Critical-Chains

Collaborative Project

Project Start Date 1st July 2019
Duration 36 Months

Deliverable D7.6 (Public)

Gap analysis of current relevant standards

Published by the Critical-Chains Consortium

Version 1.3 Date: 25/01/2020

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP7

Document Responsible: CEA

Contributors: **As Planned:** RINA-C, ERARGE, EY, IMEC, CEA
As Needed: UREAD, GT

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 D7.6 “Gap Analysis of Current Relevant Standards” sets out the various regulatory and standardisation requirements to support the financial infrastructures and operational layers within the financial sector. Accordingly, it presents a gap analysis of regulatory, standardisation, compliance and certification instruments. This includes a review of existing standards with respect to the reference authorities (e.g., ISO, IEEE, ETSI, FIDO Alliance, OpenID Foundation, OASIS, NIST) and highlights the challenges for regulatory authorities in attempting to keep up with the rapid pace of Fintech innovation and emergent new business models e.g., those offering new mobile money and cryptocurrency-enabled transaction services. This is followed by a description of the standardisation seeking activities performed by the Critical-Chains project. The aim is to motivate the development of any regulatory standards as required to best support the sectoral adoption and operational deployment of the Critical-Chains accountability by design solution stack.

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

Deliverable D7.6 Document History

Versioning			
Version Number	**Date**	**Contributors' name and organisation**	**Changes**
V0.1	24/09/2020	CEA	Initial deliverable structuring
V0.2	06/10/2020	UREAD	Further Deliverable structuring and elaboration of some sections
V0.3	30/11/2020	RINA-C	Contributions on Regulatory Standards, Privacy and Security Standards, Compliance Audit and Assurance Standards
V0.3	30/11/2020	ERARGE	Security Interoperability Standards, Fido Extensions, etc.
V0.3	30/11/2020	GT	Distributed Ledger
V0.3	30/11/2020	RINA-C	Contribution to inventory and gap analysis
V0.3	30/11/2020	CEA	Contribution to inventory
V0.3	23/12/2020	EY	Contribution to inventory, gap analysis, and impact
V0.3	23/12/2020	UREAD	Accountability by design in Critical-Chains
V1.0	12/01/2021	RINA-C, CEA	Deliverable structure finalisation
V1.1	18/01/2021	RINA-C, CEA, IMEC	Minor revisions and formatting
V1.3	25/01/2021	RINA-C, ERARGE, UREAD	Final review and edits as required.

Internal Review History

Internal Reviewers	**Date**	**Comments**
UREAD	04/01/2021	Review and edits throughout

External Review History

Internal Reviewers	**Date**	**Comments**
FHG	18/01/2021	The references are not numbered. Sometimes the headings are indented. Some sections have only one subsection which results in an odd numbering.
JR	22/01/2021	Consistency issues in the formatting, the font and the line spacing. The text in the figures is too small. Potentially an overview figure how chapters' 1-4 influence chapter 5 could contribute to clarity. Additional formatting (important words in bold or italic) could make the reading of the document easier.

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

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 Figures

List of Tables

Executive Summary

This deliverable D7.6 “Gap Analysis of Current Relevant Standards” analyses the standardisation and regulations activities relevant to the Critical-Chains project.

This deliverable is comprised of 6 chapters:

Chapter 1 presents a short summary introduction of the Critical-Chains and the scope of the project.

Chapter 2 provides the brief summary of the Critical-Chains domain and the description of the main building blocks of Critical-Chains.

Chapter 3 sets out the inventory of current standards relevant to the Critical-Chains accountability by design solution stack. This includes a review of the standards with reference to the respective standardisation bodies (ISO, IEEE, ETSI, FIDO Alliance, OpenID Foundation, OASIS, NIST) as well as Blockchain and smart contracting related standards examined on a layer-by-layer basis including the Blockchain layer (P2P network, proof of x, consensus rules, transaction recording, smart contracts and digital signing) and crypto-currencies.

Chapter 4 presents the analysis of the operational context-specific regulatory and standardisation gaps which is devolved into:

- The transversal standardisation requirements including those relevant to financial systems, system-of-systems, privacy, security, interoperability, integrity, monitoring, self-audit, compliance assurance, certification and governance.
- Vertical standardisation requirements comprising Fintech, financial transaction settlement, pre-payment cards, mobile money, crypto-currencies, online transactions (e-banking, e-purchasing, e-government), and Insurtechs including policy purchasing and renewal, claim submission and settlement.

Chapter 5 includes Critical-Chains Standards Seeking contributions, including Multi-factor Authentication and Cryptographic Primitives.

Chapter 6 presents the conclusions offering insights arising from the analysis and the activities performed.

****

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 Introduction

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

The technologies to be deployed consist of:

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

1.1 Background

This deliverable D7.6 takes as input the overview of the laws, regulations, standards and best practices relevant to the Critical-Chains operational deployment context provided in deliverable D2.7 “Regulatory Compliance and Accountability-by-Design model”.

1.2 Scope of this Deliverable

The scope of this deliverable is the analysis of the gap of current standards with topics relevant to Critical-Chains topics. This deliverable creates a link to relevant standardisation bodies and groups which could have an impact on Critical-Chains. The link will be created by active participation in working groups and by establishing bilateral communication channels. Important aspects of the Critical-Chains development work will be represented in the standardisation groups by the participating consortium partners. This deliverable will also present assessment of major differences or alignment between relevant standards in force (ISO, IEEE, CEN, ETSI, etc.) and Critical-Chains goals and outcome in terms of features impacting the solutions promoted by the project.

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

2 Critical-Chains Domain

This section will briefly cover the domain of Critical-Chains, and the technologies involved. Critical-Chains has 3 main objectives – the Critical-Chains Main Framework, Cyber-Physical Security as-a-Service (CPSaaS), and Data flows and information modelling. Critical-Chains is largely involved in financial technology and targets financial authorities, financial market infrastructures, stock markets, insurance companies, internet banking and ATMs. The Critical-Chains Main Framework is a cloud infrastructure that is composed of Platform and Software-as-a-Service layers and is able to detect and tackle fraudulent/illicit transactions. The framework is highly scalable and most importantly, has a focus on security and privacy such that the framework is a Secure Cyber Framework. This is ensured through the existence of firewalls, intrusion detection systems, packet inspection and other cyber-security tools.

The framework is designed for both end users and financial authorities and has the potential to interact with IoT and Big Data applications and is designed to be interoperable with the other prior mentioned objectives. Critical-Chains also presents an innovative triple accountability model that takes advantage of Blockchain and digital signing to prevent authentication threats.

Within Critical-Chains objectives, there is a focus on offering multiple distinct technologies in the form of 'as-a-service' to clients. X-as-a-Service is a collective term which implies the delivery of X to a client as a service. In the domain of Critical-Chains these technologies are Hardware Security-as-a-Service (HwSaaS), Blockchain-as-a-Service (BCaaS), Crypto-as-a-Service (CryptaaS), Authentication-as-a-Service (AUTHaaS), and Flow Modelling-as-a-Service (FMaaS). Data flows and information modelling encompasses FMaaS and Cyber-Physical Security as-a-Service encompasses the other as-a-service models.

- Blockchain-as-a-Service (BCaaS) – Based on Keyless Signature Infrastructure; provides services to enable clients to build, host and use their own Blockchain applications and smart contracts on a Blockchain infrastructure. In the case of Critical-Chains, this Blockchain infrastructure is Ethereum/KSI Blockchain that provides decentralised trusted collaboration with accountability at all layers and enables cross-hierarchical and cross-sectoral working.
- Crypto-as-a-Service (CryptaaS) – Exists at a software level within Critical-Chains. Clients are offered as a service a cryptographic backend that enables symmetric cryptography, hashing, truly random number generation, prime number generation and key generation.
- Hardware Security-as-a-Service (HwSaaS) – Exists at a hardware level within Critical-Chains. It provides data and information security and privacy preservation at all layers of a cloud. This is achieved through IoT connectivity and Hardware Security Module which takes advantage of truly random number generation.
- Authentication-as-a-Service (AUTHaaS) – Offers authentication and authorisations services that are strengthened through hardware-based secure IoT sticks and biometric authentication. AUTHaaS is a complete Identity Access Management system that supports authentication protocols such as eIDAS while also providing Identity Broker functionalities.
- Flow modelling-as-a-Service (FMaaS) – Big data analytics has the potential to protect companies from cyber-attacks. In FMaaS techniques such as machine learning are applied to create effective models for protection against cyber-attacks. The flow data of companies and clients is processed within this 'as-a-Service' model to inform them of potential cyber-attacks.

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 Inventory of Current Standardisation Bodies Relevant to the Critical-Chains Project

This chapter reviews existing standards and regulations relevant to the Critical-Chains project. The review describes the situation as it is today.

3.1 Audit/certification for cybersecurity and privacy aspects

This section focuses on the audit and certification regulations relevant to the Critical-Chains project.

3.1.1 ISO

Regarding the certification for the cybersecurity and privacy aspects, the ISO/IEC 27001 standard, the ISO/IEC 27032 guidelines and the ISO/IEC 29100 standard have been identified.

The ISO/IEC 27001 “Information technology - Security techniques - Information security management systems – Requirements” is the international standard that sets out the specification for an information security management system (ISMS), including aspects relating to logical, physical and organisational security.

The ISO/IEC 27032 “Information technology - Security techniques - Guidelines for cybersecurity” is an international standard that provides indications for improving the state of IT security, tracing the unique aspects of this activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP).

The ISO/IEC 29100 “Information technology - Security techniques - Privacy framework”**:** covers a policy framework, privacy architecture, a privacy capability assessment model as well as a Code of Practice for protection of personally identifiable information (PII) in public clouds.

3.1.1.1 ISO/IEC 27001

In the current market scenario, characterised by the rapid growth of digital services that require effective protection measures from a cybersecurity and compliance perspective, the ISO 27001 standard represents the basic solution for protecting corporate information.

ISO/IEC 27001 is an International Standard developed for the purpose of providing the requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System, including aspects related to logical, physical and organisational security. This standard provides the requirements for adopting an adequate Information Security Management System (ISMS) in order to preserve of the confidentiality, integrity and availability of information by applying a risk management process and giving stakeholders confidence in the adequacy of risk management.

ISO/IEC 27001 is structured in 2 parts: a “High Part” that specifies the requirements for the Information Security Management System (ISMS) included in clauses from 4 to 10, and a “Low Part”, the Annex-A, in which are listed the Security Controls. The exclusion of any requirements specified in points 4 to 10 is not acceptable if an organisation wants to declare its compliance with this International Standard.

The setting of the ISO/IEC 27001 standard is based on the process approach, structured in different phases that include safety policy, risk identification, risk analysis, risk assessment and treatment, risk

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

review and reassessment, use of procedures and tools such as internal audits, non-conformities, corrective and preventive actions and surveillance, with a view to continuous improvement.

The standard defines the requirements of a management system following an approach based on risk management.

The main activities envisaged by the Standard in the design and implementation of the Management System are:

- the definition of the company context and the scope of certification;
- carrying out a preliminary training phase for the Project Team and defining the roles and responsibilities for the figures in charge of managing information security;
- carrying out a risk assessment investigation which, using adequate tools and methodologies, identifies the threats that have an impact on the security of corporate information and assesses the related risks;
- the definition of the control objectives and the identification of the security measures adopted in order to mitigate the identified risks;
- the formalisation of a risk treatment plan aimed at creating (if not already available) or improving the necessary documentary (e.g. internal policies and procedures), organisational (e.g. roles and responsibilities) and technological solutions;
- the preparation and provision of training for company personnel and any interested third parties;
- conducting audit sessions in order to verify the correct application of the security measures (technical and organisational) defined by the company.

System documentation is required as well as documentation on risk analysis and procedures and controls to support the ISMS. The compliance conditions include the planning and implementation of self-control activities managed by the company, with its own or external personnel, provided that in both cases they have the necessary skills.

Annex A, "Control objectives and controls", contains the controls that the organisation must comply with. They concern the policy for security, asset management, human resource security, physical and environmental security, communications and operational management, physical and logical access control and management of incident monitoring and handling (related to information security), business continuity management and regulatory compliance. The organisation must justify which of these controls are not applicable within its ISMS, for example if it does not fit the scope of the organisation.

The choice of ISO/IEC 27001 information security standard ensures greater security for the platform, through risk control and minimisation of threats, and resilience against cyber threats; this enables to maintain a high level of security of personal and financial data processed by the platform. ISO 27001 is a standard which needs to be maintained by the organisation by conducting risk assessments which enables management and key stakeholders to maintain information security risks.

3.1.1.2 ISO/IEC 27032

As part of the ISO/IEC 27000 family of standards, ISO 27032 outlines security techniques and provides guidelines for cyber security. This best-practice framework enables organisations to use ISO 27032 to implement tools and techniques and formulate an effective cyber security policy.

The ISO/IEC 27032 standard provides guidelines regarding the protection and long-term sustainability of business processes. In addition, it equips individuals with the ability to develop a policy framework which identifies the processes that are the most vulnerable to cyber-attacks. ISO/IEC 27032 Cybersecurity training provides a real-world solution to individuals for protecting their personal and organisation data from phishing scams, cyber-attacks, hacking, data breaches, spyware, espionage, sabotage and other cyber threats.

As written in the document, an effective way to confront Cybersecurity risks involves a combination of multiple strategies, taking into consideration the various stakeholders. These strategies include:

- Industry best practices, with collaboration of all stakeholders to identify and address Cybersecurity issues and risks.
- Broad consumer and employee education, providing a trusted resource for how to identify and address specific Cybersecurity risks within the organisation.
- Innovative technology solutions to help protect consumers from known Cybersecurity attacks, to stay up to date and be prepared for new exploitations.

The guideline digs into many areas of Cybersecurity, such as the nature of Cybersecurity, various threats, vulnerabilities, attack mechanisms, along with other essential information, and provides contribution regarding best practices for helping ensure the confidentiality, integrity, and availability of one’s critical system resources. It focuses on consumer and employee education to assist stakeholders in playing an active role to address the Cybersecurity challenges with guidance for: roles policies, methods, processes and applicable technical controls.

ISO/IEC 27032 Cybersecurity Management enables to:

- Protect the organisation’s data and privacy from cyber threats;
- Develop best practices to managing Cybersecurity policies;
- Build confidence to stakeholders for security measures;
- Strengthen skills in the establishment and maintenance of a Cybersecurity program;
- Improve the security system of organisations and their business continuity;
- Respond and recover faster in the event of an incident.

The main difference between ISO/IEC 27032 and ISO/IEC 27001 is in its respective scope. ISO/IEC 27032 derives from and supports ISO/IEC 27001, which is related to the Information Security, not regarding the nature of the asset to protect, while ISO/IEC 27032 considers only digital assets, naturally included into information security assets. Moreover, ISO/IEC 27032 focuses on information systems and includes guidelines to prevent information leakage, to encrypt communication channels and to make sure information will not be deciphered if accessed by “external” people.

The choice of ISO/IEC 27032 is therefore dictated by the need to ensure the cybersecurity of the platform and of the processed data as a complement and support to ISO/IEC 27001.

3.1.1.3 ISO/IEC 29100

ISO/IEC 29100 provides a high-level framework for the protection of personally identifiable information organisational, technical, and procedural aspects in an overall privacy framework. This standard, the drafting of which preceded the entry into force of GDPR, does not use the term "personal data", but "personally identifiable information (PII)".Also, it does not use the term "data subject" for interested parties, but "PII principal".

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

ISO/IEC 29100 provides a framework that intends to help define organisations privacy safeguarding requirements related to PII within an ICT environment. This privacy framework specifies a common privacy terminology, defines the actors and their roles in processing personally identifiable information , describes privacy safeguarding considerations and provides references to known privacy principles for information technology.

In some jurisdictions, this International Standard's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII.

This Standard can aid in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII, spur innovative solutions to enable the protection of PII within ICT systems and improve organisations' privacy programs through the use of best practices.

The privacy framework provided within this International Standard can serve as a basis for additional privacy standardisation initiatives, such as for: a technical reference architecture, the implementation and use of specific privacy technologies and overall privacy management, privacy controls for outsourced data processes, privacy risk assessments and specific engineering specifications.

The last paragraph of this Standard presents the "privacy principles", divided into 11 sections, and they are applicable to natural persons and organisations involved in all transactions involving information and communication technology systems or services where privacy controls are required for the processing of personal data:

1. consent and choice;
2. legitimacy and specification of the purposes;
3. limitation of collection;
4. data minimisation;
5. use, storage and communication limits
6. accuracy and quality;
7. openness, transparency and disclosure;
8. participation and access by individuals;
9. responsibility;
10. safety;
11. compliance.

Due to the increasing number of information and communication technologies that process PII, it is important to have international information security standards that provide a common understanding for the protection of PII. This International Standard is intended to enhance existing security standards by adding a focus relevant to the processing of PII.

The choice of ISO/IEC 29100 is dictated by the fact that it is a standard international privacy framework that can be used as a support tool for a correct upholding of the GDPR and it is a reference document that can be used by privacy engineers (rather than a legal document).

3.1.2 OASIS

The Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit international standards organisation that works on the development, convergence, and adoption of open standards for cybersecurity, Blockchain, Internet of Things (IoT), cloud computing, and other areas. In the following, two OASIS standards relevant to the Critical-Chains project are presented.

3.1.2.1 SAML

The Security Assertion Markup Language (SAML) is a standard developed by the Security Services Technical Committee of OASIS (OASIS Security Services TC, 2008). The standard defines an XML-based framework for describing and exchanging authentication and authorisation information between an identity provider and a service provider. The current version SAML v2.0 defines three types of statements in the form of SAML assertions to carry out authentication and authorisation information: authentication, attribute, and authorisation assertions. The SAML assertions are carried out in a set of XML-based protocol messages that are specified in SAML v2.0. SAML v2.0 specification also provides a set of protocol message bindings and a set of profiles utilising SAML assertions, protocol messages, and their bindings.

3.1.2.2 XACML

The Extensible Access Control Markup Language (XACML) is the de facto standard for attribute-based access control systems (that are known also as policy-based access control systems). The standard is developed by the OASIS XACML Technical Committee (Lockhart & Parducci, 2020).

XACML is implemented in XML to provide a standardised way for expressing and enforcing access control policies. Even though XML makes the specification of policy complex and verbose, it provides powerful flexibility and expressiveness of access policies.

An XACML request is a collection of attribute name, value pairs for the subject (user), action (operation), resource, and environment attributes. The environmental attributes are subject and resource independent, and may include the current time, day of the week, or threat level.

3.1.3 NIST

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce. Two NIST standards relevant to the activities carried out in the Critical-Chains project are presented in the following sub-sections.

3.1.3.1 Random number generators

Cyber-physical security is indispensable in any smart system where the generated and flowing data should be encrypted. This is a very natural need of any cyber-physical system where cryptographic operations, e.g. encryption/decryption, hashing, key generation, and key management take place.

One of the basic principles of cryptography is the Kerckhoff's hypothesis (Martin, 2017). According to this hypothesis, the overall security of any cryptosystem is completely dependent on the security of the key, and that all other parameters of the crypto system are publicly observable. Thus, the cryptographic algorithms are assumed as open as long as the key generation scheme is not secure. In real life, many systems actually use well-known symmetric and asymmetric cryptographic algorithms (AES, 3DES, RSA, ECDSA, SHA) which have been applied in many dimensions and all experts are aware of their strengths and weaknesses. As a matter of fact, randomness criteria play a crucial role in cryptographic key generation.

There are two basic types of generators used to produce random sequences: true random number generators (TRNGs) and pseudorandom number generators (PRNGs) (Ergün & Özog, 2007). TRNGs generate random numbers from a physical process, rather than by means of an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect involving a beam splitter, and other quantum phenomena. The presence of unpredictability in these phenomena can be justified either by the theory

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

of unstable dynamical systems and chaos theory (Ergün, et al., 2011) or by the non-deterministic nature of quantum mechanics. While TRNGs take the advantage of non-deterministic entropy sources, PRNGs generate bits in a deterministic manner. The PRNG-generated sequence is not truly random, because it is completely determined by an initial value, called the PRNG's seed (which may include truly random values). PRNGs tend to benefit from the external source of randomness (e.g., mouse movements, delay between keyboard presses etc.) which are practical in use but still predictable.

Vulnerability analysis of a cryptosystem is to check whether the system relies on a hardware-based RNG or not. Then, this RNG should be TRNG. To meet the true randomness criteria, three test suites are applied on a sufficient length of bit sequences, which have been accepted as de-facto standard randomness test:

- NIST-800-22 Randomness Test Suite (NIST 800-22, 2010)
- DieHard Test Suite (Marsaglia, s.d.)
- Big Crush Test Suite (L'Ecuyer & Simard, 2007)

Among these three tests, NIST-800-22 randomness test suite is the widely accepted and practical standard, as addressed by the well-known FIPS-140-2[1] and FIPS-140-3[2] published by NIST. As standardised by NIST, the security requirements for cryptographic modules emphasise the use of TRNGs in cryptographic modules, as addressed in HwSaaS and CryptaaS in Critical-Chains. The typical outputs of the proposed TRNG (See D5.5 for details) must pass all 15 criteria of NIST-800-22 Randomness Test Suite which are listed below:

1. The Frequency (Monobit) Test: The purpose of the test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence.
2. Frequency Test within a Block: The purpose of the test is to determine whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness.
3. The Runs Test: The purpose of the test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow.
4. Tests for the Longest-Run-of-Ones in a Block: The purpose of the test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence.
5. The Binary Matrix Rank Test: The purpose of the test is to check for linear dependence among fixed length substrings of the original sequence. Note that this test also appears in the DIEHARD battery of tests.
6. The Discrete Fourier Transform (Spectral) Test: The purpose of the test is to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness.
7. The Non-overlapping Template Matching Test: The purpose of the test is to detect generators that produce too many occurrences of a given non-periodic (aperiodic) pattern.
8. The Overlapping Template Matching Test: The focus of the Overlapping Template Matching test is the number of occurrences of pre-specified target strings.

[1] https://csrc.nist.gov/publications/detail/fips/140/2/archive/2001-10-10
[2] https://csrc.nist.gov/publications/detail/fips/140/3/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

9. Maurer's "Universal Statistical" Test. The purpose of the test is to detect whether or not the sequence can be significantly compressed without loss of information
10. The Linear Complexity Test: The focus of this test is the length of a linear feedback shift register (LFSR). The purpose of this test is to determine whether or not the sequence is complex enough to be considered random.
11. The Serial Test: The purpose of the test is to determine whether the number of occurrences of the 2^m m-bit overlapping patterns is approximately the same as would be expected for a random sequence.
12. The Approximate Entropy Test: The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m+1) against the expected result for a random sequence.
13. The Cumulative Sums (Cusums) Test: The purpose of the test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behaviour of that cumulative sum for random sequences.
14. The Random Excursions Test: The purpose of this test is to determine if the number of visits to a particular state within a cycle deviates from what one would expect for a random sequence.
15. The Random Excursions Variant Test: The purpose of this test is to detect deviations from the expected number of visits to various states in the random walk.

3.1.3.2 Attribute Based Access Control (ABAC)

The attribute-based access control (ABAC), as described in NIST SP 800-162 (NIST, 2014), is a logical access control methodology where access to objects is controlled by evaluating rules against the attributes of (a) the subject or user requesting access, (b) the target object for which access or a transaction is being requested, and (c) the environment relevant to a request. ABAC is built on these basic core capabilities that evaluate attributes and environment conditions, and enforce rules or relationships between those attributes and environment conditions. To implement ABAC, one of the standards used to develop common terminology and interoperability across access control systems is the OASIS’s XACML standard.

3.1.4 OpenID Foundation

The OpenID Foundation (OIDF) is a non-profit international standards development organisation that promotes and enhances the OpenID community and technologies by providing needed infrastructure and help in promoting and supporting adoption of OpenID.

3.1.4.1 OpenID Connect

OpenID Connect is a standard controlled by the OpenID foundation (OpenID, s.d.). This standard describes a suite of lightweight specifications of an identity layer built on top of the OAuth 2.0 authorisation framework standardised by IETF. OpenID Connect provides a framework for identity interactions via REST like APIs. It enables clients to verify the identity of a user based on the authentication performed by an authorisation server, as well as to obtain basic profile information about the user. Information about the performed authentication is returned in a JSON Web Token (JWT), called an ID Token. OpenID Connect specification defines also different authorisation flows that dictate what response types an authorisation request can request and how tokens are returned.

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

3.1.5 IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organisation for electronic engineering and electrical engineering. An IEEE standard on tamper proofing is presented in the following subsection.

3.1.5.1 Tamper Proofing

For tamper proofing on authentication between two wireless nodes is usually done by measuring the distance between the two nodes. Most of the current solutions are vulnerable to the so-called man in the middle attack. To prevent this you need a form of Secure Distance Bounding. Imec is doing research and development on high accuracy phase-based ranging for narrowband transceivers such as BLE or 802.15.4.

- The Bluetooth LE 5.1 standard does not have any form of protection against the man in the middle attack. Imec is actively participating with the BT SIG.
- IEEE 802.15.4z – The UWB standard aims to enable the next generation secure keyless access for vehicles (solving relay attack problem), secure corporate and home buildings augmented access, secure proximity-based mobile payments, etc. Security must rely on secure distance measurements.

3.2 Standards/regulation in fintech & Insurtech

The nature of the relationship between technological innovation and financial intermediation is the subject of in-depth study - from different perspectives - in numerous public and private international forums, with regard to the impact that technological transformation is having on the financial system on an international scale. The rapid developments in the Fintech and, particularly, the Insurtech industry, do not only affect the operations of the insurance industry, but are also highly disruptive to the operation of the competent regulatory authorities. New Fintech applications of a broad range and with very different nature, meanings and functions, new methods and channels of product distribution, new forms of cooperation between industry players, and even the entry of non-financial institutions in the financial markets, all in a global digitalised environment create added complexities to the regulators when exercising their supervisory competences and powers. Furthermore, for the market supervision to be effective, the regulator must have access to all the necessary and appropriate information concerning its operation and its participants. In the insurance sector and under the applicable Solvency II regime, insurance regulators mainly draw such information from the reports disclosed by the insurance undertakings, which, however, were not designed with a view to cover the Fintech revolution. As such, regulators need to find alternative means and methods, to obtain appropriate and sufficient information concerning the interplay between Fintech applications and its operation in the insurance market, thereby enhancing their so-called “Regtech” capabilities.

It is a major challenge everywhere to design an adequate policy framework for Fintech. Authorities need to help bring the potential benefits of technological developments to fruition, for the good of the economy and financial system. Fintech promises to increase efficiency in delivering financial services, widen their range, increase competition and promote financial inclusion. On the other hand, policymakers must address a set of risks that could merit public intervention. In particular, increasing reliance on technology and unregulated third-party providers throws operational risks into sharper relief; new payment systems and instruments could compromise market integrity and, ultimately, the monetary system; new products may be mis-sold to consumers who do not understand their risks or

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

cannot afford to bear them; and the business opportunities created by new technologies may erode privacy and encourage unethical conduct.

To varying degrees, regulators are striving to deal with all those challenges across a number of jurisdictions. But it remains to be seen whether these policy actions will be enough to safeguard an orderly modernisation of the financial industry, let alone address the ongoing risks that technology poses to the achievement of key social objectives.

According to BIS report “Regulating fintech: what is going on, and where are the challenges?”, Fintech-related policy measures can be usefully classified into three groups: (i) those that directly regulate Fintech activities; (ii) those focused on the use of new technologies in the provision of financial services; and (iii) those that promote digital financial services more specifically. The first group of measures relates to the regulation of specific activities such as digital banking, peer-to-peer (P2P) lending or equity raising, robo-advice and payment services. The second group includes new rules or guidelines on market participants’ use of technologies such as cloud computing, biometrics or artificial intelligence. The third group covers enabling policy initiatives such as those related to digital identities, data-sharing and the establishment of innovation hubs, sandboxes or accelerators. Over the last few years, most jurisdictions have applied policy measures in some or all of these three areas.

In general, technological developments have not yet resulted in any major upheaval in the structure of financial regulation. In their core content, the rulebooks on prudential safeguards, consumer protection and market integrity remain broadly unaffected.

The European Commission has taken numerous steps to fully comprehend and evaluate the Fintech phenomenon and its implications for the financial services sector. In its relevant Communication describing an EU Fintech Action Plan, the Commission views Fintech as a domain where the themes of financial services and digital single market meet. According to the Commission, Fintech applications have the ability to provide better access to finance and improve financial inclusion, assist in the deepening and broadening of the EU capital markets, facilitate the achievement of compliance obligations for regulated entities, but at the same time create new challenges both to such regulated entities, and to regulatory authorities, and the markets at large as well. One of the primary issues examined by the Commission in its Fintech Action Plan is the issue of the licensing requirements that may apply to Fintech providers and applications under the EU or respective national sector specific laws, which aim to enable effective supervision, consumer protection, and uniform operating conditions. Considering the fact that national regulators do not always adopt uniform approaches on the implementation of these requirements, and that new financial services may not always fall into the scope of the applicable EU law provisions, the Commission invited the ESAs to map the current authorising and licensing approaches for innovative Fintech business models, and issue, where appropriate, guidelines on such approaches and procedures. In particular for licenses, a banking license is still required for any activity entailing a substantial risk transformation of funds raised from the public. Moreover, little has been done to develop specific licensing requirements for digital banks.

The Commission’s Action Plan refers to other issues to be further addressed for Fintech solutions to be able to enhance the quality of the financial products and services provided in the EU Single Market, and for any potential risks, such as cyber related risks, data, consumer and investor protection, and market integrity issues to be effectively tackled. Such points include, among others, the development of common EU standards for Fintech solutions, the need to enhance interoperability, removing obstacles to the use of cloud computing services by means of EU guidelines, cross-sectoral self-regulatory codes of conduct or standard contractual clauses, strengthening the cyber resilience of the financial sector, etc. Standard setting processes should be based on the principles of openness, transparency and consensus, in accordance with Regulation (EU) No 1025/2012 on European standardisation. For standards to be pro-competitive, participation should be unrestricted and the procedure for adopting the standard should be transparent, enableing stakeholders to effectively inform themselves of standardisation work. Effective access to the standard should be provided on fair, reasonable and non-discriminatory terms.

As emphasised, the importance of broad industrial and institutional stakeholders' contribution to the ongoing activities cannot be underestimated. An open and consensus-driven approach to standards creation will be essential. In light of this, the most efficient and effective way to galvanise and secure the support of the right participants to ensure the relevance and success of any standards initiatives that ensue could be to convene a Fintech standards community via which to spearhead the ongoing investigation and standards creation work.

3.2.1 FIDO Authentication

FIDO (Fast IDentity Online) authentication is a set of standards for fast, simple, strong authentication which has been developed by the FIDO Alliance[3], an industry association with representatives from a range of organisations including Google, Microsoft, Mozilla, and Yubico. The proposed standards aim to enable phishing-resistant, passwordless (if possible), and multi-factor authentication. The main motivation of this standard is to ease the authentication process for end users and not to make them bored with the long and impractical authentication procedures. The alliance has improved online user interfaces by making strong authentication easier to implement and use, such as WebAuthn and FIDO2 for Android. The applications over web browsers involve passing a cryptographic challenge from the server to the authenticator, and returning the authenticator's response to the server for validation. The server stores the user's public key credentials and account information. During an authentication or registration flow, the server generates a cryptographic challenge in response to a request from the application. It then evaluates the response to the challenge.

The FIDO Alliance maintains a list of certified third-party products, including server solutions. Some of the web's most popular tools and apps are already using FIDO authentication, including Google Accounts, Dropbox, GitHub, Twitter, and Yahoo Japan.

The FIDO protocol authenticates a user to a server, using a token (e.g. smartcard, USB token, etc.), in a way that the user is not impersonated without being in possession of her/his token, even if the username and the password of that user have been compromised. The protocol runs between a user, a Token (SecureStick in Critical-Chains), a FIDO Client embedded in the user's web browser (e.g. Critical-Chains main web interface), and a server (on which Critical-Chains XaaS components are orchestrated), after the establishment of a secure TLS between the last two entities.

FIDO specifications define ubiquitous, technology-agnostic security standards aimed primarily at mobile authentication. FIDO2 is delivered as an extension to FIDO to improve the efficiency of authentication processes in browsers and desktop applications as well. As depicted in Figure 1, the specifications under FIDO2 support existing passwordless FIDO UAF (Universal Authentication Framework (Balfanz, et al., 2013)) and FIDO U2F (Universal 2nd Factor authentication (Balfanz, 2015)) use cases and expand the availability of FIDO Authentication. Users that already have external FIDO-

[3] https://fidoalliance.org/

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

compliant devices, such as FIDO security keys, will be able to continue to use these devices with web applications that support WebAuthn. Existing FIDO UAF devices can still be used with pre-existing services as well as new service offerings based on the FIDO UAF protocols.

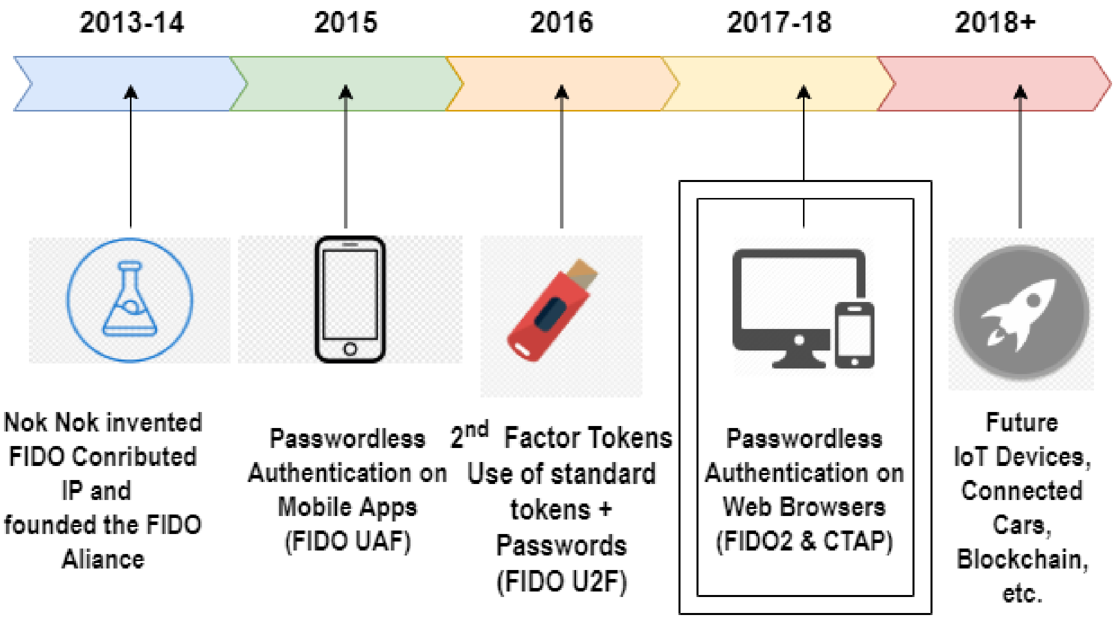
2013-14
2015
2016
2017-18
2018+
Nok Nok invented FIDO Conributed IP and founded the FIDO Aliance
Passwordless Authentication on Mobile Apps (FIDO UAF)
2nd Factor Tokens Use of standard tokens + Passwords (FIDO U2F)
Passwordless Authentication on Web Browsers (FIDO2 & CTAP)
Future IoT Devices, Connected Cars, Blockchain, etc.

Figure 1. FIDO history

FIDO Alliance has proven the FIDO's impact on mobile devices, and FIDO2's impact on browsers and desktops. Additionally, as the use of biometric authentication is becoming widespread, especially in Fintech industry, the Alliance decided to play a significant role in bolstering the overall value proposition of biometrics (Dunkelberger, 2018). The FIDO standard paves the way for seamless integration of multiple authentication methods, where fingerprinting can be combined with other modes like facial recognition and behavioural biometrics in a frictionless experience.

FIDO Alliance encourages the sector to meet the requirements of IoT-enabled cyber-physical systems and Blockchain. Critical-Chains Consortium is also aware of this trend as the project goals are aligned with the use of Blockchain and cyber-physical security. The authentication solutions proposed and implemented in Critical-Chains aims to improve the FIDO and FIDO2 by integrating SecureStick, facial biometric authentication (AUTHaaS) and the use of hardware-based reliable cryptographic components (HwSaaS) in Blockchain-enabled financial transactions.

3.3 Emerging standards

This section reviews existing standards and regulations on emerging technologies, for instance on the Blockchain and distributed ledgers.

3.3.1 Blockchain and Distributed Ledger Standards

Cryptocurrencies all-time highs and following adoption announcements from large players including PayPal and Square. Governments, as Bermuda and China, are rolling out digital currencies. Industries from mobility to mining are collaborating in unprecedented ways to explore and implement Blockchain technology. These are positive signs for a technology that was riddled with hype and, in some cases, fraudulent behaviours. However, something can obstruct the progress of technology: standards.

With emerging technologies, coalescence around technical and regulatory standards has marked a turning point. They provide a baseline for interoperable systems and for businesses to operate smoothly in a cross-jurisdiction manner. For users of the technology, these standards are often the baseline for consumer protection and setting performance expectations.

Standards are generally created and adopted in one of three ways (adapted from the Handbook of Innovation and Standards[4]):

- By convention (de facto standard): a practice, behaviour or configuration becomes broadly accepted through repetition and use.
- By fiat (de jure standard): imposed by an edict or regulation by a government or other institution.
- By negotiation: as agreed formally among stakeholders in an activity or enterprise.

In some ways, Blockchain upends traditional models of standard-setting, given the decentralised governance and ability to embed standards within the build of the protocol. Other areas have mimicked structures used to create coherence in distributed systems such as the internet.

Familiar standard-setting entities, such as the Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE) and International Organization for Standardization (ISO), continue to develop voluntary information technology standards. Some, such as ISO and IEEE, among others, have formed dedicated working groups on Blockchain and distributed ledger technologies, but their focus areas and outputs are early-stage.

With respect to emerging (recently published or upcoming) Blockchain and DLT standards produced by the ISO/TC 307 working group, the contents of the following ISO documents are known (be they in published or unpublished form):

- *ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary* - a published document that defines the basic terms relating to Blockchain and distributed ledger technologies. The meanings of terms and concepts are clarified in support of the additional texts produced by the working group (in the domain of ISO/TC 307 standards). It further supports the understanding of other Blockchain and DLT related source information. Its goal is to promote improved communication and understanding of this emerging area.
- *ISO/TR 23244:2020 - Blockchain and distributed ledger technologies: Privacy and personally identifiable information protection considerations* - a published document that provides an overview of the issues and practical concerns related to privacy and personally identifiable information (PII) protection; the information contextually relates to Blockchain, DLT systems and their applications. Privacy and PII protection issues are "...considered major barriers to the adoption of DLT-based solutions." This document "...identifies and assesses known privacy-related risks and the way to mitigate them, as well as the privacy-enhancing potential of Blockchain and distributed ledger technology."
- *ISO/TR 23455:2019 - Blockchain and distributed ledger technologies: Overview of and interactions between smart contracts in Blockchain and distributed ledger technology systems* - a published document that provides an overview of smart contracts in Blockchain and DLT systems. It deals with the nature of smart contracts in detail, including their history, underlying

[4] Hawkins, Richard & Blind, Knut & Page, Robert. (2017). Handbook of Innovation and Standards.

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

concepts, benefits, typical operations, on- and off-chain interactions, life-cycle, legal status and applications; however, there is less emphasis in the text on the legally binding use of, and applications for, smart contracts.

- *ISO/DIS 23257 - Blockchain and distributed ledger technologies: Reference architecture* - a currently unpublished document that presents a reference architecture for DLT-based business solutions. It contains information on the following subject areas: relevant definitions and concepts (including system organisation, nature of access, type of consensus, and the roles and responsibilities of participants); business use-cases (provided as high-level information for several business domains); and reference DLT system architecture (detailing its various tiers/layers and their functional components). The document clarifies the potential role for Blockchain and DLT systems as "...a broader solution to public reporting and auditing...".
- *ISO/DTS 23258 - Blockchain and distributed ledger technologies: Taxonomy and Ontology* - a currently unpublished document that provides taxonomic and ontological support for the additional texts produced by the working group (in the domain of ISO/TC 307 standards). In relation to Blockchain and DLT systems, it presents a taxonomy of relevant concepts and terms, DLT systems, application domains, use-case purposes and economic activity. Furthermore, its resulting ontology covers the analytical classes and attributes of Blockchain and DLT systems, as well as the relationships between their concepts.
- *ISO/DTS 23635 - Blockchain and distributed ledger technologies: Guidelines for governance* - a currently unpublished document that provides "clarity and guidance for organisations, industry and governments on how governance can be implemented and executed in Blockchain and distributed ledger systems in general." The document highlights several emerging governance questions regarding ownership, decision rights, accountabilities, and incentive structures that cannot be addressed by applying traditional governance mechanisms to Blockchain and DLT systems. It expresses the potential for smart contracts to provide decentralised governance mechanisms, and it aims to the future standardisation of DLT systems to improve issues of accountability in distributed ledger environments.

For completion, the document *ISO/DTR 23245 - Blockchain and distributed ledger technologies: security risks, threats and vulnerabilities* will no longer be published in its current form; the text addresses the known security vulnerabilities of Blockchain and DLT solutions. It details the associated risks and potential impacts of these security vulnerabilities, provides related examples of mitigations, describes the current state-of-security of Blockchain and DLT technology, and includes content to inform the future standardisation of Blockchain and DLT technology. Despite this document's official cancellation, the important points it addresses (and others relating to Blockchain and DLT system security) are likely to be included in future work, which attempts to address these underlying security issues.

The exact nature of the following, un-finalised documents is unclear. However, information on their progress towards publication is provided:

- *ISO/TR 23576 - Blockchain and distributed ledger technologies: Security management of digital asset custodians* (currently under publication).
- *ISO/CD TR 3242 - Blockchain and distributed ledger technologies: Use cases* (at committee).
- *ISO/WD TR 23249 - Blockchain and distributed ledger technologies: Overview of existing DLT systems for identity management* (in preparatory stages).

- *ISO/AWI TS 23259 - Blockchain and distributed ledger technologies: Legally binding smart contracts* (in preparatory stages).
- *ISO/AWI TR 23642 - Blockchain and distributed ledger technologies: Overview of smart contract security good practice and issues* (in preparatory stages).
- *ISO/WD TR 23644 - Blockchain and distributed ledger technologies: Overview of trust anchors for DLT-based identity management (TADIM*; in preparatory stages).
- *ISO/WD TR 24332 - Information and documentation: Application of Blockchain technology to records management — Issues and considerations* (in preparatory stages).
- *ISO/AWI TR 6039 - Blockchain and distributed ledger technologies: Identifiers of subjects and objects for the design of Blockchain systems* (proposal is approved).
- *ISO/AWI TR 6277 - Blockchain and distributed ledger technologies: Data flow model for Blockchain and DLT use cases* (proposal is approved).

3.3.1.1 Application Layer

Digital signing and smart contracts are two aspects of the application layer to which the process of standardisation is particularly important. The new and emerging standardisation of each of these aspects is covered in this section.

ISO documents that relate to digital signing include:

- *ISO/DIS 23257 - Blockchain and distributed ledger technologies: Reference architecture* - the document mentions digital signatures as an element of the cryptographic services operating in the DLT Platform layer. The DLT Platform layer contains the core functions of the DLT systems running in a DLT node. Furthermore, such functions may be responsible for establishing and maintaining communication between nodes, i.e. the DLT Platform layer connects hardware or network infrastructure to relevant functional support services in the API layer. As a capability of the DLT Platform layer, cryptographic services include digital signatures to ensure security compliance and tampering resistance for DLT systems. More specifically, digital signatures ensure that a receiver receives a transaction without intermediate parties modifying or forging the contents of the transaction, while also ensuring that the transaction originates from senders with access to the private keys.
- *ISO/DTR 23245 - Blockchain and distributed ledger technologies: security risks, threats and vulnerabilities* - the document outlines general security considerations, including the appropriate choice of cryptographic algorithms and protocols. As Blockchain and DLT technologies are based on several cryptographic algorithms and protocols (such as the use of digital signatures and hash functions) it advises to provide sufficient compromise/vulnerability resistance; algorithms and protocols present significant security risks where (1) mistakes in their design offer exploitable vulnerabilities to attackers and/or (2) when computational power grows beyond the capabilities of the original design (as with future developments in quantum computing, for example).
- *ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary* - the meaning of the term digital signature is provided and its relation to Blockchain and distributed ledger technologies is clarified.
- *ISO/TR 23244:2020 - Blockchain and distributed ledger technologies: Privacy and personally identifiable information protection considerations* - types of digital signature are detailed as privacy enhancing technologies applicable to Blockchain and DLT systems; they are listed as standard cryptographic techniques in this field.

ISO documents that relate to smart contracts include:

- *ISO/TR 23455:2019 - Blockchain and distributed ledger technologies: Overview of and interactions between smart contracts in Blockchain and distributed ledger technology systems* - the document deals with the nature of smart contracts in detail, including their history, underlying concepts, benefits, typical operations, on- and off-chain interactions, life-cycle, legal status and applications. However, the document lays less emphasis on the legally binding use of, and applications for, smart contracts.
- *ISO/DIS 23257 - Blockchain and distributed ledger technologies: Reference architecture* - this document offers supplementary information regarding smart contracts in the context of DLT system architecture. These architectural considerations include the determinism of smart contract logic, programming options, selecting the location and timing of execution, use of dedicated or arbitrary peers, and more.
- *ISO/DTR 23245 - Blockchain and distributed ledger technologies: security risks, threats and vulnerabilities* - descriptions of state management vulnerabilities that can affect smart contract use (bugs, for example) are included.
- *ISO/DTS 23258 - Blockchain and distributed ledger technologies: Taxonomy and Ontolog*y - the document provides an overview of the smart contract concept, including its definition, availability, usability, location (smart contracts may exist on system nodes) and typical outcomes. It supports the definitions in ISO 22739 and elsewhere.
- *ISO/DTS 23635 - Blockchain and distributed ledger technologies: Guidelines for governance* - expresses the potential for smart contracts as a decentralised governance mechanism in Blockchain and DLT systems. In addition to providing 'off-chain' instruments of governance, it suggests that "Accountability in principle will increasingly be enacted technically instead of institutionally through written contracts. Smart contracts enable for specifying and enforcing accountability using codified rules on-chain." The document presents the main issues of accountability that the current implementations of smart contracts in Blockchain and DLT systems are facing.
- *ISO/TR 23455:2019 - Blockchain and distributed ledger technologies: Overview of and interactions between smart contracts in Blockchain and distributed ledger technology systems* - an extended description of the implementation, execution process and life cycle of a smart contract is provided.
- *ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary* - the meaning of the term smart contract is provided and its relation to Blockchain and distributed ledger technologies is clarified.
- *ISO/AWI TS 23259 - Blockchain and distributed ledger technologies: Legally binding smart contracts* - this document is in its preparatory stages, and the exact nature of its content is unclear.
- *ISO/AWI TR 23642 - Blockchain and distributed ledger technologies: Overview of smart contract security good practice and issues* - this document is in its preparatory stages, and the exact nature of its content is unclear.

3.3.1.2 Blockchain Layer

The Blockchain layer lays the foundational structure of the Blockchain. It determines the computing language the Blockchain will be coded in and any computational rules that will be used on the Blockchain.

Main principles and common definitions of the Blockchain layer are covered in this section:

- Permission: Blockchain networks can be categorised based on their permission model, which determines who can maintain them (e.g., publish blocks). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned. In simple terms, a permissioned Blockchain network is like a corporate intranet that is controlled, while a permissionless Blockchain network is like the public internet, where anyone can participate. Permissioned Blockchain networks are often deployed for a group of organisations and individuals, typically referred to as a Consortium.
    - Permissionless: Permissionless Blockchain networks are decentralised ledger platforms open to anyone publishing blocks, without needing permission from any authority. Permissionless Blockchain platforms are often open-source software, freely available to anyone who wishes to download them. Since anyone has the right to publish blocks, this results in the property that anyone can read the Blockchain as well as issue transactions on the Blockchain (through including those transactions within published blocks). Any Blockchain network user within a permissionless Blockchain network can read and write to the ledger. Since permissionless Blockchain networks are open to all to participants, malicious users may attempt to publish blocks in a way that subverts the system. To prevent this, permissionless Blockchain networks often utilise a multiparty agreement or 'consensus' system that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system. Examples of such consensus models include proof of work and proof of stake methods. The consensus systems in permissionless Blockchain networks usually promote non-malicious behaviour through rewarding the publishers of protocol-conforming blocks with a native cryptocurrency.
    - Permissioned: Permissioned Blockchain networks are those where users publishing blocks must be authorised by some authority (be it centralised or decentralised). Since only authorised users are maintaining the Blockchain, it is possible to restrict read access and to restrict who can issue transactions. Permissioned Blockchain networks may thus enable anyone to read the Blockchain or they may restrict read access to authorised individuals. They also may enable anyone to submit transactions to be included in the Blockchain or, again, they may restrict this access only to authorised individuals. Permissioned Blockchain networks may be instantiated and maintained using open source or closed source software. Permissioned Blockchain networks may also be used by organisations that need to control and protect their Blockchain more tightly. However, if a single entity controls who can publish blocks, the users of the Blockchain will need to have trust in that entity. Permissioned Blockchain networks may also be used by organisations that wish to work together but may not fully trust one another. They can establish a permissioned Blockchain network and invite business partners to record their transactions on a shared distributed ledger.
- Hash function: An important component of Blockchain technology is the use of cryptographic hash functions for many operations. Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data, and derive the same result proving that there

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

was no change in the data. Even the smallest change to the input (e.g., changing a single bit) will result in a completely different output digest.

- Blocks: Blockchain network users submit candidate transactions to the Blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the Blockchain network. The chosen nodes may be non-publishing full nodes as well as publishing nodes. The submitted transactions are then propagated to the other nodes in the network, but this by itself does not place the transaction in the Blockchain. For many Blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the Blockchain by a publishing node.
- Smart Contracts: The term smart contract dates to 1994, defined by Nick Szabo as "a computerised transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries." Smart contracts extend and leverage Blockchain technology. A smart contract is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the Blockchain network, e.g. Ethereum's smart contracts, Hyperledger Fabric's chaincode. The smart contract is executed by nodes within the Blockchain network. All nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the Blockchain. The smart contract code can represent a multi-party transaction, typically in the context of a business process. In a multi-party scenario, the benefit is that this can provide attestable data and transparency that can foster trust, provide insight that can enable better business decisions, reduce costs from reconciliation that exists in traditional business to business applications, and reduce the time to complete a transaction. Smart contracts must be deterministic, in that given an input they will always produce the same output based on that input. Additionally, all the nodes executing the smart contract must agree on the new state that is obtained after the execution. To achieve this, smart contracts cannot operate on data outside of what is directly passed into it, e.g. smart contracts cannot obtain web services data from within the smart contract – it would need to be passed in as a parameter. Any smart contract which uses data from outside the context of its own system is said to use an 'Oracle'. For many Blockchain implementations, the publishing nodes execute the smart contract code simultaneously when publishing new blocks. There are some Blockchain implementations in which there are publishing nodes which do not execute smart contract code, but instead validate the results of the nodes that do. For smart contract enabled permissionless Blockchain networks (such as Ethereum) the user issuing a transaction to a smart contract will have to pay for the cost of the code execution. There is a limit on how much execution time can be consumed by a call to a smart contract, based on the complexity of the code. If this limit is exceeded, execution stops, and the transaction is discarded. This mechanism not only rewards the publishers for executing the smart contract code, but also prevents malicious users from deploying and then accessing smart contracts that will perform a denial of service on the publishing nodes by consuming all resources, e.g. by using infinite loops. For smart contract enabled permissioned Blockchain networks, such as those utilising Hyperledger Fabric's chaincode, there may not be a requirement for users to pay for smart contract code execution. These networks are designed around having known participants, and other methods of preventing bad behaviour can be employed, e.g. revoking access.

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 Ethereum network, that will be considered the main network of the project in the first phase of the pilots, relies on standards provided by the Ethereum community in the Ethereum Improvement Proposals (EIPs), a description of standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards. Active standards in this space are related to Ethereum Request for Comment (ERC) tokens, where, many of the widely recognised applications of Blockchain are enabled by ERC token standards, which define the motivation, specification and implementation for Ethereum-based tokens. Notable examples include:

- ERC-20: The following standard allows for the implementation of a standard API for tokens within smart contracts. This standard provides basic functionality to transfer tokens, as well as allowing tokens to be approved so they can be spent by another on-chain third party.
- ERC-721: The following standard enables for the implementation of a standard application programming interface (API) for non-fungible tokens (NFT) within smart contracts. This standard provides basic functionality to track and transfer NFTs.
- ERC-1155 Multi Token Standard: A standard interface for contracts that manage multiple token types. A single deployed contract may include any combination of fungible tokens, non-fungible tokens or other configurations (e.g. semi-fungible tokens).
- ERC777 Token Standard: This standard defines a new way to interact with a token contract while remaining backward compatible with ERC-20. It defines advanced features to interact with tokens. Namely, operators to send tokens on behalf of another address—contract or regular account—and send/receive hooks to offer token holders more control over their tokens.

3.3.1.3 P2P Network -Blockchain Layer

The networking layer is where the rules set up on the protocol layer are actually implemented. At this level, we can find the following principles and common definitions:

- Transactions: A transaction represents an interaction between parties. With cryptocurrencies, for example, a transaction represents a transfer of the cryptocurrency between Blockchain network users. For business-to-business scenarios, a transaction could be a way of recording activities occurring on digital or physical assets. The data which comprises a transaction can be different for every Blockchain implementation, however the mechanism for transacting is largely the same. A Blockchain network user sends information to the Blockchain network. The information sent may include the sender's address (or another relevant identifier), the sender's public key, a digital signature, transaction inputs and transaction outputs.
- Asymmetric-Key Cryptography: Asymmetric-key cryptography enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public. To do this, the transactions are 'digitally signed'. This means that a private key is used to encrypt a transaction such that anyone with the public key can decrypt it. Since the public key is freely available, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key. Alternately, one can encrypt data with a user's public key such that only users with access to the private key can decrypt it.
- Addresses: Some Blockchain networks make use of an address, which is a short, alphanumeric string of characters derived from the Blockchain network user's public key using a cryptographic hash function, along with some additional data, e.g. version number,

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

checksums. Most Blockchain implementations make use of addresses as the "to" and "from" endpoints in a transaction.

- Private-Key Storage: With some Blockchain networks (especially with permissionless Blockchain networks), users must manage and securely store their own private keys. Instead of recording them manually, they often use software to securely store them. This software is often referred to as a wallet. The wallet can store private keys, public keys, and associated addresses. It may also perform other functions, such as calculating the total number of digital assets a user may have.
- Ledger: A ledger is a collection of transactions. Throughout history, pen and paper ledgers have been used to keep track of the exchange of goods and services. In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralised trusted third party, i.e. the owner of the ledger on behalf of a community of users. These ledgers with centralised ownership can be implemented in a centralised or distributed fashion, i.e. just one server or a coordinating cluster of servers.
- Consensus Models: A key aspect of Blockchain technology is determining which user publishes the next block. This is solved through implementing one of many possible consensus models. For permissionless Blockchain networks there are generally many publishing nodes competing at the same time to publish the next block. They usually do this to win cryptocurrency and/or transaction fees. They are generally mutually distrusting users that may only know each other by their public addresses. Each publishing node is likely motivated by a desire for financial gain, not the well-being of the other publishing nodes or even the network itself. A key feature of Blockchain technology is that there is no need to have a trusted third party to provide the state of the system—every user within the system can verify the system's integrity. To add a new block to the Blockchain, all nodes must come to a common agreement over time; however, some temporary disagreement is permitted. For permissionless Blockchain networks, the consensus model must work even in the presence of possibly malicious users since these users might attempt to disrupt or take over the Blockchain. In some Blockchain networks, such as permissioned, there may exist some level of trust between publishing nodes. In this case, there may not be the need for a resource intensive (computation time, investment, etc.) consensus model to determine which participant adds the next block to the chain. Generally, as the level of trust increases, the need for resource usage as a measure of generating trust decreases. For some permissioned Blockchain implementations, the view of consensus extends beyond ensuring validity and authenticity of the blocks but encompasses the entire system of checks and validations from the proposal of a transaction to its final inclusion on a block.
  - PoW: In the proof of work (PoW) model, a user publishes the next block by being the first to solve a computationally intensive puzzle. The solution to this puzzle is the "proof" they have performed work. The puzzle is designed such that solving the puzzle is difficult but checking that a solution is valid is easy. This enables all other full nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected. A common puzzle method is to require that the hash digest of a block header be less than a target value. Publishing nodes make many small changes to their block header, e.g. changing the nonce, trying to find a hash digest that meets the requirement. For each attempt, the publishing node must compute the hash for the entire block header. Hashing the block header many times becomes a computationally intensive process. The target value may be modified over time to adjust the difficulty (up or down) to influence how often blocks are being published.

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

For example, Bitcoin, which uses the proof of work model, adjusts the puzzle difficulty every 2016 blocks to influence the block publication rate to be around once every ten minutes. The adjustment essentially either increases or decreases the number of leading zeros required. By increasing the number of leading zeros, it increases the difficulty of the puzzle, because any solution must be less than the difficulty level – meaning there are fewer possible solutions. By decreasing the number of leading zeros, it decreases the difficulty level, because there are more possible solutions. This adjustment is to maintain the computational difficulty of the puzzle, and therefore maintain the core security mechanism of the Bitcoin network. Available computing power increases over time, as does the number of publishing nodes, so the puzzle difficulty is generally increasing.

- PoS: The proof of stake (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it. Stake is often an amount of cryptocurrency that the Blockchain network user has invested into the system (through various means, such as by locking it via a special transaction type, or by sending it to a specific address, or holding it within special wallet software). Once staked, the cryptocurrency is generally no longer able to be spent. Proof of stake Blockchain networks use the amount of stake a user has as a determining factor for publishing new blocks. Thus, the likelihood of a Blockchain network user publishing a new block is tied to the ratio of their stake to the overall Blockchain network amount of staked cryptocurrency. With this consensus model, there is no need to perform resource intensive computations (involving time, electricity, and processing power) as found in proof of work. Since this consensus model utilises fewer resources, some Blockchain networks have decided to forego a block creation reward; these systems are designed so that all the cryptocurrency is already distributed among users rather than new cryptocurrency being generated at a constant pace. In such systems, the reward for block publication is then usually the earning of user provided transaction fees.

3.3.1.4 Cryptocurrencies

The IEEE is the main organisation centred on the production (or future production) of standards relating to cryptocurrencies; it has produced the following relevant standards (with many still in the approval stages of development):

- *IEEE 2140.1-2020 - IEEE Standard for General Requirements for Cryptocurrency Exchanges* (self-discipline and professional ethics of cryptocurrency exchange platforms, as well as relevance between them and to cryptocurrency wallets are covered in this standard);
- *IEEE 2140.5-2020 - IEEE Standard for a Custodian Framework of Cryptocurrency* (a framework of a custodian service for cryptocurrency and token assets is defined in this standard);
- *IEEE 2143.1-2020 - IEEE Standard for General Process of Cryptocurrency Payment* (see below for description);
- *IEEE P2143.2 - Standard for Cryptocurrency Payment Performance Metrics* (this document is in early stages of development);
- *IEEE P2143.3 - Standard for Risk Control Requirements for Cryptocurrency Payment* (this document is in early stages of development);

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

- *IEEE P2140.2 - Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges* (this document is in early stages of development);
- *IEEE P2140.3 - Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges* (this document is in early stages of development);
- *IEEE P2140.4 - Standard for Distributed/Decentralized Exchange Framework using DLT (Distributed Ledger Technology*; this document is in early stages of development).

IEEE 2143.1-2020 defines both sides of a digital currency payment: how a consumer can purchase goods or services using cryptocurrency, as well as how the business can receive fiat money in return. In defining this process, *IEEE 2143.1-2020* is intended to ensure that digital currency payments are convenient for users while keeping the system fair and secure for both parties in a transaction. The standard is intended to enable consumers to easily filter and identify companies they want to work with by delivering a globally recognised set of criteria for addressing common concerns about instability and uncertainty in digital currency, and, ultimately, for fostering trust in the practice. In turn, the standard aims to serve as a guide for electronic payment institutions around the world by providing guidance on both the technical and business aspects of cryptocurrency.

The following documents that relate to cryptocurrencies have been, or are soon to be, produced by the ISO working group (ISO TC/307):

- *ISO/DIS 23257 - Blockchain and distributed ledger technologies: Reference architecture* - the document defines and describes tokens, cryptocurrencies and digital coins (such as Bitcoin). Cryptocurrencies are associated with building value for virtual coins or tokens, and a token is a digital asset that represents a collection of entitlements. Categorisations of extrinsic, intrinsic or representative value for tokens are also defined.
- *ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary* - the meaning of the term cryptocurrency is provided and its relation to Blockchain and DLTs is clarified.
- *ISO/DTS 23258 - Blockchain and distributed ledger technologies: Taxonomy and Ontology* - the document defines the terms crypto-asset, cryptocurrency, electronic payment and token exchange, with emphasis on the decentralised nature of these concepts.
- *ISO/DTS 23635 - Blockchain and distributed ledger technologies: Guidelines for governance* - the document describes the use of cryptocurrency as a governance mechanism for incentivising consensus in permissionless DLT systems. In permissionless systems, participants may be anonymous or exempt of any formal relationships or contractual obligations. And, as such, "these systems rely on novel economic incentives based on game theory to achieve consensus, manifested through reliance on on-chain tokens, i.e. mostly cryptocurrencies."

4 Operational Context Specific Regulatory and Standardisation Gaps

This chapter aims to analyse the operational context-specific regulatory and standardisation gaps in terms of both transversal and vertical requirements.

4.1 Transversal standardisation Processes-Requirements-GAPS to be targeted for standards seeking

With respect to transversal requirements, the focus is directed towards financial services on interoperability, integrity, privacy, audit and compliance.

4.1.1 Financial Services as a System-of-Systems

This sub-section focuses on the analysis of regulatory and standardisation gaps specific to financial services.

4.1.1.1 Interoperability

The interoperability of systems, tools, and services are tackled in an onion-like interoperability scheme which is composed of:

- Foundational interoperability: the first level of interoperability, foundational, or technical, interoperability enables basic technical end-to-end data exchange from one information technology system to another.
- Syntactic interoperability: this is the ability of systems to exchange structured data and refers therefore to the packaging and transmission mechanisms for data among stakeholders, tools, services, subsystem, and systems. Syntactic interoperability defines the structure or format of data exchange and is achieved through tools such as JSON, XML, CSV, etc. Syntactic interoperability is the first stage of real interoperability and it is the pre-requisite of semantic interoperability.
- Semantic Interoperability: Ontology-driven semantic approaches are applied to improve the border crossing/multi organisational/multi-cultural understanding. This is achieved by automatic or semi-automatic interpretation and use of exchanged information within financial systems. More specifically, ontologies are foreseen as the main drivers to address this challenge. Super-concepts associated with domain ontologies present a formal, explicit specification of a shared conceptualisation. The conceptualisation specified by each super-concept ontology is usually devoted to representing a certain phenomenon, topic, or subject area, and designed with a certain purpose. SAREF[5] is one of the widely-accepted ontologies, namely Smart Applications REFerence ontology that enables connected devices to exchange semantic information in many applications' domains.
- Operational interoperability, or pragmatic interoperability: this refers to the business process integration of interoperability beyond the boundaries of a single organisation aligned with the system of systems concept. The achievement of full interoperability is the goal of organisations (including not only financial and insurance organisations but also other authorities and customer enterprises) with a pragmatic approach where organisations and all stakeholders wish to attain pragmatic (realistic) interoperability or above. Hence, enabling the interoperability between applications requires agreement in the format and meaning (syntax

[5] https://www.etsi.org/technologies/smart-appliances

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

and semantics) of exchanged data including the ordering of message exchanges and harmonised co-working within the System of Systems.

IEEE has a number of existing standards (current and under development), activities, and events that are directly related to creating the IoT environment, recognising the value of the interoperability of systems and the benefits this technology innovation brings to the public. Among these, the following standards are the foremost ones:

1. IEEE P2302™/D0.2 Draft Standard for Inter-cloud Interoperability and Federation (SIIF) focuses on the interoperability at cloud level supporting the federated clouds and edge networks.
2. IEEE P2413-2019 promotes cross domain interaction, aids system interoperability and functional compatibility.
3. IEEE 1451-99 is focused on developing a standard for harmonisation of Internet of Things (IoT) devices and systems. This standard defines a method for data sharing, interoperability, and security of messages over a network, where sensors, actuators and other devices can interoperate, regardless of underlying communication technology.

Moreover, there exist prominent standards for interoperability of systems:

- ISO-14258 (ISO-14258:1998, 2014, is used by organisations, seeking integration between their different independent systems, to define rules and concepts for their enterprise models with the intent to guide the process of interoperation.
- ISO 15926 focuses on the interoperability which is defined as the ability of different types of computers, networks, operating systems and applications working together effectively, without prior communication, in order to exchange information in a useful and meaningful manner.
- ISO 15745 defines the generic elements and rules for describing integration models and application interoperability profiles (AIPs), as well as their component profiles, process profiles, information exchange profiles, and resource profiles.
- The main ETSI IoT standardisation activities are conducted at radio layer in 3GPP (LTE-M, NB-IoT and EC-GSM-IoT) and at service layer in oneM2M.

Interoperability in Blockchain area is still a promising area presenting a gap to be filled by communities. Blockchain interoperability efforts can be divided into two groups: open protocols and multi-chain frameworks.

- Open protocols: Standardised protocols that enable Blockchains to communicate with each other without intermediaries or trust processes needed. The most recognised open protocol is the Atomic Swap.
- Multi-chain frameworks: Blockchains can plug into a framework to become a part of the standardised ecosystem and transfer data and value between each other. Multi-chain frameworks are more complicated than open protocols. They are often referred to as the "internet of Blockchains."

There exist prominent projects focusing on Blockchain interoperability:

1. Cosmos: It runs on the Tendermint Byzantine fault tolerance protocol where zones are all connected to the Cosmos Hub and can interact with each other (Buchman & Kwon, 2016) (Braithwaite, et al., 2020).

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

2. Polkadot: The distinguishing characteristic of Polkadot is that it facilitates not only transactions but also data exchange (Wood, 2016). The Polkadot ecosystem contains parachains (individual Blockchains that became part of the Polkadot environment), and a relay chain that is a central connector between parachains.
3. Aion: Most Blockchain systems are not able to accommodate large amounts of data. Aion addresses this issue by using a high-performance virtual machine and a scalable database (Spoke, 2017).
4. Ark: Ark (Košič, et al., 2018) aims to create a Blockchain interoperability solution that is scalable and adaptable. Therefore, Ark automated the creation of new Blockchains within the ecosystem. As a result, users can create new Blockchains within minutes.

P3203 Working Group[6]- IEEE Standard for Blockchain Interoperability Naming Protocol is being improved by a working group aiming to define a set of protocols that enable Blockchain networks to locate each other's trusted nodes through standardised names.

Critical-Chains tackles the interoperability at technological, syntactic, semantic and organisational level as the requirements rely on domain ontologies and data format (see D2.7 for details) and also the links at system level where XaaS components are interlinked with each other. Hence, this approach can be a pre-normative study to demonstrate the system of systems in finance domain as most of standards are widespread and not focusing specifically in finance domain. Technical reports delivered within the project can be used as a basis for more compact standards for the interoperability of IoT, Blockchain, service-oriented architectures in the Fintech domain.

4.1.1.2 Integrity

Data integrity is a crucial requirement in any financial operation as it is mandatory to protect data from alteration, substitution, insertion, or deletion. Integrity requirements are tackled together with the confidentiality requirements which are for protecting data from unauthorised disclosure whereas data integrity deals with the security threat of unauthorised modification of data which is either saved in storage or transmitted over the network.

The following standards aim to draw a framework to enable integrity in financial transactions:

- ISO/IEC 27001 Information Security Management. The ISO 27001 provides guidelines for setting up an information security management system (ISMS) and comprises policies and procedures that help safeguard customer data by considering the integrity as well.
- ISO 15489-1.2011. Information and documentation – Records management – Part 1: Concepts and principles. ISO 15489 establishes the core concepts and principles for the creation, capture and management of records taking appropriate action to protect their authenticity, reliability, integrity and usability as their business context and requirements for their management change over time.
- ISO 15782-1:2009. Certificate management for financial services. ISO 15782 are designed to maintain the integrity of financial messages and support the service of non-repudiation
- ISO 16609:2012: Financial services — Requirements for message authentication using symmetric techniques. This standard aims to protect the integrity of transmitted banking messages and for verifying that a message has originated from an authorised source. A list of

[6] https://standards.ieee.org/project/3203.html

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

block ciphers approved for the calculation of a message authentication code (MAC) is also provided.
- ANSI - Accredited Standards Committee X9 (ASC X9) - technical standards for the financial services industry. This standard presents a set of rules for the cryptographic functions providing confidentiality, authentication, and data integrity services for financial information.
- BCBS 239 - Basel Committee on Banking Supervision's standard number 239. This standard aims to regulate the banking operations which are able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability
- International Financial Reporting Standard 9 (IFRS9). IFRS9 addresses the accounting for financial instruments. It contains three main topics where data integrity is crucial: classification and measurement of financial instruments, impairment of financial assets and hedge accounting.

The integrity is a wide term as it should cover the interoperability of subsystems as the financial data travelling within a cyber-physical ecosystem. There exist many standards, especially in the IoT area (e.g. IEEE P2413-2019 for the architectural framework for the IoT; IEEE 1451-99 for harmonisation of IoT devices and systems; IEEE P2510 defines quality measures, controls, parameters and definitions for sensor data related to IoT implementations). These standards have become diversified to many areas. However, there still exist gaps in standards to improve the data integrity by Blockchain.

Blockchain technologies may play an important role in improving data integrity, even can be standardised in future provisions. For instance, the original mining process, still used for Bitcoin and Ethereum Blockchain, is based on the proof of work (PoW) which enjoys many fascinating properties related to data integrity. When a block is part of the chain, all miners have agreed on its contents, hence it is practically non-repudiable and persistent (unless an attacker has the majority of miners' hash power that are able to create a fork of the chain). Assuming a majority of hash power controlled by honest miners, the probability of a fork of depth n is $O(2^{-n})$ (Bonneau, 2015).

The International Standards Organization (ISO) is working on a series of Blockchain and Distributed Ledger Technology standards called ISO/TC 307. This week the ISO published a business plan[7] which says the first standards will be released no later than 2021. Critical-Chains Consortium follows the related actions as the Blockchain-as-a-Service has the potential to improve the terms of this standard in emerging titles mentioned by ISO as

- privacy and personally identifiable information protection (no date)
- Security risks and vulnerabilities (no date)
- Overview of identity (no date)
- Reference architecture (2021)
- Taxonomy and Ontology (unclear)
- Legally binding smart contracts (2021)
- Overview of and interactions between smart contracts in Blockchain and DLT systems

[7] https://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_307__Blockchain_and_distributed_ledger_technologies_.pdf?nodeid=19772644&vernum=-2

4.1.1.3 Privacy, Audit & Compliance

As mentioned in the previous section, the ISO/IEC 27001 standard provides a framework of policies and procedures for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system. ISO/IEC 27032 instead provides a set of guidelines for improving the cyber security situation in an organisation through the development of a security framework based on risk management. ISO/IEC 29100 provides a high-level privacy framework for the protection of personally identifiable information within information and communication technology systems.

The aforementioned standards therefore deal with the management of cybersecurity and the privacy aspects of the platform in a general way, without considering the imposition of specific technologies. In the case of Critical-Chains, from the analysis carried out on the standards, some gaps with respect to the standards can therefore be detected regarding Blockchain and Artificial Intelligence (AI), Cryptocurrencies and Digital Wallets.

For what concern AI, standards can play a constructive role in enabling the widespread use of responsible AI. For example, they can establish common building blocks, and risk management frameworks, for companies, governments and other organisations. This may take the form of standards in 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. The international standards development organisations ISO and IEC have set up a joint committee, the ISO / IEC JTC 1 / SC 42, which will carry out standardisation activities for artificial intelligence in the next few years.

Blockchain has some items that could be targets for further standardisation, including: Basic data models for Blockchain, consensus algorithms, storage algorithms, signature algorithms and web-based access protocols. ISO/TC 307, was also formed to implement the standardisation of Blockchain technologies and distributed ledger technologies. For now, however, only one document has been prepared, ISO 22739: 2020 Blockchain and distributed ledger technologies - Vocabulary, which provides the fundamental terminology for these technologies, but no guidelines on controls and security.

Regarding the cryptocurrency a security standard in the crypto space, commonly referred to as CCSS (Cryptocurrency Security Standard), was introduced in 2014 to provide guidance specific to the secure management of cryptos. The CCSS is an open standard that focuses on the cryptocurrency storage and usage within an organisation. CCSS is designed to augment standard information security practices and to complement existing standards, i.e. ISO 27001, not replace them. The CCSS standard only focuses on the secure management of the crypto wallets. Additional security measures will be required to secure the environments within which the crypto-security management components operate. These should be in particular focusing on:

- Trust, so that the supporting international financial ecosystem can warrant its financial payments and financial transactions.
- Binding liability, so that investments supporting a financial ecosystem do not have negative legal ramifications.
- Privacy, so that the individual, as a consumer, with the supporting financial infrastructure can ensure that information remains private when needed.

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 Digital Wallet ecosystem is in a very early stage where few, if any, standards exist. Neither informal nor formal standards exist in most areas. It is clear that there is a need for standards and open protocols. The Digital Wallet space is going to require standards for interoperability and assurance that the Digital Wallets are fit for purpose and safe to use. Standards and certifications are woefully missing from the Digital Wallet landscape at this time. Standards are required at many levels: Self Sovereign, Key Management, Portability Guardianship Delegation, Certification and Trust Hubs. Some areas already have standards in place that Digital Wallets can work towards: for what concerns authentication, the FIDO Alliance Standards (U2F, UAF, and FIDO2) and OpenID Connect, W3C (WebAuthn), and others provide frameworks that Digital Wallets can integrate and support.

4.2 Vertical standardisation Processes-Requirements-Gaps to be targeted for standards seeking

This section presents the standardisation gap analysis from the vertical perspectives of processes and requirements.

4.2.1 Transactions & Financial Transaction Settlement

The simplest description of a financial transaction is that of an agreement or a communication carried out by a buyer and a seller who use a transaction of any type to carry out the payment of the good/ service offered. In the transaction we will have as object a good or a service which will be offered in exchange for a consideration of an economic nature.

The purpose of the next chapters will be to deal in greater depth with the following issues relating to financial transactions:

- Funds Transfer
- Pre-payment & Credit Cards
- Mobile Money
- Cryptocurrencies

4.2.1.1 Funds Transfer

Electronic funds transfer (EFT) refers to the method of transferring money from one bank to another, using computerised systems and therefore without the intervention of banking staff.

An electronic transfer of funds shall consist of an operation where the funds are moved from one institution to another, or even from one account to another, upon notification by a client of the institution. The customer after ordering the transfer receives the confirmation of the transfer from the institution, which before making the transfer proceeds to make the necessary checks. Only after the necessary controls, the funds will be available to the beneficiary institution/client of the transfer. EFTs require both the sender and recipient to have bank accounts. In the absence of this condition the transfer would be not possible.

Generally, as mentioned above, the process of transferring funds consists of a series of electronic orders, which may consist of accounting procedures for crediting or debiting to a given account. More simply a transfer of funds consists of a series of payment instructions, which begin with the order of transfer by the originator of the transfer, then the person who sends the money, and end with the receipt of the funds by the beneficiary, or to whom the transfer is addressed.

We find below a list of subjects/institutions who may be involved in a transfer of funds:

- Transferor, for example, natural person, commercial entity – the person who initiates a transfer through a request;
- Beneficiary - the last part to be credited or paid following a transfer of funds;
- Payer Financial Institution - the financial institution receiving the transfer instructions from the originator and the transmission of the instructions to the next party in the transfer of funds;
- Financial institution of the beneficiary - the financial institution which is to credit or pay the beneficiary party.

In the previous analysis we have identified some of the subjects mainly involved in a transfer of funds, it must be considered that in more complex cases of funds transfers, more subjects than those mentioned above, may be involved, such as other institutions.

The easiest transfer of funds can take place between two clients of the same institution, just think of a transfer of money between two clients of the same bank, everything would be very simple and fast. The institution makes the mandatory book entries in its accounting system and after having carried out all the necessary checks, the transfer is complete. After few days, the beneficiary will be able to verify that the transfer has been credited to his account.

4.2.1.2 Pre-Payment & Credit Cards

Credit cards and prepaid cards are one of the payment methods that can be used as an alternative to pay cash. In this historical epoch, digitalisation and technological advancement are leading, ever faster, from paying in cash to paying with electronic methods.

In addition to digitalisation, consumer preferences have led to this change. Consumers consider electronic payments to be safer, faster and more convenient, which is why the use of cash is fading over time. Credit cards and prepaid cards fully centre what nowadays is understood as an electronic payment method, and consumer choices are showing preference for the latter.

The credit card is issued by a bank or other financial intermediary under a contract; between consumer and banking institution, it allows purchases at any type of facility that can range from shops to supermarkets to online shops and, if permitted by the bank, cash withdrawals from ATMs. The amounts spent are paid by the cardholder after use, generally on a monthly basis, in a single payment or in instalments; they are usually debited from a current account, but direct payment is also possible.

Pre-payment are one of the most popular payment methods used online, many banks have stated that this payment method can be considered the safest, both from the buyer’s and the seller’s point of view. The seller will only send the product after receiving the money transfer from the customer, this constitutes a guarantee of security for the seller. For this reason, this payment method is considered the preferred on online stores, which very often offer discounts for customers who decide to pay with this method.

The added value of prepaid payment methods is what many customers who have unfavourable credit ratings or do not have credit cards, can easily use this payment method as an alternative.

4.2.1.3 Mobile Money

Mobile money development motivation grows from localised needs and central banking needs. There is always the need to bring different currencies into market for specific use. Communities can build trust and control the currency. Most of this development is not completely legal or compliance rules

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

have been interpreted. Central banks look for tools that allow better understanding how money supply and demand work near real time. It is important to see how standardisation work have been done.

The work is being undertaken mainly by standards development bodies such as the International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), and by ICT industry and financial institutions.

ISO has published the following documents (under working group ISO/TC 68/SC 9):

- *ISO 12812-1:2017, Core banking — Mobile financial services — Part 1: General framework.*
- *ISO/TS 12812-2:2017, Core banking — Mobile financial services — Part 2: Security and data protection for mobile financial services.*
- *ISO/TS 12812-3:2017, Core banking — Mobile financial services — Part 3: Financial application lifecycle management.*
- *ISO/TS 12812-4:2017, Core banking — Mobile financial services — Part 4: Mobile payments-to-persons.*
- *ISO/TS 12812-5:2017, Core banking — Mobile financial services — Part 5: Mobile payments to businesses.*

ISO has also examined successful models in nations where bank accounts, and therefore debit and credit cards, are rare – such as M-PESA in Kenya, a mobile phone-based money transfer service that enables branchless banking – to ascertain whether they could be incorporated into standards.

The Directive on Payment Services (PSD) was established by the European Commission to provide a single framework for payment standards and obligations, resulting in the Single European Payments Area (SEPA). The SEPA territory consists of many European countries and also includes countries which are not part of the euro area or European Union. The SEPA initiative aims to overcome technical, legal and market barriers between countries in order to create a single market for retail payments in euros and will include a SEPA card standardisation programme as well as one for mobile money services.

Despite this, in the ISO standards listed in section 3.3.1.4 above (relating to Blockchain and DLT systems), there is currently no work relating to the standardisation of mobile money in this vertical; the current and near-future publications of the Blockchain and DTL Systems working group are intended to lay the ground work for the future standardisation of more specialist, esoteric topics, such as the application of mobile money in the context of Blockchain-backed DLT systems. As such, it is important to target the following gaps for standards seeking:

- Common identity rules and methods
- Best practice sharing
- Traffic analysis and data using rules and methods
- Security of the wallets
- Protocols that can be used with different mobile money applications

4.2.1.4 Cryptocurrencies

See section 3.3.1.4 for information on current and future works of the IEEE relating to cryptocurrencies.

The majority of the ISO work relating to the standardisation of cryptocurrencies, referred to by the ISO standards listed in section 3.3.1.4 above, is of a general and preliminary nature. Indeed, the current

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

and near-future publications of the Blockchain and DLT Systems working group are intended to lay the ground-work for the future standardisation of more specialist, esoteric topics, such as the application of Blockchain-backed cryptocurrencies in the vertical of Financial Transaction Settlement. That said, relevant documentation, which is likely to standardise only individual aspects - or perhaps only small numbers of the key components of this vertical – is not likely to be produced (without targeting) for some time. Therefore, with relevance to Blockchain-backed cryptocurrencies in the vertical of Financial Transaction Settlement, it is important to seek the standardisation of as much of the pertinent, currently unorganised information as possible, given that cryptocurrencies in general are defined in relatively simple terms in the documents mentioned above (as being associated with building value for virtual coins or tokens, for example). The GAPS to be targeted for standards seeking include:

1. Offerings warranty mechanisms
2. Backer trust level
3. Money laundering prevention mechanisms
4. Differences between cryptocurrencies understandable

4.2.2 Online Transactions

Online transactions are a payment method by which money or funds are transferred via an electronic transfer. In recent years, online transactions are becoming more and more protected and secure, very often transactions are protected by passwords and codes that are only available to the user making the transaction.

When referring online transactions, it must be considered that all these transactions take place with the connection to an internet network. This shows how much the internet has revolutionised the world of payments, because an internet connection is the starting point for all types of transactions that will be processed.[8]

In the following chapters the following types of transactions that can be made online will be treated:

- E-Banking
- E-Purchasing
- E-Government

4.2.2.1 E-Banking

E-Banking is a system that enables any customer of a particular bank or other financial institution to complete operations directly from the online platform of the institution of which it is a customer.

Over the years other names have been assigned to this type of service, such as internet banking, because to access the dedicated platforms you need a device with an internet connection, or home banking, because the customer can carry out all the operations comfortably from home via his mobile phone or his PC.

E-Banking, which today is also carried out by banks, is built entirely on the internet and allows those with a current account to be able to conduct all banking transactions via the internet, without having to physically go to their bank.[9]

[8] https://www.toppr.com/guides/business-studies/emerging-modes-of-business/online-transactions-and-security-of-e-transactions/

[9] http://www.finanza-blog.it/home-banking-cos-e-come-funziona-e

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

To be able to take advantage of online banking, you just need an internet connection and a PC. Often it is not necessary to have a PC to be able to carry out all the operations offered by the bank, just a smartphone with an internet connection.

Once in possession of an internet connection and a device from which to log in, the customer can enter the bank's virtual port through the access credentials. Once logged in the customer can select the operation to be performed and the platform will indicate all the actions to be taken to complete the procedure.

Several definitions have been given on E-Banking, two have been selected below:

“The provision of information or services by a bank to its customers, via computers, television, telephone, or mobile phone” (Daniel, 1999).

"An electronic connection between bank and customer in order to prepare, manage and control financial transactions" (Burr, 1996).

The services that this type of platform can offer are different, such as:

- Electronic Fund Transfers
- Debit Card
- Utility Bills Payment
- Bank Account / Balance Statement
- Credit Card
- Prepaid Smart card.

A system such as that of E-Banking can have great benefits to both the consumer and the bank. From the consumer's point of view, accessibility and convenience (24-hour services), new services or service differentiation, utility payments, bill payments, rapid money transfer, are just some of the benefits. Analysing from the bank side, lower operational costs of the banks automated process (elimination of manual processes, improved efficiency and timeliness), accelerated credit decisions, and improved customer communication and relationship, are aspects that can facilitate the task of banks.

A list of some disadvantages that can be identified when we talk about E-banking should be considered. Certainly the main disadvantage linked to this type of service is that related to security, cyber-attacks are constantly increasing, this puts financial and personal information at risk, of users registered on the platform. Another issue that could be inconvenient for customers, is that of the absence of a physical agency where they can go for any eventuality, this could cause inconvenience to users. The last point on which to dwell in the context of banking criticalities is the great challenge that internet represents, that is, not all customers have an internet connection or rather, not all customers are familiar with using a service provided entirely online, since the customer takes a long time to access the platform, the speed of the operations offered by the platform will be of little importance, this could be a reason for some customers to turn away.

4.2.2.2 E-Purchasing

With the development of new technologies more and more traders and retailers rely on new electronic systems for more efficient and faster management of their supply chains. The development of the internet has created new markets. A consumer with an internet connection can search for and find a wide variety of goods and services of any kind. Electronic purchasing systems also provide up-to-date information on the state of the buying or selling process, as well as other details on consumer

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

preferences, availability of previously exhausted products, real-time shipment updates, and automated warehouse management. We can affirm that the E-purchasing offers of the advantages is from the side of the buyer that from the side of the seller, facilitating the life to both the parts.[10]

Another very important issue when we treat the theme of E-purchasing is that transparency and accuracy are facilitated by the use of this system, this is because the exchange of data and electronic storage enable you to have a data management tracked by the system. We can then say that any exchange of information and goods/ services remains registered on the platform. This leads to having a guarantee of data security both on the side of the buyer and the seller.

In addition, a very sensitive and important issue needs to be addressed, namely data security for the free trade in goods and services on online platforms, we need a security system that guarantees users, both on the buyer's side and on the seller's side, that their information and data remain safe throughout the purchase/sale process. Only under these conditions users will feel free to make any kind of purchase on the online platforms.

4.2.2.3 E-Government

E-government often means digital administration or the digital management system of public administration. This type of management enables to process documentation and manage procedures with computer systems, using information and communication technologies.

The aim is to optimise the work of institutions and to offer users, whether they are citisens or businesses, new services or faster services. It helps to give an added value to all those involved in this type of service.

Under the macro-category of E-government, we focus on two services that enable the achievement of results in an effective and efficient way, such as:

- E-administration, a service that has the scope to improve the administration and the management of the governments, impacting on the cost reduction and performances, and facilitating the services for electronic way. All this happens thanks to the ICTS (information and communication technologies).
- E-information, a service through which organisations can transmit information through electronic means of communication.

The introduction of technology within public administration services leads to a significant reduction in time. Furthermore, the E-government is the first step towards the reduction of administrative procedures.

Obviously, this process leads to the implementation of networks and other similar technologies, which can lead to problems related to data and information security. To avoid this problem, it is necessary to adopt forms of platform and system protection.

4.2.3 Insurtech

The neologism, formed by the word's insurance + technology, identifies everything that is innovation technology - driven in the insurance field: software, applications, start-ups, products, services, business models.

[10] http://tfig.unece.org/contents/e-purchasing.htm

Insurtech is the application of technology innovation in the insurance industry value chain to solve known challenges and discover unknown opportunities, in order to deliver value for customers. We have seen that Insurtech players boom globally since 2015.

Within this context, we can see incumbents, Insurtechs and facilitators as main Insurtech ecosystem participants:

- Incumbents: The scope of Insurtech's capability to deliver innovative solutions across the value chain make them a very attractive partner for incumbents, in fact, Insurtechs are often playing an enabling role, as a problem solver or innovation agent within the existing firms. Established players are receptive to cooperate with global Insurtechs wishing to test their ideas in the market, and talent is considered to be fairly available. However, legal and regulatory professionals highlighted[11] obstacles such as tight regulations and high capital barriers to entry. Incumbents are particularly concerned about increasing data privacy and transparency compliance requirements.
- Insurtechs: Insurers may not necessarily know how to engage Insurtech or understand their digital offerings. In principle, when two parties seek to enter a partnership, a minimum level of understanding of the other party's DNA needs to be achieved. Insurtechs operate to a different rhythm to incumbents. Each brings differing and complementary propositions to the table. The DNA of each party needs to be understood and leveraged in the way the partnership is constructed and also leveraged in a commercial sense. Insurtechs should educate incumbents not only on what products and services they bring to the table, but their unique methodology for creating customer-centric, value-creating products and services.
- Facilitators: Leaders in government, non-profit organisations and co-working communities, and advisory professionals continue exploring strategic partnerships and connecting incumbents with Insurtechs to identify and help establish digital capability. Incubating a high impact environment for ideation with the right tools, resources and funding mechanisms may result in rapid designs and test solutions that reduce overall risk to an incumbent's business that would otherwise not be addressed. Further development in the levels of understanding of Insurtech among key stakeholders is needed. Education and consequent knowledge will promote partnerships and inform a sustainable Insurtech strategy.

In recent years in all sectors we have noticed a strong transformation and advancement of new technologies, insurance has been among the industries slower to adapt to digitisation and to grasp the digital transformation of their sector. All of this has led to a radical change involving the way business is done, processes, data management, and approach with customers.

"Blockchain technology is considered by many not only useful for insurance, but a real flywheel"[12]. However, cybersecurity represents the biggest challenge for the insurance industry, this is because cybercrime is taking hold, and each have had a very high cost to the insurance industry. Computer security is one of the main drivers for the insurance business in the coming years.

4.2.3.1 Policy Purchasing and Renewal Online

The new technologies are leading to the transformation of all sectors, starting from the sale of goods online, we arrived in a short time to the provision of services entirely online. This is also what is

[11] EY Report : Insurtech: Enabler or Disruptor?, September 2018

[12] https://www.insuranceup.it/it/scenari/insurtech-che-cos-e-e-quali-sono-i-suoi-pilastri/

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

happening in the insurance sector, the services of insurance companies can take place online entirely, from purchase to renewal.

The customer interested in a particular service can find all the information and the data sheet on the platform of the insurance company, in addition to this can receive advice via chat, on the same platform. This means that the customer is able to sign an insurance policy contract without having to go to the agency or in the office. The same applies to customers wishing to renew their policy, as the customer can automatically renew the contract through the online platform, directly from his smartphone and his PC, from the comfort of home.

It shows how important it is to treat security in this context. It is fundamental that the customer can carry out all the operations on the platform, without the risk of any cyber-attack.

4.2.3.2 Claims submission and Settlement

As previously mentioned in the in the chapters above, the customer can carry out any type of operation through the online platform. This also applies to requests and questions from users, which can be made directly on the platform, by contacting a consultant or directly through the chat dedicated to questions and requests from users, very often these types of platforms have a section dedicated to user questions with answers, which explain to users how to solve the problem or their request. If the dedicated section does not help the customer, the customer can always contact the assistance directly to talk to a consultant indicated to his category of request or problem.

This type of service brings customers closer to the company, allowing customers to feel important to the company. Showing users how important they are for the company, and how much it cares about their requests and problems, trying to solve the problems in the shortest possible time.

The intent is to make customers feel followed at every stage of the request. Consequently, the final goal is to always resolve any type of request made by the consumer, if possible.

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

5 Critical-Chains Standardisation-oriented Activities and Impact

This chapter presents Partner involvement and activities in regulations and standards relevant to the Critical-Chains project.

5.1 Work within Critical-Chains on multi-factor authentication and cryptographic primitives

Multifactor authentication (MFA) is tackled in Critical-Chains in comparison with the FIDO protocols. As depicted in Table 1, The security levels are defined, starting from L(-1) to L2. Users may confirm their claimed identity via:

- “Something they know”, e.g. password, PIN or security questions.
- “Something they have”, e.g. smart card, token or smartphone for receiving a one-time password (OTP).
- “Something they are or do” (based on biometrics), e.g. fingerprint, face, iris or signature.
- “What they do”, which is related to continuous identity verification based on user behaviour in a system and abnormal pattern.
- Combinations of above.

FIDO and FIDO2 present authentication solutions for mobile phones or desktops, over web browsers, which usually aims to utilise a password and/or token, and recently biometrics for passwordless authentication. Passwordless authentication is also promoted especially for easier online shopping where users are authenticated by a smart phone application or sometimes only by tokens or biometric features. In Critical-Chains FIDO-X is promoted as the highest security level, L2, which enables the modular use of passwords, tokens and biometric, either together or singular. This approach brings efficiency to apply various security levels depending on the security requirements of financial operations. For instance, in online shopping where payments are below a certain amount (say 200 €), L0 can be applied. For higher amounts of payment L1 can be selected. For the most critical financial operations like contracting, clearing, catbond, etc. L2 can be selected.

Table 1. MFA Security levels re-defined in Critical-Chains

	Factors			
FIDO Compliance	**Security Level**	PWD (sth u-know)	Token like SecureStick (sth u-have)	Facial biometric (sth u-are)
NA	L-1	●		
(FIDO2)	L0		●	○
(FIDO)	L1	●	●	
(FIDO-X)*	L2	●	●	●

Such a MFA mechanism is integrated with cryptographic schemes to secure any financial data. Here, Crypto-as-a-Service, one of the XaaS presented in Critical-Chains, can be used to encrypt any financial data fully or partly according to a policy aligned with the security levels. For instance, L2 can be applied to any personal data or financial records of a company whereas L0 or L-1 can be selected to see the shopping statistics of a person in full compliance with GDPR. Such discussions are left to the second iteration of the project.

5.2 Work within Critical-Chains on accountability-by-design

Following the new directives imposed, e.g. GDPR, the management of data in the context of smart contracts acquires an important role. In this regard the Blockchain can contribute to the solution of some issues related to the data responsibility, such as, for example, security and protection of user data, security with regard to the tracking and storage of transactions, security with regard to payments, which in the case of smart contracts takes place automatically on the occurrence of contractual conditions.

The Blockchain platform will undertake a twofold objective. On the one hand, decentralised management of the transaction ledger, and on the other hand, support of decentralised execution of smart contracts, hence automatic execution of contract functions.

The accountability-by-design model is similar to the RACI model where on each phase of the project each unit/body/single person will have responsibilities related to the specific scope, the units identified as accountable will be directly responsible for the task in question, and an accountable must approve the work that the person responsible provides. There must be only one accountable specified for each task or deliverable.

Cryptocurrencies. The majority of the ISO work relating to the standardisation of cryptocurrencies, referred to by the ISO standards listed in Section 3.3.1.4 above, is of a general and preliminary nature. Indeed, the current and near-future publications of the Blockchain and DLT Systems working group are intended to lay the ground-work for the future standardisation of more specialist, esoteric topics, such as the application of Blockchain-backed cryptocurrencies in the vertical of Financial Transaction Settlement. That said, relevant documentation, which is likely to standardise only individual aspects - or perhaps only small numbers of the key components of this vertical – is not likely to be produced (without targeting) for some time. Therefore, with relevance to Blockchain-backed cryptocurrencies in the vertical of Financial Transaction Settlement, it is important to seek the standardisation of as much of the pertinent, currently unorganised information as possible, given that cryptocurrencies in general are defined in relatively simple terms in the documents mentioned above (as being associated with building value for virtual coins or tokens, for example).

Firstly, an overview of the roles identified for the laws / regulations and the respective level of participation is offered, referring to the RACI matrix for greater understanding and accuracy as depicted in Figure 2.

The analysis of the RACI Matrix highlights the fact that there are no compatibility issues about the GDPR, the NIS and the AML 5, while it is evident that there are discrepancies between the GPDR and PSD2

In particular, the AML5 mentions among its duties the need to apply the GDPR and identifies the specific figure of the Data Controller as responsible and accountable role in order to enforce the regulation.

Both the NIS and the GDPR start from the same application approach, which asks companies and their managers to put data & security governance at the centre from the design of any business process and procedure. Both regulations push towards a unified strategy, capable of applying the directives as a whole and acting with a view to integration between standards and systems.

On the contrary, the PSD2 and the GDPR present some aspects that highlight the application complexity resulting from a lack of coordination of the rules.

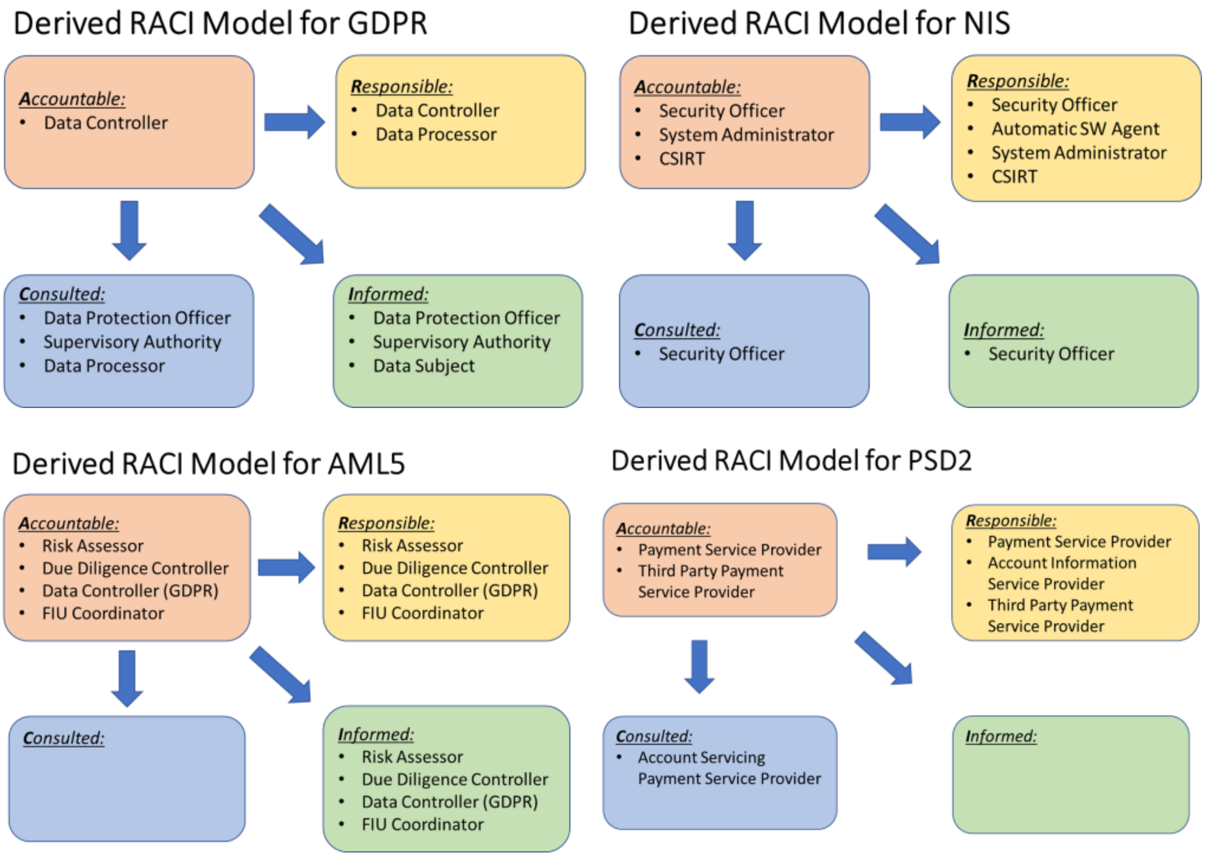

Figure 2. Derived Raci Model for GDPR, NIS, AML5 and PSD2

PSD2 has introduced and regulated new services that will allow users of banking and payment services to contact operators of non-bank derivation, defined as third parties or Third Parties Provider (TPP), to request the execution of payment and other activities related to payment services. TPPs operate by interposing between the customer and the payment services provided by banks. The entry of TPPs into the payment system generates the need to frame and, where possible, regulate relations between them and the operators of the traditional banking system.

A first aspect to consider concerns access to the data of the interested party (the customer). The new services governed by PSD2 require, in order to function, a more rapid interaction between the data available to the banks and the TPPs which, in order to perform their services, need to be able to promptly access the customer data processed by the bank. The trend in PSD2 is, therefore, to make customer data more accessible to third parties. According to PSD2, banks are in fact required to provide TPPs with some data of their customers in order to allow TPPs to provide their services, unless such data qualifies as sensitive payment data. In turn, articles 13 and 14 of the GDPR impose on the data controller the obligation to provide the data subject with a series of specific information regarding the processing of personal data concerning him.

If several subjects are involved in the processing, as occurs in the case of "concurrence" between banks and TPP, the problem arises of establishing who is required to provide the data subject with the information and to acquire and keep the relative consent if this is necessary. In other words, it is

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

necessary to ask who between the bank and TPP should be the data controller of the process, and therefore who should cover the role of accountable in the RACI matrix, at the time of data processing by TPP.

The personal data protection framework of the TPP is one of the most critical and controversial aspects, starting with the question of whether the TPP should be considered the owner or manager of the processing. If it were necessary to frame the bank as the data controller and the TPP as the data controller, it would be necessary to enter into a contract which, in accordance with art. 28 of the GDPR, regulates the processing carried out by the TPP. At this point, the bank should exercise strict control over the TPP's work. The PSD2 establishes that no contract can be requested from the TPP to access and use the personal data of the customer of the bank who has chosen to use the TPP services.

Any refusal by the bank to provide customer data to the TPP would constitute a breach of PSD2. Conversely, if the bank decides to comply with PSD2 and provide customer data to the TPP, in the event of a data breach and violation of the rules to protect customer confidentiality by the TPP, the bank may be liable under the GDPR. The bank and the TPP could be classified as two independent data controllers. In this case, however, the problem would arise of regulating the transfer of data from the bank to the TPP. In fact, the customer first establishes a relationship with the bank: when the customer requests the TPP to provide the new PSD2 service, the TPP does not collect the data directly from the customer, but acquires them through access to the data of the bank

The general rules on data protection provide that its processing is lawful only if at least one of the conditions of lawfulness listed in art. 6 of the GDPR, among which the one in which the interested party has given consent to the processing for one or more specific purposes is relevant. A "consent" also refers to art. 94, of the PSD 2 which provides for the explicit consent of the user for access, processing and storage by the PSPs of their personal data necessary for the provision of the respective payment services. The consent defined in PSD2 establishes that a PSP can access, process and store the personal data necessary for the provision of its payment services only with the explicit consent of the payment service user. This is overall in line with the GDPR, including the similar right to data portability. Furthermore, the GDPR contains more extensive rules on the use of explicit consent as a basis for processing. For example, the consent of the data subjects (customers) must be given freely, specific and informed, the controller (PSP or TPP) must demonstrate that such consent has been provided and the data subject must be able to easily withdraw the consent in every moment. The definition, function and purpose of consent described by the GDPR and PSD2 are not, however, completely homogeneous and superimposable, since while the GDPR refers to the protection of natural persons - data subjects - and the processing of their "personal data, the PSD2 focuses instead on data protection of "users" in general of payment services.

5.3 Work outside Critical-Chains towards the policy community

This section covers dissemination actions in working groups, presentations towards the policy community, discussions in regulatory domain, etc. Table 2 summarises Partner presence in standardisation committees and working groups.

Table 2. Partner presence in standardisation committees

Partner	Standardisation committee/bodies	ISO	Topic

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

GT	Blockchain and Distributed Ledger Technologies	EVS/TC 75	Blockchain and distributed ledger technologies: Vocabulary
GT	Smart grids	EVS/TC 58	Electricity metering equipment - Particular requirements - Part 21, Part 22, Part 23 and Part 24.

Guardtime is a founding member of the new standardisation committee EVS/TC 75 “Blockchain and Distributed Ledger Technologies”. The Estonian Centre for Standardisation registered the new Technical Committee EVS/TC 75 “Blockchain and distributed ledger technologies” on 13/1/2020. The Committee’s objectives include providing input to EU and international standardisation activities and creating relevant Estonian terminology. The Committee will reflect the activities of JTC 19 “Blockchain and Distributed Ledger Technologies”, a joint committee of European standardisation organisations CEN and CENELEC, and the ISO TC/307 “Blockchain and distributed ledger technologies” (referred to several times in this document).

In addition, the committee has produced of an equivalent document to “ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary” (produced by the ISO TC/307 committee), with relevance to Blockchain and DLT systems in general, smart contracts, digital signing and cryptocurrency; all of these topics are mentioned above with reference to ISO 22739:2020.

Guardtime is also a founding member of the standardisation committee for smart grids, EVS/TC 58. The committee has been established since 2015, and its publications are available via the Estonian Centre for Standardisation. The Committee’s objectives are similar to those of EVS/TC 75: it reflects the work of many international committees, including those of the IEC, CLC and CEN; an example publication of the committee’s is “EVS 929:2016 - Smart grid: Terminology”.

RINA-C organised the workshop: "Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop” that was focused on below topics of sectoral interest:

- Financial Sector Cyber-Physical Security Protection
- Authentication & Accountability Models across the Financial Sector Flows, IOT & Blockchain
- Regulatory Harmonisation & Compliance Challenges: Tensions, Technological & Policy Enablers (PSTD 2, eIDAS, AML, GDPR, NIS)
- Training Harmonisation: e-Portfolio & Workplace-based Incident-Responsive Security Training

It was divided into three sessions:

- Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm
- Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector
- Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)

The workshop was supported by the Financial Sector (POSTEIT, Caixa Bank), and from the security and Blockchain research projects particularly SOTER and other Cyber-watching network security projects.

5.4 Work within Critical-Chains on regulatory and standardisation compliance

Critical-Chains must be complaint with all regulations, legislations and recommended adopted standards applicable to it within the EU before deployment. Through regulatory compliance analysis these regulations and standards have been identified, technical requirements have been extracted and then applied in the design and development of Critical-Chains. This section will briefly review the main regulations that Critical-Chains is compliant with.

The following EU directives and regulations were looked at under scrutiny in the regulatory compliance analysis process: General Data Protection Regulation (GDPR), Privacy and Electronic Communications directive (ePD)[13], Payment Services Directive (PSD2)[14], Fourth Money Laundering Directive (AML4)[15], Security of Network & Information Systems Regulations (NIS)[16], Electronic Identification and Trust Services (eIDAS)[17]. The regulatory requirement design process of Critical-Chains was not limited to these regulations, and other standards such as FIDO have been examined.

This analysis process revealed the relevant clauses from each piece of legislation to Critical-Chains. Once these clauses had been documented, the technical partners then derived technical requirements and assigned it to the respective building block within Critical-Chains the requirement applied to. There are 7 building blocks in Critical-Chains, and each has its own technical requirements. Therefore, different considerations were required across the building blocks in order for the whole construct to comply with regulatory bodies.

Although Critical-Chains consists of 7 explicit building blocks, the system as a whole is interoperable between each layer. Users on the Critical-Chains system are given a single-identity from which they can access any layer. FIDO standards aim to achieve a fast and simple login experience; by using a single identity across all layers, Critical-Chains aimed for this same target.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849
[16] https://www.legislation.gov.uk/uksi/2018/506/made
[17] Critical-Chains Deliverable D2.7 "Regulatory Compliance and Accountability-by-Design model"

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

6 Conclusions

This report D7.6 “Gap analysis of current relevant standards” has first set up the domain of the Critical-Chains project within the financial sector and defined the project technologies focusing on three key development areas: i) the Critical-Chains Main Framework as a Cloud infrastructure, ii) the Cyber-Physical Security-as-a-Service (CPSaaS) comprising different critical security services, and iii) Data flows and information modelling. The report has provided an inventory of current standards relevant to the Critical-Chains domain. This includes a review of existing standards with reference to the respective standardisation organisation bodies (ISO, IEEE, ETSI, FIDO Alliance, OpenID Foundation, OASIS, NIST) as well as emerging Blockchain and distributed ledger related standards. Based on this inventory, the report has analysed the operational context-specific regulatory and standardisation gaps with respect to both transversal and vertical standardisation requirements. The report has also presented Critical-Chains oriented activities and their impact regarding the accountability by design, regulatory and standardisation compliance, and towards the policy community and standards-seeking contributions on multi-factor authentication and cryptographic primitives.

The analysis of the Standards also revealed some gaps with regard to the technologies applied in the Critical-Chains project, in particular with regard to artificial intelligence and the Blockchain. What is highlighted is that this lack of standardisation for these cutting-edge technologies is about to be filled in the next few years by international standardisation organisations, e.g. ISO and IEC: a joint committee, the ISO / IEC JTC 1 / SC 42, have been set up and will carry out standardisation activities for artificial intelligence. Another technical committee, the ISO / TC 307, was also formed to implement the standardisation of Blockchain technologies and distributed ledger technologies; so far a single document has been drawn up, the *22739: 2020 Blockchain and distributed ledger technologies - Vocabulary*, which provides the fundamental terminology for these technologies, but no guidelines on controls and security.

The RACI matrix allowed a clear identification of the roles and the respective level of responsibility for the individual tasks, in order to highlight in particular the accountable roles. The analysis of the RACI matrix reveals that GDPR, AML5 and NIS can co-exist without creating overlaps or inconsistencies between regulations. On the other hand, however, an overlap between GDPR and PSD2 is evident, which affect fundamental nodes such as that of consent to data processing and the univocal identification of an accountable role for data processing. It is difficult to interpret if the explicit consent as provided for by this provision is to be understood as the only legal basis to be put in place for this type of processing and if, more generally, this is comparable to the consent regime provided for by the General Regulations on data protection.

References

(NIST) Internal Report 8202, n.d. *Blockchain Technology Overview, National Institute of Standards and Technology.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

Balfanz, D., 2015. Fido u2f implementation considerations. *FIDO Alliance Proposed Standard (2015): 1-5.*

Balfanz, D., Hill, B. & Hodges, J., 2013. Fido uaf protocol specification v1.0.

Bitcoin/Bips, GitHub, n.d. [Online]
Available at: github.com/bitcoin/bips

Bonneau, J. e. a., 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *In 2015 IEEESymposium on Security and Privacy, pages 104{121. IEEE, 2015.*

Braithwaite, S. et al., 2020. Tendermint blockchain synchronization: formal specification and model checking. *In International Symposium on Leveraging Applications of Formal Methods (pp. 471-488). Springer, Cham..*

Buchman, E. & Kwon, J., 2016. Cosmos: A network of distributed ledgers.

Courcelas, L., 2020. *EU Blockchain Observatory & Forum 2018-2020: Conclusions & Reflections,* s.l.: EU Blockchain Forum, 25 June 2020.

Dunkelberger, P., 2018. FIDO2 puts biometrics at heart of web security. *Biometric Technology Today 2018.8 (2018): 8-10..*

Ergün, S., Güler, Ü. & Asada, K., 2011. IC truly random number generators based on regular & chaotic sampling of chaotic waveforms. *Nonlinear Theory and Its Applications, IEICE 2.2 (2011): 246-261.*

Ergün, S. & Özog, S., 2007. Truly random number generators based on a non-autonomous chaotic oscillator. *AEU-International Journal of Electronics and Communications 61, no. 4 (2007): 235-242.*

Ethereum/EIPs, GitHub, n.d. [Online]
Available at: github.com/ethereum/EIP

Finextra & BSI, 2016. *A roadmap for fintech standards.* [Online]
Available at: http://smarttokenchain.com/wp-content/uploads/2016/07/FIN_BSI_long_v7_final.pdf

IEEE, 2016. *Standards – IEEE Blockchain Initiative,* s.l.: s.n.

Košič, K., ČERNEC, R., BARNSLEY, A. & THOORENS, F., 2018. Building an open-source blockchain ecosystem with ARK. *OTS 2018 Sodobne informacijske tehnologije in storitve. 2018:45.*

L'Ecuyer, P. & Simard, R., 2007. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS) 33, no. 4 (2007): 1-40.*

Lockhart, H. & Parducci, B., 2020. *OASIS eXtensible Access Control Markup Language (XACML) TC.* [Online]
Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

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

Marsaglia, G., n.d. *DIEHARD Statistical Tests.* [Online]
Available at: https://tams.informatik.uni-hamburg.de/paper/2001/SA_Witt_Hartmann/cdrom/Internetseiten/stat.fsu.edu/source.tar.gz

Martin, K., 2017. Everyday Cryptography: Fundamental Principles and Applications. *2nd Edition, Oxford University Press.*

NIST 800-22, 2010. *Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications,* s.l.: National Institute of Standards & Technology.

NIST, 2014. *NIST Special Publication 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf

OASIS Security Services TC, 2008. *Security Assertion Markup Language (SAML) V2.0 Technical Overview.* [Online]
Available at: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

OpenID, n.d. *OpenID Connect.* [Online]
Available at: https://openid.net/connect/
[Accessed 2020].

Papadimitriou, O., 2009. *How Credit Card Transaction Processing Works: Steps, Fees & Participants.* [Online]
Available at: https://wallethub.com/edu/cc/credit-card-transaction/25511/

Spoke, M., 2017. Aion: The third-generation blockchain network. *Whitepa-per.*

Wood, G., 2016. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper.*

World Bank Group, 2019. *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits.* [Online]
Available at: http://documents1.worldbank.org/curated/en/954851578602363164/pdf/Prudential-Regulatory-and-Supervisory-Practices-for-Fintech-Payments-Credit-and-Deposits.pdf

Zcash/Zips, GitHub, n.d. [Online]
Available at: github.com/zcash/zips