology Acceptance Model (TAM), Davis (1989), (Figure 2), and the Unified Theory of Acceptance and Use of Technology (UTAUT), by Vankatesh, Morris, Davis, and Davis (2003), (Figure 3), are the commonly cited methodologies for the evaluation of the end-user technology acceptance as extended through unifying various models of IT acceptance by combining and integrating the elements of eight prominent models:

- Theory of Reasoned Action
- TAM – Technology Acceptance Model
- Motivational Model
- TPB – Theory of Planned Behaviour
- Combined TAM-TPB
- Model of PC Utilisation
- Innovation Diffusion Theory
- Social Cognitive Theory

TAM has received considerable attention from researchers in the IT field over the past decade although it ignores crucial factors such as technology readiness or compatibility. However, TAM has been widely used in many areas, for instance, e-Government applications as it presents a widely-adopted set of constructs such as perceived-ease-of-use, perceived usefulness, attitude toward using a system, behavioural intention to use a system and finally the actual use of a system. UTAUT has built on TAM by considering other factors such as readiness, interoperability, compatibility, and scalability which has led many researchers to apply UTAUT or TAM-UTAUT hybrid models in technology assessment.

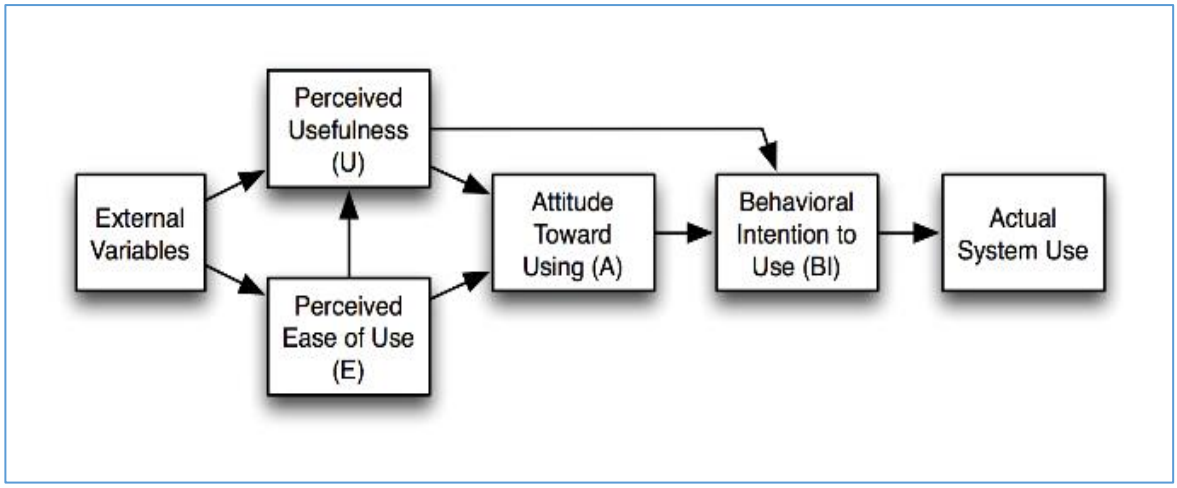

Figure 2: Technology Acceptance Model, Davis (1989)

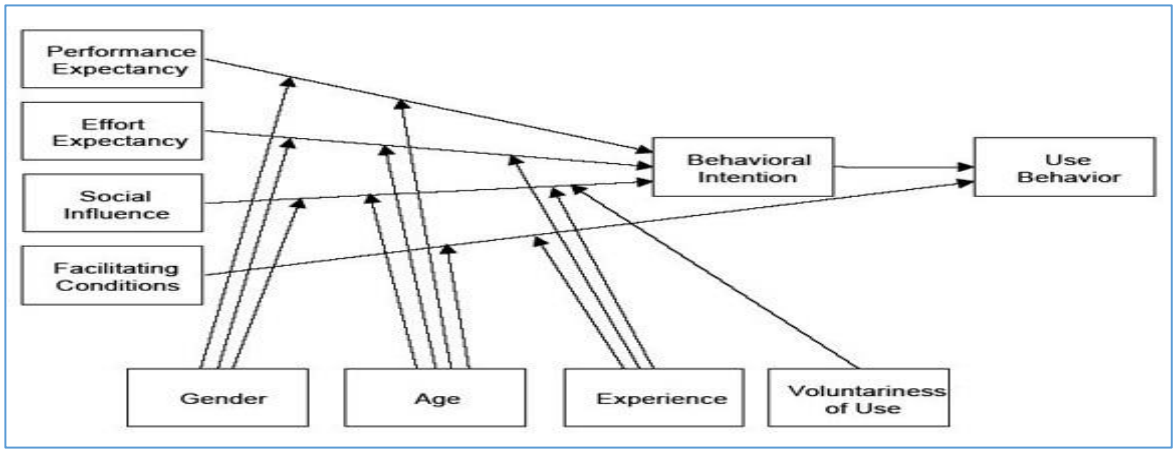

Figure 3: Unified Theory of Acceptance and Use Technology, Vankatesh (2003)

According to Vankatesh, in UTAUT, there are several metrics for an evaluation process, such as attitude, behavioural intention, anxiety, playfulness, self-efficacy, effort expectancy, facilitating conditions, image, objective usability, performance expectancy, perceived ease of use, perceived enjoyment, perceived usefulness, perception of external control, social influence, subjective norm and voluntariness. The factors of measurement and analysis are, therefore: reliability, validity, means, standard deviations, correlations, factor analysis and structural equation modelling.

UI-REF is distinguished from the above two techniques by its commitment to:

1. An ontological and systematic analysis of all possible metrics appertaining to relevant context-aware operational performance metrics, evaluation of sustainable perceived usability, ELSI Impacts, Socio-economic Impacts.
2. An underpinning of well-established psycho-cognitive principles governing the user's Human Judgement and thus integrating the consideration of the interplay of Human Pleasure-Pain-Recall theoretic biases that unavoidably affect perceived human usability evaluation, technology acceptance and social acceptability
3. Analysis of Transitional and longer term enduring usability and acceptability of the system based on Dynamic Usability Relationship Modelling based on pre-experience, point-of-experience and post-experience usability evaluations in the context of each sequence of serial instances of the user using the system.

4. Integrating all user-centred co-design tools and techniques and encompassing the subsets of relevant metrics as included in TAM-UTAUT with higher use-context-specific semantic resolution so as to deliver actionable co-design evolution of the system.
5. Integrating usability evaluation with a framework for requirements ranking review which is after all the raison d'être for any system evaluation within a user-centred agile evolutionary co-design process.

The approach adopted in the Critical Chain evaluation plan is consistent with and inclusive of the TAN-UTAUT techniques as it not only extends well beyond the criteria these techniques allude to but also assesses and analyses these within a context-aware ontological framework and system-of-system relationship-based perspective.

This implies that UI-REF approach amply serves to provide the knowledge basis to support technology acceptance modelling as it integrates high-resolution usability analytics based on both ex-ante and ex-post evaluation of levels of priority criteria. Priority criteria include safety, security, privacy, autonomy, and, comfort of citizen, organisation, ELSI, societal, and sustainability, sensefulness, usability, scalability, affordability. These constitute the over-riding metrics for consideration of not just technology acceptance but also social acceptability and the social materiality of innovation. These aspects are particularly important in the context of disruptive innovation as in the case of FinTechs, and new forms of digital transformative intermediation that constitute the deployment context of the Critical-Chain innovation. As such the usability knowledge arising from the planned integrative usability evaluations through the scheduled trials will be harnessed to also support the analysis of technology acceptance and social acceptability of the Critical-Chains system.

2.2. Evaluation Plan Phases

This section sets out the procedure to be followed for the preparatory and actual user trialling phases. The evaluation is an important process that needs to be well prepared and planned. This section explains how to implement the UI-REF Methodology described in the previous section.

1st Step: Sub-system lab-based testing and debugging process

Once the different components are developed taking into account the defined architecture and the requirements that are described in WP2, each Partner responsible for a component needs to proceed with lab-based tests that evaluate the individual behaviour of each of the components and debug the different errors that will be found. This step is crucial to have ready-to-use components for the Integration Boot Camp.

2nd Step: System integration and conformance testing Boot Camp

A physical Boot Camp will be organised to finish the integration of the components that should have been successfully lab-based tested individually. The objective of this meeting is to solve the last errors related to the integration of all the components of the platform. The final objective of this Boot Camp is providing a system ready for evaluation in each pilot.

3rd Step: Establish the mapping from use-contexts, to user scenarios to use-cases and KPIs

The deployment contexts and thus the Use-Cases and KPIs to be assessed will be established. This includes the functional, non-functional, human factors, ethical, legal, societal aspects requirements. As will be described in detail in this document, the initial analysis has already been done and explained in this deliverable. However, this initial analysis will be reviewed and modified after the system is integrated and tested. Chapter 4 summarises the Use-Cases that are described in detail in previous deliverables and an initial set of KPIs per Pilot.

4th Step: Prepare the evaluation scenarios and settings

A non-trivial and insightful evaluation will be prepared by ensuring the evaluation scenarios and settings inclusive of the spectrum of targeted application domains, workflow stages, contexts and settings, actors

(sex/gender/age-inclusive). The scenarios and the evaluation process are described in Chapter 5 of this deliverable.

5th Step: Set out the sequence of the trials

The sequence of steps for the actual trials will be set out, this includes the Healthy Consent process and the end-to-end privacy protection of any personal data by design and by default.

6th Step: Establish a protocol

A protocol based on a unified ontological model and Likert Scale range for users will be established. This protocol provides quantitative and qualitative data as Point-of-Experience of the usability evaluation extracted from the self-expressions and responses of the pre-and-post-experience questionnaires and interviews. It is important that the interviewer and the interviewed user agree on a Likert Scale range to avoid misleading conclusions from the language used in the interviews. An initial draft of the Pre- and Post-Experience questionnaires are included in Annex 1.

7th Step: Specification of location and dates for the interviews

It will be necessary to agree on the venue, time reserved and dates for the pre-and-post-experience interviews with the users. During this step, the users will also be notified about the respective questionnaire templates, the data capture modes and the protocols that have been previously defined.

8th Step: User-side system configuration.

The user-side system configuration is the specific set-up of the elements that are necessary for the evaluation in each of the scenarios of the pilots.

9th Step: User familiarisation and training to use the system.

Once the system is correctly set up for the user, a user familiarisation period is necessary. Hence, training will be provided to the user. Correct familiarisation and training promote goodwill toward the new platform, minimise attrition and even increase the retention, providing a more diverse insight evaluation.

10th Step: Establish a technical support line

Even although the user will be familiar with the platform and will have received an educating training, a technical support line will be established. In addition, a protocol for providing the users with evaluation-time technical support during evaluation execution will be set up. This technical support will answer any question, problem or doubt that could appear during the evaluation process.

11th Step: Perform the post-experience questionnaire

At the conclusion of the evaluation period, the post-experience questionnaire will be performed. It is crucial to perform the post-experience questionnaire as soon as possible to collect a good and insightful opinion of the evaluation.

12th Step: Collect and compile the questionnaires

The questionnaires will be given to different users and at different times to adapt to their availability. Once, the different evaluations have been carried out, it is necessary to collect the data from the various sources deployed. The collected data will be compiled and analysed together.

13th Step: Analysis of the results

The analysis of the results will show certain usability issues that need to be resolved in the next phase. This might include re-prioritisation of the requirements to be actioned and implying transformative sectorial and cross-sectorial impacts (short-term/long-term) for socio-ethically reflective co-design.

14th Step: Tabularisation of recommendations

A tabularisation of the recommendations for requirements, refinements and/or re-prioritisation results as formative, summative, illuminative, integrative evaluation results will be needed considering the results of the evaluation

15th Step: Technology Acceptance & Social Acceptability Analysis

An analysis of the end-user technology acceptance metrics will provide the knowledge basis to support technology acceptance and social acceptability of the new technology developed.

2.3. Key Performance Indicator Identification

With KPIs, a company can measure its progress in reaching its goals. In contrast to more general performance metrics, they only indicate critical progress for the success of the company. Therefore, it is important to work on the defining points of all the different tasks necessary for reaching the goals. This means, it is necessary to define new KPIs for each use-case, therefore for this deliverable identifying specific KPIs for all the pilot areas. In order to do this systematically, to illustrate KPIs a clear definition and structure is necessary. In any event, they need to be identified by a name, a description and a unit of measurement. This is necessary to guarantee their uniqueness and avoid any misunderstandings regarding their definition. In addition, in Critical-Chains, the KPIs have been subdivided into categories (functional, non-functional, ethical and legal, human factors), into sections, such as cost maintenance and have been prioritised according to the UI-REF methodology. This provides an additional structure and a better overview. For this approach, it is important to first get the ontological domain knowledge to identify the stakeholder's desires, needs and concerns.

2.4. Key Performance Indicator Evaluation

To evaluate the KPIs, the results measured in Critical-Chains will be compared to other systems that are present in the market. Analysing the market situation carefully and considering business matters as well as technical capabilities, it can derive a baseline, which serves as the starting point or market average, and a target value, that Critical-Chains wants to reach. The baseline and the target value must be evaluated for each KPI. In order to measure how far the results from Critical-Chains are from either the baseline or the target, it is necessary to define how and how often the data should be recorded. When the data points from our Critical-Chains system are collected, it is possible to calculate the difference from the baseline at each point in time. By using the target value, two additional thresholds can be defined to get three value ranges and assess the level of fulfilment of KPI by the system as "below expectations", or, "meets expectations", or, "exceeds expectations". As an example, considering Time Performance for the use-case "Clearing and Settlement" see Table 1: KPI Example; the relevant KPI is defined as the time, on average, for a transaction to be executed" and it is measured in seconds. This data will be collected at the end of each transaction and the values will be averaged monthly. The baseline is deduced from the properties of the Ethereum Blockchain, e.g. 15 seconds. Considering the business and technical situation, it could lead to 10 seconds for the target value. Then, the additional threshold around the target can be defined, e.g. at 7 seconds. The KPI can now be rated by checking if it lies above the threshold or even the baseline.

Table 1: KPI Example

KPI:	Time Performance
Source of data:	System statistics
Method of evaluation:	Data to be collected at the end of each transaction. The values obtained will be averaged monthly. *t* = The time evaluated in Critical-Chains
Baseline	15 sec
Target	10 sec
Time Performance Rating:	**Range of Values:**

Exceeds Expectations	$t \leq 7$
Meets Expectations	$7 < t \leq 15$
Below Expectations	$15 < t$

2.5. Audit and Compliance Assessment Process

The main purpose is to determine the level of compliance with certain regulations of the Critical-Chains Framework and its components already in the design and development phase. In order to do this, four stages of the compliance assessment process are identified: planning, assessment, reporting and revision.

1. **The planning stage** consists of creating models based on standards or regulations, selecting the component that is going to be evaluated and finally assigning all or part of the templates to the component. A template will be created by extracting the more relevant points from a cyber-security perspective. In Critical-Chains, those templates will be based on GDPR, NIS, PSD2 and AML/4. The set of templates associated with the component constitutes the checklist.
2. **The assessment stage** consists in associating the requirements to the points of the regulation contained in each assigned template. On the basis of the requirements, for each point of the checklist, it is necessary to establish whether the component in question is compliant, is not compliant or is not applicable to that point.
3. **The reporting stage** consists in visualising the results of the evaluation in the form of reports and statistics. The degree of compliance with the templates is expressed as a percentage, this value can be taken into account as a KPI.
4. **The revision stage** consists of reviewing the requirements if the result of the assessment is deemed unsatisfactory.

This overall process, described above, is iterative, whenever a non-compliance occurs it is possible to review the requirements and carry out the evaluation again.

Figure 4 below inllustrates the Compliance Assessment Process.

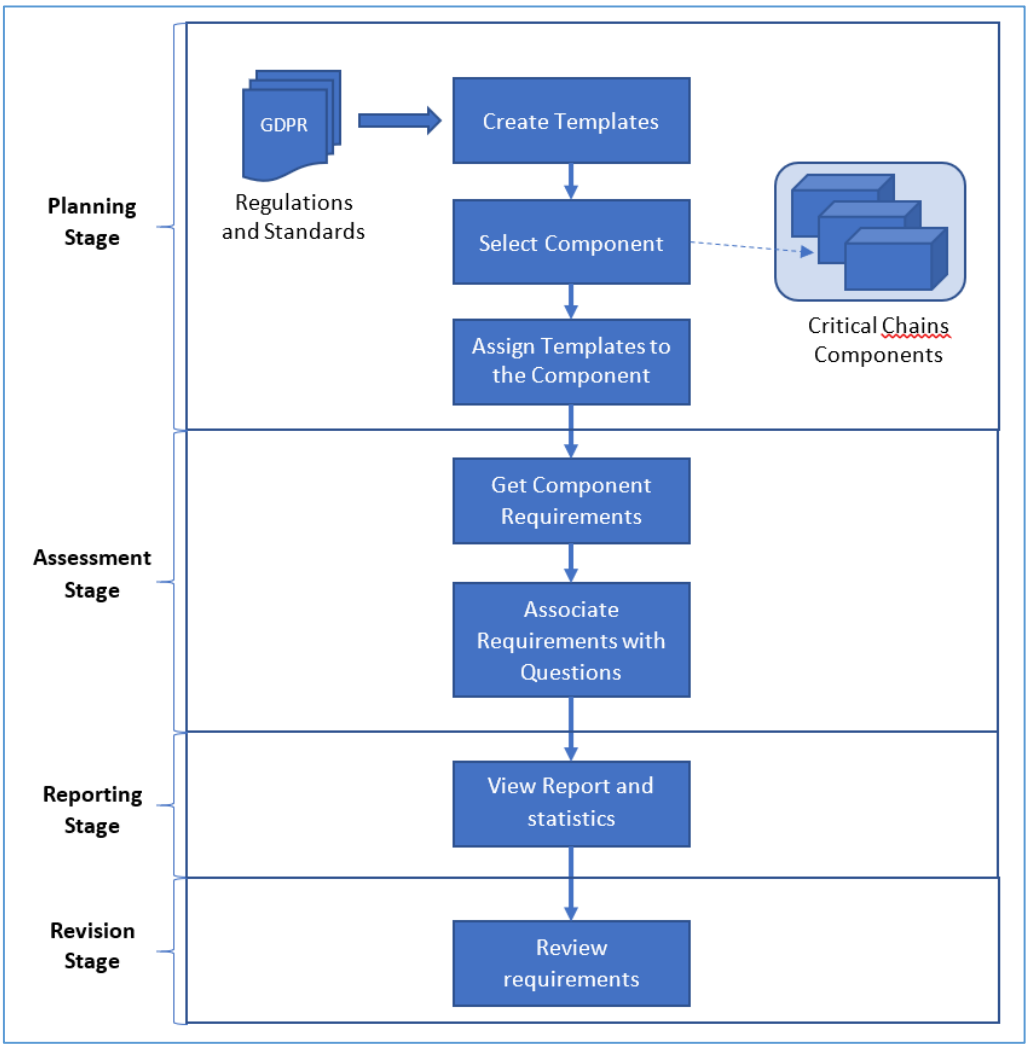

Figure 4: Compliance Assessment Process

3. Ontological Domain Knowledge Analysis

Fintech describes the financial technology and the industry encompassing any kind of technology in finance from stakeholders to consumers. Fintech enables companies, businesses, and consumers to manage their financial processes, containing a different kind of sector such as banks, financial non-profit, investment management, payments, exchanges and the insurance sector. These sectors are increasingly developing their own technology about financial services offerings that are accessible, personalised, transparent and cost-effective. In recent years, the incumbents come up with new kinds of Fintech versions of services such as foreign exchange and peer to peer payments. However, many Fintech applications mainly target consumers, therefore, there are gaps in Fintech between both stakeholders and the consumers' side that need to be fulfilled.

3.1. Analysis of the Emerging Needs of the Fintech Sector

3.1.1 Stakeholder Gaps

The Fintech Sector has experienced a deep transformation with new services that are taking place on a global scale. There is a big gap in the Fintech market from Stakeholder's point of view. The services that

are available in the Fintech market do not provide a neutral environment with the user's multiple financial services. Many stakeholders need is to see all their financial products in a unique frame to analyse their customers' behaviour together and track their company's financial status. This unique speciality could adapt stakeholders to new Fintech services easier and it will lower the marketing barrier to small service providers as well.

The research study carried out by an antivirus firm called Bitdefender indicates that financial sector companies face 300 times more cyber-attacks compared to other industries (Fintech-time 2018). Sometimes, a new technology comes with risks in terms of ease of use. Particularly the financial services involve storing customers' data and regulators are very concerned about the security in this topic. Therefore, Fintech companies should handle these kinds of attacks in order to provide the needed security to protect this critical information. Cyber-attacks not only endanger banks, but it is also putting at risk any other sector companies. As a result, new security approaches are needed, and the current ones need to be updated.

Although Fintech services usage has recently risen, there is another data privacy issue that concerns stakeholders, sharing customer's data with non-financial companies. It is very hard for financial authorities to develop regulatory responses to assist innovation and provide safe financial systems. Many policymakers examine closely Fintech developments and their impacts on markets. To assist this process, the Centre for Latin American Monetary Studies (CEMLA) established the Fintech Forum made of 18 Latin American and Caribbean (LAC) Central Banks that launched a stream of work to analyse Fintech regulatory aspects in the region and created a task force, known as the REG WG. (2019 REG WC Report).

Even although there are as yet no Fintech regulation that directly stipulate the pre-requisite regulatory requirements for qualifying as a Fintech company, there are many regulations that indirectly affect the operation of Fintech companies. For example, there is a regulation that defines Payment Services that is applicable to the Fintech companies focused on payments. Settlement. However, for analysing the market and regulations, regulators need access to actual transactional requirements. For instance, in Turkey, there is the Financial Services Act 6493 which focuses on Payment Services indicated below.

Act no. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions Article 12:

> *1. All the transactions required for operating a payment account including the services enabling cash to be placed on and withdrawn from a payment account,*
>
> *2. Execution of payment transactions, including the transfer of funds on a payment account with the user's payment service provider, direct debits, including one-off direct debits, payment transactions through a payment card or a similar device, credit transfers including standing orders,*
>
> *3. Issuing or acquiring payment instruments,*
>
> *4. Money remittance,*
>
> *5. Execution of payment transaction, where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT devise and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services,*
>
> *6. Corresponding services enabling bill payments.*

If any operation of the Fintech Company falls into any of these categories, a licence from BRSA (Banking Regulation and Supervision Agency) will be required. Since many Fintech companies and their services do not fit into traditional banking categories that are in any case heavily regulated, most of the new Fintech companies start without licences, they acquire them at a later stage. Acquiring licences is a high cost for a young company and regulations can be changed at any time.

Central banks need to balance the money supply and demand in more challenging situations than before. More transactional data is needed for this and Fintech companies can provide it. Blockchain-based currencies and services can provide visibility to central banks.

Large financial institutions have been able to build up mutual trust over a long history of cooperation. Small competitive Fintech companies must discover new trust-building tools, environments and motivations. Much more trust is needed to operate the emerging financial markets.

Most of the Fintech operations are based on cloud environments that bring the needed flexibility and cost-effectiveness. Cloud services require you to trust a cloud service provider (CSP). The data is only as secure as the CSP – and cloud service providers do not always give all the levers needed to understand and manage the security (confidentiality and integrity) of data and processes. Cloud services are also exposed to insider threats from CSP employees and contractors. Furthermore, commercial CSPs can be a subject to extraterritorial legal mandates (e.g. law enforcement data access requests from foreign countries) or conflicting commercial incentives (to monetise data in other ways or gain competitive insight into how your business functions).

Cloud services have unique security vulnerabilities, such as multi-tenancy issues and malicious hypervisor attacks and suffer from the same security issues as self-provisioned IT services. Major cloud services pose an attractive target for attackers – a security exploit can give global access to many high-value customers – and both nation-state and criminal hackers are paying growing attention to commercial cloud services. Even when cloud services are secure, misconfigurations and administrative errors frequently create security holes. With the growing complexity and virtualisation of cloud architectures, this problem is getting worse.

A growing list of horizontal and sectoral regulations means compliance, certification, auditing and reporting to a growing list of different government and private bodies that means an immense cost. Governments are risk-averse when it comes to information security. They need to ensure absolute sovereignty over their data. Failing this mandate is not just a business risk but a failure of one of its main tasks as a government. Data protection law alone is not enough fall back – e.g. there are exceptions for national security, which is precisely the area that every government must address. For public services, government bodies have an extra layer of administrative law that often imposes further restrictions on how data can be processed. Guidelines on individual information systems are often written into law. Government agencies also face transparency and oversight mandates that need third-party auditing. “Government” is not one enterprise, but a series of agencies and bodies with their own mandates and sometimes conflicting agendas. Making a single whole-of-government approach to IT systems is difficult. Governments also need to take particular care to avoid lock-in or dependence on a single source of cloud services. Governments must provide “universal service”, which means they face additional difficulties in jettisoning old legacy systems or standardising processes on a single platform.

Over the last decade, the paradigm for cybersecurity has been largely perimeter control, signature-based heuristics and Artificial Intelligence (AI) probabilistically making assertions of potential compromise. This approach breaks down in the era of cloud and edge/IoT – services are running on someone else’s infrastructure, so there is no perimeter to protect. Security and audit costs have also skyrocketed, especially in the log ingestion and analysis space. Vendors typically charge by the number of logs stored, which means escalating costs with growing data volumes. Log analysis cannot be fully automated, which means expensive security teams in the private sector and – frequently – nothing at all in the public sector. Also, breaches are detected weeks or months after they occur, leaving it too late to act. Regulators have supported new cloud security standards and certifications, but these are static check-boxing exercises that confirm the compliance of cloud service at the point of audit (e.g. once a year), but do not provide ongoing compliance for platforms and services that are constantly renewing and updating.

3.1.2 Consumer Gaps

The Incumbent Fintech companies have realised that existing and emerging enabling technologies, mobile and cloud are changing customer's expectations significantly. However, Fintech is not taking advantage to meet the customers' expectations because it is difficult to adapt legacy systems. Therefore, "new kinds on the block" have emerged to fill gaps as new Fintech providers in areas related to new transactional modes, payments, loans and investments.

Many Fintech incumbents are viewed with a perceived trust deficit from the customers' perspective. Interviews show that customers do not trust Fintech operations for loans or transactional operations as much as they trust Payments with the traditional actors. Fintech companies have been developing services to provide great value to customers. These services are mainly based on electronic services such as e-invoice, e-payments and e-government services. The purpose of these new services is to raise awareness and gain customer trust by directing service promotions at customers to match their monthly behavioural analysis.

Not all companies are aware of Fintech technologies. Such "non-adapters" believe that traditional methods will continue to be dominant, and they believe they are more secure compared to Fintech services or products. However, customers have started to realise that Fintech services and products are secure and friendly and non-adapter companies have begun to shift to new technology areas. As the gaps in the Fintech area are met, non-adapter companies have start to offer new products, and customer awareness of the available range of services has increased; however there is still a real need for transparent platforms for benchmarking and comparison of various service offering in the emerging financial services market.

3.1.3 Fintech Metrics

The SWOT (Strengths, Weakness, Opportunities and Threats) of Fintech from Customer and Stakeholders perspectives is presented below (see Figure 5). As seen, there are many strengths and opportunities for the Fintech sector. However there exist significant weaknesses and threats ae well. Innovations such as the Critical-Chains project will attempt to fulfil the gaps in the Fintech sector in order to reduce weaknesses and threats; (see Figure 5 below).

Trust in the digital domain needs specific tools and education to ensure take-up and scale-up. Trusted institutions are in a position to establish a framework for the benchmarking of Fintech services. Digital services can support the processes. Transparency and comparison between the different security options will build more trust. From a customer standpoint, it is useful to know how new Fintech services compare to traditional bank services. Informed risk-taking can be a much better alternative than having to opt for monopoly offering. The next steps will define specific success metrics to achieve the business models that can be more sustainable in the Fintech domain.

Some examples of metrics that can be considered for Fintech services company rating (e.g. on a 1-10 scale ranked from least to best value) are: process descriptions available (n); data leaks per year (n); capital (EUR); turnover growth (EUR); customers per year (n); regulations adapted (Y/N).

One of the widely adopted market analysis schemes is called Boston Matrix Analysis Figure 6 below). By its official name, the Boston Consulting Group's product portfolio matrix[1] (BCG matrix) is usually designed to help with long-term strategic planning, to help a business consider growth opportunities by reviewing its portfolio of products to decide where to invest, to discontinue or develop products. In line with the BCG Matrix terminology and analysis, most Fintech companies start off as a service with no market share and a low market growth segment (Dog), moving to high market growth (Problem child). However, the next steps are uncertain as Cash Cow segment companies have been acquired by traditional banks and only a few Fintech companies have become Stars. (See the D2.3. for Critical-Chains Boston matrix analysis).

[1] https://strategicmanagementinsight.com/tools/bcg-matrix-growth-share.html

Figure 5: SWOT Analysis for the Fintech Domain

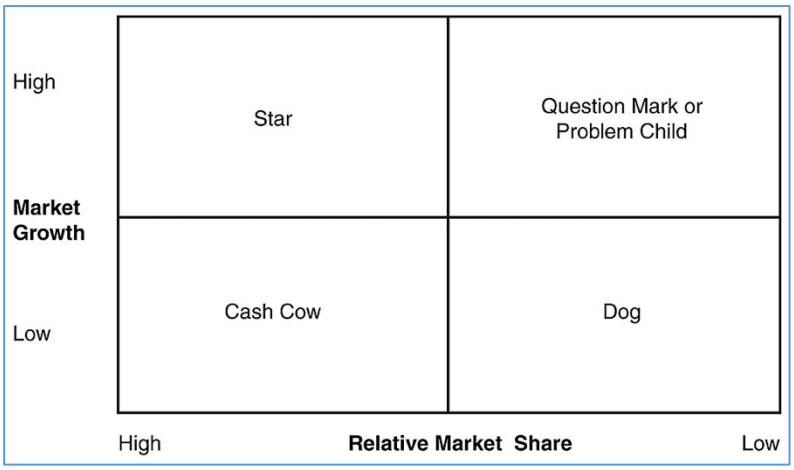

Figure 6: Boston Matrix Analysis

3.2. Stakeholders Interviews Questionnaires

The technology can define how the actors interact with each other and their way of running a business. Initial interviews have been carried out with different stakeholders in order to define the relevant human actors interacting with the technology used in each of the pilots. The interviews helped to generate the first version of the requirements.

3.2.1 Toll Collection Pilot Interviews

Four interviews were conducted related to the Highway Toll Collection Pilot. The interviews targeted 4 profiles as follows: **i)** The Operator of the Toll Highway; **ii)** the Authority who owns the Highway and audits the Toll Highway transactions); **iii)** the expert in the Toll Back Office System; and **iv)** the expert in Cybersecurity.

According to the Operator of the Toll Highway a certain data TAG is exchanged in a Remittance Processing of TAGs. In addition, it was explained that the owner of the device must accept future

payments but should be aware that the payment process might take several days and the operator of Toll Highway also indicated that interchanged data is not currently encrypted.

The experts in Back Office Systems stated that in order to use Blockchain Technology, the new platform would need to be easily accessible, secure and guarantee a maximum time response and total availability.

Cybersecurity Experts explain that the passwords of the users must be stored and encoded with an expiration date linked to each user's encoded passwords. In addition, the authentication process that is in the framework should be carried out by a Single Sign-On System and the management roles, users and their password should be centralised in one place. They also indicated that the communications need to be encrypted with SSL certificates.

3.2.2 Insurance Pilot Interviews

The insurance sector has evolved to incorporate Fintech, rather rapidly, by providing new services such as loans. With their customer database, insurance companies have had the chance to gain trust easily compared to other sectors. Although Insurance companies know their customers, according to the interviews there are new requirements that need to be fulfilled. Insurance companies support innovations related to Fintech. The interviews show that there is a large proportion of the consumers who use payment applications such as PostePay, Apple Pay, and SatisPay. The use of these applications needs the requirements to communicate among themselves. Supporting App-to-App payments creates the need for communication among laptops and mobiles. According to the questionnaire outcome, customers trust transaction and loan operations when these involve only small financial transactions. Although the insurance company customers use Fintech services, their use is still limited because customers do not trust these new services. This case points out that there is a need for data protection and the ability to handle "man in the middle type of attacks.

3.2.3 Banking Pilot Interviews

Banking interviews focused on subjects such as Clearing Systems, Settlement System, Ethical Compliance, Laws and Regulations, Online Banking, Mobile Banking, Physical Banking and Card Banking. The interviews were conducted from two different perspectives: Customers and Companies. Although Fintech is more focused on the customers' side, Critical-Chains focuses on fulfilling the needs of both sides. In the banking sector, a customer should be able to open and close a new account and see its detailed information such as the balance or deposit and being able to withdraw funds. In addition to the customer's need, the companies should be able to apply for loans and to see analytics based on their financial balance. Above all, users should be able to sign contracts through smart contracts and users should be able to verify their identity.

3.2.4 Financial Market Infrastructure Interviews

Financial Marketing Infrastructure interviews were focused on digital and mobile payments. Customers, Bank Clerks, Audit, Risk Managers and IT Management areas were interviewed. Customers expect emerging technology to enable 24-7 availability. In addition, offers from all financial actors need to be evaluated. The Financial Marketing Infrastructure goal is to create a user experience tailored for each individual customer which is consistent among all the different channels such as online portals, mobile applications and ATMs. Hence, there are requirements that need to be considered in order to achieve these goals.

From a Regulatory/Audit compliance perspective, there is a need to ensure integrity and reliability of operational data being processed Identification and assessment should be carried out by the Risk Managers when facilities such as loans are requested. For efficiency and to maximise the trust, reliability of data and availability in near real-time, tools for automated identification of risks are essential deemed Risk Managers.

In conclusion, Fintech services need to gain the customers' trust. The operational needs highlighted by the actors interviewed for each of the 4 pilot application domains have informed the specification of the capabilities of the Critical-Chains platform which has been duly designed to cover all their requirements. The interviews showed the customers' expectation to be able to receive all their financial services requirements in one place and have the assurance of regulatory mechanisms to safeguard their privacy and their data from being shared with other companies.

3.3. Stakeholder Requirements

Deliverable 2.3 has already presented a list of ranked requirements. Hence, this section includes only the requirements that have been modified or included in the list described in the previous deliverable. The requirements give an idea of what a system should be capable of from the stakeholder side and how the system covers the requirements. Table 2 and Table 3 show exmples of the requirements. D2.3 has specified the prioritised requirements to be provided by the Critical -Chains system.

Table 2: Company Financial Audit Advisory Use-Case

Requirement No.:	**REQ-L0-034**
Name:	**Recommendation Analytics about the Financial Situation of a Company**
Description:	A company should be able to get recommendations about how to improve the financial situation
Reason/ Comments:	Companies might be required by law or also for economic purposes to get insights into their financial situation and decide what can be done according to the recommendation.
Indicative priority	Desirable
Related Building Block:	BB#4.3: Authentication/Authorisation-as-a-Service (AuthaaS) BB#4.3.1: Secure Stick BB#4.3.2: Facial biometric authentication (if needed) BB#7: Software-Based Audit and Compliance Tool

Table 3: Check Financial Services in One Channel Use-Case

Requirement No.:	**REQ-L0-035**
Name:	**Check Financial Services in One Channel**
Description:	A company should be able to see all its financial services through one channel.
Reason/ Comments:	A company may be using a different kind of services, to be able to ease of use, companies should be able to see all their financial services from one channel
Indicative priority	Desirable
Related Building Block:	BB#4.3: Authentication/Authorisation-as-a-Service (AuthaaS) BB#4.3.1: Secure Stick BB#4.3.2: Facial biometric authentication (if needed) BB#7: Software-Based Audit and Compliance Tool

3.4. Introduction to the Pilot Validation Domains

This section will set out the specific aspects of each of the application domains, Banking, Insurance, Road Toll Collection and Financial Infrastructures, to establish a comprehensive approach; each domain section is divided three sub-sections: Introduction, Uses-Cases and the KPIs. An introduction to the context and the status of each domain by setting out the background is given. Secondly, it has been produced as a consequence of the UI-REF and to prove this framework has methodologically-guided for evaluation, also, to understand the nature of the selected pilot area and revising the knowledge-set of the previous approaches which has been completed in Deliverable 2.3 as the first phase.

A KPI is a measurable value that demonstrates how effectively an organisation is achieving its key business objectives. The third section of this document defines the performance indicators for each pilot domain with reference to the respective use-context and use-scenario to be support in each pilot. Within the context of the Critical-Chains, the evaluation in terms of the KPIs has been established as a methodologically-guided framework. The tables below (Tables 2-6) defined and assessed for the banking area. The KPIs have been structured in an ontological form according to domain demands, needs and gaps which have been analysed first, then the requirements and the related use-cases have been investigated. The ontological approach has provided a comprehensive set of the KPI definitions for the evaluation process.

3.4.1. Banking Sector

3.4.1.1 Introduction to the Banking Pilot

The European banking sector has attracted too much attention during the last ten years. There are several explanations for this: the effects of the global financial crisis on the resilience of banks, the structural role of the banking sector on the success of the government's anti-crisis actions, the susceptibility of the banking institutions to the Euro crisis, and the difficulties of large banks in Italy and Germany, which were perceived as some of the most successful ones in recent decades. The financial crisis had an adverse effect not only on small national banks but also on international institutions that have shown that assessing the performance of the banking sector is still a significant problem not only for the academic approach but also for the National and International Regulators (Balcerzak et al 2017).

Banks are basically business entities that have a special role to play in national economies. Banking institutions may be categorised as financial intermediaries engaged in the allocation of excess liquidity among individuals. They take deposits from institutions with surplus resources and provide these services to inadequate businesses in the form of loans which are essential at the micro and a macro-economic level (Balcerzak et al 2017). During “normal” times, it significantly influences financial effectiveness and potential growth of enterprises. This influence is even more important during the periods of market turbulence or crisis when the liquidity of the banking system determines the effectiveness of monetary authorities, governments’ stabilization and the anti-crisis actions (Brózda 2016, Janus 2016). However, from the perspective of measuring the efficiency of banking institutions, the range of banking services is currently much more diverse than simple financial intermediations. This is the reason why it is very difficult to define or to measure the bank's “production” outcomes. Fundamental dynamics in recent years, such as deregulation increased the competition related to the globalisation process; during the 2007-2008 financial crisis, its long-term consequences have led to increased stress in the industry, it also pressured the banks to minimise their costs and it increased the productivity of operations (Balcerzak et al 2017).

Nowadays, indicative simplistic analytical methods cannot offer an objective identification of ineffective bank operations, which could separate them from the effective ones because they are not operating under conditions of similar returns of scale (Zarinkamar and Akbar 2014). Simple financial indicators cannot capture the multiple natures of inputs and outputs, thus, the multivariate nature of the efficiency phenomenon (Balcerzak 2016, Balcerzak, Pietrzak 2016). These factors decrease the usefulness of standard financial ratios as tools for assessing the effectiveness of the group of banks. In any event the

ethos of our methodologically-guided approach to dynamic usability evaluation based on the UI-REF framework (Badii 2008) is that any features are valued only in the usage-context that are valued by the user and thus worth usability evaluating; therefore, a usage-context-aware analysis of the financial sector (Banking, Fintech, Insurance) and Highway Toll Collection operational workflows has enabled a coherent linkage of use-contexts and scenarios and their supportive Critical-Chains use-cases and their KPIs to ensure relevant, effective and efficient evaluation of each functionality of the system that matters, in the context that it matters most to the users in their everyday routine operations.

3.4.1.2 Use-Cases

The following are the use-cases to be evaluated within the context of the Banking Pilot.

Use-Case No:	**UCA007**
Name:	Smart Contracting + Transactions

This Use-Case explains the Blockchain integration to the Critical-Chains framework and the usage of the overall benefits of Blockchain technology. It describes the involvement of a financial authority between any two parties according to the Triangular Accountability Model which is proposed within the context of Critical-Chains.

Use-Case No:	**UCA008**
Name:	KYC/AML + account management

This use-case covers the overall compliance aspects. It covers GDPR and the governmental standards in the context of the usage. Authentication-as-a-Service will be relevant to this particular use-case and both development and the whole architecture would consider these aspects under the name KYC/AML.

Use-Case No.:	**UCA009**
Name:	Interbank transactions

The Use-Case covers:

- Blockchain-as-a-Service (Mapping of the nodes)
- Blockchain-as-a-Service (Synchronization of the Nodes)
- Critical-Chains Main Framework (APIs for each of the node i.e. Banks)
- Overall System (Compatibility of the user-applications between the nodes in the context of an integrated system)

It covers the component-specific work model and the overall system usage with the user-application between all parties involved in the Critical-Chains framework.

Use-Case No.:	**UCA010**
Name:	International Transactions (Remittance)

In the presented use-case, the accessibility of the Critical-Chains framework has been explained considering the two different aspects. Firstly this supports the transactions between banks located abroad and internal banks of the given county. The idea here is that any bank in Europe may become a party of Critical-Chains and the whole architecture should inter-operate seamlessly. Secondly, an individual should be able to use Critical-Chains-enabled applications, money transaction per se, from anywhere around the world and should be able to make transaction with any party whose operation is similarly Critical-Chains-enabled.

Use-Case No.:	**UCA011**
Name:	Cryptocurrencies

In the presented use-case, the multi-action way of Blockchain integration has been explained within the context of the Critical-Chains framework. The integrated e-wallet of the Critical-Chains framework will aid individuals to support Non-Governmental Organisations (NGOs) or any kind of start-ups per se, via the Critical-Chains-enabled direct integration of Blockchain-as-a-Service with auditability by the authorities. In this way Blockchain usage with Critical-Chains will be more robust and accountable.

Use-Case No.:	**UCA012**
Name:	Clearing & settlement

In the presented use-case, both the architectural and the Critical-Chains components aspects have been explained as in UCA009. However, in this use-case, verification of transactions between the parties has been considered as well. As a solution to this case, Blockchain technology aids as a verification method which will be provided by a specified consensus algorithm in the network and this aspect particularly considered. The investigation has focused on:

- Blockchain-as-a-Service (Specified consensus algorithm to verify transactions by the involved parties)
- Blockchain-as-a-Service (Mapping of the nodes)
- Blockchain-as-a-Service (Synchronisation of the nodes)
- Critical-Chains Main Framework (APIs for each of the nodes i.e. Banks)
- Overall System (Compatibility of the user-applications between the nodes in the context of an integrated system)

This Use-Case covers the component-specific work model and the overall system usage with the user-application between all parties involved in the Critical-Chains framework.

Use-Case No:	**UCA013**
Name:	Credit & Loans (Credit cards, microcredits)

In this use-case, Critical-Chains multi-functionality has been explained. The microcredits in the context of purchasing have been considered as a Blockchain-related aid, in the development phase micro-credit specialised smart-contracts will also be produced in this context to fulfil the expectation of the end-user. On the other hand, the credit card system has been considered to fulfil any kind of banking operation with Critical-Chains. The framework will also be designed to provide proper payment methods within its Critical-Chains Main Framework and third-parties other than banks (Shops - Stores) may be able to direct the payments to the Critical-Chains powered secure payment pool via an API.

Use-Case No.:	**UCA014**
Name:	Mortgage (Property Loans)

In this use-case, the Critical-Chains components increase the quality service. Flow Modelling as-a-Service model in Critical-Chains is mainly focused on the profile-based anomalies and fraud detection. However, for this kind of usage context, this system is optionally used for assessing the credit score of a person. In addition, the Authentication-as-a-Service model of Critical-Chains increases the trust of the person, based on the verification during the approval stage of the mortgage. Lastly, supported by Blockchain technology, smart-contracts are programmed as a payment method for a secure 2-party trustable payment system for long-term mortgages.

Use-Case No:	**UCA015**
Name:	Investments / (stocks, securities, cash, real state)

This use-case covers an API to the stock sharers (i.e. Sensorium) that enables sharing stocks and trading in the regular stock market. Using Blockchain technology reduces the stock market fraud and protects

end-users and sharers. The stock exchange records can be inserted into the Blockchain-enabled distributed ledger. Therefore, all involved parties in the trade need to trust each other.

Use-Case No:	**UCA016**
Name:	Business banking

This use-case covers the need for insights and business intelligence tools. The Critical-Chains Framework is able to fulfil these needs. The whole ledger data from the Blockchain-as-a-Service model feeds the Flow Modelling-as-a-Service to detect anomalies. However, in order to fulfil the need, it is necessary to provide business intelligence tools to give insights into both stakeholders and the end-users via its applications. This data is produced out of the transactions. The data is processed in the Critical-Chains Main Framework.

Use-Case No.:	**UCA017**
Name:	Personal/Private banking

This use-case covers the essential need of the end-users and the stakeholders. The sequence of the Authentication as-a-Service models (with Hardware Security-as-a-Service), the verification of identities and the authentication processes are explained in detail.

Use-Case No:	**UCA018**
Name:	Credit scoring

As described in UCA014, Critical-Chains increases the quality service. Flow Modelling-as-a-Service is focused on profile-based anomalies and fraud detection. However, this system is optionally used for assessing the credit score of a person. Assessing the credit score of an individual is based on an algorithm that uses information from the profiles such as how many bills to pay are expired, how much money they gain, what kind of assets do they have. Using this data, the Flow Modelling-as-a-Service can be specialised for the credit-score measuring. In addition, the Authentication-as-a-Service increases the trust of the person, based on the verification during the approval stage of the mortgage procedure. Lastly, supported by Blockchain technology, smart-contracting is programmed as a payment method for a much secure 2-party trustable payment system for long-term mortgages.

Use-Case No.:	**UCA019**
Name:	Debt collection

This use-case covers the smart-contracting structure. The Blockchain-as-a-Service model can provide smart-contracts and these contracts are autonomous contracts. For example, the debt collection, when an individual would like to have credit/loan from a bank, the bank can set up the specified contract and the debt collection conditions need to be included as parameters of the loan. The smart contract can take the conditions of the loan as parameters and covers the debt collection process automatically until the date of the debt ends.

Use-Case No.:	**UCA020**
Name:	Digital/online/mobile banking

In this use-case, a mobile application for banking is created fulfilling the requirement of accessibility from anywhere supported by the cloud infrastructure which will be provided by the Critical-Chains Main Framework.

Use-Case No.:	**UCA021**
Name:	Blockchain for micropayments

This use-case is focused on the trust of the system and the involved parties. This use-case is based on the integration of the Authentication-as-a-Service within the Critical-Chains architecture. The design of

the Authentication-as-a-Service and the interconnected component of the Hardware Security-as-a-Service model supports the required identification and authentication. On the other hand, the autonomy of the smart-contracts supported by the Blockchain-as-a-Service model will provide an effective, efficient payment solution against the regular solutions.

Use-Case No.:	**UCA022**
Name:	Blockchain for remittance

This use-case supports the banking operations for transactional and payment settlement. In contrast to UCA010 emphasis here is placed on the ease of operation for stakeholders, ease of use for end-users and cost-effectiveness perspectives for both sets of users. Any bank in Europe may become a party of Critical-Chains and the whole architecture should inter-operate seamlessly. This supports individual Critical-Chains-enabled financial transaction from anywhere around the world and should be able to make transaction with any party whose operation is similarly Critical-Chains-enabled.

3.4.1.3 Key Performance Indicators

In further sections, the evaluation will be held with these KPIs specifically for the banking area. Table 4 below sets out the KPIs for the Banking Pilot.

Table 4: KPIs for the Banking Pilot

Categories	Sections	KPI	Metrics	Unit	Target Value	Rating	Range	Comments	Prioritization
Non-Functional	Spesification	Performance	The time it takes, on average, for a transaction to be executed = **Block Period**	s	10s	Exceed Expectations	1< x ≤ 7	The ethereum transactions approves in 15 seconds minumum per se.	Mandatory
						Meet expectations	7 < x ≤ 15		
						Below Expectations	15 < x ≤ 20		
		Scalability	The replication of blockchain data over the cloud environment = **Blocksize**	kb	30kb	Exceed Expectations	40> x ≥ 30	Blockchains scale best with lightweight metadata, provenance, transaction information, and audit information. Currently, the average Ethereum block size is anywhere between 20 to 30 kb in size.	Desirable
						Meet expectations	30 > x ≥ 20		
						Below Expectations	20 > x ≥ 10		
		Accessibility	The percentage of the time that the Critical-Chains services available/functional	%x	%99.99	Exceed Expectations	100> x ≥ 95	Only 8 hours of downtime in a year.	Mandatory
						Meet expectations	95 > x ≥ 90		
						Below Expectations	90 > x ≥ 85		
		Security	Possibility of data tamper against conventional methods and prevention for 51% vulnerability attack	%x	13%	Exceed Expectations	10> x ≥ 0	Easy to leak users' personal information, also security bottleneck is 51% attack which means that a group of miners controls more than 50% of the blockchain network's mining hash rate, or computing power	Mandatory
						Meet expectations	20> x ≥ 10		
						Below Expectations	30 > x ≥ 20		
		Efficiency	Energy consumption against conventional methods	TWh	2.43 TWh	Exceed Expectations	3.5> x ≥ 1	Against regular server-based banking services	Desirable
						Meet expectations	6> x ≥ 3.5		
						Below Expectations	8.5 > x ≥ 6		
	Maintenance	Operational Complexity	Amount of manual inspection	[1,10]	4	Exceed Expectations	4 > x ≥ 1		Optional
						Meet expectations	7 > x ≥ 4		
						Below Expectations	10 > x ≥ 7		
Functional	Cost	Operational Cost	Avarage Transaction Cost	$	0.45$	Exceed Expectations	0.4 > x ≥ 0.1		Desirable
						Meet expectations	0.7 > x ≥ 0.4		
						Below Expectations	1 > x ≥ 0.7		
	Banking Business Process	Flexibility	Interfaces that integrates with both current and future components	[1,10]	6	Exceed Expectations	10 > x ≥ 7	Designing the infrastructure considering the optional requirements as well. (Future needs or possibilities)	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Integrity	Immutability of the transactions	[1,10]	7	Exceed Expectations	10 > x ≥ 7	The distributed ledger of Critical-Chains provides integrity which is a feature of the Blockchain-as-a-Service	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Ethical and Legal		Privacy	Proper usage of pseudonymization and anonymization techniques applied	[1,10]	9	Exceed Expectations	10 > x ≥ 7	Critical-Chains end-users should stay anonymous while making transactions to the other end-users. However, the authority must audit individuals. Therefore in the authority's aspect, the end-user should be accountable.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Transparency	Trust to new functionalities of the banking	[1,10]	8	Exceed Expectations	10 > x ≥ 7	End-users trust banks for traditional functions, not for the new functionalities with transparent operations trust can be provided.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		GDPR	Personal data management platform in an off-chain storage	[1,10]	10	Exceed Expectations	10 > x ≥ 7	The platform not only provides mechanisms for Data Subject rights but also plays as a role of a Data Controller for handling personal data processing and demonstrating data accountability.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Human Factors		Ease of Use	Fit with the business process/environment	[1,10]	6	Exceed Expectations	10 > x ≥ 7	User-friendly financial status dashboard and 3-step secure transaction process	Desirable
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Motivation-to-Change	Promising accessible, secure, handy and efficient infrastructure	[1,10]	10	Exceed Expectations	10 > x ≥ 7		Desirable
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		

3.4.2. Insurance Sector

3.4.2.1 Introduction to the Insurance Pilot

In the last twenty years, the European insurance sector has undergone a deep transformation. A series of EU directives have provided a strong incentive to create a continent-wide single market for insurance services. Their aim was to foster competition, making entry into local markets easier for foreign companies , through direct sale or, as actually happened, though Mergers and Acquisitions (M&As). A higher degree of competition, would lead to more efficient use of the productive factors (X efficiency) and thus a reduction in cost. At the same time, M&As would create international groups capable of exploiting scale efficiency weighed against an increase in market power in national markets (Zanghieri 2009). Figure 7 illustrates the insurance cash flow models.

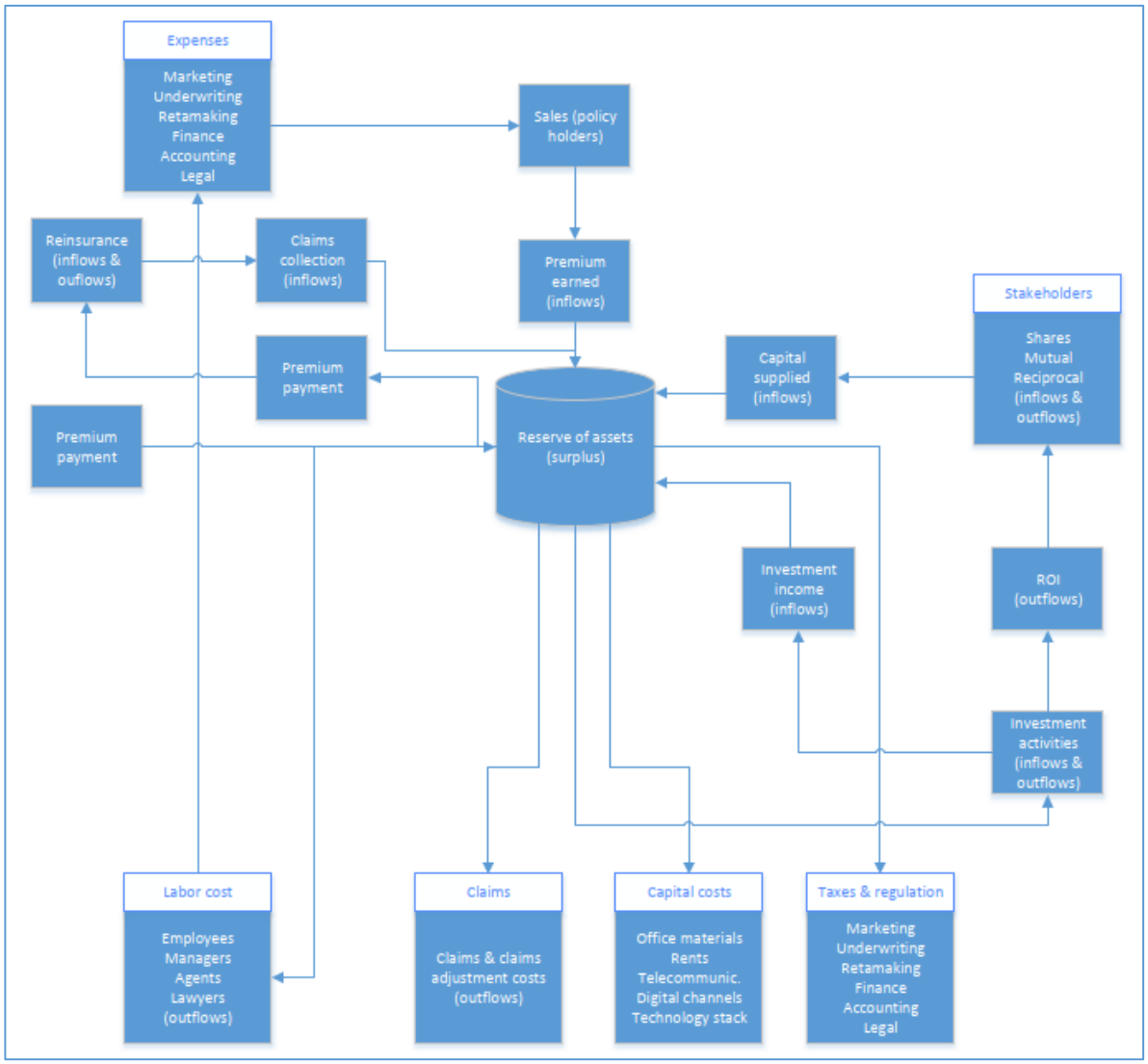

Figure 7: Insurance Cashflow Models

Insurers in Europe are uniquely challenged to stimulate growth and drive innovation and the face of a near-recessionary economic environment, with an extraordinary low-interest rate and negative yield curves. Rising customer expectations, ageing populations and workforces, intensifying competition (including from non-traditional players) and closer regulatory scrutiny add further complexity to the industry outlook for the next few years. In many ways, European insurers face a more difficult environment than their counterparts in other global regions, if only because the future industry growth

is highly dependent on broader economic growth in the region ("EY 2020 Insurance Outlook.").There are many theories that explain how insurances can maximise and improve their operations. The financial portfolio theory for an insurance company views the activity of an insurer as a levered investment operation that borrows funds, by issuing risky obligations and investing part of these funds in securities (Nourani, 2016).

Other strategic moves include divesting from businesses in non-core and unprofitable markets, as well as selling back books of business — often to private equity players — at the right pricing levels. Many insurers are also looking to cloud technology to enable digital transformation and faster development of new digital products. Of course, as they transition to the cloud and more digitally oriented portfolios, insurers must strengthen cybersecurity frameworks.

Given recent results, European insurers have understandably focused on reducing costs and upgrading technology. These efforts have been underway for years but have yet to deliver breakthrough returns. The bottom-line pressures have forced insurers to explore creative options - from acquisitions of Insurtechs for ecosystem development to green-field deployments and "New Co" creation to cloud migrations. However, core legacy systems remain in place at many firms and in some cases prevent insurers from adopting new technology, including launching apps or moving to the cloud. Compared to their peers in other regions, some European insurers are lagging behind in some innovation areas. Those firms that can apply lessons learned from leaders elsewhere can quicken the pace of their own transformations.

According to the EY report "European Insurance Outlook 2020", the main trends identified that are reshaping the insurance industry are:

1. **Digitise sales and distribution:** Life insurers can and should be more digital in everything they do. This is true of both the products they sell and how they sell them. Current life insurance products are generally not digitally enabled or available through digital channels. As a result, customer needs are not yet reflected in the product pipeline or in product development processes. Furthermore, the value proposition for most products is too general and narrow. Most consumers are looking for a more holistic and personalised approach that is driven by their individual needs. The digitisation journey is inevitable, but some sort of face-to-face interaction will be necessary because of the complexity of life insurance products. The life insurance industry needs to digitise the sales force to improve productivity. Distribution dynamics are shifting in other ways. As life insurers simplify their products, they can do so more digitally; although they must simultaneously seek the right human-technology balance. In this transition, cybersecurity should always be at the forefront of one's mind for life insurers. As digitisation progresses, this focus should only increase as they hold large amounts of valuable personal information. For insurers in particular, predictive analytics and advanced anomaly detection techniques are the two ways of strengthening their cybersecurity frameworks.
2. **Achieve cost efficiency:** Nearly all major insurance groups in Europe are working towards cost targets they have set for themselves. Most insurers are on their second or third major cost reduction initiative. They are also taking several natural steps, such as divesting from underperforming businesses and moving to more sustainable business models. The continued maturation of consolidators and early signs of adoption among life insurers is another cost management trend worth watching. Cost efficiency is a priority for several reasons. With no investment yields, life insurers are still paying 60% to 75% of their earnings as dividends, mainly to sustain the share price.
3. **Leverage IoT and connected insurance:** Life and health insurers recognise the need to adopt innovative technologies to get closer to their customers. IoT and connected sensors are among the top-priority technologies they will use to realise more customer-driven practices. Innovation in this space initially came on the non-life side, particularly with telematics, where Europe has been a pioneer. For example, Italy has one of the highest telematics adoption rates in the world.

Leading brands and Insurtechs in protection and health have subsequently gained a significant presence across the continent.

IoT experiments and pilots are fairly advanced in many areas. Increasingly, they involve concepts from behavioural economics to help people reduce risks and make better decisions. Universities continue significant research into these areas, and insurers should look at incorporating relevant findings as they develop new value propositions and design new products. This is an opportunity for insurers to boost customer engagement and deliver new benefits at a time in which their products are seen as increasingly uncompetitive. Such an ecosystem is a business environment for insurers to realize the promise of connected insurance. Some will want to be at the centre of their ecosystems, while others will want to provide niche services. Data privacy regulations are one major barrier to insurers' adoption of IoT-based devices. GDPR, for example, may limit insurers' ability to collect data from these devices. Consumer reluctance to share data is another challenge. With the changing definition of personal data (including location data), much of the sensor data insurers hold may fall within the scope of the new regulation. Usage of AI and other technology to create insights from these data might also be restricted, given the requirement to inform individuals about automated decision-making processes. To resolve these challenges, insurers will need to evaluate new products and services relative to GDPR from the earliest phases of development. The goal must be to design privacy and trust requirements directly into their systems and data collection practices.

3.4.2.2 Use-Cases

Below you may find the use-cases, within the context of the Insurance Pilot.

Use-Case No.:	**UCA024**
Name	Reinsurance

The current reinsurance operations can become overly complex and inefficient in some cases. Each risk in a facultative reinsurance contract has to be underwritten independently, which could take up to three months and involve various parties including the ceding company, reinsurers, brokers, and the client. Contracts include huge sums that cannot be insured by one party in order to minimise the risk. If Blockchain can be used to facilitate reinsurance transactions, it has the potential to radically change how certain reinsurance transactions are handled. Certainly, the role of reinsurance intermediaries will diminish in the process given the peer-to-peer nature of the technology. Gone will be the need for the reinsurers to ask the cedent for detailed premium and loss data on the reinsured book of business when all that detail will be part of the Blockchain transaction ledger. Given that it will reside on both the cedent's and reinsurers' secure computer systems simultaneously, the need for separate premium and loss bordereau will be eliminated. A reinsurer can merely examine the ledger and will have at its fingertips all the premium and loss transactions entered by the cedent as part of the Blockchain.

Use-Case No.:	**UCA025**
Name	Cat Bond

A Catastrophe Bond is an instrument that transfers risk from one party to another. Insurance is also a risk transfer instrument and an easy way to think of a Catastrophe Bond is to think of it as insurance in reverse. Catastrophe Bonds are only made available to parties with the highest level of trust as there is a risk that they may not be repaid. Parties that are considered very trustworthy are large cities like San Francisco and Tokyo. These cities can use Catastrophe Bonds to cover the damages of a natural disaster like an earthquake or a tsunami. Since we mentioned the concept of trust, Blockchain plus Catastrophe Bonds will bring benefits to society. This combination enables cities to transfer catastrophe risk to investors all around the world. Such diversification benefits the everyday investor's portfolio and most importantly, Blockchain will make Catastrophe Bonds more popular, enabling every city to have access

to immediate finance in case disaster strikes. This will enable cities to fund emergency plans and save thousands of lives.

Use-Case No.:	**UCA026**
Name	Travel insurance

This use-case will be based on a casual dynamic that will determine the result of the insurance placement. As an example, the cancellation or a delay of a flight (with consequences for the customer) will automatically trigger the insurance premium after a reliable demonstration of the event thanks to the use of oracles linked to smart contracts. These oracles will verify the effectiveness of the delay by enabling the customer to be reimbursed in a matter of minutes (today the process takes more than a few days). The trigger event and his verification will activate the smart contract properties.

3.4.2.3 Key Performance Indicators

In addition to overcoming a "traditionalist" culture in the sector, which is not oriented - at least so far to the creation of new business models based on collaboration, within the context of Critical-Chains, we believe it is important to identify and select the correct correlation models between traditional insurance and Insurtechs. To do this it is necessary to consider the different areas, ranging from business strategy, architectures and technologies, organisation and processes, methodologies, selection criteria and assessment KPIs - to build approaches and capabilities adapted to different realities and business contexts. Table 5 below sets out the KPIs for the Insurance Pilot.

Table 5: KPIs for the Insurance Pilot

Categories	Sections	KPI	Metrics	Unit	Target Value	Rating	Range	Comments	Prioritization
Non-Functional	Spesification	Performance	The time it takes, on average, for a transaction to be executed = **Block Period**	s	10s	Exceed Expectations	1 < x ≤ 7	The ethereum transactions approves in 15 seconds minumum per se.	Mandatory
						Meet expectations	7 < x ≤ 15		
						Below Expectations	15 < x ≤ 20		
		Scalability	The replication of blockchain data over the cloud environment = **Blocksize**	kb	30kb	Exceed Expectations	40> x ≥ 30	Blockchains scale best with lightweight metadata, provenance, transaction information, and audit information. Currently, the average Ethereum block size is anywhere between 20 to 30 kb in size.	Desirable
						Meet expectations	30 > x ≥ 20		
						Below Expectations	20 > x ≥ 10		
		Accessibility	The percentage of the time that the Critical-Chains services available/functional	%x	%99.9	Exceed Expectations	100> x ≥ 95	Only 8 hours of downtime in a year.	Mandatory
						Meet expectations	99.9		
						Below Expectations	99.9> x ≥ 85		
		Security	Possibility of data tamper against conventional methods and prevention for 51% vulnerability attack	%x	13%	Exceed Expectations	10> x ≥ 0	Easy to leak users' personal information, also security bottleneck is 51% attack which means that a group of miners controls more than 50% of the blockchain network's mining hash rate, or computing power	Mandatory
						Meet expectations	20> x ≥ 10		
						Below Expectations	30 > x ≥ 20		
		Efficiency	Energy consumption against conventional methods	TWh	2.43 TWh	Exceed Expectations	3.5> x ≥ 1		Desirable
						Meet expectations	6> x ≥ 3.5		
						Below Expectations	8.5> x ≥ 6		
	Maintenance	Operational Complexity	Amount of manual inspection	[1,10]	3	Exceed Expectations	3 > x ≥ 1		Optional
						Meet expectations	7 > x ≥ 3		
						Below Expectations	10 > x ≥ 7		
Functional	Cost	Operational Cost	Avarage Transaction Cost	$	0.20$	Exceed Expectations	0.2 > x ≥ 0.1	Transactions At or Above in Current Txpool: 112	Desirable
						Meet expectations	0.7 > x ≥ 0.2	Mean Time to Confirm (Blocks): 16.7	
						Below Expectations	1> x ≥ 0.7	Mean Time to Confirm (Seconds): 207	
	Insurance Business Process	Flexibility	Interfaces that integrates with both current and future components	[1,10]	7	Exceed Expectations	10 > x ≥ 7	Insurance services blockchain based needs strong flexibility	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Integrity	Trust to new functionalities of the insurance.	[1,10]	4	Exceed Expectations	10 > x ≥ 4	Innovation mostly on business models and new technologies	Mandatory
						Meet expectations	4 > x ≥ 2		
						Below Expectations	2 > x ≥ 1		
Ethical and Legal		Privacy	Proper usage of pseudonymization and anonymization techniques applied	[1,10]	9	Exceed Expectations	9 > x ≥ 7	Insurance services handle sensitive data so it is important that the information is not only anonymized but also repudiated (GDPR)	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Transparency	Immutability of the transactions therefore the deep insights of the actions	[1,10]	8	Exceed Expectations	10 > x ≥ 7	immutability is important as long as sensitive data can be handled (i.e. right to be forgotten)	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		GDPR	Personal data management platform in an off-chain storage	[1,10]	10	Exceed Expectations	10 > x ≥ 7	The platform not only provides mechanisms for Data Subject rights but also plays as a role of a Data Controller for handling personal data processing and demonstrating data accountability.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Human Factors		Ease of Use	Fit with the business process/environment	[1,10]	8	Exceed Expectations	10 > x ≥ 8	Instant and easy to submit (i.e. travellers, last minute flyers, etc.)	Desirable
						Meet expectations	8		
						Below Expectations	8 > x ≥ 1		
		Motivation to change	Simplifies processes safely and efficiently	[1,10]	7	Exceed Expectations	10 > x ≥ 7		Desirable
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		

3.4.3. Toll Road Operations

3.4.3.1 Introduction to the Toll Road Operations Pilot

Electronic Toll Collection (ETC) is a system that enables the payment of the toll usage fee without the need of stopping for a physical transaction. It is based on remote communication technology; the payment can be carried out automatically and without having to make the physical payment either in cash or on credit card. It is a faster alternative that replaces the classic toll booths and it ensures a constant flow of vehicles avoiding the more and more common vehicular congestion. This wireless system is becoming very common for smart management of highways, especially in countries with high vehicle flow.

The so-called TAG is a small, not bigger than a wallet and is extremely light. The TAG or transponder needs to be placed inside the vehicle and the TAG communicates with the gate and as a result, there is no need to stop to pay for the usage. When the driver goes through the toll collection station or gate, the system identifies the user and registers the pass in the list of transactions automatically. In this way, there is a considerable reduction in queues and waiting times.

Although various Toll Collection schemes are in operation depending on the national legislation and business models, the Toll Collection Pilot is generally composed of three types of users similarly to other conventional models; as follows: The Toll Operator, the Merchant and the Authority. The Authority is the owner of the Highway, the Toll Operator is responsible to the Highway for a certain number of years that are reflected in a contract between the Authority and the Operator, the merchant is in charge of carrying out the payments with different banks. This schema is compatible with an interoperable case, where the Merchant could be substituted by a second operator. In both cases, there is an indispensable need for trusted exchange of lists between them.

In addition, there are three different types of list that are consulted or updated: TAG List, Transaction List and Black List. The TAG List describes the registered TAGs, each of them associated to a bank account; the Black List, that describes the TAGs that have not paid previous transactions and as a result, they are not allowed to use the Toll Lane again; and the Transaction List that enumerates the registry of uses per TAG.

To be able to circulate on the Toll Lane, the driver needs to sign a contract that provides the TAG allowing drivers to use fast lanes. This contract links the TAG to a bank account number. Once this is validated, the Toll Operator updates the TAG List of the registered vehicles that can use the fast lanes. Then, a vehicle with its TAG passes through an interoperable Toll Highway, the Toll Highway gate reads the TAG and checks the TAGs List. If the detected TAG is in the TAG List, the vehicle is allowed to pass. However, it could happen that the TAG is in the Black List. Then, the barrier should close because the vehicle is no longer allowed to circulate in the Toll Lane.

In the current system, the Toll Operator and the Merchant exchange the lists that have been described previously to update each other with the operations that have been carried out. In parallel, the Toll Operator needs to inform the Transaction List and the payment information to the Authority that owns the Road in different audits. Hence, the Authority needs to have the right to check the Transaction List to calculate the taxes that correspond to particular usage.

More detailed information about the Toll domain is described in D2.3 Specifications and Architectural Design and further details of the scenarios are described in Chapter 5 of this document.

3.4.3.2 Use-Cases

Below you may find the use-cases, within the context of the Toll Road Pilot.

Use-Case No.:	**UCA001**
Name	Remittance send of TAG transactions detected in the Toll Highway

Toll Operator and its Back office system, reads the TAG of a vehicle crossing the Toll Highway, registers the related interoperable TAG transaction with a unique identification (TAG_ID, Plaza, Lane, Date, Time, Transaction ID, Toll amount) and all related data necessary for collecting the transit and sends it to the Merchant in order to charge it.

Use-Case No:	**UCA002**
Name	Remittance reception & processing

The merchant sends a remittance reception notification of a successful payment operation to the Toll Operator.

Use-Case No:	**UCA003**
Name	Remittance reception & rejection

The merchant sends a remittance reception notification of a failed payment operation to the Toll Operator.

Use-Case No:	**UCA004**
Name	Blacklist reception

The Back office of the Toll Operator System periodically receives a Black List from the Merchant in order to allow free pass or not through the fast lanes for TAGs included in the Blacklist.

Use-Case No:	**UCA005**
Name	Transactions audit & taxes payment

The Toll Operator publishes interoperable TAG transaction information to Authority for audit and taxation purposes.

Use-Case No.:	**UCA006**
Name	Role-bases system access

Only authorised users may access customer transactions information. Customers' data should be stored and accessed consistently and securely even under unexpected failures or security attacks.

More information about these use-cases can be found in the deliverable *D2.3 Specifications and Architectural Design.*

3.4.3.3 Key Performance Indicators

The KPIs described in Table 6 below could be updated considering the input from other WPs that develop the necessary components for the Pilot.

Table 6: KPIs for the Toll Collection Pilot

Categories	Sections	KPI	Metrics	Unit	Target Value	Rating	Range	Comments	Prioritization
Non-Functional	Performance	Scalability	Maximum number of transactions per day	Transactions/day	800	Exceed Expectations	x>1000	It is necessary to know the maximum number of transactios than can be registered per day	Desirable
						Meet expectations	10000> x ≥ 500		
						Below Expectations	x<500		
		Capacity	Number of TAG Transactions that can be included in a Blockchain Transcaction	Seconds	0.2	Exceed Expectations	x>0.5	It is necessary to know the insertion time of a transaction.	Desirable
						Meet expectations	0.5> x ≥ 0.2		
						Below Expectations	0.2> x ≥ 0.09		
		Frequence	Response time to of a request to check a list	Seconds	0.5	Exceed Expectations	x>1	It is necessary to know the response time of a check a list.	Desirable
						Meet expectations	1> x ≥ 0.5		
						Below Expectations	0.5> x ≥ 0.1		
	Maintenance	Operational Complexity	Amount of manual inspection	[1,10]	4	Exceed Expectations	4 > x ≥ 1	It is necessary to know the number of inspections.	Optional
						Meet expectations	7 > x ≥ 4		
						Below Expectations	10 > x ≥ 7		
		Accessibility	The percentage of the time that the Critical-Chains services available/functional	%x	%99.99	Exceed Expectations	100> x ≥ 95	Only 8 hours of downtime in a year.	Mandatory
						Meet expectations	95 > x ≥ 90		
						Below Expectations	90 > x ≥ 85		
	Cost	Operational Cost	Avarage Transaction Cost	€	0.45 €	Exceed Expectations	0.4 > x ≥ 0.1	It is necessary to know the avarage cost by transaction	Desirable
						Meet expectations	0.7 > x ≥ 0.4		
						Below Expectations	1 > x ≥ 0.7		
		Efficiency	Energy consumption against conventional methods	TWh	2.43 TWh	Exceed Expectations	3.5> x ≥ 1	Against regular toll services	Desirable
						Meet expectations	6> x ≥ 3.5		
						Below Expectations	8.5 > x ≥ 6		
Functional	Toll Process	Auditions	Number of Audits by the Authority	day/month	4	Exceed Expectations	10 > x ≥ 7	It is necessary to know the number of audits.	Optional
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Flexibility	Interfaces that integrates with both current and future components	[1,10]	6	Exceed Expectations	10 > x ≥ 7	Designing the infrastructure considering the optional requirements as well. (Future needs or possibilities)	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Integrity	Reduction of misinterpretations between users (black list drivers that use the Toll Collection)	Drivers	0	Exceed Expectations	10 > x ≥ 7	Represents the number of conflicts between the Toll Operator and Merchant	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Transparency	Immutability of the transactions	[1,10]	8	Exceed Expectations	10 > x ≥ 7	The distributed ledger of Critical-Chains which would be provided by the Blockchain-as-a-Service	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Ethical and Legal	Ethical Compliant	Privacy	Proper usage of pseudonymization and anonymization techniques applied	[1,10]	9	Exceed Expectations	10 > x ≥ 7	Critical-Chains end-users should stay anonymous while making transactions to the other end-users. However, the authority must audit individuals. Therefore in the authority's aspect, the end-user should be accountable.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		GDPR	Personal data management platform in an off-chain storage	[1,10]	10	Exceed Expectations	10 > x ≥ 7	The platform not only provides mechanisms for Data Subject rights but also plays as a role of a Data Controller for handling personal data processing and demonstrating data accountability.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Human Factors	Ease of Use	Easy to use for the current employees	Fit with the business process/environment	[1,10]	6	Exceed Expectations	10 > x ≥ 7		Desirable
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		

The target values represented above are only an initial estimation that depends on the circumstances of the pilot. Thus, it could be refined before the first evaluation.

3.4.4. Financial Infrastructures

3.4.4.1 Introduction to the Financial Infrastructures Pilot

Financial Market Infrastructures (FMIs) have key importance for the correct functioning of the financial system, especially in terms of supporting clearance and settlement of financial operations such as payments, securities, and derivatives contracts; a financial infrastructure enables money to move throughout an economy, functioning as a platform for transactions, whether these are payments, financing, or the transfer of bonds and stocks. FMIs represent a cornerstone for the regular functioning of advanced economies and play a crucial part in fostering financial stability. The overseeing of key FMIs constitutes one of the main prerogatives for central banks and monetary authorities to promote safety and efficiency of the economic system.

It is commonly accepted that an eventual FMI lack in terms of solvency or operational interruptions is likely to lead to a situation of systemic instability; for this reason, the well-functioning of important FMIs is also fundamental to preserve financial stability and their appropriate monitoring is inherent for the purpose of maintaining financial stability.

According to Principles for Financial Market Infrastructures (PFMI) issued jointly by the Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements (BIS) and the International Organisation of Securities Commissions (IOSCO) in April 2012, FMIs include systemically important payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories (Diehl, 2016); In particular:

- **Payment systems (PSS):** an agreed-upon operational infrastructure consisting of a set of instruments, procedures, and rules which enable the transfer of financial resources between the members of the system. A PSS is composed of the members and the entity operating the agreement between members.
- **Central Securities Depositories (CSD):** provision of securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and compensations. CSDs play a crucial part in guaranteeing the integrity of securities issues by ensuring that securities are not unintentionally, or fraudulently generated or deleted or their details changed.
- **Securities Settlement Systems (SSS):** all the institutional and technical disposition necessary for the settlement and the preservation of securities. The SSSs enable the maintaining and transfer securities, either free of payment or against payment (delivery versus payment) or against another asset (delivery versus delivery) operating on a real-time gross settlement, gross settlement or net settlement basis. A settlement system permits the clearing of the obligations of participants.
- **Central Counterparties (CCP):** interposition between the actors of a contract traded in one or more financial markets. CCP becomes the buyer to every seller and the seller to every buyer making possible the performance of open contracts. The presence of CCPs significantly diminishes risks to participants through the multilateral netting of exchanges by imposing more effective risk controls on all members of the system.
- **Trade Repositories (TR):** an entity that maintains a centralised electronic database of transaction data. A centralised and well-designed collection, storage, and dissemination of data that operates with effective risk controls can fulfil an important role in terms of improving the transparency of transaction information to relevant/public authorities, fostering financial stability, and helping the identification and prevention of market abuse. TRs must provide information with the aim of reducing risk, supporting operational efficiency and effectiveness,

and saving costs for both individual entities and the market. This type of FMI is particularly used in the growing sector of OTC derivatives.

FMIs do not constitute rules or regulations but form a basis used by many regulators to shape their own rules for the industry. In addition, a FMIs can assume an operational role (ex.: transferring securities for settlement, or novating derivatives for clearing) or a supervisor role.

Bitcoin, a cryptocurrency and Blockchain network, provides, at a base level, many functions that look like the operations provided by some of the FMIs described above. For example, Bitcoin keeps tracks for all value units on its Blockchain offering the rudimentary function of a CSD. In addition, the network has the capacity to ensure that Bitcoins are not fraudulently created or removed from the network and that their details are not inappropriately changed (sent).

Since Bitcoin enables all participants to create a transaction to send Bitcoins to other members of the system, once integrated into a mined block these transactions are confirmed and effectively transferred. Thus it is possible to see the Bitcoin settlement process as tantamount to that of the SSS. The operations of an SSS, in fact, allow for a security to be moved from one party to the other.

However, Blockchain, at the moment, does not offer many of the fundamental assumptions for the formation of an effective market on a large scale and it is hard to imagine that regulators would permit the removal of the need for CSDs, SSSs, or PSs as legal entities and they cannot offer all of the functions necessary to support the bandwidth of transactions or depth of assets even in a smaller financial market.

A solution could come from overcoming existing technological challenges and gaining a wider adoption amongst market practitioners through a change in the paradigms associated with FMIs as we understand that it imposes the need for change within business models of CSDs, SSSs and PSs. As an example, a CSD might no longer need to maintain the ledger of who owns what, but will still function to ensure that the assets that an issuer has on a decentralised ledger are genuine and if an issuer defaults or has a corporate action on assets held on the ledger, the CSD can ensure an orderly removal or replacement of assets on the ledger (Platt, 2017).

3.4.4.2 Use-Cases

Below you may find the use-cases, within the context of the Financial Infrastructures Pilot.

Use-Case No.:	UCA027
Name	Acquisition of a Financial Digital Asset

“Acquisition of a Financial Digital Asset” is a use-case where several components of the Critical Chain platform are actively used. The login of the user will be addressed using the Authentication-as-a-service component and all the included modules (KYC, Biometric Authentication and 2Factor Authentication). The user will then interact with the specific FMI D-App. The Distributed-App will call the API exposed by the Enterprise Service Bus in order to invoke the Blockchain-as-a-Service modules, particularly the Smart Contracting module for the execution of the smart contracts. The notifications to the user will be managed by the Workflow-as-a-Service module. During each step, the Flow Modelling-as-a-Service will monitor the network traffic and detect anomalies/attacks to the platform.

Use-Case No.:	UCA028
Name	Redemption of a Financial Digital Asset

“Redemption of a Financial Digital Asset” is the use-case is the follow-on to the previously described use-case UCA027 and describes the operation to redeem a financial asset bought before by a user. The login phase will leverage the Authentication-as-a-service component and all the included modules (KYC, Biometric Authentication and 2Factor Authentication). The functionality exposed by the FMI Distributed-App will call the API exposed by the Enterprise Service Bus in order to invoke the Blockchain-as-a-Service modules, in particular the Smart Contracting module for the execution of the smart

contracts required for the operation at Blockchain level. When the transaction is completed, the user will be notified by the Workflow-as-a-Service module.

3.4.4.3 Key Performance Indicators

The evaluation will be performed by reference to the KPIs as listed in Table 7 below.

Table 7: KPIs for the Financial Infrastructures Pilot

Categories	Sections	KPI	Metrics	Unit	Target Value	Rating	Range	Comments	Prioritization
Non-Functional	Specification	Performance	The time it takes, on average, from the financial investment request by the user and when the wallet is actually updated	s	25s	Exceed Expectations	15 < x ≤ 20	The ethereum transactions approves in 15 seconds minimum per second.	Mandatory
						Meet expectations	20 < x ≤ 30		
						Below Expectations	30 < x ≤ 40		
		Scalability	How much time it takes to scale-out the platform in order to respond to a sudden increase of requests	sec	100	Exceed Expectations	1< x ≤ 80	Scaling the solution should be very simple, with zero or minimal configuration needed both on systems and applications	Optional
						Meet expectations	80 < x ≤ 120		
						Below Expectations	120 < x ≤ 1000		
		Accessibility	The percentage of the time that the Critical-Chains services available/functional	%x	%99.99	Exceed Expectations	100> x ≥ 95	The percentage must be very high because Financial Market Infrastructure cannot experiment long downtimes without large impacts on all the financial actors	Mandatory
						Meet expectations	95 > x ≥ 90		
						Below Expectations	90 > x ≥ 85		
		Security	An estimation of the CyberRisk, calculated using the results of Vulnerability Assessment tools on the components involved in the pilot	[1,10]	6	Exceed Expectations	0 < x ≤ 5	It is very important that the components exposed to internet do not have critical vulnerabilities	Desirable
						Meet expectations	5 < x ≤ 7		
						Below Expectations	7 < x ≤ 10		
		Efficiency	Energy consumption against conventional methods	TWh	2.43 TWh	Exceed Expectations	3.5> x ≥ 1	Against regular server-based banking services	Desirable
						Meet expectations	6> x ≥ 3.5		
						Below Expectations	8.5 > x ≥ 6		
	Maintenance	Operational Complexity	Amount of manual inspection	[1,10]	4	Exceed Expectations	4 > x ≥ 1	This value must be considered an estimation of the amount of effort needed for the mainteinance of hardware infrastructure, software infrastructures and distributed applications related to financial market	Optional
						Meet expectations	7 > x ≥ 4		
						Below Expectations	10 > x ≥ 7		
Functional	Cost	Operational Cost	Avarage Transaction Cost	$	0.45$	Exceed Expectations	0.4 > x ≥ 0.1		Desirable
						Meet expectations	0.7 > x ≥ 0.4		
						Below Expectations	1 > x ≥ 0.7		
	Financial Market Infrastructures Business Processes	Flexibility	Percentage of mobile devices available in the market that can be used to perform the transaction	%x	60	Exceed Expectations	70 < x ≤ 100	A large percentage of models with updated software should be supported. Mobile devices with old and vulnerable operating systems should not be supported for security reasons.	Mandatory
						Meet expectations	50 < x ≤ 70		
						Below Expectations	0 < x ≤ 50		
		Integrity	Trust to new functionalities of the Financial Market Infrastructure	[1,10]	7	Exceed Expectations	10 > x ≥ 7	End-users trust banks for traditional functions, not for the new functionalities	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Ethical and Legal		Privacy	Proper usage of pseudonymization and anonymization techniques applied	[1,10]	9	Exceed Expectations	10 > x ≥ 7	Critical-Chains end-users should stay anonymous while making transactions to the other end-users. However, the authority must audit individuals. Therefore in the authority's aspect, the end-user should be accountable.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		Transparency	Immutability of the transactions	[1,10]	8	Exceed Expectations	10 > x ≥ 7	The distributed ledger of Critical-Chains which would be provided by the Blockchain-as-a-Service	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
		GDPR	Personal data management platform in an off-chain storage	[1,10]	10	Exceed Expectations	10 > x ≥ 7	The platform not only provides mechanisms for Data Subject rights but also plays as a role of a Data Controller for handling personal data processing and demonstrating data accountability.	Mandatory
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		
Human Factors		User acceptance tests	Overall result of user acceptance test performed by validating stakeholders	[1,10]	6	Exceed Expectations	10 > x ≥ 7		Desirable
						Meet expectations	7 > x ≥ 4		
						Below Expectations	4 > x ≥ 1		

4. Expected Behaviour of Critical-Chain Components

In accordance with the context-aware forensic analysis of usability relationship-based evaluation as required under our system evaluation methodology (UI-REF), the Effects, SideEffects, CrossEffects and users' Affects (ESEA) resulting from their usage of Critical-Chains-enabled use-cases shall be assessed and recorded in the respective ESEA tables for each use-case. The ESEA tables contain 6 different aspects; thus resulting in 6 categories of consideration from the perspective of the stakeholders. The following tables (Tables 7-14) are to set out to extract the essential information for the assessment of the usability-acceptability and social acceptance of the Critical-Chains-enabled applications and the resulting Effects, SideEffects, CrossEffects and users' Affects (ESEA).

4.1. Critical-Chains Main Framework

Critical-Chains Framework incorporates the Critical-Chain Cloud that comprises of the typical Infrastructure-, Platform- and Software-as-a-Service layers (IaaS, PaaS, and SaaS). The main Framework has up-to-date tools and services which are widely accepted by the community. However, the main framework will also be improved by adding new tools and assets as it provides an elastic and scalable environment. The framework will be suitable for IoT and Big Data applications as it has effective Data Injection tools (e.g. Kafka, RabbitMQ and Cassandra); streaming tools (Spark Streaming); Hadoop-based Big Data processing facility; various storage tools suitable both for high-frequency streaming databases (MongoDB, HDFS, Cassandra, or Azure Cosmos DB) and semantic triple stores (Virtuoso); practical visualisation tools such as Tableau; and efficient search utilities like Solr or elastic search. It will also be capable of providing selective notification messages to subscribers (Pub/Sub) through Redis and SignalR or SocketID.

Figure 8 below, presents the Critical-Chains main frameworks interrelationship with the other Critical-Chains components. The designed model fulfils the requirements of the stakeholders and is also compatible with the Authentication-as-a-Service, Flow Modelling-as-a-Service and the Blockchain-as-a-Service which plays a key role in the project to fulfil the stakeholder and the end-user requirements in the first place.

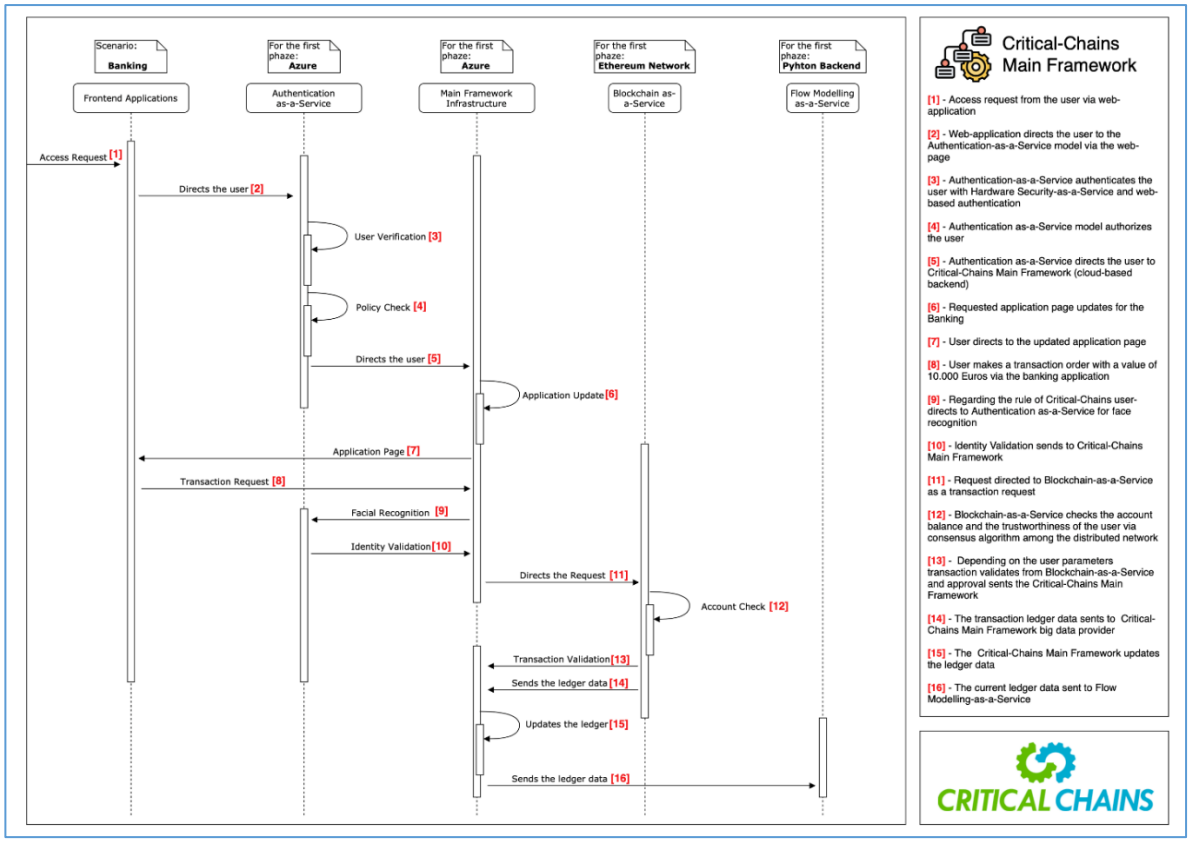

Figure 8: Critical-Chains Main Framework Behaviours

Table 8 below describes the investigation and analysis of ESEA metrics.

Table 8: ESEA Metrics for the Evaluation of the Main Framework

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Availability for the users which indicates the potential downtime a year	At least %99.99 in order to be accepted by the users	Usage of the system except for maximum downtime of 8 hours in a year	The higher operational cost for stakeholders	The higher pricing for the end-users
	Security of the overall Infrastructure	The proper security levels and standards for the expected attacks	The more reliable and robust system for users	The time between two steps increases	The boredom from the system
	Integration with the X-as-a-Service models	Expected request time between steps maximum 15ms	Knowledge of the security with user-friendly and quick system usage	More time lost in the Authentication than the conventional models	Affected motivation-to-Change for end-users
Functional	Supported financial services	Banking, Insurance, Clearing, and Toll of Roads	The higher service radius to Fintech user	The higher complexity of backend operations	The higher system bugs
	Multi-function all in one app	Financial services under one roof	Ease of use	The higher risk of confusion in the app-usage	Loss of interest

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
	Service failure	Expected back-up activities	Tamper-proof system	Need for 3rd phase protection	Explicit in the 3rd phase
Human Factors	Man-Machine Interaction	Straightforward screen navigation	The ability to easily move around in apps	Lack of trust in the framework	Boredom from the system
	Front-end Applications	Screen design with relatively few point-and-click operations	The ability to easily sign or create transactions	Lack of trust in the process	Boredom from the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of the possible data leak	Loss of the customer
Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage
	Compliance	Compliance for human rights	Obedient to human rights	Non-informed actions with personal data	Non-informed actions with personal data
Socio-Economic	Cost-efficient App	The cost-efficient financial operations with one-app	Ability to control the financial situation with one-click	Lack of trust in the process	Boredom from the system
	Transparency	Consensus on the integrity of the financial infrastructures and operations	Trust for the knowledge of the process and increased healthy financial environment	Manipulation from abusive users	Loss of interest

4.2. The Secure Cyber Framework

The secure cyber framework has the purpose of protecting the whole Critical-Chains network against attacks and security violations. In order to achieve the goal of having a holistic resilience framework, that is robust against threats from the outside and also detects anomalies in internal data flows, modules like deep packet inspection, intrusion detection and firewalls are used. The data analysis of different kinds of data sets with state-of-the-art machine learning algorithms allows for the detection of critical points in the network and the provision of a thorough risk assessment, as well as possible countermeasures. One of the most feared attacks on online platforms are DDoS attacks.

To protect a network against such threats it is important to know customer's behaviours and to distinguish between normal failures during password entering and malicious attacks. Also, the attempts of unauthorised access to accounts have to be recognised as such, because the counter strategies differ greatly for different kinds of attacks. The secure cyber framework analyses all login attempts to guarantee that only authorised users have access to their accounts and attackers are blocked, such that they can harm neither the users' account nor the Critical-Chains framework. Figure 9 briefly illustrates the Secure Cyber Framework behaviours.

As in every part of life, security comes with a cost. In the case of Critical-Chains, this cost is not a reduction of user privacy, as this, too, is a main concern of the secure cyber framework. However, other aspects such as larger energy consumption, longer execution times for system functions or additional actions, that might seem unnecessary to end-users, could limit the success of the framework. The following Table 9 presents the ESEA analysis for the secure cyber framework.

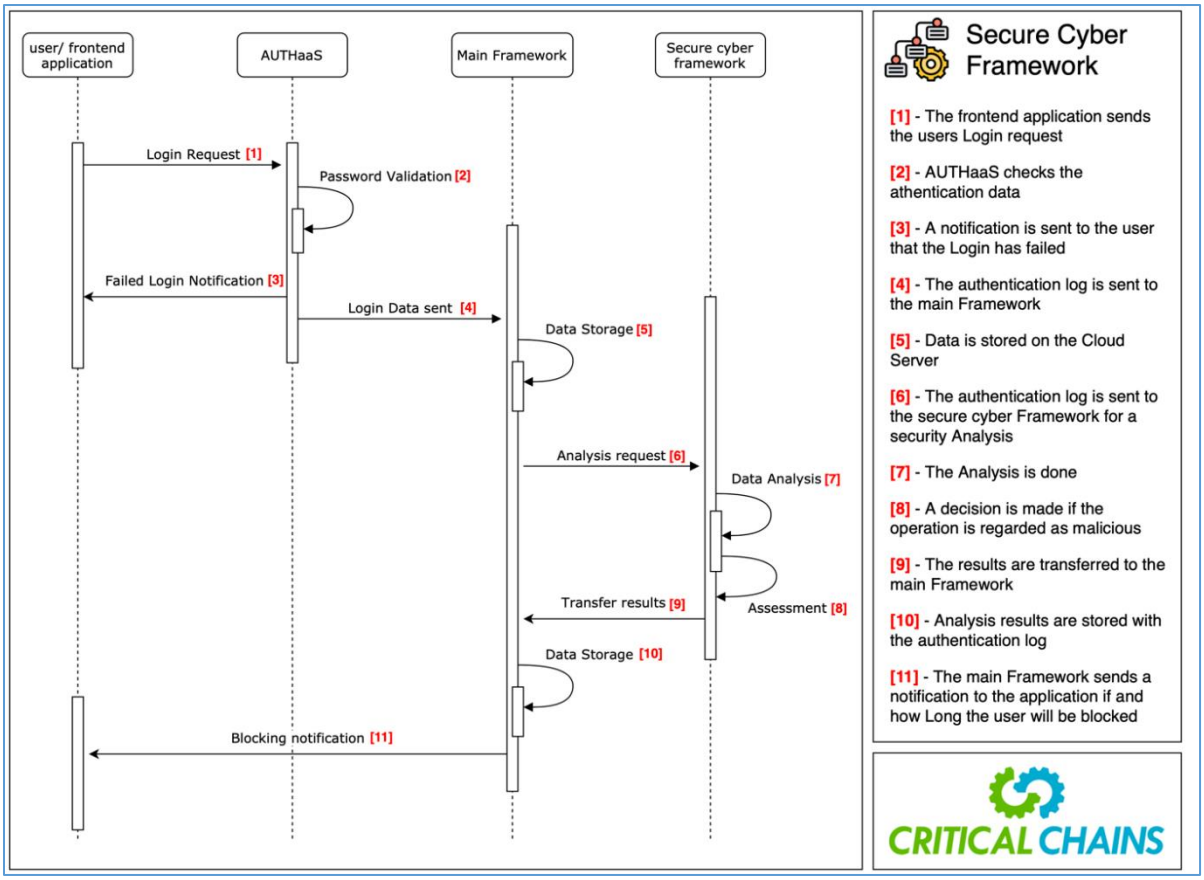

Figure 9: Secure Cyber Framework Behaviours

Table 9: ESEA Metrics for the Cyber-Physical Security Framework

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Intrusion detection	99.99% of attacks should be discovered in time	Robust network	Additional computational cost	Higher energy cost
	Authentication logs	All access attempts (metadata) are stored	Threats are discovered	Higher need for disk space	More hardware components
	Blocking of unauthorized users	The computational effort for blocking can be neglected	Risk of unauthorized access is minimized	Lazy users are punished	User frustration
Functional	Data analysis	All attack strategies are recognized as such	Prevention of unauthorized system accesses	Periodical updates	Server downtime

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
	Firewalls	No unauthorised access to any system components	Additional steps for communication of system components	Longer waiting times	User frustration
Human Factors	ML algorithms for anomaly detection	Anomalies are detected without explicit (man-made) observations	High-level security with low effort	Reliance on Blackbox systems	Lack of trust
Social Factors	Privacy	Preserving user privacy	Users feel secure	Irritating security features	Frustration of customers
Ethical and Legal	Data Security	No data leakage	User trust	Complex security measures need for the latest security technologies	Additional software development and maintenance, Training courses for developers
Socio-Economic	Fraud detection	Victims get notified, Malicious accounts are deactivated	Customers trust each other	Ceasing awareness	Users will be spoofed with legal methods

4.3. Flow Modelling-as-a-Service

The growing digitisation of the business world places companies at more risk of cyber-attacks more than ever before. Big data analytics provides the ability to protect financial infrastructures against such attacks. Big data security analytics involves the ingestion, processing, and analysis of data in order to derive actionable information. In recent years, various security analytics techniques and approaches, such as advanced machine learning algorithms, have become more powerful and effective. Within the context of Critical-Chains the Flow Modelling-as-a-Service is proposed as a utility to detect anomalies in financial transactions, the system presents a novel approach for the detection of anomalies and regarding fraud actions by approaching the problem through the user-basis analysis. Furthermore, it may be described as a holistic network that bases on AI-powered algorithms to analyse profile-based actions in the system. The operation of the Flow Modelling observes individual-based actions such as money transactions, policy-purchases, incomes, assets to define the anomalies and as the result of fraud or not. Figure 10 briefly illustrates the Flow-Modelling-as-a-Service Behaviours.

However, the idea of observing the action and the activities may raise awareness of what would be the expected impacts on the users and society. Therefore, the following analysis given in Table 10 below will examine the user perceived affects. The interrelation of Flow Modelling-as-as-a-Service with other components is set out above, the resulting sequence enables the understanding of the nature of Flow Modelling. By contrast Table 10 below sets out the ESEA metrics appertaining to Flow Modelling as-a-Service.

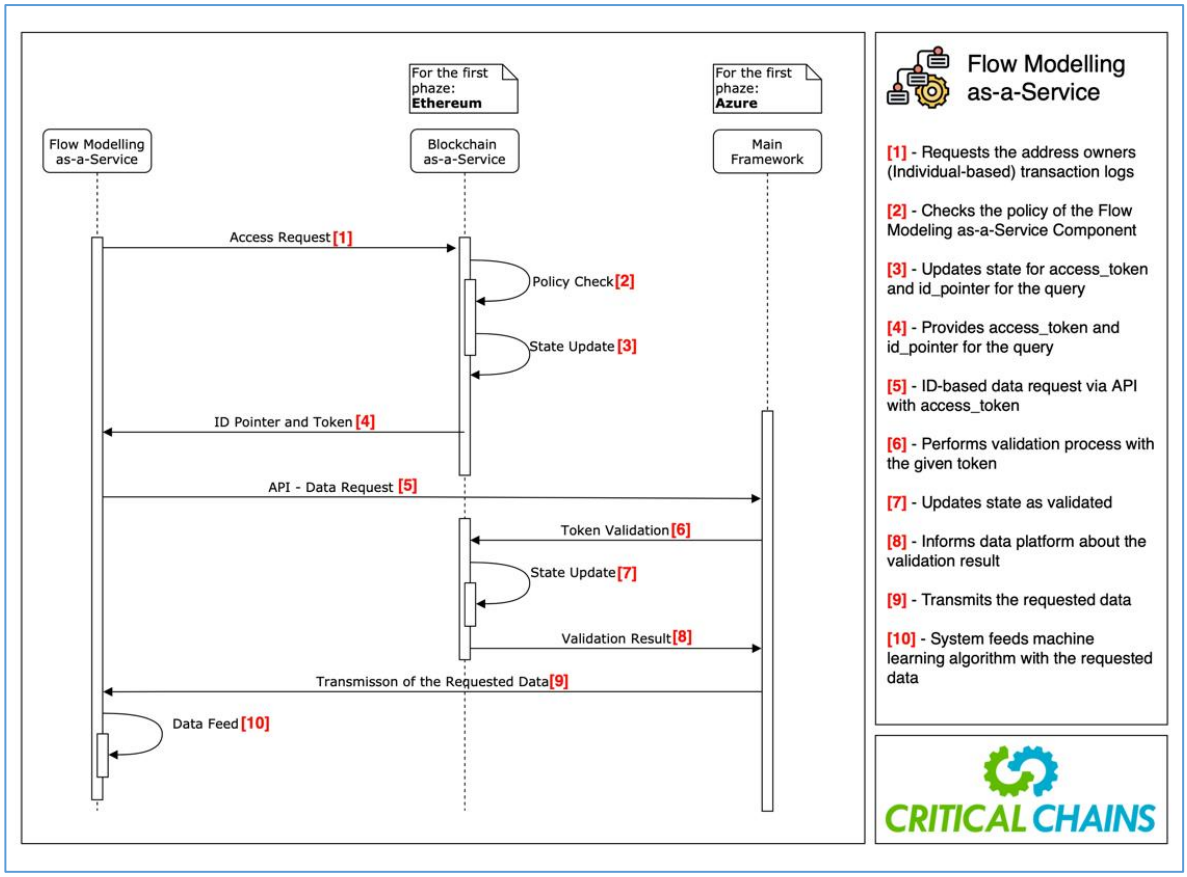

Figure 10: Flow Modelling as a Service Behaviours

Table 10: ESEA Metrics for Flow Modelling-as-a-Service

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Number of predictions at a time	At least %90 of the actual anomalies	More robust financial corporations	The higher hardware cost for computation	The higher energy consumption
	Response time to transactions	No later than ten minutes	Precise analysis with almost real-time activity observation	The higher secure storage need	The higher cost
	Ledger data updating	At least every ten minutes	More reliable classification of anomalies and frauds	The higher need for the data pipeline security	The higher operational needs
Functional	Supported data types	The network, authentication and transactional data	The higher protection of all system entries	The higher the complexity of the algorithms	The higher latency less performance
	Interactive dashboard	Easily traceable user activities	Ease of use	The higher risk of data leak	Loss of trust
	Service failure	Expected back-up activities	Tamper-proof system	Need for 3rd phase protection	Explicit in the 3rd phase

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Human Factors	Activity Monitoring	The pursuit of non-personal data	Mutual trust for a reliable system	Fear of behaviour	Boredom from the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of the possible data leak	Loss of the customer
Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage
	Profiling	Trust for profiling	Trust for profiling	Monitoring unnecessary data	Commercialised profiling
	Compliance	Compliance for human rights	Compliance for human rights	Non-informed actions with personal data	Non-informed actions with personal data
Socio-Economic	Financial Scoring	More precise financial scoring for fairness	Trust to financial result	Fear of behaviour	Boredom from the system

4.4. Cyber-Physical Security-as-a-Service

The Cyber-Physical Security-as-a-Service consist of three component as follows:

1. Blockchain-as-a-Service,
2. Cryptography-as-a-Service (Hardware-as-a-Service)
3. Authentication/Authorisation as-a-Service

The following sections address each of the above in turn.

4.4.1 Blockchain-as-a-Service

Blockchain-as-a-Service is a unique model that enables the use of cloud-based services to develop, use and host their Blockchain apps, functions and smart contracts. In a simple way, they provide fully fledged Blockchain platforms to ease the development process. Blockchain-as-a-service companies act as a bridge between enterprise companies and enterprise Blockchain platforms.

Within the context of Critical-Chains, Blockchain-as-a-Service (BCaaS) is the third-party creation and management of cloud-based networks for companies in the business of building Blockchain applications. Benefits of Distributed Ledger Technologies could be sorted as offering business value and efficiency, for example, assisting compliance, asset tracking, supply chain management, and generally displacing intermediaries. The focus is on multi-party scenarios (across organisations, departments, individuals, etc.), where the ledger provides a transparent and reliable source of facts across administrative domains and improvement in the operations lifecycle. As such, BCaaS offerings are emerging to make Blockchain technology more accessible to businesses, by reducing the overheads of adoption. The precise nature of a BCaaS deployment depends on the service provider, application specifics, and enterprise goals.

Ethereum could be considered as a provider of distributed BCaaS since it supports smart contracts and has standardised guidelines for creating new tokens and applications. As a result, companies can launch

their own application, using the public Ethereum distributed infrastructure through its peer-to-peer network of nodes. Figure 11 below briefly illustrates the Blockchain-as-a-Service Behaviours. ESEA metrics of the Blockchain-as-a-Service are set out in Table 11 below.

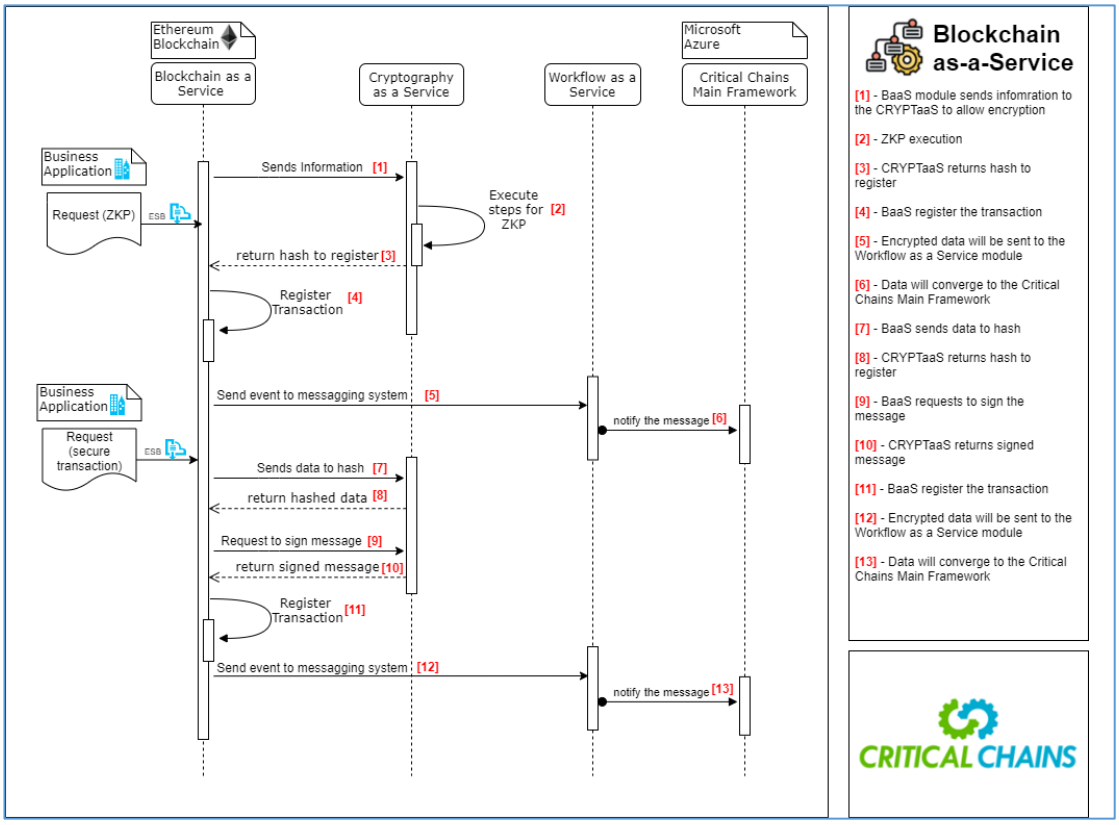

Figure 11: Blockchain-as-a-Service-Behaviours

Table 11: ESEA Metrics for Blockchain-as-a-Service

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Number of predictions at a time	At least %90 of the actual anomalies	More robust insurance corporations	The higher hardware cost for computation	The higher energy consumption
	Response time of smart contracts	Few seconds	Precise execution of business logics	Business logics conflicts	Delay automation
	Ledger data updating	At least every ten minutes	More reliable classification of anomalies and frauds	The higher need for the data pipeline security	The higher operational needs
Functional	Supported data types	The network, authentication and transactional data	The higher protection of all system entries	The higher the complexity of the algorithms	The higher latency less performance
	Interactive dashboard	Easily traceable user activities	Ease of use	The higher risk of data leak	Loss of trust

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
	Zero-Knowledge Proof	The secure and scalable authentication protocol for client-server applications	Fast and lightweight zero knowledge proof (ZKP) algorithm which provides security of the conventional PKI	Undetectable Backdoor in zk-SNARK	Group of challenge-response authentication protocols, in which parties are required to prove the correctness of their secrets, without revealing these secrets.
Human Factors	Activity Monitoring	The pursuit of non-personal data	Mutual trust for a reliable system	Fear of behaviour	Boredom with the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of the possible data leak	Loss of the customer
Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage
	Profiling	Trust for profiling	Trust for profiling	Monitoring unnecessary data	Commercialized profiling
	Compliance	Compliance for human rights	Compliance for human rights	Non-informed actions with personal data	Non-informed actions with personal data
Socio-Economic	Financial Scoring	More precise financial scoring for fairness	Trust to financial result	Fear of behaviour	Boredom from the system

4.4.2 Cryptography as-a-Service/Hardware Security-as-a-Service

The Cryptography as-a-Service (CryptaaS) is a component enabling implementation of cryptographic algorithms (symmetric and asymmetric encryption algorithms) on hardware devices e.g., Hardware Security Module (HSM), Secure-Stick (USB stick). The Hardware Security-as-a-Service (HWSaaS) component relies on the CryptaaS component to provide a multi-factor authentication that is designed to comply with the FIDO standards.

Using the HWSaaS and the CryptaaS components, the user logins using its unique ID that can be either a phone number or a national identity number (or similar). No password associated with the ID is asked for but only the user is requested to plug his SecureStick device (a hardware token) into the PC or the mobile device, e.g. smartphone. The PIN is then requested for the authentication between the SecureStick and the user. If the PIN is correct, the SecureStick verifies the PIN and activates itself. Then, the browser (as a communication middleware) performs the authentication process between the SecureStick and the FIDO server. After the successful authentication, the user is connected to the main framework, and he/she can reach the services presented on his/her page. The user would be authorised to make and complete transactions excluding the high-volume or critical transactions. For such critical transactions, the customer is warned about the biometric (facial) authentication that is required for his/her transaction. Then, the browser requests access to the camera. Finally, the biometric

authentication is realised on the SecureStick and reported to the server. Passing through this stage, the transaction is finalised or proceeded. With proper usage of HWSaaS and CryptaaS, none of the personal data will be placed in the cloud or on an online environment, thus the personal data will only be kept in the Secure-Stick. Figure 12 below, briefly illustrates the CyptaaS and HWSaaS Behaviours. Table 12 further below, presents the ESEA analysis of the HWSaaS and the CryptaaS components.

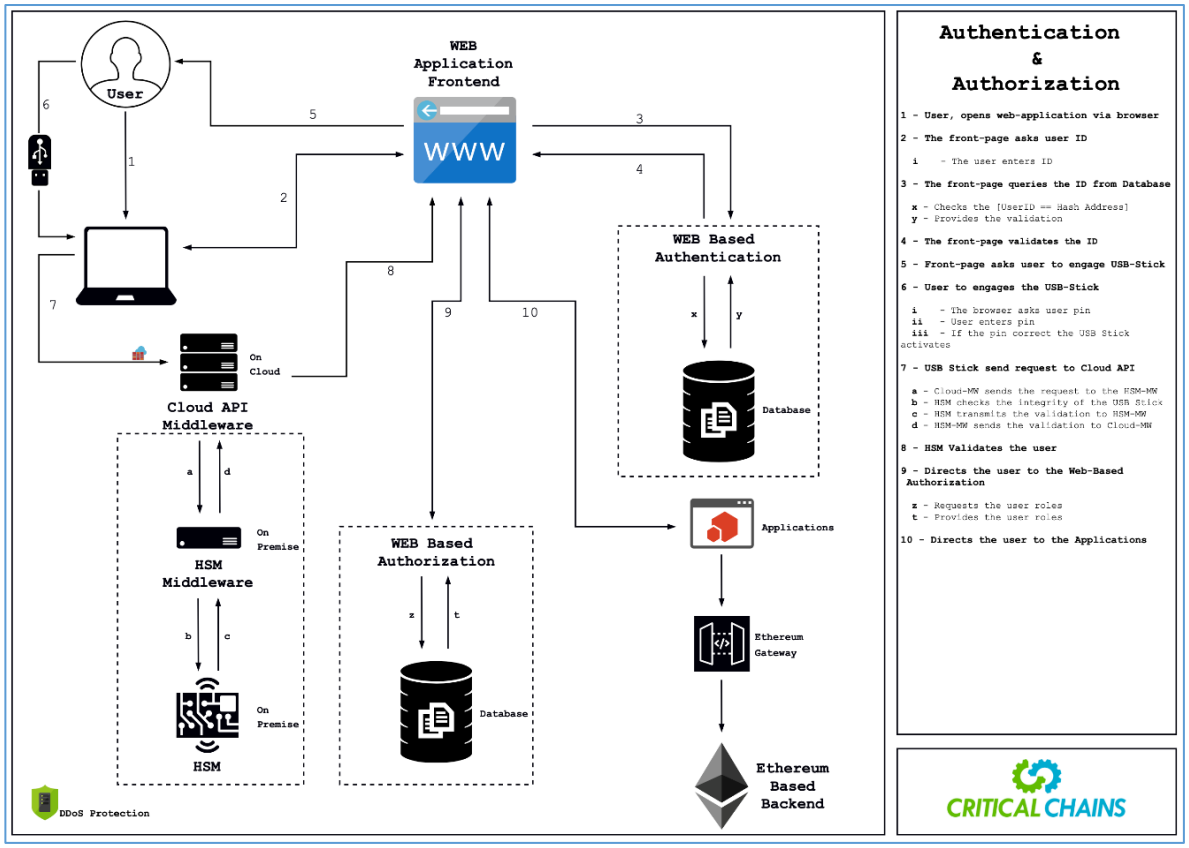

Figure 12: Cryptography as a Service/Hardware-Security-as-a-Service

.

Table 12: ESEA Metrics for Cryptography as-a-Service/Hardware as-a-Service

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	FIDO server response time to authentication	Less than 1 second	Less user boredom from the system	Higher cost for computation	More hardware components
	SecureStick response time	Less than 1 second	Less user boredom from the system	Higher cost for computation	More expensive hardware components
Functional	Biometric accuracy	Less than 0.5% Equal Error Rate among at least 1000 subjects	Less risk of blocking legitimate users or multiple re-authentications	Higher cost for computation	More expensive hardware components
	Personal data	Biometric data stored in the Secure Stick	User empowerment in protecting its personal data	Fear of possible data leak	Loss of customers
	Service failure	Expected back-up system	More robust financial corporations	Higher cost for computation	More hardware components
Human Factors	Man-Machine Interaction	Straightforward screen navigation	Ability to easily move around in apps	Lack of trust in the framework	Boredom from the system
	Front-end Applications	Screen design with relatively few point-and-click operations	Ability to easily choose the supported authentication mechanism/ select the application the user has access to	Lack of trust in the process	Boredom from the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of possible data leak	Loss of customers
Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage
	Profiling	Trust for profiling	Trust for profiling	Monitoring unnecessary data	Commercialized profiling
	Compliance	Compliance for human rights	Compliance for human rights	Non-informed actions with personal data	Non-informed actions with personal data

4.4.3 Authentication/Authorisation as-a-Service

The authentication as a service (AUTHaaS) component is responsible for the authentication and the authorisation processes of users (e.g., individuals, applications, Blockchain services, IoT devices, etc.).

For the authentication process, the AUTHaaS component may rely on an internal identity provider provided by the Critical-Chains platform, or on an external one (e.g., eIDAS server).

The AUTHaaS component supports an authentication workflow that can be either initiated by the identity provider or by the service provider. For an authentication that is initiated by the identity provider, the user navigates to a dashboard where he/she is asked to authenticate using biometric authentication.

After a successful authentication, the user can navigate through the different applications which he/she is authorised to access by clicking, for instance, on their logos situated in the dashboard. The identity provider must know the links to these applications, and these applications must trust the identity provider to validate the unsolicited token received from the user and signed by the identity provider. Figure 13 below, briefly illustrates the AuthaaS Behaviours from the perspective of identity provider initiated authentication.

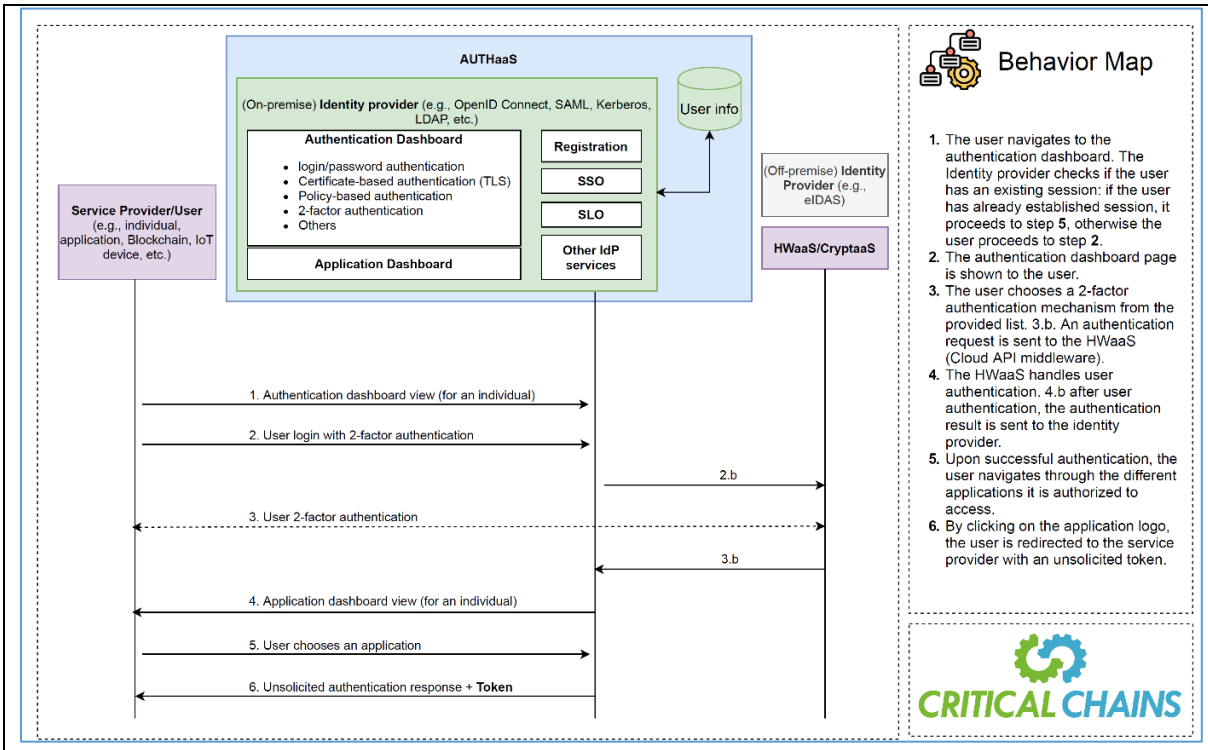

Figure 13: Authentication/Authorisation-as-a-Service Behaviours: Identity Provider Initiated Authentication

Regarding the service provider-initiated authentication, it starts with the user first navigating to the service provider and then getting redirected to the identity provider.

After user authentication, the user is redirected back to the service provider with a token. Figure 14 below, shows the AuthaaS behaviours from the perspective of server provider-initiated authentication.

The authorization process is based on token-based access, i.e., the user provides a token along with the access request and based on the token the AUTHaaS responds with the access decision, either permit or deny access.

The authentication process of the user can be followed by the authorization process if the security of the service or resource requested by the user is managed by the Critical-Chains framework. Figure 15 below, depicts the authorisation behaviours.

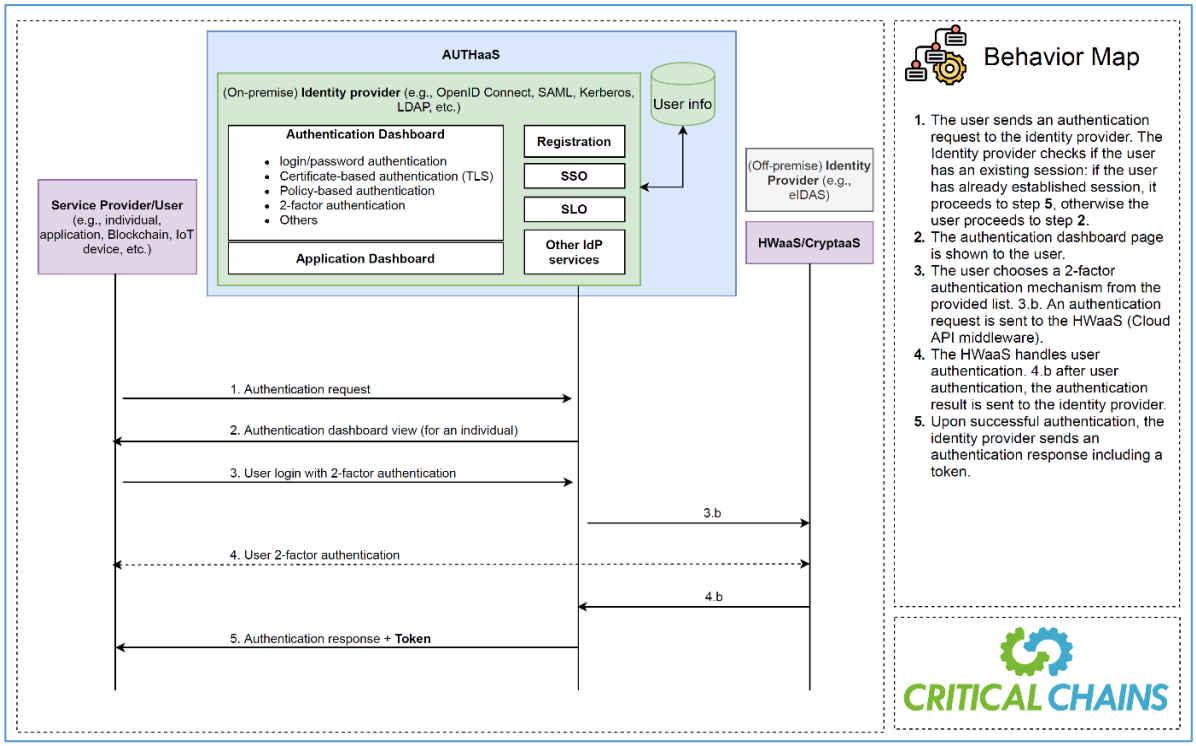

Figure 14: Authentication/Authorisation-as-a-Service-Behaviours: Service Provider Initiated Authentication

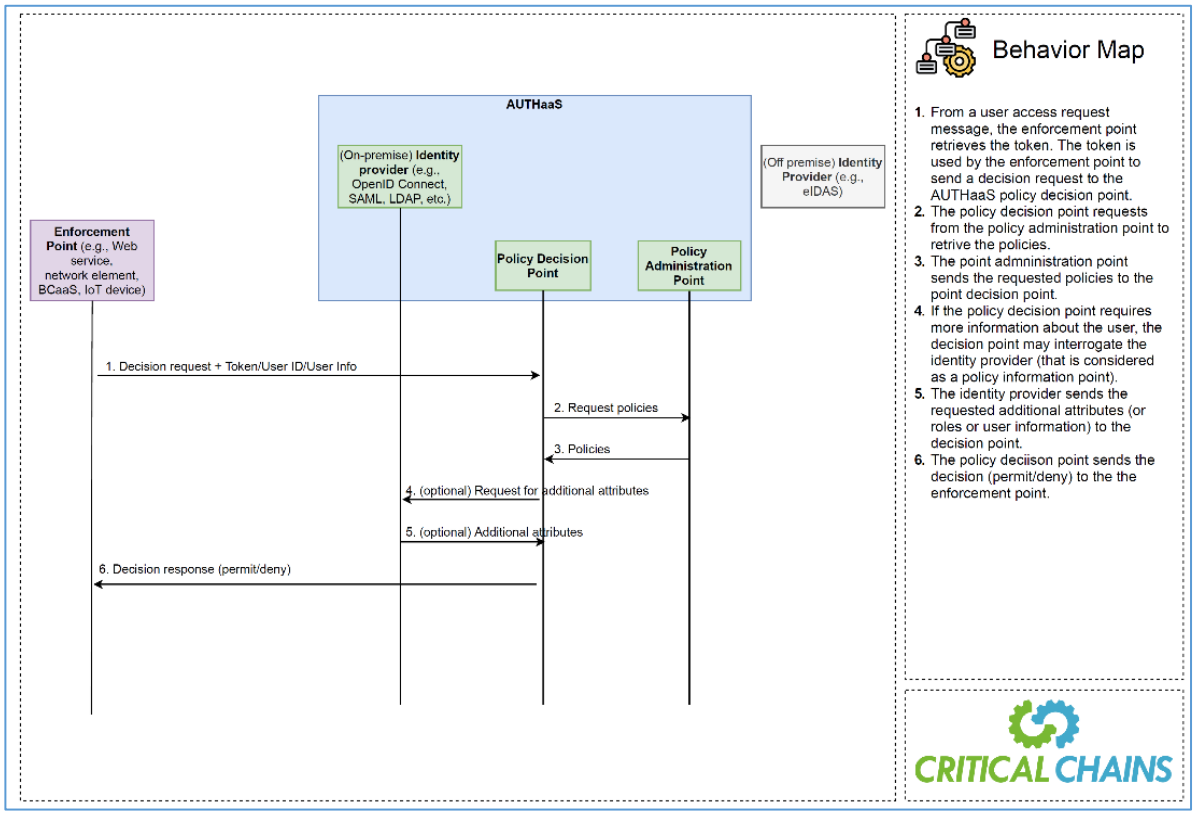

Figure 15: Authentication/Authorisation-as-a-Service Behaviours: Authorisation

Table 13 below, presents the indicative analysis sets of the ESEA metrics for the evaluation of the Critical-Chains AUTHaaS.

Table 13: ESEA Metrics for Authentication/Authorisation as-a-Service

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Number of authenticated authorised users at a time	Number of authentications/ authorisations per second > 30	More scalable financial corporations	Higher cost for computation	More hardware components, higher energy consumption
	Response time to authentication/ authorisation requests	Less than 1 second	Almost transparent user authentication/ authorisation	Higher cost for computation	More hardware components
Functional	Blocking unauthorised users	Blocked access to all unauthorised users	Controlled access to sensitive services and resources	Higher risk of user confusion in the Critical-Chains platform usage	More user frustration
	Supported authentication mechanisms	At least 3 different supported authentication mechanisms (login/password, TLS, 2-factor)	Different levels of protection for different types of users	The higher complexity of the authentication algorithms and protocols	Higher latency, less performance
	Personal data	Personal data stored and used for authentication/ authorisation	Different levels of protection for different types of users	Fear of possible data leak	Loss of customers
	Service failure	Expected back-up system	More robust financial corporations	Higher cost for computation	More hardware components
Human Factors	Man-Machine Interaction	Straightforward screen navigation	Ability to easily move around in apps	Lack of trust in the framework	Boredom from the system
	Front-end Applications	Screen design with relatively few point-and-click operations	Ability to easily choose the supported authentication mechanism/ select the application the user has access to	Lack of trust in the process	Boredom from the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of possible data leak	Loss of customers
Ethical and Legal	Transparency	The explanation for the collection, usage and sharing of information	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
	Profiling	Trust for profiling	Trust for profiling	Monitoring unnecessary data	Commercialised profiling
	Compliance	Compliance for human rights	Compliance for human rights	Non-informed actions with personal data	Non-informed actions with personal data
Socio-Economic	Financial Scoring	More precise financial scoring	Trust to financial result	Fear of behaviour	Boredom from the system

4.5. ATM Integration

The banking remittance service in Blockchain enables customers to register in minutes thanks to an advanced KYC and to immediately sends funds all over the world thanks to the use of a native asset or cryptocurrency backed by fiat money. A Blockchain solution would drastically reduce costs associated with cross-border payments and therefore raise the margin of TX fees whist Biometric Identification for a payment request would be the disruptive application for the ATM service. Figure 16 below shows the ATM integrtaion behaviours.

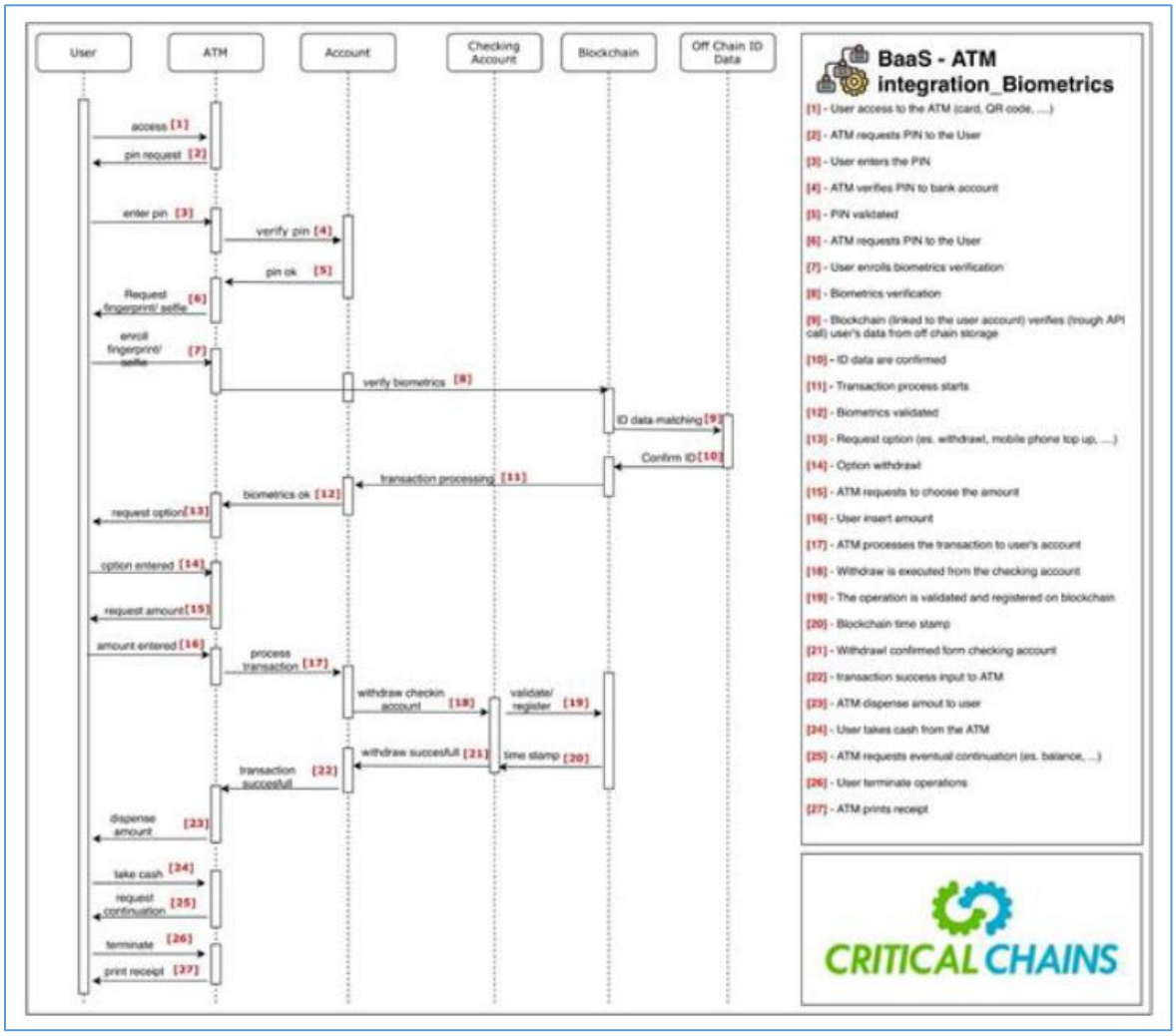

Figure 16: ATM Integration Behaviours

Table 14 below, presents the indicative analysis sets of the ESEA metrics for the evaluation of the Critical-Chains ATM integration.

Table 14: ESEA Metrics for the ATM Integration

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Number of false positives during the match between biometric identification and identity document	No more than 0,0002% of the total authentication attempts	Accurate authentication mechanism.	Avoid potential frauds	Loss of end-user customers if too many authentication attempts are needed
	Integration with legacy ATM systems	Set of interfaces that enable the connection with legacy ATM systems and infrastructures (connection to interbank networks and compliance with ISO-8583 Standard)	Easy integration for new banks using the platform	Higher complexity for the definition of external interfaces	A minor number of banks will use the platform if the integration with their systems is not easy
	Customizable dashboards for banks/cashiers	At least two different templates	Quick adaptation for new banks using the platform	Higher complexity for the definition of user interfaces	A minor number of banks will use the platform if the dashboard cannot be customised
Functional	Near real-time reconciliations and clearing	Reconciliation happens in no more than 30 secs	Easier clearing processes among banks	The level of complexity of the architecture increases	Higher energy consumption introduced by the Blockchain
	Interactive dashboard	Easily traceable user activities	Ease of use	The higher risk of data leak	Loss of trust
	Service failure	high availability -Expected back-up activities	A tamper-proof system, Redundancy in terms of hardware, software and services,	Higher costs for back-up activities and redundancy	Loss of trust from banks and end-users
Human Factors	Activity Monitoring	The pursuit of non-personal data	Mutual trust for a reliable system	Fear of behaviour	Boredom from the system
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of the possible data leak	Loss of the customer

Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared (GDPR compliance)	Trust for the knowledge of the data pipeline	Non informed data collection	None relevant personal data usage
	Profiling	Trust for profiling	More fair and dependable system	Monitoring unnecessary data	Commercialized profiling
	Compliance	Compliance for human rights	Obedient to human rights	Non-informed actions with personal data	Non-informed actions with personal data
Socio-Economic	Financial Scoring	More precise financial scoring for fairness	Trust to financial result	Fear of behaviour	Boredom from the system

4.6. Toll Collection System

The Toll Collection System component is a front-end component adapted for the Toll Collection domain. This component will be adapted for the three types of users (Toll Operator, Merchant and Authority). The Toll Collection System will be adapted to the user needs and rights. The overview of the Toll Collection System behaviours can be seen in Figure 17.

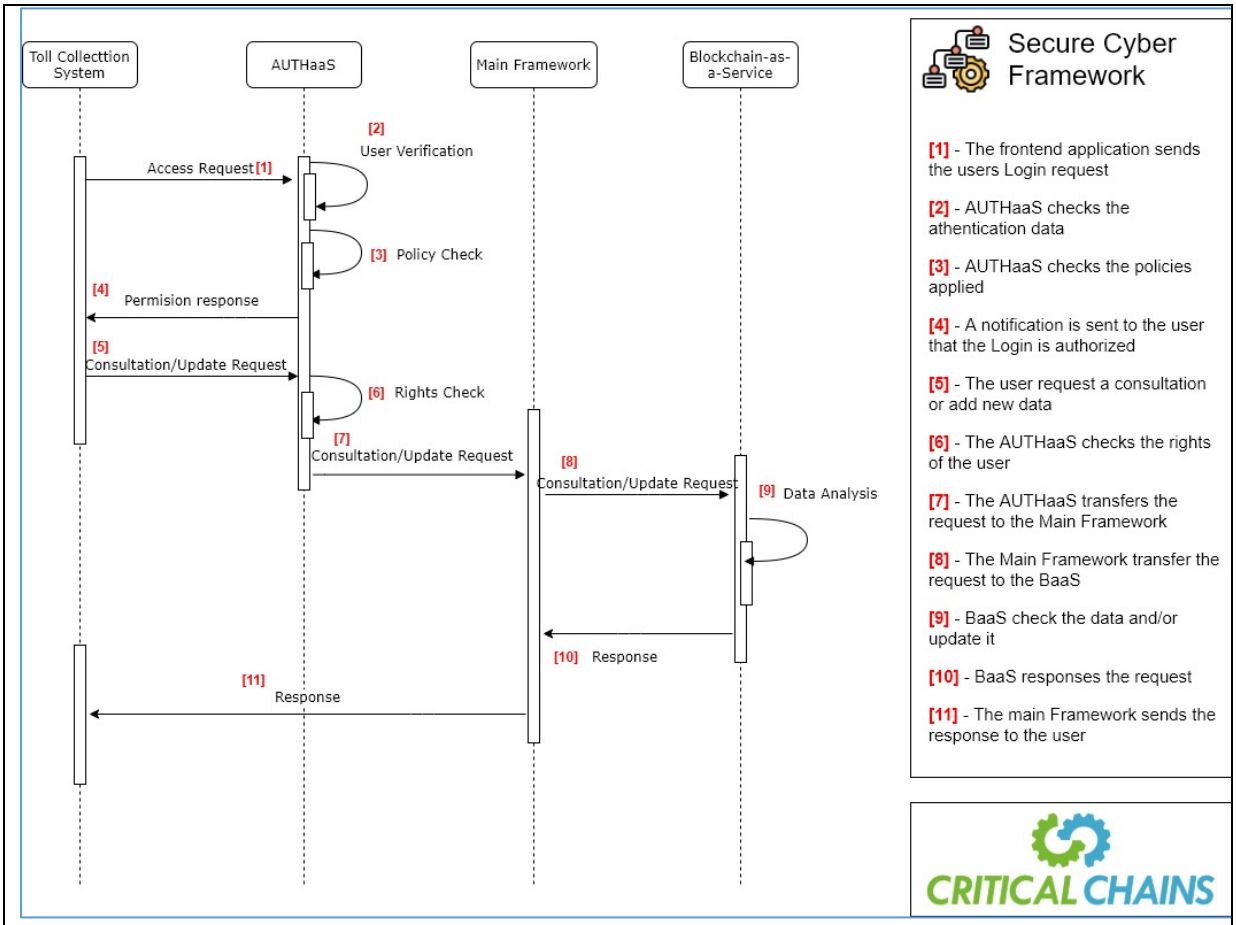

Figure 17: Toll Collection System Behaviours

Table 15 presents the indicative analysis sets of the ESEA metrics for the evaluation of the Critical-Chains-enabled Toll Collection System.

Table 15: ESEA Metrics for the Toll Collection System

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Non-Functional	Integration with the X-as-a-Service models	Expected request time between steps maximum 15ms	Knowledge of the security with user-friendly and quick system usage	More time lost than the conventional models	Affected motivation-to-Change for end-users
Functional	Support Legacy System	Support the different lists used in Toll Domain	No need to adapt to the current process	The higher complexity of backend operations	The higher system bugs
	Multi-function all in one app	Toll services under one roof	Ease of use	The higher risk of confusion in the app-usage	Loss of interest
Human Factors	Man-Machine Interaction	Straightforward screen navigation	The ability to easily move around in apps	Lack of trust in the framework	Boredom from the system
	Front-end Applications	Screen design with relatively few point-and-click operations	The ability to easily check or register transactions	Lack of trust in the process	Boredom from the system

Aspects	Definition	Satisfaction	Effects	Side-Effects	Cross-Effects
Social Factors	Privacy	Preserving user privacy	Comfort within the system	Fear of the possible data leak	Loss of the customer
Ethical and Legal	Transparency	The explanation of how the information is collected, or used, or shared	Trust for the knowledge of the data pipeline	Non informed data collection	Non-relevant personal data usage
Socio-Economic	Cost-efficient App	The cost-efficient financial operations with one-app	Ability to check and update the list with one-click	Lack of trust in the process	Boredom from the system
	Transparency	Consensus on the integrity of the users of the Pilot	Trust for the knowledge of the process	Lack of privacy against external actors	Non-relevant personal data usage

5. Evaluation Process

In the sections below, each pilot is evaluated with the applicable use-scenarios in the particular use-contexts and from the various user perspectives to ensure the inclusive methodologically-guided user-centred evaluation of all relevant effects and impacts arising from the deployment of each functionality of the system.

5.1. Use Scenarios Specification in the Banking Sector and KPI Evaluation

Clearing & Settlement Scenario

In the use-scenario**,** an individual pays for some services at a point of service terminal of Sensorium Inc. The point of service terminal is issued by The Big Company Bank and the credit card of the individual is issued by the Millennials Bank. The two banks are using the Critical-Chains framework for settlement and clearing of their opposite transactions.

1. An individual, pays at a point of sale terminal for some services, using their credit card.
2. The transaction is recorded on the Critical-Chains Blockchain by the bank that issues the point of sale terminal.
3. The bank of the credit card issuer is informed about the transaction and initiates a transfer of money to the bank of the company.
4. The transaction with the money is also recorded on the Critical-Chains Blockchain.

In the stated use-scenario an individual initiates a service terminal (credit-card POS). The amount of the payment is then transferred from the service terminal to the individual. Then the user initiates the service terminal with his/her credit card to make the payment with the specified amount. The service terminal is issued by The Big Company Bank and the credit card issued by the Millennials Bank. In the present scenario the individual uses the contactless payment method for the purchase after the usage payment validation notification instantly appears in the smart-phone of the individual for the validation and the e-wallet for mobile validation issued by the Millennials Bank. In this process, the payment order directed from The Big Company Bank to Millennials Bank because of the interconnection of banks (nodes). Immediately after the individual validates the payment from their smartphone the transaction validation takes approximately 10 seconds according to the usage of Ethereum based Blockchain network. After 10 seconds the transaction should be validated, the result recorded in the distributed ledger and the approval arrives at the service terminal.

According to the usage-context, Critical-Chains is expected to handle 25, 346 transactions (According to Ethereum's current performance) at the same time as happens in the concurrent Clearing and Settlement processes because of the block size integrated into the designed architecture; as each block is to support 30kb of transactions which affects the scalability of the system. Transactions can be made at any time during the day. While operations are made, 51% of vulnerability attacks are blocked, this means miners cannot control more than 50% of the Blockchain network or computer power usage of a private and permissioned network.

Besides the non-functional features, there are functional aspects that are considered within the context of the Critical-Chains framework which are; Cost and Banking Business Process. While clearing and settlement are being carried out from the bank side, the cost will be expected to be at around 0.3 Euros per transaction. On the maintenance side with the usage of the smart contracts the whole process is based on autonomy therefore the number of manual inspections will be expected to be around 2 out of 10 compared to the regular systems. Critical-Chains Framework also provides companies with flexibility which means infrastructure can be designed considering optional requirements arising from their needs. However, within reason, it is the responsibility of the companies to gain trust from their customer in the new functionalities to support the integrity of their operations.

According to the use-scenario of the Clearing and settlement use-case, while making transactions end-users should remain anonymous. Although users should stay anonymous, the authority must audit individuals which means that end-user should be accountable, this explanation covers Privacy under the Ethical and Legal aspects. The Critical-Chains framework already designed to de-link the personal data usage of the account addresses for the data processing features.

As human factor aspects, the Critical-Chains framework covers ease of use and motivation to change. Critical-Chains framework procures user-friendly financial status dashboard and a 3-step secure transaction process feature under ease of use with high security.

Mortgage (Property Loans) Scenario

In the use-scenario, Johnny and Jane, a couple (two individuals), want to buy a house. They ask the Millennials Bank for a property loan.

1. A bank employee sets up a smart contract for a property loan, after checking if the individuals for the loan are credit worthy.
2. The individuals use their secure sticks to authenticate themselves and sign the smart contract regarding their property loan.
3. The smart contract is recorded on the Critical-Chains Blockchain.
4. Both the bank and the individuals can check the current state of the smart contract at any time.

In the use-scenario the couple applies to the Millennials Bank for a loan via their mobile phone. Usually, the end-users are obliged to visit the physical premises of the bank for large loan however within the capability of the Critical-Chains framework and with its accessibility 100% of the time, the couple applies for the credit from their smartphone. The Authentication-as-a-Service model enables mutual trust at the highest level because of the multi-factor authentication enabled high security.

In the sequence, the couple opens the Critical-Chains based Millennials Bank mobile application via smart-phone then authenticate themselves to the system with their USB-stick via Bluetooth. The steps between the authentication and the entry to the system are expected to take around 8 seconds while providing the FIDO1 Standard. Next, the couple completes a smart-loan-contract application for the loan by filling in the values of the requisite parameters; namely, the duration of payment, the amount and the detailed justification of the credit, then, the smart-contract appears in the Millennials Bank system. For regulatory compliance the Millennials Bank has to submit this information, as provided by the couple, to the financial scoring service EquiX Corp.

The EquiX Corp uses the Flow Modelling as-a-Service and they are also a node in the Critical-Chains framework. Due to their permission rights the couple's application seen as an address without any personal identifier information, therefore the Critical-Chains preserve privacy in the system with zero-knowledge of any personal data as processing only the relevant indirect identifier type of data. Afterwards, with the de-linked address information, the EquiX Corp establishes a call-back from the Flow Modelling-as-a-Service autonomously. Right after the financial score is established from the EquiX Corp the interest of the credit is assessed and inserted as a parameter of the smart-contract to complete the process. The financial-scoring result is calculated instantly and from the application to the establishment of the smart-contract, the average time expected for the whole process is around 30 seconds. Finally, for transparency, the entire procedure can be seen on the couple's tablet screen, step-by-step, to enable them to examine the correctness, consistency and integrity of the process.

The Critical-Chains architecture is expected to handle 10.000 loan applications at a time and the Flow Modelling as-a-Service can provide financial results expected to be around 5000 users at a time. Therefore, for each company, the number of instant-secure loans could be up to 5000 at a time. On the maintenance side with the use of smart contracts, the whole process is based on autonomy therefore the number of manual inspections expected is around 4 out of 10 compared to regular systems.

From a human factors viewpoint, provided the risk of algorithmic bias and adversarial attacks on the system are avoided, the efficiency gains arising from the autonomous operations of the financial scoring and the credit application processes, would be expected to lead to greater interest in Critical-Chains-enabled application.

To the extent that the deployment of Critical-Chains liberates the users from the tyranny of some of the cumbersome banking procedures, this would confer efficiency gains and greater accuracy and auditability. However the trade-off has to be considered between such operational advantages and the higher energy consumption compared to conventional banking services. In such considerations the motivational strategies such as sustainable energy solutions can be evaluated to ensure the take-up of Critical-Chains-enabled application is implemented such that any adverse environmental impacts are avoided or minimised consistent with the sustainable modus operandi of advanced data centres.

Blockchain for the remittance scenario

In the use-scenario**,** the banking remittance service in Blockchain enables customers to register in minutes thanks to an advanced KYC and to immediately send funds all over the world owing to the use of a native asset or cryptocurrency backed by fiat money. A Blockchain solution would drastically reduce costs associated with cross-border payments and therefore raise the margin of TX fees.

1. Biometric identification and registration to the service
2. Money sent as Blockchain transactions and regulated periodically with bank transfer
3. Payments are recorded in Blockchain and the reconciliations are immediate
4. Cashier receives Blockchain transaction and gives to the receiver the equivalent in legal currencies
5. Receive legal currencies in cash or wallet recharge
6. Token or Cryptocurrency concept design
7. App or software for operator dashboard
8. Biometric ID system
9. API for integration
10. Smart contract design

In the stated use-scenario, an individual registers a request to send funds internationally. Before registering the application, biometric identification has been carried out to complete registration to the service. In the sequence, the user initiates the application to send funds with the requested amount. The transaction cost is the same for each operation which means the cost of the transaction does not change according to the number of requests or the amount of the money that the end-users' wish to transfer. App-wallet and ATM integration are allowed in terms of Customer interaction. Payments are recorded in a Critical-Chains distributed ledger which is provided by the Blockchain-as-a-Service. Each transaction received will be converted into legal currencies and this process is expected to take approximately 10 seconds, also the steps between those actions envisioned under 15 seconds. Transactions can be made at any time according to the customer's needs it means the Critical-Chains platform is available 100% of the time as foreseen value. While Blockchain for remittance operations are made, 51% vulnerability attacks are blocked, this means miners cannot control more than 50% of the Blockchain network or computer power usage of a private and permissioned network.

Apart from non-functional features such as performance, accessibility, and security, there are functional features that need to be considered. Customers can access transferred funds from their wallet application or cash which brings ease of use as a human factor. From the maintenance side with the usage of smart contract, the process is based on autonomy which means the number of manual inspections expected will be around 3 out of 10 compared to the ordinate system. To keep customer

interaction at a high level, the Critical-Chains framework provides flexibility to banking for remittance. Flexibility brings a designable infrastructure taking into consideration optional requirements arising from the customer's needs.

Although customers are familiar with traditional operations from the banking sector, it is the companies' responsibility to gain trust from end-users in the banking remittance process in the matter of Integrity. The Critical-Chains framework provides customers with a 3-step secure transaction process with high security and a customisable dashboard for all the parties. As a result, the banking remittance use-case scenario provides accessible, secure and efficient infrastructure as an advantage of the Critical-Chains framework.

5.2. Use Scenarios Specification in the Insurance Sector & KPI Evaluation

Reinsurance Scenario

The use-case-scenario mentions the increase in the transparency of the insurers' reinsurance contracts. In the case of risk transfer from the insurance company a reinsurer may be assisted by Blockchain to realise the number of retrocessionaires (a reinsurer of a reinsurer) and the way in which they further divided the risk with the reinsurer. Likewise, it would make easier the exchange of information on the paid claims, especially claims reserves, among all the listed participants in the risk underwriting, which would make their adequacy of technical reserves better. The insurer would quickly and easily get the necessary information about all the retrocessionaires, for improving the capital efficiency and meeting demands for capital adequacy. Reinsurance Blockchain-based allows the exchange of information on risk and claims among insurers, reinsurers while further retrocessionaires are made easier and faster. The modern process of reinsurance is rather inefficient and has not been innovated in the last hundred years. Inefficiency leads to delay in contracting process on reinsurance and claims, which brings reputational risk for the insurer and possible problems with cash flow.

Blockchain technology offered by Critical-Chains can improve the process of reinsurance. If all the reinsurance contracts were included in the distributed ledger, the need for reconciliation would be unnecessary since all the data would be in one place in the unique record whose copies are with all the insurers and reinsurers. There would be one standard for data processing and one platform which would be executed automatically. This would accelerate the process, optimise cash flows and provide a completely integrated information system. According to KPIs proposed in section 3.4.2.3 we can compare existing and future reinsurance processes as set out in Table 16 below.

Table 16: Comparison of Existing and Future Reinsurance

Existing Reinsurance	Future Reinsurance
Contract manually defined on paper (more probability of human error)	Contract digitally defined on Critical-Chains or Insurance/reinsurance platform (based on online forms Blockchain-based)
Written and oral negotiation of every contract between more brokers and the reinsurer	Automated negotiation between more brokers and the reinsurer
Data are manually processed by all the participants for themselves	Data are entered only once and processed automatically in the Blockchain network
Invoices and receivables are made for one-self, so everyone's reconciliation is needed	Invoices and accounts receivable are generated by the network, so the reconciliation is not necessary
Complicated and long-lasting adjustment causes a delay in money transfer	Money transfer is faster and automated since there is no reconciliation
Copies of the contract are kept locally	The contract is kept in the Blockchain network

Reinsurance Blockchain-backed process must simplify processes safely, efficiently and fit the process environment from the human factors highlighted in use-scenario KPIs, but also be compliant regard ethical and legal factors as GDPR.

Catastrophe Bond Scenario

The use-scenario aims to accelerate and simplifying transaction processing along with the claims and settlement process between investors and insurers in the natural catastrophe insurance segment. As a result of Blockchain technology, processes can be automated and rendered more secure by eliminating the need for certain instances made by human inputs.

The settlement system simply requires two items of information that are incorporated into the programme:

- The event must have been declared a natural catastrophe.
- The location of the insured event must correspond to the region recorded as having suffered a natural catastrophe.

The aim is to avoid a repetition of Storm Xynthia (February 2010), when most victims were no longer in possession of the necessary documents to file claims and had to wait more than a year to receive the insurance payment. This type of incident, in addition to being costly and time-consuming, damages the reputation of insurers and makes customers sceptical of the insurance system.

The use of a smart contract-based system for catastrophe insurance improves the way claims are handled while reducing human input (as the contract is automated). When an event that meets predefined conditions occurs, all eligible catastrophe insurance contracts are automatically executed using the smart contract code. This code also directly activates insurance payments without the customer having to provide the necessary documentation. In this way, costs can also be significantly reduced for KYC teams, third-party administration and claims.

The structure of this new kind of catastrophe bond is still quite like the traditional one where the major difference is that the smart contract replaces the SPV in its entirety. Also, a third party—an oracle—is included.

In a hypothetical scenario, we can assume that an issuer wants €100 million in the case of an earthquake with a magnitude equal to or greater than 5.0 hits City X. They are willing to pay 6% premiums to their investors if there is no incident within one year. The data required to evaluate the trigger is provided by the Control Authority Y, which receives a fee of €50,000 for its services. In case of a covered event, all affected assets must be generally assigned to the issuer.

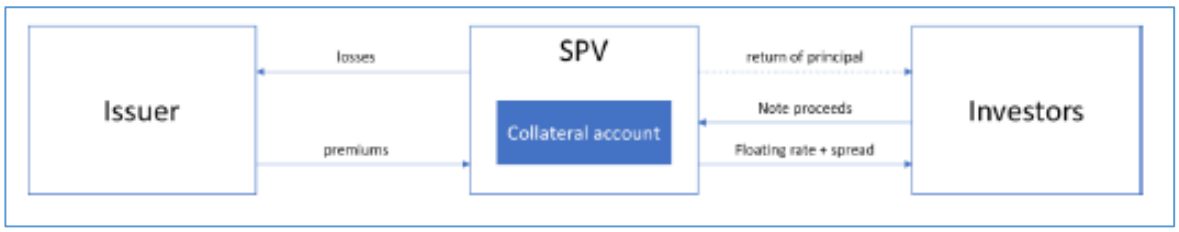

Figure 18: Traditional Implementation

Generally, in traditional implementations, the first steps are to establish a Special Purpose Vehicle (SPV) in a tax-efficient jurisdiction to act as an intermediary between the issuer and the investors and then establish agreements between them; see Figure 18 above. In addition, in order to neutralise the issuer's credit risk, investments must be fully secured, with the escrow account managed by the SPV. Depending

on the guarantee structure, this may leave investors still exposed to credit risk in addition to the expected insurance risk.

In a volatile, uncertain, complex and ambiguous world, it is necessary to implement solutions with flexibility and customisation in mind, as well as interoperability, efficiency, security, scalability and accessibility. Use cases can change or become redundant rather quickly and trading partners can be exchanged. The idea developed within the Critical-Chains is to design the solution, so that the definition of risk is as variable as possible, while still ensuring high levels of trust and efficiency. The same is true for the structure of collateral, which could range from risk-free to low-risk-low return-return, as variable as possible, while providing maximum confidence in its implementation.

The structure of this new type of cat bond is still very similar to the traditional one. The main difference is that the intelligent contract replaces the SPV in its entirety. In addition, a third party (an oracle) is included. The purpose of an oracle is to provide data for the evaluation of activation, without being further involved in the agreement. An oracle may also not know what the transmission of data or who else is involved. It is sufficient to know the compensation they receive when the data is transmitted. This ensures neutrality in the assessment of the claim.

The end-to-end process would be as follows:

- Start with the issuer
- Creation of the smart contract
- Pushing it into the Blockchain
- Pre-financing it with investor rewards and oracle commission.

Figure 19 illustrates the above Smart-Contract-enabled process.

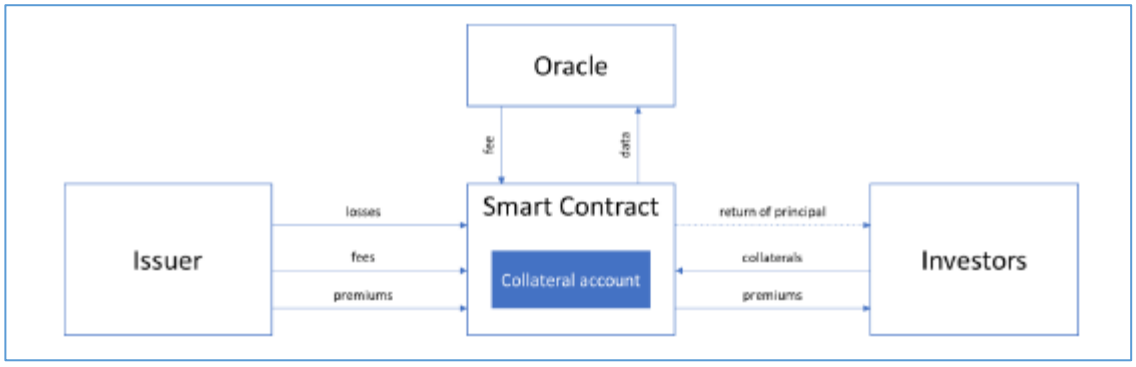

Figure 19: The Smart Contract Approach

From this point, the Cat Bond is accessible to the other members of the Blockchain network and at the next step, members of the Blockchain network can invest in the Smart Cat Bond.

At this point, investors verify the information advertised by the issuer by now and know they will receive 6% plus principal after one year, unless there was an earthquake with a magnitude greater than or equal to 5.0. It is enough for them to send the funds because the smart contract is programmed to handle the rest.

Two things could happen next:

- The oracle measures an earthquake in City X with a magnitude of 5.0 or more and submits that information to the Smart Cat Bond - the Smart Contract would send the predefined oracle fee of €50,000 to the oracle and all the remaining funds to the issuer.
- The year passes without an incident and the investors can reclaim their funds plus premium

- The issuer can reclaim the oracle fee, as the investors claim their principal back, plus the promised premium.

There is no way that the issuer, the oracle or the investors receive inappropriate funds, simply because the smart contract contains no logic to do so.

Note the difference between traditional contracts and smart contracts: traditionally a contract is negotiated, written, signed and sealed. However, when the issuer pushes his Cat Bond into the Blockchain, they might not know a single investor, but the smart contract is signed, sealed and even prefunded by them at that point already.

In Critical-Chains, the identical Blockchain infrastructure that supports investments in smart financial instruments could also support completely different smart contracts, such as one for exchanging assets without an intermediary, or one that functions as an auction house. This is what makes the Blockchain network an ecosystem with its own right.

Travel Insurance Scenario

The use-scenario aims to exploit Blockchain capability as a neutral 3rd party for parametric insurance and particularly for travel insurance or flight delays.

Parametric insurance is an established facility but Blockchain technology gives it a new value and provides complete automation and transparency. The major features of parametric products are:

- Claims are paid when the predefined values of risk parameters are measured, for instance, the level of water in the river, the number of rainless days, and so on. The parameters must be consistent, easily measured and constantly up to date.

- The source of information for parameters needs to be automatically measurable and entirely independent from the influence of insurers and the insured.

This type of insurance has big advantages: fast and consistent payment of claims, transparency of products, maximum simple administration with insurers, the impossibility of fraud in insurance, small uncertainty as the parameters are usually simple risks, the possibility to insure the risks which have not been insured so far, etc. Blockchain technology can completely automate the work with parametric insurance products.

To better highlight travel insurance Blockchain-based within the Critical-Chains project, we can take as an example the China Airlines case, wherein February 2019, the strike organised by China Airlines pilots resulted in more than 60 cancelled flights. A total of 30,000 passengers were affected in this seven-day strike action over working conditions and benefits. Consequently, China Airlines offered a compensation scheme to passengers affected by flight delays and cancellations. For flights delayed 6 hours or more including connecting flights due to cancelled flights, China Airlines promised to cover accommodation, food, and transportation expenses incurred by the change of the itinerary. However, passengers must submit their boarding passes or related invoices/receipts for China Airlines to review these documents and handle each claim with discretion.

Apart from airlines' compensation, some passengers have the tendency to buy travel insurance, including travel inconvenience insurance. They can also receive compensation from insurers. Because of strike or weather conditions, insurers often offer compensation for flight delays, cancellations, changes, or reductions. Passengers then must go through a complicated claim settlement process by providing related evidence and/or documents. When flights are delayed or cancelled, they need to request proof from airlines, provide their boarding passes, and fill in documents. Normally, it takes about one to two weeks to complete a claim settlement process. Therefore, how to simplify the travel insurance claim settlement processes has become an important issue for insurers.

This is the process flow for existing travel inconvenience insurance:

- Customer goes to buy insurance at the counter

- Flight gets delayed
- Obtain claim application, Proof of delay, Boarding Pass
- File Submission / Rejection
- Claim settlement after investigation.

Within the Critical-Chains project and according to KPIs for the insurance use-scenarios, Blockchain can speed up the above travel inconvenience insurance process integrating flight information to automate travel inconvenience insurance processes and reduce claim settlement time by simplifying insurance application and claim settlement processes:

- The insurer insures himself against flight delay/ cancellation
- The delay/ cancellation occurs
- Specified conditions are met
- Critical-Chains solution will send a claim notification to the insured automatically
- The compensation will be paid into the insured's designated account through the solution's autonomous claim pay-out system
- The insured no longer needs to request documentation of proof from the airline in case of flight delays

5.3. Use Scenarios Specification for Toll Road Operations & KPI Evaluation

Toll Operator & Merchant exchange Scenario

A customer of the Toll Collection Service who has associated his/her bank account to a TAG device which is installed in their specific vehicle decides to make use of it. The driver passes through a fast lane of the Toll Highway with an automatic opening of the barrier that avoids any waiting time or delays in their trip. As explained in section 3.4.3, there are three different types of list that are consulted or updated by the different users (Toll Operator, Merchant, and Authority) and three different lists: TAG List, Transaction List, and Black-List.

The merchant requests the payment of the users who are registered in the Transaction List, from the bank account associated with the TAG registered in the Transaction List. This process takes place automatically from the driver's point of view. The Toll Operator and the Merchant uses a Smart Contract in the Critical-Chains Blockchain-as-a-Service to automate the exchange of information among them.

In sequence, a driver with a TAG passes through a fast lane of the Toll Highway. The Interoperable Toll Operator front-end system reads the TAG device, detects the related vehicle and verifies the TAG identification as not included in the current received Black List, and the barrier automatically opens. Then, the Back-Office System of the Operator registers the transaction in the Critical-Chains distributed ledger which is provided by the Blockchain-as-a-Service.

Finally, the Merchant receives a notification of that particular transaction. Then the Merchant triggers the payment procedures with the corresponding bank. Once the payment has proceeded, it notifies the Toll Operator through the Critical-Chains Blockchain-as-a-Service via Main Framework that the transaction has been successfully paid.

Black List Scenario

This scenario is focused on the exchange of the Black List and its consequences. The Black List represents the list of TAG IDs that have not paid their transactions. Hence, the TAG that is included in the Black List is blocked until they pay their previous debts. This Black List can be updated by the Merchant or the Operator when any of them receive the notification of any issue with payment.

Currently, in a scenario without Critical-Chains Framework, both the registry of transactions and the updates of TAG Lists processes are independent and conflicts could arise when a driver who had an issue with the last request of payment from the Merchant uses the Toll Road before the Toll Operator has been notified that they are included in the Black List. It could happen that a driver with debts that should have been registered in the Black List, circulates on a Toll Lane that has not updated the list yet, and therefore the barrier is opened and the driver is allowed to pass, increasing more the debt.

Merchant or Toll Operators can receive a list of invalid tags either because they have been cancelled or blocked by an unpaid transaction. In this scenario, the Merchant updates the current Black List in the Critical-Chains Blockchain-as-a-Service via Main Framework. The Merchant updates the Black List and changes the status of the BlackListed TAG to "Sent to Operator" status. Once the Toll Operator has been notified the Black List is updated to "Received" and the Black List is replicated internally in the Back Office to the fast lanes gates.

Therefore, in this scenario, a TAG transaction is recorded in the Critical-Chains distributed ledger. The Merchant is informed of it and proceeds to apply the corresponding fee through the corresponding bank. However, this fee is not received due to a problem with the bank account associated with the TAG. Hence, the Merchant updates the TAG Transaction to "Uncollectible" status because the payment process is not completed, and the TAG is recorded on the Black List and is not allowed to use the Fast Lane until it solves the unpaid transaction.

This scenario is also applicable when there is interoperability between two operators and they need to exchange lists. In that case one of the actors will be Operator 1 and the 2nd actor instead of the merchant will be Operator 2.

Transactions Audit & Taxes Payment Scenario

The Authority is the owner of the Highway and it was granted a concession agreement with the Toll Operator to operate the Highway. The agreement states that the Operator is responsible for the Highway for a certain amount of years. This means that the Operator is responsible for providing an adequate service to its customers in exchange for a certain fee per use. The Authority who has built the Highway does not need to provide any service during the concession, but it will receive certain fee/taxes per use. Thus, the Authority income is directly related to the volume of traffic reported, and therefore the Authority needs to audit and check periodically the list of transactions to calculate the amount that the Operator needs to pay.

KPI Evaluation

Taking into consideration the three scenarios, it is necessary to measure different KPIs to evaluate this Pilot divided into Non-Functional, Functional, Ethical and Legal and Human Factors. The performance of the Critical-Chains Platform in the Toll domain needs to be measured in terms of Scalability, Capacity and Frequency that needs to fit the user needs. As has been explained in the scenarios, the response time and capacity to manage the different requests demanded is key in this domain. Those are reflected in the number of transactions per day and the response time. In addition, there are the maintenance and cost features that are essential to consider the viability of using new technologies especially due to the usage of high computational power that can increase energy consumption compared to the current system, with the usage of high computational power related to Blockchain technology.

Apart from non-functional features, there are functional features that need to be considered. The Authority can access to a trustworthy database which is a distributed ledger-based in the inviolability of the Blockchain that also reduces the number of conflicts between the different users (Merchants and Toll Operators). Nevertheless, the new platform needs to be compatible with the current technology of the operators and merchant that detects the TAGs and trigger the automatic payments.

On the Ethical and Legal aspects, proper usage of anonymisation and/or pseudonymisation techniques should be applied to comply with GDPR. Although users should stay anonymous, the authority must

audit individuals which means that end-user should be accountable, this explanation covers Privacy under the Ethical and Legal aspects.

On the human factor aspects, with the usage of the trustworthy operations in the Toll domain processes, the employees will be motivated to change to a Critical-Chains based application because it will reduce the number of misinterpretations between the different users.

5.4. Use Scenarios Specification for Financial Infrastructures & KPI Evaluation

Acquisition of a Financial Digital Asset Scenario

An employee of the public administration wants to subscribe to a pension fund, and he wants to do it through a Smart Contract because that makes it safer.

1. At the beginning of the procedure, the investor sends the subscription request to the fund that starts the Smart Contract;
2. A smart contract is set up between the fund buyer and the funds emitter, checks and the verifications (e.g. AML/KYC, etc.) are executed by the Smart Contract;
3. After calculating the Net Asset Value, the Smart Contract instrument checks that all the preconditions are met, and then independently executes the transaction between the client and the fund;
4. A percentage of the share of the digital fund is created and exchanged for the equivalent amount of digital currency;
5. The Smart Contract sends the confirmation of the transaction to the fund buyer.

The evaluation of the use-case “Acquisition of a Financial Digital Asset” will take into consideration several aspects from a different points of view. From a performance perspective, after the secure login, the most important metric to consider is the time the platform takes to process a request of acquisition of a financial digital asset by an end-user and produce the tangible result that consists in a token stored in the wallet of the user.

The number of requests that the platform must process can vary over time. Thus, the platform must be able to scale in order to maintain the overall performance at the right level and respond with timing that should be consistent and predictable for all the actors involved and particularly for the end-user. The platform must be always available, possibly without issues related to the availability, hence this aspect will be considered during the evaluation phase.

The use-case “Acquisition of Financial Digital Asset” requires the processing of very sensitive data because the wallet of a user could store digital assets with a very high monetary value. For this reason, it is fundamental to ensure the security of the transactions and the data processed. A very effective way to reduce the risk coming from external threats, and particularly from cyber threats that can compromise the security of the platform, is to reduce the probability of being successfully attacked. This can be achieved in several ways but an effective method is to perform a vulnerability assessment on systems, software infrastructures and applications and take actions in order to eliminate the vulnerabilities found.

As to the functional aspects, the cost for each transaction will also be evaluated, the percentage of mobile devices currently available on the market that can support the solution in terms of the version of the operating system, hardware and software compatibility, etc.

From an ethical and legal perspective, some metrics will be calculated to evaluate the level of privacy enforced by the solution through the use of pseudonymisation and anonymisation techniques as well as compliance to GDPR during the processing of user data.

Finally, a set of user acceptance tests will ensure that the solution will be accepted by the validating stakeholders, taking into consideration the overall user experience.

Redemption of a Financial Digital Asset Scenario

An employee of the public administration wants to redeem a financial asset that they purchased earlier:

1. At the beginning of the procedure, the investor sends the subscription request to the fund that starts the Smart Contract.
2. A smart contract is set up between the fund buyer and the fund's emitter, checks and verifications (e.g. AML/KYC, etc.) are executed by the Smart Contract.
3. After calculating the Net Asset Value, the Smart Contract instrument checks that all the preconditions are met, and then independently executes the transaction between the client and the fund.
4. A percentage share of the digital fund is created and exchanged for the equivalent amount of digital currency.
5. The Smart Contract sends a confirmation of the transaction to the fund buyer.

One of the major benefits of using the Blockchain technology for this use-scenario is the ease of reconciling all the information needed to fulfil the transaction among the different nodes and actors of Critical-Chain. Thus, an important metric to consider is the time the platform takes to process a request by an end-user to redeem a financial digital asset and update the personal wallet of the end-user with the equivalent amount of digital currency.

Another aspect that will be evaluated is the scalability of the platform when there are peaks in requests. In these cases, all the actors should have a consistent user experience without underperformance or delay that could cause disaffection of the users.

The transactions should be fulfilled ensuring the integrity, availability and confidentiality of the data processed. This requires enforcing security on every single component used by this use-scenario and perform a vulnerability assessment to measure the level of cyber risk, ensuring that it does not exceed the maximum tolerable level.

In regard to the functional aspects, the cost for each transaction will be evaluated and the percentage of mobile devices currently available on the market that can support the solution in terms of the version of the operating system, hardware and software compatibility, etc.

From an ethical and legal perspective, some metrics will be calculated to evaluate the level of privacy enforced by the solution through the use of pseudonymisation and anonymisation techniques as well as the compliance to GDPR during the processing of user data.

Finally, a set of user acceptance tests will ensure that the solution will be accepted by the validating stakeholders, taking into consideration the overall user experience.

6. Use-Cases-to-Requirement Mapping

The Use-Case & Requirement Matrix clarifies the relationship between requirements sets and the Use-Cases supported by them. This will enable the contingent re-prioritisation and/or refinement of respective requirements and accordingly the responsive iterative co-design of the system based on the context-aware usability and impacts evaluations as planned and set-out in this document.

Table 17 below, sets out the Use-Case-to-Requirement Mapping.

Table 17: Use-Cases-to-Requirements Mapping

USE CASES	REQUIREMENTS
UCA001	REQ-L3-023 REQ-L3-024 REQ-L3-025 REQ-L3-026 REQ-L1-014 REQ-L1-015 REQ-L1-020 REQ-L2-038 REQ-L2-039 REQ-L2-041
UCA002	REQ-L1-014 REQ-L1-015 REQ-L1-020 REQ-L2-038 REQ-L2-039 REQ-L2-041 REQ-L3-027
UCA003	REQ-L1-014 REQ-L1-015 REQ-L1-020 REQ-L2-038 REQ-L2-039 REQ-L2-041 REQ-L3-028
UCA004	REQ-L1-014 REQ-L1-015 REQ-L1-020 REQ-L2-038 REQ-L2-039 REQ-L2-041 REQ-L3-031
UCA005	REQ-L1-014 REQ-L1-015 REQ-L1-020 REQ-L2-038

USE CASES	REQUIREMENTS
	REQ-L2-039
	REQ-L2-041
	REQ-L3-029
	REQ-L3-030
UCA006	REQ-L1-014
	REQ-L2-018
	REQ-L2-017
UCA007	REQ-L0-008
	REQ-L0-017
	REQ-L0-022
UCA008	REQ-L0-009
	REQ-L0-018
	REQ-L1-005
	REQ-L1-006
	REQ-L1-007
	REQ-L2-028
	REQ-L2-029
UCA009	REQ-L0-025
	REQ-L0-026
	REQ-L0-027
	REQ-L0-028
UCA010	REQ-L0-025
	REQ-L0-026
	REQ-L0-027
	REQ-L0-028
UCA011	REQ-L0-025
	REQ-L0-026
	REQ-L0-027
	REQ-L0-028
UCA012	
UCA013	REQ-L0-019
	REQ-L0-029
	REQ-L0-030
	REQ-L0-031
	REQ-L0-032

USE CASES	REQUIREMENTS
UCA014	REQ-L0-019 REQ-L0-029 REQ-L0-030 REQ-L0-031 REQ-L0-032
UCA015	
UCA016	REQ-L0-010 REQ-L0-011 REQ-L0-012 REQ-L0-013 REQ-L0-014 REQ-L0-015 REQ-L0-016 REQ-L0-020 REQ-L0-021
UCA017	REQ-L0-001 REQ-L0-002 REQ-L0-003 REQ-L0-004 REQ-L0-005 REQ-L0-006 REQ-L0-007 REQ-L3-001
UCA018	REQ-L0-021 REQ-L0-029
UCA019	
UCA020	REQ-L0-001 REQ-L0-002 REQ-L0-003 REQ-L0-004 REQ-L0-005 REQ-L0-006 REQ-L0-007
UCA021	REQ-L1-028 REQ-L2-023

USE CASES	REQUIREMENTS
	REQ-L2-022
	REQ-L3-015
UCA022	REQ-L2-022
	REQ-L2-023
	REQ-L3-015
UCA023	REQ-L1-028
	REQ-L2-023
	REQ-L3-015
	REQ-L2-022
UCA024	REQ-L3-002
	REQ-L3-005
	REQ-L3-012
UCA025	REQ-L3-002
	REQ-L3-006
	REQ-L3-007
UCA026	REQ-L3-004
	REQ-L3-005
	REQ-L3-006
UCA027	REQ-LO-002
	REQ-LO-009
	REQ-LO-011
	REQ-LO-013
	REQ-LO-018
	REQ-LO-022
	REQ-LO-028
	REQ-L1-005
UCA028	REQ-LO-004
	REQ-LO-009
	REQ-LO-011
	REQ-LO-013
	REQ-LO-018
	REQ-LO-022
	REQ-LO-028
	REQ-L1-005

7. Conclusions

This deliverable has pursued a methodologically guided approach to planning the implementation of the holistic evaluation of the performance and impacts if the adoption of the critical-chains system. This has led to the adoption of the integrative requirements engineering and usability evaluation framework UI-REF for the evaluation of the Critical-chains solution just as it has been deployed in the requirement elicitation and prioritisation of the stakeholder's requirements. This fulfils the commitment to maintaining a user-centred agile evolutionary iterative development whereby evaluation includes the KPIs and metrics to cover not only the evaluation of performance and usability criteria but also the direct and indirect impacts of the system functionalities as design an as deployed in the operational content and thus the likely user-acceptance level and societal acceptability of the system.

Accordingly deliverable has establish a usability and acceptability evaluation plan with the relevant templates for the assessment of the psycho-cognitively mediated usability criteria including the point-of-experience, and, pre/post-experience usability-relationship-centric evaluation of users'-perceived quality of experience. This will enable the holistic evaluation of usability and indirect impacts of the system as designed and as operational deployed in the prototypical workflows as shall be evaluated in the for critical-chains pilot application domains.

This delivers thus supports the end-to-end agile evolutionary co-design process which has deployed an ontologically committed methodology linking the integrative formative and iterative cycles of holistic usability evaluation and requirements re-prioritisation to support the user co-design process.

The Annexes present the reference user-experience evaluation questionnaires to support the assessment of usability, user-acceptance, acceptability and impacts consistent with the methodologically guided system evaluation plan for the pilots in the demonstrator application domains.

8. References

[Al-Adawi et al 2005] Al-Adawa Z, Yousafzai, S, Pallister, J. Conceptual model of citizen adoption of e-government, Proceedings of the second International Conference on Innovations in Information Technology (IIT), 2005.

[Arner et al 2017] Arner, D W, Barberis, J and Buckley R, P. Fintech and Regtech In a Nutshell and The Future in a Sandbox, SSRN Electronic Journal, DO - 10.2139/ssrn.3088303, 2017.

[Badii 2008] Badii, A. User-intimate requirements hierarchy resolution framework (UI-REF). AmI-08: Proceedings of the Second European Conference on Ambient Intelligence, 2008.

[Badii and Rolfe 1996] Badii A and Rolfe R. Boundary sensitised information relationship management, Proceedings of the 1st UKAIS Academy of Information Systems (UKAIS), Cranfield University, UK, 1996.

[Badii et al 2009] Badii A, Fuschi D, Khan A, Adetoye A. Accessibility-by-Design: A framework for delivery-context-aware personalised media content re-purposing, Proceedings of the Symposium of the Austrian HCI and Usability Engineering Group, 2009.

[Balcerzak 2016] Balcerzak, A, P. Technological potential of European economy, proposition of measurement with application of Multiple Criteria Decision Analysis; Montenegrin Journal of Economics 12, no. 3 (2016): 7–17, 2016.

[Balcerzak and Pietrzak 2016] Balcerzak, A P and Pietrzak M, B. Quality of institutions for knowledge-based economy within new institutional economics framework; Multiple Criteria Decision Analysis for European countries in the Years 2000–2013, Economics & Sociology 9, no. 4, 2016.

[Balcerzak et al 2017] Balcerzak A, Kliestik, T, Streimikiene, D, Smrčka, L. Non-parametric approach to measuring the efficiency of banking sectors in European Union countries, Acta Polytechnica Hungarica, vol 14, no 7, 2017.

[Bank of International Settlements 2013] Authorities' access to trade repository data, Bank for International Settlements and Board of International Organization of Securities Commissions, Committee on Payment and Settlement Systems, https://www.bis.org/cpmi/publ/d110.pdf, 2013.

[Brózda-Wilamek 2016] Brózda-Wilamek D, Transmission mechanism of the Federal Reserve System's Monetary Policy in the conditions of zero bound on nominal interest rates, Equilibrium 11, no. 4, 2016.

[Davis 1989] Davis, F D. Perceived usefulness, perceived ease-of-use and user acceptance of information technology, MIS Quarterly 13(3), 319-339, 1989.

[Degerli 2019] Degerli, K. Regulatory challenges and solutions for Fintech in Turkey. Procedia Computer Science 158, 2019,

[Diehl et al 2016] Diehl M, Kabadjova B, Heuver, R, Martinez-Jaramillo S, Analysing the economics of financial market infrastructures, IGI publishers, DO - 10.4018/978-1-4666-8745-5**,** 2016.

[Eva and Badii 1998] Eva M, Badii A, What will it do to us? Predicting the cultural impact of new ICT Applications Deployment, Proceedings of the 3rd Projectics Conference, Bayonne-Cedex, France, 1998.

[Fintechtime 2018] Finans Sektörü 300 Kat Daha Fazla Saldırıya Uğruyor: http://Fintechtime.com/tr/2018/ 10/finans-sektoru-300-kat-daha-fazla-saldiriya-ugruyor, 2018,

[Hurteau et al 2009] Hurteau, M, Houle, S, Mongiat, S. How legitimate and justified are judgments in program evaluation? Journal of Evaluation, vol 15, 2009DO - 10.1177/1356389009105883, 2009.

[Janus 2016] Janus, J. The transmission mechanism of unconventional monetary policy, Oeconomia Copernicana, vol 7, no. 1, DO - 10.12775/OeC.2016.001, 2016.

[Law no. 6493] Law no 6493 on payment and securities settlement systems, payment services and electronic money institutions, 2013 http://www.loc.gov/law/foreign-news/article/turkey-new-law-transfers-oversight-of-payment-system-providers-to-central-bank/

[Nourani 2016] Nourani M, Devadason E S, Chandran, V G R. Measuring Technical Efficiency of Insurance Companies Using Dynamic Network Data: An Intermediation Approach, Technological and Economic Development of Economy Vol 24, DO - 10.3846/20294913.2017.1303649, 2016.

[Platt 2017] Platt C, Blockchains as Financial Market Infrastructures, Medium, 2017. https://medium.com/@colin_/Blockchains-as-financial-market-infrastructures-fmis-8a6d02e13212

[Zanghieri 2009] Zanghieri P. Efficiency of European Insurance Companies: Do Local Factors Matter? SSRN Electronic Journal DO - 10.2139/ssrn.1354108, 2009.

[Zarinkamar et al 2014] Zarinkamar, R T, Alam-Tabriz, A. Bank Branch Operating Efficiency: Evaluation with Data Envelopment Analysis, Management Science Letters, 2307–12, DO - 10.5267/j.msl.2014.9.004, 2014.

Turkish Banking Law no. 5411 (2005). https://www.tbb.org.tr/en/Content/Upload/Dokuman/130/Banking_Law_No_5411-3bsm.pdf

****

9. Annex1: Indicative Questionnaires for the Financial Sector

Pre-Experience and Post-Experience Questionnaire

Questionnaire and/or Interview list for the Pre-Experience usability Evaluation with respect to the operational deployment of the Critical-Chain system in Fintech Operations

This section presents an initial version of the Pre-Experience and Post-Experience questionnaires. The objective is to be able to compare the answers re Preceived Pre-Experience and Post-Experience usabilty and thus user satisfaction levels in each Phase. In addition, there are certain quantitive measures of KPIs that can be evaluated directly from the system. Further, this questionnaire can be adapted for various usability evaluation settings involving different users with distinct roles and skill sets as appropriate to the particular phases of the operational processes in which they would be engaged.

Assigning a number reflecting your judgment in your answer to HOW type of questions
Please note in all the questions that follow, wherever the question requires that you express your Qualitative Assessment about any aspect of the performance of your current Fintech solution and/or its impacts, then please select a number for your answer consistent with the following scale of qualitative ranges set out below as a Reference Scale.

-2	-1	0	+1	+2
Very Unsatisfactory	*Unsatisfactory*	*Adequate*	*Satisfactory*	*Very Satisfactory*

Indicative Pre-Experience Questionnaire - Fintech Applications Domain

Aspects	Questions	Description	Prioritisation
General	What are you using now for Fintech operations?	Please specify your current platform/application.	Mandatory
General	Which of your workflows are related to Fintech?	Please specify your workflows.	Mandatory
User Satisfaction	How satisfied are you with the performance of your current Fintech provider?	Please specify your usability satisfaction level according to the above Reference Scale **-2/-1/0/ +1/+2** which?	Desirable
User Satisfaction	What are the usability issues and performance deficiencies in your current platform?	Please specify the performance deficiencies.	Desirable
Timeliness	Does your current platform provide information in a timely fashion?	Please state **Yes/No** as may be the case, and state what stage of your WF is thus most affected positively or negatively in	Desirable

		terms of efficiency effectiveness, throughput, **other?**	
WF(Phase) Objectives	What operations do you use the most?	Please refer to the list of common operational stages and rank those you use in the order of most used.	Mandatory
Perceived Usefulness	What are the pain/pinch points you have experienced in your current operational deployment setup?	List and rank the difficulties you face with the current system in everyday operational process pipelines.	Desirable
Functionality	What are the missing functions related to your daily operations in your current application?	Please name the functionalities.	Desirable
Value System	If your difficulties and missing functions can be provided by another substitute program would you use it or are there any other criteria to be considered for your situation?	Please explain your most deeply-valued criteria and trade-offs relevant to your operational situation.	Desirable
User Satisfaction	Overall how satisfied are you with the accessibility of the current system?	Please use the above Reference Scale to indicate your overall satisfaction level re system accessibility **-2/-1/0/ +1/+2** which?	Optional
Accessibility	Can you access your current platform from a mobile phone?	**Yes/No** **Any Comments?**	Optional
User Satisfaction	What new features/improvements would make you use a New Platform to support your Fintech operations?	?	Mandatory
Information and technical support provided to users	How helpful have you found the operational deployment guidance and/or technical support from your Fintech provider?	Please use the above Reference Scale to indicate your satisfaction level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Optional
User support information	How clear, complete and well-presented is the information supplied by your provider?	Please use the above Reference Scale to indicate your satisfaction level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Integration	How satisfactory is the support provided in your current system for configuring and integration of data from the legacy systems?	Please use the above Reference Scale to indicate your satisfaction level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Reliability – Banking	Does your current system support all your banking operational needs?	Which of your banking operational are supported and which are not supported by your current system?	Mandatory
Accessibility – Banking	Can you track all of your financial services through one channel?	Please specify the channel if any	Mandatory
User Satisfaction – Insurance	How satisfactory do you find the current insurance sector operational solutions?	Please use the above Reference Scale to indicate your satisfaction level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	

Timeliness – Insurance	Does your current insurance solution provide linked and timely information and alerts Compared to Instant Insurance solutions?	**Yes/No** Any Comments?	Mandatory
General – Insurance	Overall, how satisfactory do you find the Instant Insurances?	Please use the above Reference Scale to indicate your satisfaction level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
General – Insurance	Do you believe that the emerging Insurtechs (e.g. Lemonade) would be better than your currently deployed solution?	**Yes/No** Any Comments?	Optional
General – Insurance	Do you think that Blockchain technology could add useful capabilities to the insurance sector solutions?	**Yes/No** Any Comments?	Optional
PEU – Insurance	What new features/improvements would make you use a New Platform to support your Insurance operations?	?	Desirable
Attitude – Insurance	Overall, what features of new Insuretech do you believe would make these platform be more comfortable to use?	?	Desirable
User Satisfaction– Insurance	Overall how do you rate the quality of the user-experience with your currently deployed Insurtechs solution?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
Functionally – Insurance	What are the most needed but missing features of performance of your currently deployed Insurtechs solution?	?	Mandatory
Access – Insurance	How do you rate the accessibility of the design and access to adequate user support from your currently deployed Insurtechs solution?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
Accessibility – Insurance	Does your current insurance solution enable the tracking of all of your insurance services through a single channel?	**Yes/No** Please specify the channel if any	Mandatory
Accessibility – Financial Market Infrastructures	Can you access all your financial investment services through one channel?	Please specify which is the channel or the multiple channels if you use many of them.	Mandatory
Reliability – Financial Market Infrastructures	Which of your financial investment operations are fully reliably supported by your	?	Mandatory

	current platform and which are not?		

Indicative Post-Experience Questionnaire - Fintech Applications Domain

Aspects	Categories	Questions	Definition	Prioritisation
	Performance	How satisfied are you with the response time of the Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Performance	How does the average Critical-Chains transactions throughput rate affect your workflow compared to the throughput of your current Fintech system?	. Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
	Security	How satisfied are you with the reliability of Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Security - Banking	How satisfied are you with the security protection provided by the Critical-Chains for reciprocal financial operations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Efficiency - Banking	How do you rate the efficiency of Critical-Chains support for smart-contacts for your transactions processing?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Efficiency - Banking	How do you rate the efficiency of the Critical-Chains financial-status checking?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Security - Insurance	How satisfied are you with the critical-chain-enabled security of for insurance operations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Efficiency - Insurance	How efficient do you find the Critical-Chains-enabled smart-contracts support for your insurance applications e.g. for Instant Insurance activations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Security – Financial Markets	How satisfied are you with the security of Critical-Chains-enabled financial investments operations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Efficiency - Financial Markets	How do you rate the efficiency of Critical-Chains support for smart-contacts for your financial investments applications?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Efficiency - Financial Markets	How do you rate the efficiency of the Critical-Chains-enabled support for financial investments status checking?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable

	Efficiency	How efficient do you consider the Critical-Chain-enabled application to be for banking operations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Integration	How satisfied are you with the ease of integration of the system?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
	Integration	Would you prefer to integrate Critical-Chains as your Fintech provider as a solution to your work-flow demands?	**Yes/No** Any Comments?	Mandatory
	Flexibility	How easily and flexibly do you find you Critical-Chains-enabled applications can be adapted to your needs?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Functional	Feature	How do you rate the usability of the Smart Contracting feature of Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Feature	Please rank the X-as-A-Service features of Critical-Chains in the order you this as most useful?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Affects	Overall considering your experiences with Critical-Chains how do you feel about championing it integration within your operations?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
	Feature - Banking	How satisfied are you with the security protection provided by the Critical-Chains for reciprocal financial operations between two nodes?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Feature - Insurance	How satisfied are you with the new Critical-Chains feature for reciprocal checking between two nodes?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	User Satisfaction - Insurance	Would you recommend Critical-Chains Blockchain-based insurance to a friend?	**Yes/No** Any Comments?	Desirable
	Feature – Financial Markets	How satisfied are you with the new Critical-Chains feature for reciprocal financial operations between two nodes?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Human Factors	Affects	How likely is it that you would recommend Critical-Chains to a friend or colleague?	. Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable

	General	How do you rate Critical-Chains Compared to your legacy Fintech or other solutions?	. Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Mandatory
	Affects	Which feature(s) of Critical-Chains did you find least useful considering your work-flow?	?	Mandatory
	General	Which features do you like to see changed for Critical-Chains to become most useful for supporting your operations?	?	Optional
	Ease of Use	How useful did you find the user information provided with the Critical-Chains system?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Ease of Use	How satisfactory was your first experience of using Critical-Chains-enabled applications?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	Intention	Did you intend to integrate Critical-Chains-enabled applications to support all your routine operations as standard?	**Yes/No** Any Comments?	Optional
	User Satisfaction–Banking	How satisfied are you with the accuracy of financial assets information when using Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	User Satisfaction-Insurance	How satisfied are you with the accuracy of prices, terms and payment of the insurance fee when using Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	User Satisfaction - Financial Markets	How satisfied are you with the accuracy of financial investment information when using Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
	User Satisfaction	How satisfied are you with the data presentation and the data format of the transactions?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Optional
	Affects	How satisfied are you with the response time of the Critical-Chains-enabled Multi-Factor Authentication?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Social Factors	Societal	How do you assess the energy efficiency and environmental sustainatbility trade-offs in deploying Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Desirable
Ethical and Legal	Privacy	How well-protected do you believe your personal data would be when using Critical-Chains-enabled applications?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. **-2/-1/0/ +1/+2** which?	Optional

	Privacy	How privacy/fraud risk-exposed do you feel, given the immutability and transparency of information in Blockchain as deployed within the Critical-Chains?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. -**2/-1/0/ +1/+2** which?	Desirable
	Privacy	How do you feel about Critical-Chains profiling for fraud detection and financial scoring?	Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by this question. -**2/-1/0/ +1/+2** which?	Desirable

10. Annex 2: Indicative Questionnaires for the Toll Collection Domain

Pre-Experience and Post-Experience Questionnaire

Questionnaire and/or Interview list for the Pre-Experience usability Evaluation with respect to the operational deployment of the Critical-Chains platform as the Highway Toll Collection Solution

This section presents an initial version of the Pre-Experience and Post-Experience questionnaires. The objective is to be able to compare the answers re Preceived Pre-Experience and Post-Experience usabilty and thus user satisfaction levels in each Phase. In addition, there are certain quantitive measures of KPIs that can be evaluated directly from the system. Further, this questionnaire can be adapted for various usability evaluation settings involving different users with distinct roles and skill sets as appropriate to the particular phases of the operational processes in which they would be engaged.

Assigning a number reflecting your judgment in your answer to HOW type of questions
Please note in all the questions that follow, wherever the question requires that you express your Qualitative Assessment about any aspect of the performance of your current Fintech solution and/or its impacts, then please select a number for your answer consistent with the following scale of qualitative ranges set out below as a Reference Scale.

-2	-1	0	+1	+2
Very Unsatisfactory	Unsatisfactory	Adequate	Satisfactory	Very Satisfactory

Indicative Pre-Experience Questionnaire – Highway Toll Collection Domain

Perceived Ease of Use of the Platform

To answer the following questions, please try to think of specific features i.e. functionalities that may be missing in your current Toll Collection platfprm and that you feel would be useful in enhancing the usability of the platform.

- In your opinion in what respects could the current platform be made easier to use?
- Which functionalities couldbe improved or which new ones added?

Perceived Usefulness (PU)

To answer the following questions, please try to think of features i.e. functionalities and the system interactions that you feel would be desirable e.g. to speed-up transactions or improve registered tag detection, audits, new transaction registration.

- How could a New Platform help you to be more effective in the exchange of transactions between the Toll Operator and the Merchant?

How could a New Platform be more efficient in detecting a TAG registered in the Black List?

- How could a New Platform be more useful for Audits of the Authority Controller?
- How could a New Platform save you time when you register a new Transaction?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the above questions as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Attitude (A)

To answer the following questions, please try to think of specific improvements in the design of the user interfaces and the overall look-and-feel of the system that you would consider as desireable.

- Overall, how could a New Platform be made more comfortable to use?
- How could a New Platform be more attractive compared to others in the market?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the above questions as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Intention (I)

To answer the following questions, please try to think of the most desired features of a potential new platform that you could use instead of your current platform to relieve you of any limiting/undesirable features of your current platform.

- What advantage(s) in using a New Platform would persuade you to discard your current platform and adopt the New Platform for your routine operations?

Information Presentation (IP)

Please state the specific features of the new platform that you think would be more useful in reducing the transaction registration time and improving the transaction data presentation layout.

- How satisified ar you with the formatting and presnetation of infirmation on the screen using your current platform?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the above questions as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

- What would make you use a New Platform to reduce the time needed to register a transaction?
- What would make you use a New Platform to improve the format of the data in the transaction lists?

User Satisfaction (US)

For the following questions please name the specific features of a possible new system that you would look for to enhance the reliability and flexibility performance of your current platform.

- What features make you use a New Platform to improve the reliability of your curent platform?
- What would make you use a New Platform to improve the flexibility of your current platform?
- How satisfied are you with the accessibility of the current platform?
- How satisfied are you with the timeliness and response time of the current platform?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the last two questions above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Information Quality (IQ) -Completeness

- Does the current platform provide you with all the information you need for all operational purposes (e.g. situation assessment, alertimg, audits and decison support)?

Accuracy

- What types of information accuracy issues, if any, have arisen from using your current platform?

Security

- What are the most important security threats in the Highway Toll collection domain?
- Are there any risks of lack of traceability and integrity of the data in this domain?
- Which is the biggest security risk in using the current platform?
- What security features of the current platform are the most risky in your opinion?

Measure Attribute Items System Quality (SQ) –Reliability

- How do you rate the reliability of the current platform?
- How do you rate the stability of the current platform?

Information Accessibility

- Where and in what manner does the current platform fail to provide an easy-to-access route as may be needed for operations?

Flexibility

- Can the current platform be easily adapted to meet new needs and conditions?

Integration

- Does the current platform easily integrate data from the legacy system?

Timeliness -Responsiveness

- Does the current platform take too long to respond to your actions?
- Does the current platform provide information in a timely fashion?
- Does the current platform return relevant and helpful answers to your requests quickly?
- Overall how helpfully responsive do you consider your current platform to be?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the last question above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Indicative Post-Experience Questionnaire – Highway Toll Collection Domain

Perceived ease of use of the Critical-Chains plaform

- How do you rate the usability of the Critical-Chains platform?
- How easily have you found its use in your operations?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the questions above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Perceived usefulness (PU)

- Does the Critical-Chains platform help you to be more effective in reducing the conflicts related to Blacklist?
- Does the Critical-Chains Platform save you time when you register new transactions?
- Does the Critical-Chains platform do everything you would expect it to do?
- How have yu found the effeciency of the the Critical-Chains platform in the exchange of information?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the last question above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Attitude (A)

- Overall, how do you rate the user-experience in using the Critical-Chains platform?
- Would you recommend the Critical-Chains platform to others?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the first question above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Intention (I)

- Do you intend to use the Critical-Chains platform integrated within your routine operations?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the three questions below as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

- How often did you use the Critical-Chains platform during the past testing cycle?
- Information satisfaction (IS)
- How satisfied are you about the processing speed of the Critical-Chains Platform?
- How satisfied are you about the accuracy of the information stored?
- How satisfied are you about the format of the transactions?

User Satisfaction (US)

- How satisfied are you about the reliability of the Critical-Chains?
- How satisfied are you about the flexibility of the Critical-Chains?
- How satisfied are you about the timeliness (response time) of the Critical-Chains?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the three question above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Would you expect the maintenance costs of integrating the Critical-Chains in your operational systems to be high?

How significant would you consider the maintenance costs savings/expenditure to be as a factor in your decision to integrate the Critical-Chains platform within your operations?

Please use the above Reference Scale to indicate the user-experience quality level re the criterion focused on by the three question above as appropriate; i.e. which of -2/-1/0/ +1/+2 would be your answer here?

Information quality (IQ)

Completeness

- Does the Critical-Chains platform provide you with a complete set of information as needed for your opertions?

Format

- Is the information provided well-formatted?
- Is the information provided clearly presented on the screen?

Accuracy

- Does the Critical-Chains platform produce correct information?
- With the Critical-Chains platform, are the registered transactions immutable in the database?
- Have there been any insatnces of inforamtion error in the information in using the platform?

Security

- Does the Critical-Chains platform increase security in the Toll Collection processes?
- Is the Critical-Chains platform more secure for certain threats than your current system?
  - If so which type of threats do you think the Critical-Chains platform would offer more protection against ? and which less?
- Overall what vulnerabilities/weaknesses do you think would arise from using the Critical-Chains platform?
- Do you think that the Critical-Chains platform offers effevtive safegaurds against the most damaging type of security threats ?

Ethical and Legal Data Protection Compliance

- Do you consideer the deployment of Critical-Chains platform in your operations would in any way expose your organisations to ethical issues; e.g. through lack of ethcial safegaurds?

- Do you think that the use of the Critical-Chains platform could lead to any potential Data Protection issues such as inadequate safegaurds if so what data protection risks would you consider may be more likely in using teh critical-chains platform

Measure Attribute Items System quality (SQ)

Reliability

- Does the Critical-Chains platform operate reliably?
- Is the Critical-Chains platform stable?
- Is the operation of the Critical-Chains platform dependable?

Accessibility

- Is the Critical-Chains platform easy to access?
- Does the Critical-Chains platform make the information easy to access

Flexibility

- Has the Critical-Chains platform easily adjusted to your demands or current conditions?
- Is the Critical-Chains platform versatile in addressing the needs of the domain?

Integration

- Does the Critical-Chains platform easily integrate with the TAG reader?
- Does the Critical-Chains platform effectively store data?

Timeliness

- Does the Critical-Chains platform take too long to respond to your actions?
- Does the Critical-Chains platform provide information in a timely fashion?
- Does the Critical-Chains platform return answers to your requests quickly?

****