Critical-Chains

Collaborative Project

Project Start Date 1st July 2019 Duration 36 Months

Deliverable D1.2

D1.2(a) White papers including S&T&I achievements and visionary statements

Published by the Critical-Chains Consortium

Version 2 Date 28-01-2021

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Confidential

Work Package Task: WP1

Document Responsible: RINA-C

Contributors: All Partners

Status: Final

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

Abstract

This deliverable presents an outline of the innovative results arising from the efforts of the partners within the Critical-Chains project and situates this in the broader technological, regulatory and social context of the wider innovation horizon and the landscape of emergent systems and services. This is motivated by the vision of the financial sector security and self-audit which the Critical-Chains Triple Accountability Model seeks to serve into the future.

Accordingly, this deliverable, D1.2 Whitepaper, sets out the resulting innovation with reference to both the vertical layers and the horizontal layers of the Critical-Chains Framework Architecture and as such presents the stakeholder-led holistic socio-technical perspective of the Critical-Chains innovation and its leading visionary research outlook towards robust, threat-driven, risk-based integrative security-privacy by design. This is to support the methodologically-guided accountability engineering and self-audit of cyber-physical system-of-systems, and in particular, the security and privacy protection of financial system and services infrastructure as well as their operational process integrity and compliance assurance.

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

Table of Contents

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

1 Executive Summary

The Project Objectives are to develop integrated, effective, accessible, fast, secure and privacy-preserving financial contracts and transaction solutions. This is to protect financial infrastructures against illicit transactions, illegal money trafficking and fraud that can take place through the banking clearing system and financial transactions settlement 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.
- Cyber security protection of Inter-Banks and Internet Banking, insurance and financial market infrastructures.
- Privacy protection through secure access supported by embedded systems and Internet-of-Things security.

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

2 Introduction

2.1 Scope

This deliverable takes a meta-analysis perspective and innovation horizon scanning view of the Critical-Chains results with reference to both the vertical and horizontal layers of the architecture. This includes accountability engineering, process integrity and compliance assurance supported by a methodologically-guided, ontologically committed approach to threat-driven risk-based integrative security-privacy protection by design.

Critical-Chains supports blockchain-enabled, scalable and effective "Secure & Smart Contracts" and "Secure Transactions" in banking, CCP and insurance sectors. Critical-Chains is focused on Accountability-by-Design where financial authorities are put in a multiparty blockchain-enabled triangular integrity and security for legal framework and further accreditation. We call this a Triangular Accountability Model, whereby the authorities are part of the chain, to prevent illicit transactions among criminal organisations, whilst enabling trusted transactions between two parties, A and B, via an authorised entity, e.g. bank, financial authority, insurance company, or any legal entity registered in the chain. The chain is enabled within a secure cloud of things, enabling the authentication of users and things generalised as nodes, blockchain as a service, AI-based techniques to identify network security and intrusion attacks as well as detect anomalies in financial transactions, all of which are integrated with the Critical-Chains Main Framework.

Fig.1 (a)

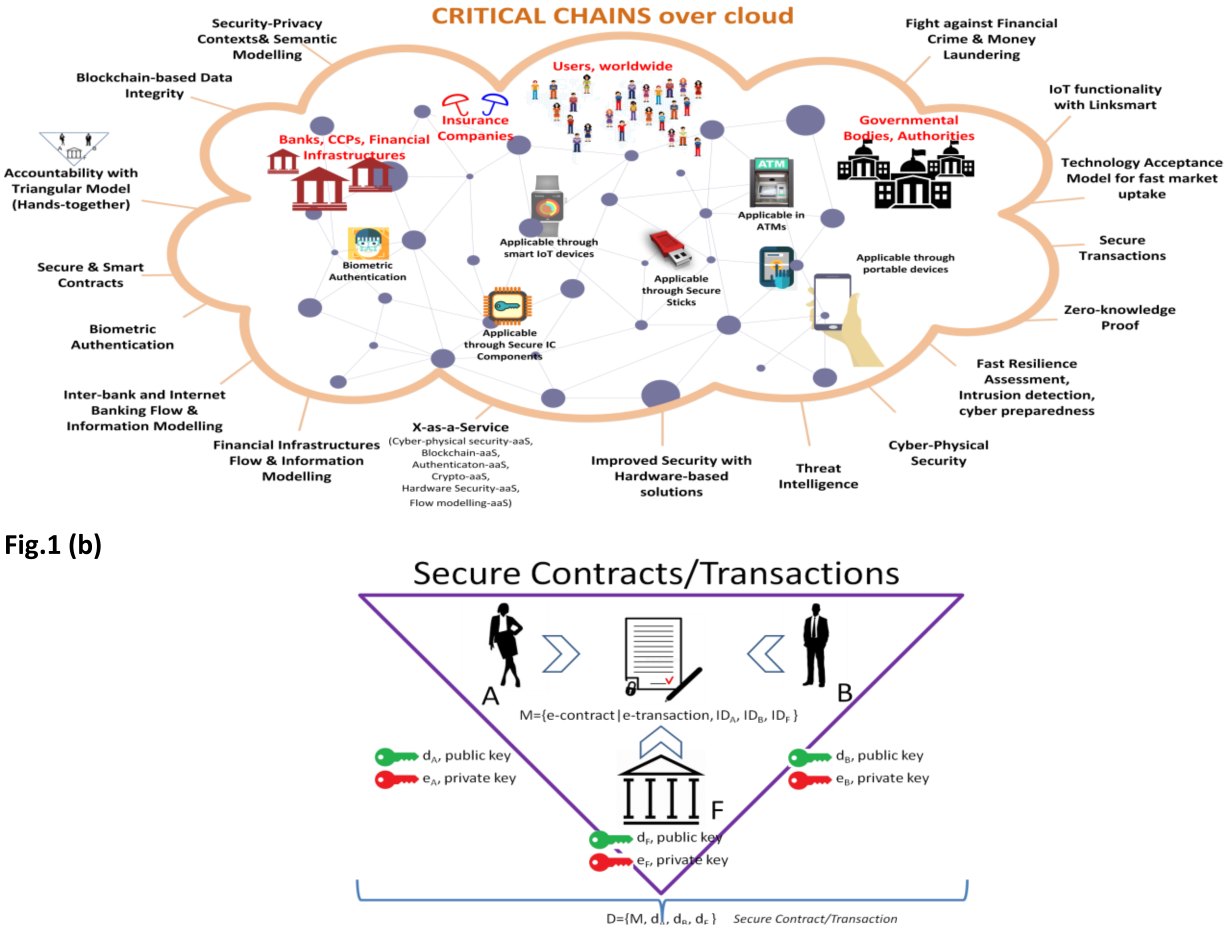
CRITICAL CHAINS over cloud
Security-Privacy Contexts& Semantic Modelling
Blockchain-based Data Integrity
Accountability with Triangular Model (Hands-together)
Secure & Smart Contracts
Biometric Authentication
Inter-bank and Internet Banking Flow & Information Modelling
Financial Infrastructures Flow & Information Modelling
X-as-a-Service (Cyber-physical security-aaS, Blockchain-aaS, Authenticaton-aaS, Crypto-aaS, Hardware Security-aaS, Flow modelling-aaS)
Improved Security with Hardware-based solutions
Threat Intelligence
Cyber-Physical Security
Fast Resilience Assessment, Intrusion detection, cyber preparedness
Zero-knowledge Proof
Secure Transactions
Technology Acceptance Model for fast market uptake
IoT functionality with Linksmart
Fight against Financial Crime & Money Laundering
Users, worldwide
Insurance Companies
Banks, CCPs, Financial Infrastructures
Governmental Bodies, Authorities
ATM
Applicable in ATMs
Applicable through smart IoT devices
Biometric Authentication
Applicable through Secure Sticks
Applicable through portable devices
Applicable through Secure IC Components

Fig.1 (b)

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

Figure 1 (a) Underpinning concept of Triangular Accountability Model and 1(b) the scope as the cloud of things

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

The Consortium structure has supported collaboration among partners to design, implement, integrate and deploy the innovations in emerging areas such as Blockchain, Cyber-physical system and Security, Artificial Intelligence (AI) and Machine Learning over the Critical-Chains main framework protected by the Secure Cyber Framework. As claimed, the XaaS approach based on services architecture works well as the consortium has designed and developed Blockchain-as-a-Service (BCaaS), Cyber Physical Security as-a-Service (CPSaaS), AUTHentication and AUTHorisation as-a-Service (AUTHaaS), Cryptography-as-a-Service (CryptaaS), Hardware Security as-a-Service (HwSaaS) and financial Flow Modelling as-a-Service (FMaaS).

The universities and research organisations, namely UREAD, CEA, JR, IMEC, and FHG have provided a strong scientific background in key topics of Critical-Chains. The participation of a leading organisation, namely INDRA, as one of the prominent enterprises in the transport market domain and EY and POSTEIT in banking and insurance sector and NETAS in ICT is a great chance for the wider dissemination and exploitation of project results. Research-oriented SMEs, namely ERARGE and GT have made a significant contribution in developing key technologies in blockchain and cyber-physical security.

3 WP-Specific Vertical Innovation Achievements & Visionary Statements

3.1 Cyber-Physical Security as-a-Service (CPSaaS)

3.1.1 Blockchain Core Data Integrity layer → Blockchain-as-a-Service (BCaaS)

Blockchain-as-a-Service (BCaaS) enables cloud-based services to develop, use and host blockchain applications, functions and smart contracts. In simple terms, BCaaS provides fully-fledged blockchain platforms to ease the development process and acts as a bridge between enterprise companies and enterprise blockchain platforms.

Within the context of Critical-Chains, BCaaS is the third-party creation and management of cloud-based networks for companies in the business of building blockchain applications. As such, Critical-Chains solution stack will support compliance, asset tracking, supply chain management, and generally displacing intermediaries. The focus is particularly 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.

Blockchain is a major game-changer for financial services core businesses, driving innovation in this space, as have Fintech companies. Blockchain environments such as Ethereum are open, flexible and can be customised to meet expected needs enabling innovation and providing new services and distributed applications. Ethereum enables Smart Contracts and Distributed Applications (ĐApps) to be built, potentially cutting out the middleman in many industry scenarios, and streamlining transactions settlement. BCaaS offerings are emerging to make blockchain technology more accessible to businesses, by reducing the overheads of adoption and driving solution scalability.

One of the goals of the Critical-Chains project is to develop an efficient and secure framework for financial transactions built on blockchain-based distributed ledger technology. The project follows the cloud-based Blockchain-as-a-Service approach in order to achieve greater flexibility, user-acceptance and relatively straightforward integration. In financial applications, guaranteed correct operation combined with external auditability of the system is a very important aspect and provides additional value.

A common limitation of permissioned blockchain networks is the reduced ability (compared to public blockchain networks) to perform full third-party audits to convince external entities in the correct operation of the system. This means that, while the members of the network may be able to validate all transactions, there are no efficient means for presenting proofs to external parties about the non-existence of data integrity compromise due to insider attacks, collusion or sophisticated attacks affecting most of the network nodes.

The wide adoption of cloud-based infrastructure introduces another risk to operating blockchain-based solutions. The security properties of a blockchain system often depend on the conditions that the network is run by multiple independent parties and each party has full control over their blockchain network nodes. In a cloud-based infrastructure, it may happen that the whole network operates within a cloud hosted by a small number of cloud service providers (one provider, in the worst case). Hence, the blockchain system may become vulnerable to attacks against one or a small number of cloud providers. Moreover, cloud service users have no direct control over the infrastructure that in principle can compromise the integrity of the whole system.

The main innovation Guardtime is aiming for, in the Critical-Chains project, is addressing these two issues described above - scalable long-term data integrity and auditability of permissioned blockchains and the integrity of cloud infrastructure. For the first issue, the goal is to combine the strengths of two different blockchain technologies so that the Guardtime KSI Blockchain will be used for anchoring Quorum permissioned network blocks to independently verifiable proofs that are secure against backdating attacks. To address the second issue, Guardtime MIDA, a cloud monitoring and integrity protection solution enables assurance and proof that virtual machines and software configurations in the cloud have not been compromised. The deployment of MIDA for Critical-Chains will provide useful feedback from real world usage to further improve the MIDA platform.

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

3.1.2 AUTHentication and AUTHorisation hardware-based secure AUTH-as-a-Service (AUTHaaS)

The AUTHaaS is one of the crucial service-based XaaS solutions in Critical-Chains. The achievements in the first half of the project have presented a great effort mainly in two modules:

- The authentication module includes all sub-systems for user registration on the Critical-Chains platform and user authentication to access the platform, offering multiple authentication factors: login/password, biometric, and policy-based authentication, in addition to an external eIDAS-compliant identity provider.

- The access control module includes common sub-systems for authorisation and access control by means of access tokens, user authentication being based on token-based authentication protocols.

AUTHaaS has been designed and developed to provide identity federation by enabling the authentication module which relies on standards and technologies, such as SAML and OpenID Connect. The proposed design simplifies the federated authentication and authorisation processes. Moreover, the module enables authentication of users with an eIDAS-compliant external identity provider. eIDAS compliance has been tackled by relying on a legacy system which has been deployed, on a largescale, as the Italian SPID (Public System for Digital Identity).

Multifactor authentication is one of the indispensable components of recent web-based XaaS applications in the Fintech area. In Critical-Chains, 3-factor authentication is considered as a reliable mechanism that incorporates the following modalities:

- Simple authentication: This is the regular authentication mode that relies only on login ID and password – what we know.

- Authentication using a SecureStick: This is a hardware token that enables user authentication - what we have.

- Biometric authentication: Face recognition is applied for user authentication - who we are.

In order to comply with the international standards and the recent and future trends in the market, the multifactor authentication services comply with the so-called FIDO standard[1]. The FIDO standard has been widely accepted by Internet giants like Google, Amazon, as it relies on the easy use of token-based authentication, especially for person authentication.

When considering IoT-enabled Fintech solutions, person authentication is not the sole authentication scheme, a further approach is needed for node authentication. For this purpose, the AUTHaaS has been designed by supporting IoT nodes. The Critical-Chains Consortium envisions a future, where diverse applications will rely on secure location and proximity information, such as, contactless payment, keyless entry systems, commissioning, or smart access control. As an inventive step, the Critical-Chains consortium has upgraded the SecureStick, which was formerly designed for person authentication, now to measure the proximity between two entities by wireless technologies. A distance bounding protocol has been developed, which enables a device to not only authenticate another device but also securely determine whether it is physically close by, in order to effectively mitigate relay attacks. This innovation is planned for deployed in tag authentication within toll collection processes.

To further enrich the authentication process, the AUTHaaS authentication module includes a policy-based authentication factor that enables at the same time, in addition to the authentication of users using their cryptographic keys, the enforcement of access policies. The access policies are cryptographically enforced thanks to a public-key encryption primitive, the attribute-based encryption (ABE). The policy-based authentication factor relies on the access control module of the AUTHaaS component to retrieve access policies, and it has been integrated into a federated identity protocol used by the AUTHaaS component.

[1] D. Balfanz, A. Birgisson and J. Lang, “FIDO U2F Javascript API.,” FIDO alliance, 2013.

3.1.3 Cryptographic backend for symmetric cryptography→ Cryptography-as-a-Service (CryptaaS)

Kerckhoffs's assumption was stated by Auguste Kerckhoffs, one of the fathers of cryptography, in the 19th century**:** A cryptosystem should be secure even if everything about the system, except the key, is public knowledge[2]. According to this assumption, which is still valid today with the evolution of IoT and blockchain, a typical cryptographic system must be designed by considering not only strong cryptographic algorithms but also cryptographic key generation schemes resilient to cyber-attacks. The Critical-Chains Consortium has focused on the development of such resilient cryptographic backend that plays a critical role in IoT-enabled blockchain infrastructures with a specific focus on the needs of the Fintech industry.

The Consortium first focused on the root causes of the security vulnerabilities. The problem was considered holistically by identifying not only cyber but also cyber-physical, including hardware-focused threats such as tampering or side channel attacks. In order to solve this problem, the Cryptography-as-a-Service (CRYPTaaS) component has been designed over a reliable and high throughput Hardware Security Module, named as Hardware Security-as-a-Service (HwSaaS), at server side enabling very fast private key generation, symmetric and asymmetric cryptographic algorithms and hashing functions, all of which are implemented at FPGA level at hardware side. The hardware-backend, HwSaaS, was integrated with the CRYPTaaS which is based on service-based architecture. CRYPTaaS, then, was integrated with the Critical-Chains main framework in the form of a XaaS. CRYPTaaS is based on open standards, such as PKCS#11[3], and is implemented by reusing, adapting and improving the OpenCryptoKi library.

The developments reported in the first half of the project have shown that the Critical-Chains main framework will be upgraded by integrating the CRYPTaaS and HwSaaS in the second iteration. The upgraded framework will enable very fast encryption and decryption of transactions that will be realised by the improved true random number generation tests and private key generation schemes. The FPGA-based applications will improve the cryptographic backend to protect any financial data and any stakeholder data, which is, for sure, a decisive and ambitious step towards GDPR compliance.

3.1.4 Data Security Hardware (HW) Security Module as-a-Service" model (HwSaaS)

Data and information security should start at the lowest layers of data transmission networks, even at the place where data is generated. This has become one of the most prominent requirements in IoT-based digital systems where the transaction volume and velocity is very high. In order to cope with high transaction rates, Critical-Chains consortium has focused on developing a Hardware Security Module (HSM), namely Hardware Security as-a-Service (HwSaaS) that is equipped with very fast true random number generator, on-device true randomness tests, key generation and management, and cryptographic functions, all of which run at hardware level. This hardware-based approach has two main advantages. First, since every critical operation is held on the hardware itself by applying fast algorithms at FPGA level and it is designed to be resilient to tampering attacks, HwSaaS presents higher throughput and less vulnerability to physical attacks. Second, since the hardware based true random number generation schemes rely on high entropy true randomness sources, guessing the generated private keys becomes nearly impossible.

There is a strong research background behind the HwSaaS, especially in the areas of true random number generation, numerical methods, nonlinear signal analysis, embedded design**.** A robust reconfigurable transient-effect based true random number generator has been developed by ERARGE researchers and engineers whose main entropy source depends on the metastability of the SR latches. The first prototype based on the designed TRNG has been integrated in the HWSaaS and it has been reported that it passes all the true randomness criteria of NIST-800-22. The proposed TRNG has also been compared to chaotic

[2] Kerckhoffs, Auguste. La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef. Librairie militaire de L. Baudoin, 1883

[3] https://www.oasis-open.org/news/pr/oasis-approves-four-public-key-cryptography-pkcs-11-standards

oscillators presenting lower cost, higher throughput and more entropy and satisfactory efficiency for financial transactions.

The wireless link required for the HwSaaS IoT communications is vulnerable to tampering, e.g., with a man-in-the-middle attack. To avoid such attack, a secure distance bounding algorithm based on the flight time has been implemented by IMEC and integrated with the HwSaaS component. The solution is being integrated on an alternative SecureStick model, with secure distance bounding capability, which will enable “things” authentication. This new SecureStick is planned for proof of concept, a s demonstrator for the toll collection pilot in the second iteration of the project. The secure distance bounding algorithm solution is currently only capable of preventing attacks on the wireless link, but it will be further improved by also detecting and signalling that the wireless link is currently under attack, which will greatly help the Critical-Chains architecture in preventing tampering attacks.

HwSaaS has been integrated with CryptaaS at laboratory scale and is planned to be deployed for real-life Fintech operations enabling a very fast, accurate and secure cryptographic operations. This promising step will enable end-to-end security as the AUTHaaS and the token-based authentication solutions will fulfil both person and node authentication. Hence, Critical-Chains main framework will be proven as a replicable framework model for the wide range of IoT-enabled blockchain solutions where “things” and “person” authentication are mandatory.

3.1.5 Data flows and information Flow Modelling-as-a-Service (FMaaS)

There has been an increasing research interest in automated financial transaction monitoring and modelling to support the detection of anomalous flows e.g. fraudulent transaction such as money laundering etc. FMaaS has a significant role in identification of such anomalies, and it can serve as a strong assistive service within the Critical-chains main framework in the form of a XaaS. For this purpose, many machines learning or graph-based AI methods have been deployed for such solutions, almost all of which have had to cope with the limitations arising from lack of real data, which has led researchers to attempt to synthesise data and/or use open synthetic data sources. The Critical-Chains team working on this area have developed, benchmarked and submitted publications on the following results:

i) An extensive range of machine learning (ML) solutions based on the most promising approaches per the state-of-the-art;
ii) A range of hybrid graph-enhanced machine learning solutions;
iii) A new synthetic data base (v 1.7) for one of the dominant transaction types (SEPA);
iv) Deployment of the resulting solutions on the Critical-Chains synthetic SEPA data as well as two open data sources as commonly deployed for benchmarking standard as well as hybrid graph-enhance solutions; and
v) Reliability analysis of machine learning-based predictions.

Accordingly**,** joint studies by UREAD, JR and FHG have so far shown that the existing ML algorithms can reliably detect anomalies within complex datasets. The results have confirmed that ML methods can successfully contribute to security in Fintech systems by way of supporting enhanced fraud detection capability. Additionally, it has been established that feature engineering and selection can critically influence the performance of certain algorithms, and that careful selection of features can increase overall performance and limit the negative influence of some features.

Moreover, the ensemble models can provide better prediction results in terms of performance metrics with/without the graph-enhanced features - these models operate by combining multiple models. Graph-enhanced features such as PageRank and Degree of the nodes play a vital role in the prediction results.

The graph-based approaches tend to contribute to feature set significance for predictive models, more than is the case with standard approaches using non-graph-based features only; hence, the graph-based approach shall be studied further in order to examine its potential extensively.

Optimisation of the performance of financial flows anomaly detectors, by evaluating and refining the candidate solutions, requires data from various financial transaction models such as SEPA, Credit Card transactions, ATM and synthetic data for other financial transactions models. This would contribute to the improvement of the models through assimilation of knowledge of different types of transactions. Accordingly, training, testing and benchmarking of the anomaly detector algorithms using various data sources is the strategy that the team has pursued and plans to continue to optimise the resulting FMaaS innovation.

Reliability analysis of the machine learning-based predictions has also been applied to support a human operator by answering the questions "How did the model come to this particular conclusion and how can I therefore trust the prediction?" Such a question may be answered through a local feature analysis based approach based on a metric called Layer-wise Relevance propagation[4,5] which evaluates the contribution of each input feature towards or against a specific classification. It has transpired that a metric comprising the relevance values (e.g., the sum of all positive Relevance values) cannot adequately support the resolution of the above questions. Further analysis needs to be performed where a combined metric is to be developed. This combined metric could incorporate quantities such as the sensitivity of a prediction under variation of certain input feature (e.g., via LIME[6]). As there are many methods for locally explaining the prediction of a black-box machine learning model, the future challenge will be to choose and combine them in a meaningful way and to prove the stability and predictive power of the new metric.

4 WP-Specific Horizontal Layers Achievements & Visionary Statements

4.1 Critical-Chains Main Framework: Integrative Technology & Secure Cloud Business Model

In the first phase, Critical-Chains standalone Main Framework specifications have been studied and the Version1 was successfully deployed by joint studies of NETAS and EY. Within the context of the development process, the Critical-Chains components have been evolved to create a fully integrative and scalable infrastructure. The overall design respected the state-of-the-art infrastructure models in which it supports the micro-service and container-based applications and modules to be run with high availability. Therefore, the related elements and serverless services have been adapted into the Main Framework and entry-level deployment of the components has been started. In particular, a strategy has been implemented to enable the progression of the planned effort despite the restrictions that had been imposed due to the global pandemic.

The progression of the Main Framework effort has created exploitable results. The **e**xploitation pathways envisaged for the project outcomes, could run in two ways as follows: First, the overall solution bundle in cloud computing can be used with the requirements and solutions in the Critical-Chains Consortium to obtain ready-to-use new cloud architectures in similar blockchain-based projects. Second, the studied security and technical requirements, specifications, solutions, and test capabilities for blockchain-based critical infrastructure can be converted into end-to-end consultancy for the future.

4.2 Blockchain based Critical-Chains Web Applications over the Critical-Chains Main Framework

The first phase studies have presented a significant improvement in applying BCaaS over the Critical-Chains Main Framework in four selected pilot areas. All partners have contributed to these pilots (D6.2), in which four different applications have been developed and deployed over the Web as standalone pilots with the incorporating the components required for the overall usage context. The conventional backend approach

[4] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0130140

[5] https://www.nature.com/articles/s41467-019-08987-4

[6] https://dl.acm.org/doi/abs/10.1145/2939672.2939778

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

has been shifted to blockchain-based business logic by the smart contracts with a good collaboration among the consortium members. The actual usability has been successfully validated. Moreover, it has been seen that the blockchain, in the data security and transparency context, is a successful tool for the Fintech world that could revolutionise the industry. However, there are still some limitations in this cutting-edge world whereby the overall system load of the blockchain does not allow the users to quickly register data in a secure way. In the first period, additional APIs and services have been deployed to overcome these challenges. Planned work to support the private blockchain in the second phase will allow the consortium to overcome such limitations.

Further, the blockchain technology is not fully compatible with the FIAT currencies, which is a major barrier in some Fintech contexts. The consortium has planned some measures to tackle these issues in the second period.

The back office solutions also play a crucial role within the Main Framework by providing them with new levels of security, trust and data integrity. Moreover, technologies used, and lessons learnt will be applicable to other solutions that have a major financial component, such as multimodal clearing houses, or other products not only for the Transport market but also in banking and insurance sectors, therefore enabling the exploitation of the results beyond the current project scope. INDRA's back office applications have been deployed presenting an effective integration of security, trust and data integrity tools.

The existing exploitation channels can be adapted to serve the distribution sector in a manner that is aligned with the solutions that the INDRA already provides. This includes international traffic and transport markets in which INDRA already has a strong presence. Indra is well-placed to support the exploitation of Critical-Chains enabled solutions to be adapted to the requirements of the transport operators in global markets,

As reported by POSTEIT and EY, banking and insurance services offered using blockchain technology can really simplify processes and consequently lower the costs related to the subscription of financial products. In fact, the achievements support this hypothesis such that the blockchain technology can be leveraged to reduce the need for intermediaries in financial processes and potentially enable the users to interact directly with financial providers.

In order to reach the broadest customer base and acceptance level by potential customers, one of the critical aspects to address is to design these innovative services in a way that the usability, and in general the user experience in the whole process, is at least at the same level as of the current commercial offerings. Thus the following key user-centred requirements will be the main driver of the developments in the second iteration of Critical-Chains:

- The framework components should be easy to adopt and integrate with different technologies
- Availability of good documentation
- Availability of support and a large community of users
- Integration with existing digital identity providers and authentication services
- Application to other domains and use cases

4.3 Context-Aware Threat-Driven Risk-based integrative Privacy & Security by Design

The results achieved for security-privacy-by-design of Critical-Chains represent a strong foundation for formalising the Privacy-Security Threat Severity Ranking to inform the classification, selection and Prioritisation of the optimal managed-mix of Countermeasures.

To support the integrated operationally context-aware, threat-driven, risk-based privacy-security protection by design, Critical-Chains has established and deployed a comprehensive analysis base underpinned by a methodology-guided and ontologically committed approach to privacy-security threat modelling

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

Specifically, the analysis focuses on such threats as could arise within the Critical-Chains target application domains as supported by the Critical-Chains triple accountability framework - namely, the Financial Infrastructures (Fintech), Open Banking, Insurances Claim Settlement and Highway Toll Collection.

The results achieved represent a strong foundation for the Critical-Chains innovation stack to deliver a framework for formalising the privacy-security threat severity ranking to inform the classification, selection and prioritisation of the optimal managed-mix of Countermeasures.

This work has **i)** established the relevant ontologies for policy enforcement and compliance audit including relevant GDPR ontology and, accordingly, **ii)** derived the relevant data models for the targeted domains and operational context assumptions based on which **iii)** all the security and privacy threat models have been developed, **iv)** this has resulted in threat lists which have been severity ranked and prioritised based on a novel threat severity calculus; and v) subsequently, the countermeasures responsive to prioritised security and privacy threats have been analysed to arrive at an optimal set of countermeasures for maximum effectiveness and efficiency in privacy-security protection.

In this way, Critical-Chains has extended the analysis adopted from the UI-REF-based requirements prioritisation methodology, to apply it to threats severity ranking and responsive safeguards requirements. Accordingly, a novel framework for Threat Severity Ranking and Countermeasure Prioritisation resolution (TSR-CMP) has been developed as supported by an intuitive tabularisation schema for the risk calculus, visualisation with colour coding to illustrate severity ranking of threats and the process of selection of prioritised countermeasures.

In this way. Critical-Chains has contributed a novel methodologically-effective, threat-driven, and model-based privacy-security by design framework - a dynamically responsive and integrative use-context-aware paradigm for security by design.

In particular, to protect the Critical-Chains framework against network attacks, a multi-protocol anomaly-based network-intrusion detection system has been devised. This multi-protocol configuration has provided very good results with low false positive rate, fast detection time and high accuracy, already tested against the CIC-IDS 2017 dataset. Moreover, a suggestive reaction system able to react to unknown attacks has been designed and developed. The system defines a new reaction paradigm thanks to its capabilities to define signatures related to the network impact instead of using already known specific attacks. Once, the suggestive reaction system is validated, inputs from the authentication anomaly-detection system will be included in order to enhance the detection capabilities of the Secure Cyber framework.

Consistent with TSR-CMP approach, the consortium has successfully deployed the Secure Cyber framework. For instance, Authentication Anomaly Detection module, as a component of the Secure Cyber Framework, with a very high detection ratio in a secured environment as a standalone module. The module development is aligned with the actual Authentication provider of the Critical-Chains (Keycloak) which in turn made the integration preparations much faster than anticipated. Moreover, two important plug-ins have been developed for the Keycloak, the first one is the custom listening plug-in to further support the integration to the other ICT projects. The second plug-in is the additional events to listen over the Keycloak server. These two achievements could be publicly disseminated as a contribution of the Critical-Chains Consortium to the open-source world.

The overall design consideration was mostly on the high elasticity and scalability of the module to be implemented to other projects or to be exploited in the form of X-as-a-Service. As such, the solutions achieved do represent successful developments. . However, there were some limitations for adaptation of the system in the actual FinTech domain. The data feed of this sub-module was based on a traffic generator script that works over the server to create data continuously. However, even the enhanced version of the script will not be able to generate realistic data compared to the real environment. Therefore, the system still needs some adjustment over time with the more realistic data, on which we will be focusing in the second phase.

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

4.4 Regulatory, Standardisation, Compliance Audit & Certification

The Audit is a procedure that organisations should use to reach a continuously productivity improvement in their organisation, and this is also a crucial dimension in Critical-Chains. The main principle of the audit process is based on the Deming cycle of Plan, Do, Check (Study) and Act (PDCA or PDSA), which is a model realising the repetition of four stages for Continuous Improvement (CI) in business process management. These stages are:

- Plan: Establish objectives and processes required to deliver the desired results.
- Do: Implement the plan from the previous step.
- Check: Evaluate the data and results gathered from the Do phase. Data are compared to the expected outcomes to identify any similarities and differences.
- Act: Also called "Adjust", this phase is where a process is improved. Records from the "do" and "check" phases help identify issues within the process.

For this project, in particular, the compliance audit has been adopted. The compliance audit is an examination of the policies and procedures of an entity or department, to assess if it complies with internal or regulatory standards. It enables organisations firstly ensure a safe working environment complying with government requirements and safety protocols intended to promote a secure and stress-free workspace. Secondly, they contribute to increase productivity, managing production downtime, and boosting profitability. Moreover, legal issues, penalties and other consequences, as disruption or even operation cessation, will be prevented and continuous operation guaranteed. Finally, a continuous and iterative compliance assessment helps to establish a good reputation, gaining public trust and prevailing in the industry by remaining aligned to industry protocols.

During an audit, the auditor needs to obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. A compliance audit checklist is a tool used by external and internal auditors to determine the organisational compliance with government regulations, industry standards, or internal policies. It enables the gathering of significant data and photographic evidence to discover gaps in processes that can be improved in order to meet requirements. When used appropriately, an audit checklist will easily identify areas of concern and enable management to take corrective actions to fix the problem.

Most central banks require commercial banks to perform the compliance audit to verify that they are compliant with those laws and regulations set. The entity may also have its internal audit in order to verify that its internal policies and procedures are being complied with.

In the regulatory landscape, the Critical-Chains Consortium has addressed the following key challenges:

- Managing the Regulators: Responding to regulatory requirements promptly, protecting both the brand and reputation;
- Compliance Strategy: Leading the strategic decision-making process from a regulatory compliance standpoint;
- Compliance Operations: Reducing compliance costs by promoting transparency and managing inefficiencies in a paper-driven process by adopting digital solutions;
- Consumer Protection: Implementing new solutions to increase the protection of the customers.

In this context, financial institutions will require more process and system enhancements, and

framework technology solutions to assist and support them in putting in place an effective and dynamic compliance framework that is responsive to market and regulatory developments.

The A&C Tool presented by RINA-C has supported the quality assurance process of the Critical-Chains platform, in order to put in place an audit of the process and to ensure compliance to current standards on the part of the Critical-Chain platform.

This is a software solution used to assess the project outcomes with reference to NIS, GDPR, PSD2 and AML/5 compliance; the objective being to create a model that will support operators in understanding how Critical-Chains building blocks can contribute to ensure compliance.

The A&C tool is a Web-based tool that is implemented over cloud, specifically a software-as-a-service developed in order to provide the essential functionalities to support the user in conducting a self- assessment and monitoring the compliance rate in order to arrive at a compliance situation assessment. so as to improve upon it. The main scope, indeed, is to audit and check the compliance of the entire financial processes with reference to the legislative linked to the directives mentioned above.

The design of the A&C tool is a customisation of the generic Audit & Compliance method that is described above to implement the Audit & Compliance Tool, an analysis and an identification of the current standards and procedures regarding Critical Chain is necessary. The analysis and identification of regulations – NIS, GDPR, AML/5, PSD2 - were conducted in document D2.7.

This investigation enables the definition of checklists composed by points that refer to each paragraph of the relevant regulations. This mechanism is in-line with the audit process, aiming to verify if the target platform, and related processes comply with standards and it determines to what extent the established criteria have been met or not. In this regard, the aim of this tool is to support the quality expert in all the processes of the Critical-Chain platform in order to make a self-assessment audit to verify the compliance with standards.

4.5 Integration Context for Regulatory, Standardisation, Compliance Audit & Certification In the Banking

industry, there are many kinds of regulations required for bankers to follow and comply. Given the potential of technologies such as cloud, blockchain and artificial intelligence, that significantly change the whole banking sector, regulators in Europe are working continuously to define and refine laws in order to take the opportunities and manage risks of that technologies. On the other hand, if banks want to take advantage of these market opportunities, they will have to adapt their internal processes to the new regulations that in some cases pose some strict constraints.

In order to benefit the sector, Critical-Chains is working to ensure compliance in the operational context of the Financial Services Sector with respect to the relevant legislative instruments; namely, EU Regulation 2016/679 (GDPR), EU Directive 2015/2366 (PSD2), EU Directive 2015/849 (AML5), EU Directive 2016/1148 (NIS). In addition, the project developed a common Accountability by Design model supported by RACI (Responsible, Accountable, Consulted, Informed) matrix which also enabled the comparison among GDPR, AML5, PSD2 and NIS in terms of roles and responsibilities. This comparison has highlighted a harmonization between GDPR, AML5 (which even contemplates the need to comply with the GDPR) and NIS that has been confirmed by the analysis of the technical requirements derived from the clauses contained in the four Directives. Identified similarities will be used as effective input to Critical Chain audit process, in order to reach a continuously productivity improvement in the framework development.

For the sake of clarity, the main principle of an audit process is the Deming cycle that is based on PDCA (Plan-Do-Check-Act): a model based on the repetition of four stages for continuous improvement (CI) in business process management. For this project, in particular, a compliance audit is adopted, as an examination of the policies and procedures to assess the compliance with internal or regulatory requirements.

This process is enabled by the Audit & Compliance Tool that supports the quality assurance of the Critical Chain framework and solutions along the development process, by putting in place a continuous assessment of the project outcomes for NIS, GDPR, PSD2 and AML5 compliance. Such action will lead to the impacting goal to promote a model able to support regulatory information symmetry between Operators of the Financial domain and Solution Providers as Critical Chains and therefore ensuring robustness and reliability of the built services by design.

The identified similarities among Directives and the use of configurable solution focused on collecting and analyse audit & compliance outcomes (i.e., such as design evidence, coverage or requirements, etc.) can support the resilience of financial services and products against an evolving environment influenced by technologies and regulation changes. This is possible for example by categorizing and map design evidence among directives enabled by the interoperability between ad-hoc compliance models set within the Audit and Compliance tool.

The eventual reuse of evidence can reduce time and cost of design reviews and analysis thus enabling a dynamic and agile process to be applied also to standardization and certification contexts. Such approach is aligned with the current efforts the standardization community is doing related to artificial intelligence and blockchain technologies (i.e. ISO / IEC JTC 1 / SC 42, ISO/TC 307) in establishing common building blocks, risk management frameworks properly targeting multi-stakeholder landscape and addressing key areas such as: governance (targeted at Board Directors and senior executives), management systems (which might include specific risk management frameworks and controls within organisations) and technical standards that are focused on factors such as terminology.

Furthermore, the security certification processes (ISO27001, Common Criteria) are today considered too rigorous and time consuming. Additionally, adequate instruments to support the certification process are deemed. A new security certification process that supports the characteristics of the FINTECH domain is necessary following an agile and incremental approach in which each technology provider of the supply chain assesses the trustworthiness of the software component creating a single “trustworthiness profile” based on indicators (legal constraints, development process constraints, collected evidence, data on operational and design vulnerabilities, etc.).

The possible evolution of standardization and certification processes is considered in Critical Chain framework being progressively supported by a unique knowledge base (i.e. the Audit & Compliance Tool) in which evidences related to Critical Chain Platform are collected and used for regulatory compliance, standards compliance and certification thus creating different views of the same model that will follow the entire lifecycle of the Platform positively impacting adoption and exploitation in the operational environment.

5 Conclusions

This Deliverable, D1.2, has outlined the innovative results arising from the Critical-Chains project and set out its innovation outlook as planned to advance the technological wavefront in accountability engineering of cyber-physical system-of-systems; in particular to support the security-privacy protection by design of the financial system and service infrastructure.

The deliverable has taken a meta-analytic view to situate accountability engineering within the broader technological context and motivate it as a visionary necessity to support the accountability, process integrity and compliance assurance of financial transaction systems in the context of the emergent financial services innovation landscape.