

PhD of National Interest in Blockchain and Distributed Ledger Technology

Research Programme

38th Cycle

Academic Years 2022/2023 – 2024/2025

Table of content

Introduction	3
Aim of the document	3
Curriculum 1: Methodologies, technologies and tools	4
Keywords:	4
Curriculum 2: Social systems and smart societies	5
Keywords:	5
Curriculum 3: Health and well-being	6
Keywords:	6
Curriculum 4: Economics and finance	7
Keywords:	7
Curriculum 5: Law and Governance	8
Keywords:	8
Curriculum 6: Industry 4.0	9
Keywords:	9
Curriculum 7: Climate, energy and mobility	10
Keywords:	10
Curriculum 8: Agriculture and agrifood	11
Keywords:	11

Introduction

Blockchain and Distributed Ledger Technology provide building blocks of the so-called “Internet of Value”, since they enable recording of interactions and transfer “value” referring to any record of ownership of asset - for example, money, securities, land titles – and ownership of specific information like identity, health information as well as other personal data.

Almost any national and international strategic research, innovation and development agenda mentions Blockchain and/or Distributed Ledger Technology as key technologies and infrastructures enabling societal progress, with a particular emphasis when they mention at the undoubtedly strategic “digital and green twin transitions” (for example: “PNR 21-27 – the National Research Programme 2021 - 2027”, “PNRR 21-26 the National Recovery and Resilience Plan” and complementary funds).

In the era of the “twin technologies”, the National Doctoral Program in “Blockchain and Distributed Ledger Technology” aims to educate and train a new generation of researchers, professionals and innovators who can provide proper answers to the scientific and innovation emerging challenges from the private sector and public administration.

Aim of the document

This document describes the Research Programme for the Doctoral Research of National Interest in Blockchain and Distributed Ledger Technology (PhD-BC&DLT). The PhD is organized in eight curricula:

- Methodologies, technologies and tools
- Social systems and smart societies,
- Health and well-being,
- Economics and finance,
- Law and Governance,
- Industry 4.0,
- Climate, energy and mobility,
- Agriculture and agrifood.

The PhD is characterized by a strong interdisciplinary and multidisciplinary approach; an overview of the main research themes and scope of the curricula is provided below. Each curriculum offers several scholarships linked to research topics which are described in detail. In order to facilitate their reading by candidates, the information relevant to each scholarship is organized in a data sheet reporting:

- the **title** of the research topic;
- the **research keywords**;
- the **reference European Research Council** sectors which provide information on the research areas, and the list of ERC sectors (for a complete list of the ERC sectors visit the https://erc.europa.eu/sites/default/files/document/file/ERC_Panel_structure_2021_2022.pdf);
- the **reference person** – i.e. the individual, researcher or professor, offering the research topic and available to provide more information via email;
- the **host university** which is the location of the main research activity; in the case of the scholarships, University IUSS of Pavia will be where most of the common activities will be organized;
- the **research topic** describing the scope and objectives of the research in more detail;
- the **research team and environment** indicating where the research activities will be carried out and where most of the collaboration with other researchers and research institutes will be based;
- the **suggested skills** – i.e. the skills that, ideally, the candidate should possess in order to succeed in their doctoral research.

Curriculum 1: Methodologies, technologies and tools

Scholarships of Curriculum 1 are coded **A###**

The curriculum "Methodologies, technologies and tools" focuses on foundational aspects of Blockchain and Distributed Ledger Technology, considering both theoretical and applied research.

Methodologies play an increasingly important role in managing and defining blockchain and, more in general, distributed ledger solutions. A key point is the definition of novel and fault-tolerant distributed consensus mechanisms, cryptographic primitives, and distributed protocols. In particular, consensus mechanisms ensure the integrity of the information stored in blockchains and improve system efficiency and defense against attacks. Data privacy needs to be achieved as well as the opportunities and challenges of blockchain-based self-sovereign identities to guarantee complete control over people's digital identities.

Other research aspects cover but are not limited to blockchain software architectures and novel approaches to blockchain-oriented software engineering. Novel metamodelling approaches represent the groundwork for Blockchain and Distributed Ledger solutions. They can be both domain and domain-independent. Specialized blockchain modeling notations can support the advance in blockchain-oriented software. In this regard, modeling standards, such as UML, BPMN, and other domain-specific languages, can be adopted. It is necessary to improve the state of the art in creating blockchain smart contracts in a high-level and user-friendly modeling language, breaking the technological barriers for non-expert users.

Blockchain software analysis and re-engineering need to be investigated to support the quality of blockchain infrastructure, smart contracts, and related dApp. Optimization aspects are also considered to guarantee the efficiency of smart contracts execution. Formal specification and advanced automatic verification techniques need to be defined, and novel approaches for smart contract testing and auditing of blockchain transactions.

Blockchain technologies are based on adopting different infrastructures such as Ethereum, IOTA, Hyperledger ecosystem, etc. In this regard, recent challenges for the support of security, scalability, reliability, interoperability and performance issues in blockchain and smart contracts on multiple blockchain platforms should be addressed. Certainly of interests are also tools, including open-source software, allowing new specific scenarios such as token sales.

In the curriculum, we also expect to identify and examine the blockchain application in emergent scenarios, including blockchain's role in the metaverse.

Keywords:

- Foundational aspects of Blockchain and Distributed Ledger Technology
- Distributed ledgers
- Distributed Computing
- Metamodeling and Management
- Distributed consensus mechanisms, cryptographic primitives and distributed protocols
- Smart Contracts
- Modelling, analysis and verification
- Model-driven software development
- Dynamic Networks
- Metaverse

Curriculum 2: Social systems and smart societies

Scholarships of Curriculum 2 are coded **B###**

Blockchain technology is increasingly seen as a tool for boosting data transparency and traceability in smart societies and social systems. As a decentralized infrastructure, blockchain can support the management of networks emerging from smart societies, like offering transparent services for the citizens, sharing public data, supporting decentralized identities (Self Sovereign Identities). In the context of social media, we see a clear evolution toward a decentralized model. Web3 proposal claims a vision of the Internet that can cut the intermediation of Big tech companies by completely decentralizing the web. This new model of the Web largely revolves around blockchain technology, which enables the integration of cryptocurrencies and tokens in many social media platforms. This gives the possibility both to reward users for their social actions and to define Non Fungible Tokens (NFTs), digital assets representing real-world objects like art, music, game items, videos so creating a new form of decentralized finance, the Social Finance (SocialFi). These platforms offer a new model which promise to be more private, secure, uncensored and compensatory for their members and to offer quality and trustable contents to the society to overcome the many issues of traditional social systems including data and content rights and monetization, fake news and excessive trolling.

The curriculum is focused on blockchain for smart societies and social systems and will develop both theoretical and applicative competences to develop new solutions for these platforms.

a) Theoretical aspects: several new and challenging theoretical issues arise when considering new models of social interaction. For instance new game theory models are required to describe the dynamics of decentralized markets. To understand the interplay among the social and economic layers at different scale requires not only the support of the technicians, but also of sociologists, lawyers, economists. Furthermore, the huge amount of transactions that a social system may generate demands for new solutions for improving the scalability of current blockchain (off-chain channels, side-chains,...).

b) Applications: several new scenarios are currently arising for the application of blockchain in the context of social and smart communities. Among them, of utmost interest are the integration of rewards and tokens in social platforms, the integration of the blockchain with metaverses, the development of blockchain-based platforms for smart communities.

Keywords:

- Smart Cities e Smart Communities
- Transparency and traceability
- Services to Citizens, Companies and Public Administrations.
- Tokenization
- Cybersecurity
- Inter-ledger technologies
- Self-Sovereign Identity
- Non Fungible Tokens (NFT) and Web3
- Social Interactions
- Vulnerabilities

Curriculum 3: Health and well-being

Scholarships of Curriculum 3 are coded C##

The curriculum on "Health and well-Being" aims to advances in the study of blockchain and DLT in creating innovative and performing solutions to improve the trust between patients and healthcare organizations as well as among healthcare organizations every time data sharing is required. Being very sensitive, the sharing of health-related data requires the compliance with several norms and policies which can be defined at European, national, or even at organization level. In this context, Blockchain and DLT can be beneficial in providing trusted environments to monitor the actual respect of these norms and policies without requiring the building of a complex, and often centralized authority, in charge of checking the compliance and where also the patients can have a role.

In this curriculum, the adoption of blockchain and DLT will be investigated considering the different types and formats of data involved in clinical and research-trials related processes. In fact, the context of the "Health and well-being" domain includes data, data-at-rest, images, genomic data, unstructured data and the approaches to decide between on-chain off-chain data management to balance between the need for trust and the system performance cannot be defined in general but depends on the type of data considered. Moreover, the potential adoption of Blockchain and DLT will consider the connection with well-established protocols (e.g., HL7 in its new FHIR version and DICOM for diagnostic images) and common systems (e.g., PACS for managing images and CRF for setting experiments). Notably, the role of blockchain and DLT in improving the management of genomic data which involve the need to manage important artifacts with a significant size will be investigated. Finally, in conjunction with the usual and fundamental role of the ethic committee which must deliberate on the possibility to manage personal data, smart contracts can be studied to enact the policies in a more agile way.

Keywords:

- Healthcare services
- Hospital's data and automated management
- Healthcare data sharing
- Healthcare data protection
- Trust-based health environments
- Distributed Ledger Technology
- Electronic Health Records
- Privacy preserving data processing
- Etics and Etics Committee

Curriculum 4: Economics and finance

Scholarships of Curriculum 4 are coded **D###**

This curriculum is aimed at Ph.D. candidates who are interested in studying blockchain and distributed ledger technology in economics and finance with a multidisciplinary approach. As one of the most notable blockchain applications, this track will consider the socio-economic, legal, organizational, and technological aspects of cryptocurrencies, central bank digital currencies and non-fungible tokens (NFTs). These include: investigating the user trust and reputation mechanisms behind the shift from institutional, centralized currencies to digital, decentralized ones; assessing how financial and governmental institutions respond to the rise of cryptocurrencies, including the emergence of central bank digital currencies; analyzing cryptocurrency and NFT transactions for the detection of anomalies, frauds, suspicious behavior (cyber-crime), communities, and motifs; business models of token-based economies; developing anonymization and de-anonymization techniques; studying the interplay between cryptocurrency/NFT and social media/virtual worlds; exploring real consequences of virtual money from the metaverse, evaluating the performance and reliability of blockchain algorithms and implementations; analyzing the sustainability of digital ledgers in terms of their energy and environmental footprint, combining game theory, economics and cryptography to understand the incentive models underlying distributed blockchain protocols. The track will also be concerned with research in platform economies and smart contracts as a way to execute actions automatically when agreed-upon conditions are met. Furthermore, it will study communication/interactions protocols to allow blockchain participants to achieve a common goal. Ph.D. candidates will have the opportunity to explore: (programming) languages for the specification of smart contracts; techniques for the analysis and verification of correctness and compliance of smart contracts; legal and regulatory aspects; game theory applied to human-algorithm interaction; psychology of money. Ph.D. candidates in this track may also study blockchain in supply chain management for the digitalization and certification of trade documents and NFTs to protect intellectual property rights.

Keywords:

- Central Bank Digital Currency
- Credit market and financial services
- Illegal markets detection
- Internet of Money
- Valuation services and financial advising
- Business models for DLTs-based financial players
- The economics of DLTs-based financial markets
- Banking & Finance
- Digital asset/Crypto-assets
- Entrepreneurial finance

Curriculum 5: Law and Governance

Scholarships of Curriculum 5 are coded E##

The curriculum on Law and Governance aims to investigate the advanced research questions in three directions:

Theoretical aspects. The blockchain represent a new form of social organization, another type of power, distinct method of decision that indubitable would change the relationships between the institutions, authorities, citizens. That arises relevant questions concerning the legitimacy of the activities conducted in the blockchain, or the validity of the smart legal contracts applied especially in some sectors like the law-making process, justice decisions, and administration services. The autonomy of the decision-maker is fundamental for preserving the normativity of the legal rules and the self-execution of the smart contracts stress some theoretical aspects and pillars of our democracy. The control of the human being in any step of these technologies is another important topic of research investigation in order to avoid manipulation, surveillance, and black-box effect.

Regulation. This track aims to research how to regulate the introduction in the society of the blockchain, distributed ledger technology, smart contract, ICO, NFT and any other connected technologies. It is fundamental to define a stable regulation in its legal foundations (e.g., theory of law) and in the specific domains (e.g., FinTech, Bank, Civil law, Labor Law, Tax Law, etc.) for supporting the emerging market. Furthermore, an international law view is necessary (e.g., UNCITRAL, UNIDROIT, HCCH) for avoiding fragmentation. On the other hand, the European Blockchain Service Infrastructure could be an occasion for regulating at the European supra-national level some principles including the digital identity. The proposal of modifications of regulation eIDAS 910/2014 aims to introduce qualified certifications for the distributed electronic ledger and it is another important example of how the regulation is shaping the emerging sector of the intermediation and disintermediation introduced by the blockchain. Another important topic to investigate is how to protect personal data and how to apply the regulation of GDPR in this context. Finally, the responsibility and liability of the effects of the smart legal contracts is a key issue that needs groundbreaking specific interdisciplinary research. All these topics require an interdisciplinary approach.

Applications. This track aims to research how to apply the constellation of blockchain technologies to the legal domain (e.g., Parliaments, Justice, Administration, Legal Firm, Anti-Money-Laundering, Anti-corruptions, etc.) and to other domains with the goal to guarantee the compliance with the legal framework. All the applications must be law-by-design and it requires legal expertise combined with technological competencies for transforming advanced solutions into market products or services. Some solutions include also legal reasoning and legal argumentation for checking the compliance before the self-execution. Several principles would be included in the applications: transparency, accountability, respect for human rights, privacy, and liability. Human-centered design is fundamental and, in this perspective, also the human-computer interactions devoted to providing usability and explicability are a key goal of this track."

Keywords:

- Smart Legal Contract
- Intelligible Contract
- Self-Sovereign Identity
- Legal reasoning
- Regulation
- Blockchain forensic
- Anti-money laundering, anti-corruption
- Private standards
- Compliance
- Business models

Curriculum 6: Industry 4.0

Scholarships of Curriculum 6 are coded F##

Industry 4.0 includes a new business vision that triggers innovation and adds value into the business by means of the integration of new pervasive ICT technologies (IoT, cloud and edge computing, AI and Machine / Deep learning) into services, products and production plants in order to provide the industrial production system with greater automation and responsiveness, efficiency, automatic optimization of process improvements etc. An important issue for a pervasive usage of Industrial Internet of Things (IIoT) entails accountability requirements for them that can be dealt with using blockchain technologies.

The curriculum on Blockchain and Industry 4.0 focuses on blockchain research for Industry 4.0 applications and covers both application and theoretical aspects. Research issues cover, but are not limited to digital user identity and accountability across business units and consortiums, scalability, interoperability and trust in blockchain systems for IIoT, transparency, information sharing, and privacy control in the next-generation of Blockchain Technology for smart applications.

The curriculum is aimed at training blockchain experts capable of guiding the integration process of Blockchain in innovative scenarios of Industry 4.0. To this end, a direct involvement of organizations playing a major role in this topic is envisioned.

Keywords:

- Technology integration in Industry
- Internet of Things
- Machine learning
- Consensus protocol
- Distributed ledger security
- Blockchain security
- Accountability
- Services, products and supply chain
- Business organization

Curriculum 7: Climate, energy and mobility

Scholarships of Curriculum 7 are coded **G###**

The curriculum on blockchain for climate, energy and mobility focuses on the key strategic orientations of the latest H2020 work programme. The objective is to provide blockchain technology and smart contracts for promoting an open, strategic, and distributed approach in the energy value chains.

Many climate programs have been established over the years. However, the intrinsic multi-lateral and international approach brings many difficulties in linking the political commitment to the technical involvement and contribution, for example, in reducing greenhouse gas emissions. First, the curriculum will study the contribution of blockchain to transparency, traceability, and trust in environment-related programs. Then it will focus on accelerating and steering the digital and green transitions through human-centred approaches and innovations. Creating more resilient, inclusive, and democratic European energy systems will prepare them to respond better to threats and disasters. Distributed energy resources (DERs) call for distributed data collection and management (smart meters, production plans, prosumers). Removing the information asymmetry between DSO, TSO, and citizens will empower them to act in the green and digital transitions.

This curriculum will study distributed methodologies to strengthen the digitally-enabled circular, climate-neutral and sustainable economy through the technical management of energy networks, the aggregation of production in virtual power plants, the management of networks for energy distribution, and the creation and management of energy communities. Attestation and validation of methodologies of energy production will distinguish the cases of green and environmental-friendly production from the traditional ones, especially for blue, green and grey hydrogen. The use of the blockchain will be applied to breakthrough business models and programs in the energy sector and energy mobility (Demand-Response, Vehicle to Grid, energy communities, certification of self-consumption, etc.). Additionally, tracking and tracing batteries for electric mobility, including managing the logic for monitoring their health status, enable such batteries to be used in second-life applications: when they are not good anymore for traction, they still maintain most of their capacity. The application-level challenges described above will be faced with innovative theoretical approaches for guaranteeing privacy (e.g. joining Secure Multiparty Computation to blockchain), security (blockchain and Attribute-based Encryption), and wide adoption (studying the relation between natural language contracts of the energy sector and smart contracts).

Keywords:

- Energy value chains
- Environment
- Disaster monitoring and management
- Resilient and inclusive energy systems
- Environmental data management
- Circular Economy
- Energy communities
- Sustainable mobility
- Battery traceability
- Smart Contracts

Curriculum 8: Agriculture and agrifood

Scholarships of Curriculum 8 are coded **H###**

The Phd candidate will study how current and next generation blockchain can support increased traceability and transparency in food supply chains and support the implementation of green and sustainable schemes. The subject of the study will cover both the application and the theoretical aspects.

From the application side, the study will contribute to the ambition of developing sustainable, productive and climate-neutral, biodiversity-friendly, and resilient farming systems providing consumers with affordable, safe, healthy and sustainable food, minimizing pressure on ecosystems, improving public health and generating fair economic returns for farmers through the exploration and development potential of the use of blockchain in the agri-food sector.

From the theoretical side, all the aspects of tracing, integrity, authentication, identification (covering also Self Sovereign Identity thematics) making use of blockchain will be considered. Characteristics of DLTs to be applied in agrifood with special attention to green and sustainability concerns will be exploited.

Keywords:

- Food supply
- Smart agriculture
- Sustainable cultivation
- Traceability
- Transparency
- Sustainable agricultural systems
- Information asymmetry
- Biodiversity and resilience
- Conscious consumption

Code	Research Topic Host	Host University
Curriculum 1: Methodologies, technologies and tools		
A01	Enterprise architecture for blockchain	University of Camerino
A02	Energy saving approaches in Blockchain technology	University of L'Aquila
A03	Analysis and verification of smart contracts with behavioural types	Gran Sasso Science Institute
A04	Engineering of trustworthy blockchain-aware applications	University of Firenze
A05	Noninterference and Reversibility Analysis in Private Blockchains	Ca' Foscari University of Venezia
A06	Dynamic Networks and Foundations of Layer-Two Blockchain Protocols	University of Roma "Tor Vergata"
A07	Smart Contracts Analysis, Verification and Testing	University "G. d'Annunzio" of Chieti-Pescara
Curriculum 2: Social systems and smart societies		
B01	DLT approaches for social applications: enhancing scalability, privacy and reliability	University of Pisa
B02	Trusted interactions in a trustless network	University of Pisa
B03	Cyber security of smart contracts for a tokenized economy	University of Milano Bicocca
B04	Blockchain for social systems and smart technologies	University of Torino
B05	Blockchain for sustainable cities and communities	University of Torino
Curriculum 3: Health and well-being		
C01	Efficient and privacy preserving management of health data based on Distributed Ledger Technology	University of Milano
C02	Blockchain and Distributed Ledger Technology (DLT) to share and protect hospitals' data	Marche Polytechnic University
Curriculum 4: Economics and finance		
D01	Blockchain and smart contracts in banking, finance and insurance	Università Cattolica del Sacro Cuore
D02	Tokenization and notarization to support SMEs' finance	University of Milano Bicocca
D03	Security of Blockchain Systems	IMT School for Advanced Studies Lucca
D04	Distributed Ledger Technology systems in credit markets and securities trading services	Marche Polytechnic University
D05	Distributed Ledger Technology for Digital Money	University of Urbino
D06	Blockchain in accounting	University "G. d'Annunzio" of Chieti-Pescara
D07	Economic aspects of blockchain and DLT systems	IMT School for Advanced Studies Lucca
Curriculum 5: Law and Governance		
E01	Legal compliance and Blockchain in the agri-food sector	University of Macerata
E02	Legal and technical analysis of Intelligible Smart Legal Contract based on Legal Reasoning in the European Regulation Framework.	University of Bologna
E03	The Law and Governance of Disintermediation Business Models	University of Firenze
Curriculum 6: Industry 4.0		
F01	Off-chain Execution of Smart Contracts on IoT Constrained Devices	University of Camerino
F02	Novel Secure and Efficient Consensus Algorithms	University of Padova
F03	"Accountability" mechanisms and procedures based on Distributed Ledger Technology	University of Calabria
Curriculum 7: Climate, energy and mobility		
G01	Blockchain Oriented Software Engineering and Applications	University of Cagliari
Curriculum 8: Agriculture and agrifood		
H01	Implementation of blockchain based smart agriculture systems	University of Bari "Aldo Moro"
H02	Blockchain and smart contracts for data quality and contrasting counterfeits in the agri-food sector	University of Palermo

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A01

Research Title: Enterprise architecture for blockchain

Research Keywords:

- Blockchain as a service
- Software architecture for blockchain
- Interoperability between blockchains
- Verification, validation, and auditing in blockchain

Reference European Research Council:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_3 Software engineering, programming languages, and systems
- PE6_4 Theoretical computer science, formal methods, automata

Reference Person:

Barbara Re, University of Camerino, barbara.re@unicam.it

Host University and Department: University of Camerino, Computer Science Division

Research Topic: Nowadays, in an interconnected society, there is a growing need for coordination among different organizations, asking for trust-aware solutions to develop advanced distributed systems. To achieve an effective digital transformation, there is also the need for closing the gap between business and supporting technology. Both academia and industry are showing an increasing interest in blockchain. However, for a large adoption of this technology, different challenges should be addressed, especially what concerns the support of **multiple blockchain platforms** and the generation of the related **smart contracts**. The aim of the Ph.D. project is to provide direct access to the blockchain potentialities breaking the technological barriers for non-expert users. Furthermore, the immutability of blockchain transactions enables the definition of **automatic analysis techniques** making possible the adoption of a certified **auditing** phase for controversy resolution. The achieved results should be evaluated in real-world scenarios, to prove the applicability and effectiveness of the solutions proposed.

Research Team and environment: The Computer Science Division at the University of Camerino is composed of senior professors as well as researchers in the early stages of their careers. The research will be conducted in a collaborative environment in the PROCesses & Services lab, where teamwork is a fundamental aspect of the group’s success. Research in computer science, carried out within the PROS Lab, deals with the development of languages and techniques for the modeling, analysis, and development of process-aware information systems and blockchain-based applications. We strive for personal development with plenty of opportunities for collaboration with students, researchers, and industry partners. The Ph.D. will also be mentored to develop their own research career (e.g., writing a Ph.D. thesis, applying for project funding, preparing auditions for academic positions) and getting on board with ongoing publications, collaborations, and projects in the Computer Science team. Camerino is a lively and beautiful town in the center of Italy not far from the seaside, it is internationally known for its high concentration of researchers and international students.

Suggested Skills: Ideally, the successful candidate should have a good background in Computer Science. A good level of skills in mathematical modeling and reasoning as well as in software engineering and programming is also required. Experiences with carrying out independent and collaborative research are merits.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A02

Research Title: Energy saving approaches in Blockchain technology

Research Keywords:

- Blockchain
- Public-key Cryptography
- Distributed ledgers

Reference European Research Council:

- PE6_4 Security, privacy, cryptology, quantum cryptography
- PE6_6 Algorithms, distributed, parallel and network algorithms, algorithmic game theory

Reference Person:

Riccardo Aragona, University of L’Aquila, riccardo.aragona@univaq.it

Host University and Department:

University of L’Aquila, Department of Information Engineering, Computer Science and Mathematics

Research Topic:

The proposed research topic concerns the study of Blockchain and Distributed Ledger technologies. It is our interest to deepen its theoretical, implementation and application aspects. From a theoretical point of view, we want to tackle the analysis and development of new models. Possible innovative impacts to be analyzed, and possibly developed, in these models are the improvement of data security and eco-sustainability, i.e. through the introduction of alternative procedures at lower energy costs. Another area to inspect concerns the simplification of the use of these technologies, reducing the complexity of IT procedures and making them implementable on devices with low energy consumption and reduced computing capability, such as smartphones or tablets.

Research Team and environment:

DISIM hosts Mathematicians, ICT Engineers and Computer Scientists who extensively cover disciplinary fields related to the proposed research: Cryptography and Cyber Security; Algebra and Algebraic Geometry; Algorithmic and Computational aspects of Distributed Systems; Algorithmic Aspects of Game Theory.

Suggested Skills:

Ideally the successful candidate should have a background in Distributed Systems (in particular some notions of Blockchain and Distributed Ledger Technology) and basic mathematical aspects of Cryptography. Moreover, the candidate should have basic knowledge of Algebra and Geometry underlying Cryptography, and should know main programming languages.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A03

Research Title: Analysis and verification of smart contracts with behavioural types.

Research Keywords:

- Smart Contracts
- Behavioural Models
- Program Analysis

Reference European Research Council:

- PE6_3 Software engineering, programming languages and systems
- PE6_4 Theoretical computer science, formal methods, automata
- PE6_5 Security, privacy, cryptology, quantum cryptography

Reference Person Maurizio Murgia, Gran Sasso Science Institute, maurizio.murgia@gssi.it

Host University and Department Gran Sasso Science Institute, Area of Computer Science

Research Topic: Behavioural types are formal models which, in the past couple of decades, have been extensively (and successfully) applied to the verification of many classes of concurrent and distributed systems. However, very little has been done for their application to smart contracts or blockchains. The aim of this project is to enrich theory and/or practice of behavioural types in the blockchain setting. For instance, behavioural types can be used for modelling smart contracts behaviour. The model can then be analyzed for correctness with standard techniques (e.g. model checking, static analysis,...). Compliance of the model with the actual smart contract code can be verified through type-checking or enforced through code-generation.

Research Team and environment: The main research activities will be carried out at the GSSI, Computer Science Area. In particular, the research topics of the scholarship fits well within the activities of the Formal Methods Group composed by two professors, three researchers and two post-doc. The group investigates formal specification, analysis, synthesis, and verification of concurrent and distributed systems. Our research spans a broad range of topics from languages, to semantic models, to software verification. The group is active on several national and international projects and among its many collaborations, the ones with the Universities of Cagliari, Lisbon, and Trento focus on the topics of the scholarship.

Suggested Skills: The ideal candidate should have the ability to understand (and reason about) formal models of distributed systems, and possibly skills in program analysis. Previous experience in programming smart contracts, in any platform, is not strictly required but very appreciated.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A04

Research Title: Engineering of trustworthy blockchain-aware applications

Research Keywords:

- Formal languages
- Verification
- Model-driven software development
- Blockchain-based applications

Reference European Research Council:

- PE6_3 Software engineering, programming languages and systems
- PE6_4 Theoretical computer science, formal methods, automata

Reference Person: Francesco Tiezzi, Università degli Studi di Firenze, francesco.tiezzi@unifi.it

Host University and Department: Università degli Studi di Firenze - Dipartimento di Statistica, Informatica, Applicazioni ‘G. Parenti’ (DiSIA)

Research Topic: Software applications increasingly exploit Blockchain technology to inject the needed trust without a trusted party. Nevertheless, the existing developing methodologies lack support to: structure a blockchain-based application according to specific needs; program the interactions with the blockchain intuitively; ensure the trustworthiness of the application’s behavior with respect to non-functional requirements established by the developer. This poses the following major challenges: finding the appropriate abstraction level of programming languages; devising effective solutions for driving developers in dealing with various, possibly conflicting, requirements imposed by blockchain; formally ensuring that the low-level code preserves the properties verified at the high-level. The research activity will address these challenges by defining an *engineering methodology for developing blockchain-based applications relying on formal languages and techniques for supporting developers throughout the whole application lifecycle*. The languages to be developed will incorporate, as first-class elements, abstractions and linguistic primitives for storing and retrieving data from the blockchain. This capability is essential for achieving *blockchain-aware programming*, where applications can explicitly refer to data and functions in the blockchain. Another distinctive feature of the methodology will be the use of formal methods for: verifying properties at a high level of abstraction; partitioning the application in code to be deployed in the blockchain and code to be executed in the runtime environment; preserving properties at the low level of abstraction via secure compilation.

Research Team and environment: The main hub of the research activity will be the Dipartimento di Statistica, Informatica, Applicazioni ‘G. Parenti’ (DiSIA, <https://www.disia.unifi.it/>) of the Università degli Studi di Firenze (<https://www.unifi.it/>). DiSIA is one of the Departments of Excellence 2018-2022 and is admitted to the selection of the Departments of Excellence 2023-2027. The research group involved in the activities related to this scholarship has strong expertise and long experience in developing engineering methodologies based on formal methods, including definition, formalization, verification, and implementation of DSLs. More recently, this approach has been applied to the blockchain domain.

Suggested Skills: The ideal candidate should have a good background in programming languages and, possibly, in formal methods and/or smart contracts. Anyone interested in Blockchain topics and enthusiastic about research is welcome to apply. Personal initiative, curiosity, and a positive, collaborative, hands-on attitude are a big plus.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A05

Research Title: Noninterference and Reversibility Analysis in Private Blockchains

Research Keywords:

- theoretical computer science
- formal methods in computer science
- parallel and distributed systems
- stochastic processes
- computer security and privacy
- reversible computing

Reference European Research Council:

PE6_4 Theoretical computer science, formal methods, and quantum computing

Reference Person: Sabina Rossi, Ca' Foscari University of Venice, sabina.rossi@unive.it

Host University and Department:

Ca' Foscari University of Venice

Department of Environmental Sciences, Informatics and Statistics

Research Topic:

Distributed computing has by now become a pervasive technology due to the widespread adoption of electronic devices connected by the Internet infrastructure, which are used by individuals, companies, and institutions to perform an increasing number of activities in a digital mode. One of the most prominent examples over the last decade is blockchain technology. This is a distributed ledger that permanently records transactions taking place among untrusted parties in a decentralized and disintermediated environment, which was devised to avoid the double spending problem in virtual currency platforms. A number of shortcomings affect public, permissionless blockchains, including conflicts between data immutability and regulations. In the specific case of innovative payment methods, there are also risks of losing monetary sovereignty and undermining financial stability, as witnessed by the fact that many central banks are exploring the issuance of what is called central bank digital currency (CBDC). For these reasons private, permissioned blockchains are getting momentum, as they could ultimately give businesses a greater degree of control. This PhD project proposal is about the use of formal methods for the compositional modeling of functional and non-functional aspects of the behavior and the structure of private blockchains. On the analysis side, relevant properties such as noninterference and reversibility are planned to be explored. The former is concerned with the absence of information leakage, due to qualitative or quantitative covert channels, from the private blockchain governance to permissioned users. The latter deals with undoing transactions, because of regulation compliance, in a way that timely brings the system in a previous consistent state.

Research Team and environment: The main hub of the research activities will be the Networking and Distributed Systems Lab of the Department of Environmental Sciences, Informatics and Statistics at the Ca' Foscari University of Venice. The group includes scientists with skills on formal methods for system verification, automated verification tools, performance evaluation and reliability analysis of computer and telecommunication systems, system and network security, cryptography. Currently the team is composed by six professors, three postdocs, three PhD students. The lab has international collaborations in Europe with e.g., School of Informatics at the University of Edinburgh, School of Computing at Newcastle University, and Department of Computing at Imperial College London.

Suggested Skills: The candidate should ideally be with a quantitative background, i.e., master's degree and PhD in Physics, Computer Science or Applied Mathematics with experience in computational tools, programming languages, data analysis. Candidates should possess English language skills.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A06

Research Title: Dynamic Networks and Foundations of Layer-Two Blockchain Protocols

Research Keywords:

- Distributed Computing
- Layer 2 Blockchain Protocols
- Dynamic Networks
- Randomized algorithms

Reference European Research Council:

- PE6_6 Algorithms and complexity, distributed, parallel and network algorithms, algorithmic game theory
- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE1_17 Mathematical aspects of computer science

Reference Person:

Francesco Pasquale, Università di Roma “Tor Vergata”, francesco.pasquale@uniroma2.it

Host University and Department:

Università di Roma “Tor Vergata”, Dipartimento di Ingegneria dell’Impresa “M. Lucertini”.

Research Topic: One of the obstacles to large-scale adoption of Bitcoin is the scalability problem related to the number of transactions that can be included in a block. A natural trade-off between scalability and decentralization actually exists in essentially all blockchains. Several approaches have been proposed and implemented so far to overcome the scalability barrier. The focus of this research topic is on one of such approaches: Layer 2 Blockchain protocols, in which an overlay network of channels between nodes is used and transactions are recorded on the main blockchain only in specific circumstances. The main goal of the research will be to explore the impact of the dynamics of the network of channels on the reliability, decentralization, and security of Layer 2 blockchain protocols.

Research Team and environment: The successful candidate will join the Distributed Computing research team at the Enterprise Engineering Department of the University of Rome "Tor Vergata", a lively research environment formed by faculty members, postdocs and PhD students. The current main research interests of the team are centered on design and analysis of distributed algorithms, with a newborn research lab focused on cryptocurrencies and blockchains. The team closely collaborate with members of European institutions like INRIA/CNRS in France as well as other Italian universities like Sapienza University of Rome and Bocconi University.

Suggested Skills: The ideal candidate has a solid background in computer science and mathematics (algorithms, cryptography, discrete probability), experience with Unix-like operating systems and some tools (Bash, Git), proficiency in at least one programming language, and strong attitude to problem solving.

Curriculum 1 “Methodologies, technologies and tools”, Scholarship code: A07

Research Title: Smart Contracts Analysis, Verification and Testing

Research Keywords:

- Smart contracts
- Program analysis
- Program verification
- Software testing
- Constrained Horn Clauses
- Satisfiability Modulo Theories

Reference European Research Council:

- PE6_3 Software engineering, operating systems, computer languages
- PE6_4 Theoretical computer science, formal methods, and quantum computing

Reference Person: Prof. Fabio Fioravanti, University “G. d’Annunzio” of Chieti-Pescara, fabio.fioravanti@unich.it

Host University and Department: University “G. d’Annunzio” of Chieti-Pescara, Department of Economic studies

Research Topic: Smart contracts are computer programs that specify and enforce the execution of contracts and agreements by automatically performing predetermined actions when some events happen or some conditions are met. The project aims to develop methods for providing formal guarantees about correctness and resource consumption of smart contracts. The activity will mainly rely: (i) on the use of logic formalisms, e.g. constrained Horn clauses (CHC), for representing smart contracts, such as Ethereum contracts written in the Solidity language, and the properties of interest and (ii) on the development of techniques for static analysis, verification and testing of smart contracts possibly combining abstraction, symbolic execution and satisfiability modulo theories (SMT).

Research Team and environment: The research activities will be carried out at the Computational Logic and Artificial Intelligence Laboratory of the University of Chieti-Pescara. The research team is composed by professors with proven experience in theoretical and applied research in computational logic and, in particular, in formal methods based on CHC transformation, abstract interpretation and SMT solvers for analysis, verification and testing of software, systems and processes with the goal of ensuring their correctness and security. The team has international collaborations with members of academic and research institutions in Europe and America. Department facilities include access to static analysis and verification software and powerful computational resources.

Suggested Skills: Ideally, the candidate should have a good background in computational logic, programming language semantics and formal methods for analysis, verification and testing.

Curriculum 2 “Social systems and smart societies”,

Scholarship code: **B01**

Research Title: DLT approaches for social applications: enhancing scalability, privacy and reliability

Research Keywords:

- Scalability
- Privacy
- Blockchain Oracles
- Inter-ledger technologies
- Self-Sovereign Identity
- Non Fungible Tokens (NFT) and Web3

Reference European Research Council:

- PE6_2 Computer systems, parallel/distributed systems, sensor networks, embedded systems, cyber-physical systems
- PE6_3 Software engineering, operating systems, computer languages
- PE6_5 Cryptology, security, privacy, quantum crypto

Reference Person: Laura Emilia Maria Ricci, Department of Computer Science, University of Pisa, laura.ricci@unipi.it

Host University and Department

University of Pisa, Department of Computer Science.

Research Team and environment The research activities will be held at the Pisa Distributed Ledger Laboratory (<https://sites.google.com/unipi.it/pisadlrlaboratory>), led by Professor Laura Ricci, who has been member of the group for the definition of the Italian National Strategy for Blockchain Technology. The Laboratory includes 2 Full Professor, 3 Research with temporary positions and 3 PhD students. The group has both national collaborations with CNR and international collaboration, among the others, with the University of Cambridge and the Ethereum foundation.

Research Topic

After the initial disruptive outbreak in the area of cryptocurrencies, the Distributed Ledger Technology (DLT) underlies many new innovative applications that can change the way people socialize and interact in everyday life. Self-Sovereign identity (SSI) creates persistent identities of people and IoT objects without the need of centralized entities, Non Fungible Tokens and (NFT), Web3 and the metaverse enable the creation of scarce digital objects used to mint unique version of artworks, collectibles etc. To make these DLT applications really pervasive, some technological pitfalls have still to be solved. The research program is centered on the investigation and the proposal of solutions to overcome these pitfalls. In particular, the topics of the blockchain scalability, of the privacy vs. the auditability, of the definition of blockchain oracles, of the inter-ledger technologies, and, in general, of layer-2 technologies, will all have a central role in the research program.

Suggested Skills: Ideally, the successful candidate should have strong background in computer science. Basic competence in the area of cryptography are considered an asset, but not strictly required.

Curriculum 2 “Social systems and smart societies”,

Scholarship code: **B02**

Research Title: Trusted interactions in a trustless network

Research Keywords:

- Social Interactions
- Trust
- Authenticated Data Structures

Reference European Research Council:

- PE6_2 Computer systems, parallel/distributed systems, sensor networks, embedded systems, cyber-physical systems
- PE6_3 Software engineering, operating systems, computer languages
- PE6_5 Cryptology, security, privacy, quantum crypto

Reference Person:

Laura Emilia Maria Ricci, Department of Computer Science, University of Pisa, laura.ricci@unipi.it

Host University and Department

University of Pisa, Department of Computer Science.

Research Team and environment The main hub of the research activities will be the Pisa Distributed Ledger Laboratory (<https://sites.google.com/unipi.it/pisadl laboratory>), lead by Professor Laura Ricci, who has been member of the group for the definition of the National Strategy for Blockchain Technology. The Laboratory includes two full Professor, 3 Research with temporary positions and 3 PhD students. The group has international collaboration with the University of Cambridge and with the Ethereum foundation. The research will be conducted in collaboration with TRAENT(<https://traent.com/>), an innovative start-up located in Pisa operating in the blockchain area.

Research Topic

The technical solutions used to create trust in a network of trustless agents generally involve the presence of centralized authorities. The recent distributed ledger technologies (DLT) has put in evidence an alternative approach which shows that trust can also be achieved by the verifiability of the interactions collected in a distributed shared ledger. By avoiding the introduction of a centralized system, it is also possible to preserve the anonymity of the agents. Even if the first applications of DLT have been cryptocurrencies, now they are applied in different areas. The main focus of the research will be to investigate the use of the blockchain to integrate multiple information systems across organizational boundaries enhancing collaboration and trust. The research program will investigate the full spectrum of technologies, from centralized to fully decentralized, able to create trust among mutually untrusted agents. The main aim is to create a system able to support collaborative, sustainable and ethical behavior of interacting entities. The focus of the research program will be the study of advanced cryptographic techniques as enablers for new verification scenarios (verifiable data structures, Zero-knowledge proofs, multi-party,...).

Suggested Skills: Ideally, the successful candidate should have strong background in computer science, in particular in the area of networking. Some basic competence in the area of cryptography are considered an asset, but not strictly required.

Curriculum 2 “Social systems and smart societies”,

Scholarship code: **B03**

Research Title: Cyber security of smart contracts for a tokenized economy

Research Keywords:

- Tokenization
- Cybersecurity
- Smart contract
- Vulnerabilities

Reference European Research Council:

- PE6_5 Security, privacy, cryptology, quantum cryptography
- PE6_3 Software engineering, programming languages and systems
- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems

Reference Person

Giovanni Denaro, University of Milano - Bicocca, giovanni.denaro@unimib.it

Host University and Department:

University of Milano - Bicocca: Department of Informatics, Systems and Communication; Department of Business and Law; School of Law

Research Topic:

Tokenization processes exploit the blockchain ecosystems to trustily store and transfer information and values. Crypto tokens can be programmed to serve many interesting use cases in a wide range of sectors, including cryptocurrencies, but also many other types of tangible and intangible assets, e.g., security assets, real estate assets, ownership rights and content licensing. At the same time, the asynchronous and non-sequential model of execution of transactions, as well as the permissivity of the programming languages that are used to write smart contracts, boosts the exposition of these processes to unprecedented vulnerabilities, increasing the risks for the users to undergo dangerous losses. The project aims to contribute new results, tools and methods to prevent, mitigate, identify and ultimately avoid these vulnerabilities, in particular with tight focus on the design and analysis of the smart contracts that are involved with the tokenization processes. A distinctive point of the project will be the aim to synergistically combine the technical means that will be studied, with the economic and juridical aspects of the application scenarios that will be considered.

Research Team and environment

The main hub of the research activities will be both the Bicocca Security Lab and the Laboratory of Software Test and Analysis. Both labs are part of the Department of Informatics, Systems and Communication of the University of Milano - Bicocca. The research team includes scientists with expertise in blockchain technology, cybersecurity, cryptography, programming languages and software analysis. The project will be carried in tight collaboration with research teams from both the Department of Business and Law, and the School of Law of the university, to elicit the requirements and the means involved with the economic and juridical aspects of the research.

Suggested Skills:

Ideally the successful candidate should have strong interest in the research topic, and own good background in computer science, software programming and computer security. Possible experience with blockchain and smart contract technologies are considered relevant assets.

Curriculum 2 “Social systems and smart societies”,

Scholarship code: **B04**

Research Title: Blockchain for social systems and smart technologies

Research Keywords:

- Distributed ledger technologies
- Tokenization
- Financial inclusion
- Smart communities

Reference European Research Council:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_5 Security, privacy, cryptology, quantum cryptography

Reference Person:

Claudio Schifanella, Department of Computer Science, University of Turin, claudio.schifanella@unito.it

Host University and Department:

University of Turin, Department of Computer Science, Department of Law

Research Topic: Blockchain technology, as decentralized infrastructure, can support the management of networks emerging from small and local communities where citizen collaborate with local stakeholders, like public administrations, associations, etc to develop social well-being. The proposal is focused on the study and the development of new blockchain-based platforms for smart communities, based on new models and tools where the use of rewards, tokenization and smart contracts in existing platforms can lead to the development of new tools for the local financial inclusion of citizen and the co-creation of public services.

Research Team and environment: (around 700 chars) The research activities will be coordinated and carried out at the Computer Science Department of the University of Turin. The research group at the Department of Computer Science is made up of researchers with different profiles and backgrounds, and has a long experience on Distributed Ledger Technologies, demonstrated by the participation in different national and international research projects (Co-City, CO3, NLAB4CIT, PININ, Blinc)

Suggested Skills: Successful candidates will have earned either a MSc degree (or equivalent) in Computer Science or a related field. They should have a good background on the fundamentals of blockchain technologies. Programming skills in commonly used programming languages for the creation of decentralized applications are an asset.

Curriculum 2 “Social systems and smart societies”,

Scholarship code: **B05**

Research Title: Blockchain for sustainable cities and communities

Research Keywords:

- Distributed ledger technologies
- Tokenization
- Financial inclusion
- Smart communities

Reference European Research Council:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_5 Security, privacy, cryptology, quantum cryptography

Reference Person:

Claudio Schifanella, Department of Computer Science, University of Turin, claudio.schifanella@unito.it

Host University and Department:

University of Turin, Department of Computer Science, Department of Law

Research Topic: The goal of this proposal is to investigate and research on blockchain-based solutions to enable and incentivize smart sustainable and community-led behaviors and to answer specific needs and challenges in a variety of fields (energy, health and well-being, mobility, social services, tourism, climate adaptation and mitigation, education) in urban and rural environments. By advancing the state of the art in Decentralized Applications, the PhD student will demonstrate the potential impact of blockchain in the context of smart cities, contributing to provide a set of transparent tools and common measures of the sustainability level of the involved communities to increase citizens’ and local stakeholders’ awareness and involvement in the implementation of urban and social innovation initiatives.

Research Team and environment: (around 700 chars) The research activities will be coordinated and carried out at the Computer Science Department of the University of Turin, in close collaboration with the Links Foundation (<https://linksfoundation.com/en/>) based in Turin, where a research period of 18 months will be carried out. The research group at the Department of Computer Science is made up of researchers with different profiles and backgrounds, and has a long experience on Distributed Ledger Technologies, demonstrated by the participation in different national and international research projects (Co-City, CO3, NLAB4CIT, PININ, Blinc)

Suggested Skills: (around 300 chars) Successful candidates will have earned either a MSc degree (or equivalent) in Computer Science or a related field. They should have a good background on the fundamentals of blockchain technologies. Programming skills in commonly used programming languages for the creation of decentralized applications are an asset.

Curriculum 3 “Health and well-being”,

Scholarship code: C01

Research Title: Efficient and privacy preserving management of health data based on DLT

Research Keywords:

- Distributed Ledger Technology
- Electronic Health Records
- Privacy preserving data processing

Reference European Research Council:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_5 Security, privacy, cryptology, quantum cryptography
- PE6_6 Algorithms and complexity, distributed, parallel and network algorithms, algorithmic game theory

Reference Person

Stelvio Cimato, Università degli studi di Milano, stelvio.cimato@unimi.it

Host University and Department

Università degli studi di Milano, Dipartimento di Informatica

Research Topic: The efficient management of the patient’s Electronic Health Record (EHR) is crucial for taking care of patients’ health in different scenarios, including telecare. The sharing and distribution of health data however poses many problems related to the privacy and security requirements, contrasting with the need of processing and accessing information. Due to their intrinsic security properties (immutability, traceability, etc.), distributed ledger technology has been introduced as viable solution for achieving EHR sharing with privacy and security preservation. Differently from centralized systems, DLT technologies can be deployed to provide platforms for the efficient sharing of e-health data generating irreversible and permanent records of patients, achieving efficient and traceable data-sharing schemes for e-medical records. The candidate will investigate the application of DLT technologies to achieve different security properties related to the implementation of an e-health data sharing platform.

Research Team and environment:

The research activities will be hosted within the SESAR Lab at the Department of Computer Science at the Università degli studi di Milano. SESAR Lab is a major technology transfer centre operating with a number of EU industrial partners in cloud computing, SLAs, and service/software assurance for Big Data, embedded, telecommunication, and health-related systems. The research group is/has been involved in a number of national and International research projects, including several FP7 and H2020 projects (SECURE-SCM, PRACTICE, TOREADOR, THREAT-ARREST, AERAS, etc).

Suggested Skills: Ideally the candidate should have a good background on data security and cryptographic protocols with a basic knowledge on distributed ledger technology.

Research Title: Blockchain and Distributed Ledger Technology (DLT) to share and protect hospitals’ data

Research Keywords:

1. Health care services
2. hospitals’ data
3. healthcare data sharing
4. healthcare data protection
5. trust-based health environments

Reference European Research Council:

- SH1 Individuals, Markets and Organisations
- SH1_10 Management; strategy; organisational behaviour
- SH1_11 Human resource management; operations management, marketing

Reference Person:

Enrico Cori, Università Politecnica delle Marche, e.cori@univpm.it

Host University and Department:

Università Politecnica delle Marche, Dipartimento di Management

Research Topic: A brief description of scope and objectives of the research topic in more detail; in other words, the research topic where the scholarship and the candidate project proposal should rely on. As written in the overall project, the curriculum on "Health and well-Being" aims to advances in the study of blockchain and DLT in creating innovative and performing solutions to improve the trust between patients and healthcare organizations as well as among healthcare organizations every time data sharing is required. The research will focus on how health services organizations can improve their internal processes in order to protect health-related data, as well as to assure compliance with norms and policies. In turn, the data protection guarantees and compliance with health protocols may have a positive impact on the appropriateness of care and on the economic and financial performance of the healthcare organizations. The innovative character of this research project relies on the fact that these internal processes will rely on Blockchain and DLT. Indeed, these tools will be beneficial to guarantee the respect of norms and policies and to assure the pursuit of the expected results, without requiring the building of a complex, and often centralized authority. In this project, a large attention will be given to the classification of data emerging in Healthcare organizations’ activity: data stream, data-at-rest, images, genomic data and unstructured data.

Research Team and environment: A brief description of the research team and environment where the research activities of the doctorate will be carried out and where most of the collaboration with other researchers and research institutes will be based during her/his doctoral program. The candidate will be involved both in the PhD education that is going to be offered in the DIMA’s Doctorate, i.e. Management & Law PhD- Curriculum of management, and in all the research and education activities that are going to be organized within the Blockchain and DLT National Doctorate. The PhD student will be able to count on an interdisciplinary research group that holds management, accounting, finance, organization, and information systems skills.

Suggested Skills: A brief description of the background/ideal skills the candidates should already possess at the moment of application in order to succeed in their doctoral research. The candidate should demonstrate a strong interdisciplinary attitude, being required to deal with both methods of Blockchain and DLT, and managerial research tools.

Curriculum 4 “Economics and finance”,

Scholarship code: **D01**

Research Title: Blockchain and smart contracts in banking, finance and insurance

Research Keywords:

- Smart contracts
- Banking
- Finance

Reference European Research Council:

- SH1_5
- SH1_4

Reference Person:

Elena Beccalli, Università Cattolica del Sacro Cuore, elena.beccalli@unicatt.it

Host University and Department:

Università Cattolica del Sacro Cuore, School of Banking, finance and insurance

Research Topic: A brief description of scope and objectives of the research topic in more detail; in other words, the research topic where the scholarship and the candidate project proposal should rely on. The research project will focus on the application of blockchain and smart contracts in finance. Relatedly, the research project will focus on crypto assets. These technologies and crypto assets are still largely deregulated and can generate risks of various kinds, particularly of a systemic nature given the interdependence of the subjects involved in the ecosystem. More specifically, the aim is to investigate the main risks and opportunities of these applications, from a managerial and governance perspectives. The regulatory and legal issues will also deserve attention. The focus is on the agents of the ecosystem, the algorithms, the risks associated with the use of these technologies and crypto assets (issuance, loans, payment services, insurance), and on the ways to mitigate these risks. The field of investigation relates to banks, insurance and financial markets.

Research Team and environment: A brief description of the research team and environment where the research activities of the doctorate will be carried out and where most of the collaboration with other researchers and research institutes will be based during her/his doctoral program. The main hub of the research activities will be the School of banking, finance and insurance at Università Cattolica del Sacro Cuore based in Milano. The School is considered as a reference research hub at national and international level for the studies in finance. Moreover, the School has recently been involved in many projects concerning the application of blockchain in finance, and received recognition for this. A strong multidisciplinary view (managerial, legal, technical) on these issues characteries the approach of the School in the study to the subject.

Suggested Skills: A brief description of the background/ideal skills the candidates should already possess at the moment of application in order to succeed in their doctoral research. Ideally the successful candidate should have a good background in banking and finance, and should have an exposure to the applications of blockchain in finance. Experience in data analysis and econometrics is considered an asset.

Curriculum 4 “Economics and finance”,

Scholarship code: **D02**

Research Title: Tokenization and notarization to support SMEs’ finance

Research Keywords:

- Digital asset/Crypto-assets
- Entrepreneurial finance
- Crypto-assets regulation
- Tokenization

Reference European Research Council:

- SH1_5 Corporate finance; banking and financial intermediation; accounting; auditing; insurance
- SH2_4 Legal studies, constitutions, human rights, comparative law

Reference Person:

Monica Rossolini, University of Milano-Bicocca, monica.rossolini@unimib.it

Host University and Department:

University of Milano-Bicocca, Department of Business and Law

Research Topic: In the context of blockchain and DLTs, tokenization refers to the process of converting physical or digital assets into tokens to guarantee the immutability of the original data. The project's main objective is to acquire and promote a thorough comprehension of the tokenized economy's essential features and the possible applications for SMEs, with a particular focus on the use of tokenization in supporting SMEs’ financing. For example, new funding instruments for SMEs, namely ICOs and STOs, have the potential to become efficient and inclusive means of raising capital for small and medium-sized enterprises, and the European Commission has recognized their importance in advancing the Capital Markets Union. A detailed analysis of the phenomenon is required to understand how to best design a pro-business environment that mitigates risks without unduly hampering financial innovation. The issue also implies an important legal aspect to investigating the construction of the new UE digital regulatory framework.

Research Team and environment: The research hub of the research activities will be the Department of Business and Law at the University of Milano-Bicocca. The activities will be developed jointly with the Crypto Asset Lab (CAL) <https://www.diseade.unimib.it/it/ricerca/osservatori/crypto-asset-lab>. CAL is a joint research initiative between the University of Milano-Bicocca and the Digital Gold Institute on crypto-assets, fintech innovation, and regulatory challenges. Several professors of the Department are members of CAL bringing different competencies: legal and financial. Thanks also to other members’ IT competencies, the CAL focuses on cryptography and blockchain technology innovations, given their relevance to privacy, security, and other applications. CAL’s close relationships with the Cryptovalues group and with EC officials, who have been involved in drafting the EU digital finance package, will be valuable for the project.

Suggested Skills: The successful candidate should have a solid basis in Statistics or Computer Science and good quantitative finance background. Experience in data analysis (preferable in Stata) is considered an asset. By the multidisciplinary approach of the research, it would be helpful if the candidate also has some notions of juridical, social, and economic issues.

Research Title: Security of Blockchain Systems

Research Keywords:

- Vulnerability assessment
- Blockchain forensic
- Illegal markets detection

Reference European Research Council:

- PE6_2 Computer systems, parallel/distributed systems, sensor networks, embedded systems, cyber-physical systems
- PE6_5 Cryptology, security, privacy, quantum crypto
- PE6_11 Machine learning, statistical data processing and applications using signal processing (e.g. speech, image, video)

Reference Person:

Gabriele Costa, IMT School for Advanced Studies Lucca, gabriele.costa@imtlucca.it

Host University and Department: IMT School for Advanced Studies Lucca, SySMA Research Unit

Research Topic: In recent years, the blockchain has emerged as one of the main technologies supporting the creation and management of distributed organizations while granting desirable security properties such as privacy and non-repudiation of transactions. Nevertheless, blockchain-based businesses can involve illegal entities and operations. For instance, many black markets and frauds leverage privacy-preserving properties of the blockchain to prevent their authors from being identified. Similarly, smart contract technology has enabled many threats that directly target the core operations of Decentralized Finance (DeFi). This activity focuses on the security aspects of the blockchain ecosystem. In particular, the relevant research topics include (but are not limited to):

- Vulnerability assessment of smart contracts;
- Illegal markets detection and analysis;
- Criminal schemes and businesses recognition;
- Machine learning-based blockchain forensic analysis.

Research Team and environment: The IMT School for Advanced Studies Lucca is a Public University School that focuses on analyzing economic, societal, technological, and cultural systems. IMT School fosters an interdisciplinary research approach characterized by the complementarity and discourse between methodologies drawn from economics, engineering, computer science, applied mathematics, and physics. The candidate will work with the SySMA research unit that deals with developing languages and techniques for the analysis, evaluation, and verification of possibly distributed systems. SySMA also studies algorithms and techniques to protect the security and integrity of computer systems, the information they store, and the people who use them.

Suggested Skills: The ideal candidate should have a Master's degree in Computer Science/Computer Engineering. Moreover, she should have a good knowledge of the fundamental notions of blockchain and basic knowledge of computer security and machine learning.

Research Title: Distributed Ledger Technology systems in credit markets and securities trading services

Research Keywords:

- Credit market and financial services
- Valuation services and financial advising
- Business models for DLTs-based financial players
- The economics of DLTs-based financial markets

Reference European Research Council:

- PE6_6 Algorithms and complexity, distributed, parallel and network algorithms, algorithmic game theory
- PE6_7 Artificial intelligence, intelligent systems, natural language processing
- SH1_4 Finance; asset pricing; international finance; market microstructure
- SH1_5 Corporate finance; banking and financial intermediation; accounting; auditing; insurance
- SH1_8 Microeconomic theory; game theory; decision theory

Reference Person:

Marco Cucculelli, Università Politecnica delle Marche, m.cucculelli@univpm.it

Host University and Department:

Università Politecnica delle Marche – Dept of Economics and Social Sciences

Research Topic: The financial sector has undergone a process of modernization never observed before. However, the increase in mistrust in the financial market, which spread worldwide following the 2008 financial crisis, brought the need for the creation of a safe and efficient ecosystem for financial transactions. One of the possible ways to create such an environment is to use blockchain technologies to facilitate an immediate and safe access to information while achieving a reduction of costs. Building on a rapidly developing – yet not consolidated – literature on blockchain in the financial industry, the research program aims to investigate how DLTs may affect the financial sector performances by influencing the efficiency of the credit and trading processes.

Research Team and environment: The program will be carried out in the Dept of Economics and Social Sciences that has a significant and long-standing expertise in applied microeconomics, finance, and data science. After studying the role of a DLT in the financial sector, the program will explore the challenges of the introduction of DLTs across different sectors. Empirical analyses (micro-econometric analysis or case studies) must be carried on to support the applied orientation of the program. Empirical models targeted at quantifying the impact of DLTs will be developed and applied to banks or other financial players, together with the identification of the business models relevant in a token-based economies. Finally, connections between DTLs and data science must be explored to make DTLs usable into the fast-growing science of data analysis.

Suggested Skills: The successful candidate should have a sound background in economics and finance. Knowledge of most used software applications for economic and financial analysis is a prerequisite. Mastering data analysis/data science and DLTs applications is a definite advantage for candidates.

Research Title:

Distributed Ledger Technology for Digital Money

Research Keywords:

- Central Bank Digital Currency
- Cryptocurrency
- Internet of Money

Reference European Research Council Sectors:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_4 Theoretical computer science, formal methods, automata
- PE6_5 Security, privacy, cryptology, quantum cryptography
- SH1_1 Macroeconomics; monetary economics; economic growth
- SH1_5 Corporate finance; banking and financial intermediation; accounting; auditing; insurance

Reference Person:

Marco Bernardo, University of Urbino, marco.bernardo@uniurb.it

Host University and Department:

University of Urbino, Department of Pure and Applied Sciences

Research Topic:

Innovative payment methods based on digital technologies have characterized the last two decades worldwide. After the widespread diffusion of Internet banking tools along with debit and credit cards, the financial crisis of 2008 and the consequent decrease of the trust in financial intermediaries has paved the way to cryptocurrencies (CC), in particular Bitcoin and the underlying blockchain technology. Since a massive adoption of CC may lead to risks of losing monetary sovereignty and undermining financial stability, many central banks are recently exploring the issuance of what is called central bank digital currency (CBDC), which would also reduce the costs associated with managing physical cash, promote financial inclusion, and hopefully discourage tax evasion, money laundering, and other illegal activities.

The research studies of this PhD scholarship will be in the setting of the emerging Internet of money, focusing on a comparison between CC and CBDC both at the conceptual level and in terms of underlying distributed ledger technology. The main goal is the development of a model-based approach to the investigation of the Internet of money.

Research Team and Environment:

The research activities will take place at the Section of Informatics and Mathematics of the Department of Pure and Applied Sciences of the University of Urbino, possibly in collaboration with other departments. The specific research team within the aforementioned section is composed of researchers and PhD students with expertise in several areas ranging from formal models for concurrent and distributed systems to performance evaluation and security analysis of computer systems and networks, including blockchain technology. The team is currently leading the national research project NiRvAna - Noninterference and Reversibility Analysis in Private Blockchain (<http://www.sti.uniurb.it/nirvana/>), with special emphasis on central bank digital currency.

Suggested Skills:

The ideal candidate has a strong background in computer science or engineering and a good attitude to interdisciplinary studies, in addition to familiarity with model-based design methodologies as well as teamwork capabilities.

Research Title: Blockchain in accounting

Research Keywords:

- Blockchain
- Accounting
- Distributed ledger
- Triple entry accounting
- Accounting digitalisation

Reference European Research Council:

- SH Social Sciences and Humanities
- SH1 Individuals, Markets and Organisations
- SH1_5 Corporate finance; banking and financial intermediation; accounting; auditing; insurance

Reference Person

Diego Valentineti, University “G. d’Annunzio” of Chieti-Pescara, diego.valentineti@unich.it

Host University and Department

University “G. d’Annunzio” of Chieti-Pescara, Department of Economic studies

Research Topic: Blockchain is one of the most recent solutions for enhancing accounting and digital reporting. This PhD project aims to foster the investigation on blockchain technology for corporate accounting and reporting by pursuing two objectives: a) analysing in deep the theoretical and conceptual underpinnings of the blockchain technology; b) designing solutions for investigating the impacts of the blockchain technology on accounting and reporting practices. The activity will rely on both theoretical and pragmatismal exploratory research approach for uncovering the consequences of adopting the blockchain technology on the production and dissemination of digital accounting information in terms of corporate transparency. The main aim is to provide feedback for regulators and policy makers in designing ad hoc solutions for the empowerment of the future users of blockchain in accounting, including the potential of enhancing the trust between market participants through blockchain-based financial information.

Research Team and environment: The research team is based at the Department of Economic studies (University “G. d’Annunzio” of Chieti-Pescara) and is composed by a group of professors and researchers with a long-standing background on accounting digitalisation. Specifically, their track records (including international top journal publications) address the use of digital tools for enhancing financial accounting and reporting, like the eXtensible Business Reporting Language, the Internet of Things, the social media, the Blockchain. The team has also international collaborations in Europe, UK and Australia with prestigious academic institutions. The Department facilities include full access to the most widespread academic and professional databases for retrieving publication sources and corporate data at global scale.

Suggested Skills: strong background in accounting (i.e., accounting information systems, double entry bookkeeping, financial reporting); good background in information technologies.

Curriculum 4 “Economics and finance”,

Scholarship code: **D07**

Research Title: Economic aspects of blockchain and DLT systems

Research Keywords:

- Mechanism design
- Business models
- Blockchain and DLT systems

Reference European Research Council:

- PE6_6 Algorithms, distributed, parallel and network algorithms, algorithmic game theory
- SH1_4 Marketing
- SH1_8 Banking, corporate finance, accounting
- SH1_9 Competitiveness, innovation, research and development

Reference Person:

Massimo Riccaboni, IMT School for Advanced Studies Lucca, massimo.riccaboni@imtlucca.it

Host University and Department:

IMT School for Advanced Studies Lucca, AXES Research Unit

Research Topic: In recent years, the blockchain has emerged as one of the main technologies supporting the creation and management of distributed organizations. We expect the candidate to study the role of economic incentives in its functioning, as well as the economic impact of its applications. In particular, relevant research topics include (but are not limited to):

- The game-theoretic analysis of consensus algorithms or the design of blockchain-based decentralized digital platforms.
- Apply social choice theory to the study of the governance of Blockchain/DLT systems. For example, governance tokens, new voting mechanisms, and decentralized autonomous organizations.
- Study innovative business models based on blockchain/DLTs and cryptocurrencies.
- Study blockchain-based digital currencies and Decentralized Finance (DeFi)
- Study the impact of blockchain and DLTs technologies on trade (for example, tracking of the supply chain) and on intellectual property (for example NFTs).
- Study how contract theory and industrial organization are affected by blockchain and smart contracts.
- Apply advanced data analytics to blockchain data.

Research Team and environment: The IMT School for Advanced Studies Lucca is a Public University School that focuses on analyzing economic, societal, technological, and cultural systems. IMT School fosters an interdisciplinary research approach characterized by the complementarity and discourse between methodologies drawn from economics, engineering, computer science, applied mathematics, and physics. The candidate will work with the AXES research unit that deals with different aspects of Economics

Suggested Skills: The ideal candidate should have a Master's degree either in Economics, business or Computer Science/Computer Engineering. Moreover, the candidate should have basic knowledge of blockchain, game theory and economics.

Research Title: Legal compliance and Blockchain in the agri-food sector

Research Keywords:

- Distributed Ledger Technologies
- Blockchain
- Food legislation
- Private standards
- Compliance

Reference European Research Council:

- SH2_4 Legal studies, constitutions, human rights, comparative law
- SH2_5 International relations, global and transnational governance
- SH2_3 Conflict resolution, war, peace building, international law
- SH2_8 Big data in political and legal studies

Reference Person:

Pamela Lattanzi, University of Macerata, pamela.lattanzi@unimc.it

Host University and Department:

University of Macerata, Department of Law

Research Topic: Food supply chains are governed by a complex regulatory framework comprising mandatory and voluntary requirements. Complying with all the relevant rules is increasingly challenging for food business operators, especially small and medium-sized enterprises. The project will investigate the potential of Blockchain and Distributed Ledger Technologies (DLTs) in facilitating food business operators to better comply with private standards and legal requirements in EU and national food legislation. Project proposals may focus on one or more topics: food safety, traceability, labelling, marketing standards, organic production, quality schemes, Trademarks, Geographical Indications, etc.

Research Team and environment: The main hub of the research activities will be the University of Macerata, Department of Law. The Department has strong expertise in establishing and managing inter-sectorial and interdisciplinary research collaborations, thanks to its experiences as coordinator of international projects, integrating legal studies with technology, engineering, and mathematics sciences (STEM). Currently, the Department is coordinating the Marie Curie - RISE project "TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology" (<https://trust-rise.eu/>), which is focused precisely on the legal framework of Blockchain and DLT technologies. The Ph.D. candidate will collaborate with TRUST's research team and be involved in the project research tasks. The Department will provide academic facilities, common services, high-quality and high-technology instrumental resources, and an important library collection.

Suggested Skills: Ideally, the successful candidate should have a good background in legal studies. Expertise in one or more fields such as law and technology, food law, EU law, private and public law, comparative law, business law, intellectual property law, are considered an asset.

Research Title: Legal and technical analysis of Intelligible Smart Legal Contract based on Legal Reasoning in the European Regulation Framework.

Research Keywords:

- Intelligible Contract
- Self-Sovereign Identity
- Legal reasoning
- eIDAS
- Smart Legal Contract

Reference European Research Council:

- SH1_14 Competition law, contract law, trade law, Intellectual Property Rights
- PE6_9 Human computer interaction and interface, visualisation and natural language processing
- PE1_1 Logic and foundations

Reference Person:

Monica Palmirani, University of Bologna, monica.palmirani@unibo.it

Host University and Department:

University of Bologna, Department of Legal Studies

Research Topic: A brief description of scope and objectives of the research topic in more detail; in other words, the research topic where the scholarship and the candidate project proposal should rely on. The research topic intends to investigate a model for combining legal theory of the contract with the smart legal contract regulations and techniques in order to provide technical specifications by-design for managing the phases of identifications, negotiation, preliminary preparation, contracting, drafting of the smart legal contract, execution of it. The main goal is to provide a theoretical model for the sustainability, explicability and accountability of the smart legal contract at least at European level according to the European Blockchain Services Infrastructure, Regulation (EU) No 910/2014 (eIDAS) and UNCITRAL principles.

Research Team and environment: The team is composed by legal scholars, computer scientists and informatics engineers with a dynamic environment where the theoretical aspects are validated on empirical European and International projects. The approach is interdisciplinary with particular attention to combine legal and technical methodologies. The PhD candidate is integrated in an international team with at least two co-supervisors. The PhD programme offers a rich training calendar with courses in different disciplines oriented to provide a holistic approach in blockchain and smart contract domain. Each PhD spends at least one year abroad. The ALMA-AI Center provides infrastructure, workshops, seminars, equipment, networking.

Suggested Skills: PhD candidate is graduated in law or in computer science/engineer informatics. In both cases the PhD calendar provides adequate courses for filling the gap and creating the necessary interdisciplinarity competences for facing the topic of research assigned. Fluent English is strongly request.

Research Title: The Law and Governance of Disintermediation Business Models

Research Keywords:

- Blockchain
- token
- business model
- decentralisation

Reference European Research Council:

- SH2_4 Legal studies, constitutions, human rights, comparative law
- SH1_5 Corporate finance; banking and financial intermediation; accounting; auditing; insurance
- SH1_15 Public economics; political economics; law and economics

Reference Person:

Filippo Zatti, University of Florence, filippo.zatti@unifi.it

Host University and Department:

The University of Florence, Department of Economics and Management

Research Topic: Blockchains are often associated with the concept of decentralisation. However, decentralisation is not always deployed, whilst disintermediation could find more attractive and viable solutions. However, it is slowed by the unavailability of updated business models and the lack of certainty in the legal framework. The research aims to identify and discuss issues, features, and criteria that could be crucial for building a successful Blockchain business model in disintermediation business models. The idea is to verify if it is possible to find a standard scheme – in terms of indicators, strategies, and type of organisation – to incentive businesses to adopt them and regulators and rule-makers could not stifle the disruptive innovation behind.

Research Team and environment: A vivid and dynamic research team formally established in March 2019 at the Department of Economics and Management of the University of Florence will offer research and high-level education tools for better development and address the PhD candidate research project. The research team, aka BABEL-Blockchains and Artificial intelligence for Business, Economics and Law (www.babel.unifi.it), has focused since then on the significant legal and economic issues being an obstacle to the adoption of blockchain technology. BABEL joined research groups at an international and national level and has organised two international conferences on hot topics about digital assets and tokenomics.

Suggested Skills: The ideal candidate for this PhD curriculum should have a solid background in the foundations of economics and legal theory besides a basic understanding of ITC and cryptography. A concrete experience in developing Blockchain applications is encouraged but not binding. Expertise in the field for academic or international accredited training courses is welcome.

Research Title: Off-chain Execution of Smart Contracts on IoT Constrained Devices

Research Keywords:

- Internet of Things
- Blockchain
- Offchain
- State channels
- Industry 4.0

Reference European Research Council:

- **PE6_2** Computer systems, parallel/distributed systems, sensor networks, embedded systems, cyber-physical systems
- **PE6_6** Algorithms, distributed, parallel and network algorithms, algorithmic game theory
- **PE6_5** Cryptology, security, privacy, quantum crypto

Reference Person:

Leonardo Mostarda, University of Camerino, leonardo.mostarda@unicam.it

Host University and Department:

University of Camerino, Computer Science Division

Research Topic: The main aim of the proposed research is to advance the blockchain state of the art by building an energy efficient blockchain solution that can run-on battery-operated sensor and actuator IoT devices. We aim at investigating novel decentralized state channel approaches that can allow efficient execution of smart contracts on IoT constrained devices. State channels that run on sensor and actuator devices not only support fast and secure micropayments but also allow to run complex distributed applications in various contexts such as Smart Cities, Building automation, Domotics and Industry 4.0. Running blockchain into IoT constrained devices would support the implementation of scalable and secure decentralised IoT systems where smart devices interact with each other without the need of a trusted party. We aim at validating our approach on a real industrial case study arising in the context of industry 4.0.

Research Team and environment: The research activities will be mainly carried out at Computer Science Division, University of Camerino, UNICAM. The candidate will be part of the Software for System and Industries research lab (<http://www.ssilab.it>) and will collaborate with various companies and research laboratory that are located in Marche Region (e.g., <https://www.mchain.it>). The candidate will have the opportunity (not compulsory) to join renown intranational blockchain and security teams from UK universities such as New Castle and Imperial College London.

Suggested Skills: Although it is not mandatory the candidate should have some basic background on security and distributed systems. Some basic knowledge on security protocols and embedded systems would be also useful.

Research Title: Novel Secure and Efficient Consensus Algorithms

Research Keywords:

- consensus protocol
- distributed ledger security
- blockchain security

Reference European Research Council:

- PE6_5 Security, privacy, cryptology, quantum cryptography
- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_6 Algorithms and complexity, distributed, parallel and network algorithms, algorithmic game theory

Reference Person

Mauro Conti, University of Padua, mauro.conti@unipd.it

Host University and Department

University of Padua, Department of Mathematics

Research Topic: Proof of Work (Pow) is one of the most widely used consent mechanisms in blockchains. However, PoWs are very expensive from an energy point of view. Proof-of-Stake (PoS) algorithms have been proposed as alternative consensus algorithms and in their different versions are currently in use in several blockchains. However, PoS mechanisms also have limitations due to, for example, time constraints and trust delegation to a third party. The objective of this project is the study of consensus mechanisms for public and permissionless blockchain, which are safe and efficient. In this project we will also consider different solutions and technologies, such as Algorand and IOTA Tangle.

Research Team and environment: The research activities will be held in collaboration with the “SPRITZ - Security and Privacy Research Group”, an internationally established group led by prof. Mauro Conti. The SPRITZ group and Prof. Conti have a long-term experience on the topic of Blockchain and Distributed Ledger, with a remarkable number of top publications as well as important international collaborations (e.g., IOTA Foundation, Blockchain Education Network). Prof. Conti is a member of the Blockchain Expert Panel of the Italian Government. The SPRITZ Research group is composed of two faculty members, ten postdoc researchers and fifteen Phd students. Several MSc students are working with the group on their thesis projects. The University of Padua can provide High Performance Computing Facilities, Cloud Computing platforms and Testing Infrastructures and car-security testbeds.

Suggested Skills: Ideally, the successful candidate should have a good background in computer science, cybersecurity and distributed systems. Also, high motivation and attitude to work in a collaborative and international environment are required.

Research Title: "Accountability" mechanisms and procedures based on DLT (Distributed Ledger Technology)

Research Keywords:

- Accountability
- Blockchain
- Smart Contract

Reference European Research Council:

- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems
- PE6_6 Security, privacy, cryptology, quantum cryptography

Reference Person:

Antonella Guzzo, University of Calabria, antonella.guzzo@unical.it

Host University and Department

University of Calabria, Dept. Computer Engineering, Modeling, Electronics, and Systems Engineering

Research Topic:

The next generation of Blockchain technology will have to increasingly take into account the aspects related to the distributed nature of cyberspace which requires a secure remote generation between entities. A significant challenge will therefore be supporting the safe, secure and responsible identification of entities and actions which involves, among other things, the identification of the entities involved and their actions carried out in the most general meaning, ranging from objects to human beings, across physical and virtual domains. Many security mechanisms, technologies and services will be involved in this scenario, depending on the nature of the distributed environment, the type of entity, the domains in which the virtual actions are performed (from the physical world to the environments) and the objectives pursued (e.g. degree of verifiability, ability to safely associate with other attributes, traceability, degree of anonymity, etc.).

Research Team and environment:

The research group includes people belonging to the two main laboratories of the Dept. Computer Engineering, Modeling, Electronics, and Systems Engineering: : (i) SPEME Lab (<https://labs.dimes.unical.it/speme/>), Head of Prof. Giancarlo Fortino, that focuses on the development of innovative methods and systems for engineering distributed intelligent, pervasive, mobile, multimedia and multisensorial systems; and (ii) Cybersecurity Lab, Head of Prof. Domenico SACCA ', that carries out research and advanced training on IT security, focusing on the protection of the end user, protection of digital and electronic payment services and on the development of innovative applications distributed with high requirements. security and privacy, identified as relevant in the analysis of the industrial context and technological innovation. The Laboratories have many collaborations with international and national universities, research centers and companies, both in the frameworks of research projects and in the context of shared research and experimental development activities.

Suggested Skills:

Ideally, the candidate should be interested in the technological and applicative aspects of the DLT research, have the ability to work in a team and be proactive in the research activity.

Curriculum 7 “Climate, energy and mobility”,

Scholarship code: **G01**

Research Title: Blockchain Oriented Software Engineering and Applications to smart energy trading and decentralized markets

Research Keywords:

- Blockchain
- Distributed Ledgers
- Smart Contracts
- Software Engineering

Reference European Research Council:

- PE6_2 Computer systems, parallel/distributed systems, sensor networks, embedded systems, cyber-physical systems
- PE6_3 Software engineering, operating systems, computer languages
- PE6_6 Algorithms, distributed, parallel and network algorithms, algorithmic game theory

Reference Person:

Roberto Tonelli, University of Cagliari, roberto.tonelli@unica.it

Host University and Department:

University of Cagliari, Mathematics and Informatics Department

Research Topic: Blockchain Oriented Software Engineering aims at providing Blockchain software development and architecture with the tools and methodologies already adopted during the last decades in software development and software system architecture, taking into account Blockchain software peculiarities. In fact Blockchain software suffers from rushed and unorganized development where failures and bugs proliferate. On the other hand traditional software engineering has to deal with a new and different paradigm. One example above all: once code is deployed on Blockchain it cannot be maintained or modified anymore. This Ph.D. program investigates software engineering for Blockchain software and Smart Contracts development with applications to specific use cases such as supply chain, energy trading, diplomas certifications and others.

Research Team and environment: The research team on Blockchain at University of Cagliari counts a full professor, two associate professors, one assistant professor and various Post-Doc and Ph.D. students, with more than 10 people involved on Blockchain technology research. There are two groups, one more oriented to practical applications and the other to theoretical background and studies. The team is among the most cited groups in the field of Blockchain summing up to more than 3000 citations on google scholar in 2021. It has been working on this field of research since 2014/15 and it regularly organizes international workshops and summer schools in the field. It received international awards for its research and the members are PI of various funded projects for more than 2.5M EURO. It is also a founder member of the IBSI (Italian Blockchain Service Infrastructure) project holding two “validator” nodes.

Suggested Skills: The candidate should have specific knowledge on software engineering and methodologies, such as Agile software development, knowledge of standard programming languages such as C and Java, of web development languages, such as javascript and/or nodejs. Further skills on cryptography and formal methods may also be required for better tackling specific topic of research.

Curriculum 8 “Agriculture and agrifood”,

Scholarship code: **H01**

Research Title: Implementation of blockchain based smart agriculture systems

Research Keywords:

- Blockchain
- Smart agriculture
- Sustainable cropping systems

Reference European Research Council:

- LS9_8 Applied plant sciences, plant breeding, agroecology and soil biology

Reference Person

Cataldo Pulvento, University of Bari, cataldo.pulvento@uniba.it

Host University and Department

University of Bari, Dipartimento di Scienze agro-ambientali e territoriali

Research Topic: Traditional intelligent farming systems manage data and program execution centrally and are subject to inaccurate data, data distortion and misuse. Blockchain-based solutions can significantly improve the performance, security and privacy of the agro-tech sector by decentralizing processes. Examples include traceability, authenticity of the food supply chain, crop insurance. This project aims is to design, implement and to evaluate a secure and lightweight blockchain-based system that uses smart farm sensors. We aim to:

- Evaluate, systematize and contextualize existing knowledge and practices on the use of blockchain in smart agriculture,
- Establish a state-of-the-art agrotechnological experimental test bed using existing platforms,
- Design a lightweight blockchain-based framework for smart agriculture by leveraging sensor data.

Research Team and environment: The student will take advantage of a research environment consisting of several laboratories for agronomic research, soil, precision agriculture and qualitative analysis; Furthermore, field studies will be carried out at the Department Agricultural Experiment Stations located in Policoro (MT) and Valenzano BA) The research team is composed of professors of agronomy and herbaceous crops, professors of Mechanical Engineering, expert technical staff for field experimental tests, laboratory analyzes and construction of experimental pilot plants. The student will be able to interact with other students involved in other research programs of the Department

Suggested Skills: Master degree, in Computing Science, Agriculture, or a related subject. Keen interest in practical problem solving in computer science, and agriculture. It is an interdisciplinary project between IT and agriculture; the student will develop different skills in the field of intelligent agriculture.

Curriculum 8 “Agriculture and agrifood”,

Scholarship code: **H02**

Research Title: Blockchain and smart contracts for data quality and contrasting counterfeits in the agri-food sector

Research Keywords:

- traceability
- transparency
- smart contract
- information asymmetry

Reference European Research Council:

- PE7_8 Networks, e.g. communication networks and nodes, Internet of Things, sensor networks, networks of robots
- PE6_5 Security, privacy, cryptology, quantum cryptography
- PE6_2 Distributed systems, parallel computing, sensor networks, cyber-physical systems

Reference Person

Pierluigi Gallo, University of Palermo, pierluigi.gallo@unipa.it

Host University and Department

University of Palermo, Department of Engineering

Research Topic: The PhD candidate will study how current and next-generation blockchain can support increased traceability and transparency in food supply chains and support the implementation of green and sustainable schemes. The subject of the study will cover both the application and the theoretical aspects. From the application side, the study will contribute to the ambition of developing sustainable, productive, climate-neutral, biodiversity-friendly, and resilient farming systems providing consumers with affordable, safe, healthy, and sustainable food, minimizing pressure on ecosystems, improving public health and generating fair economic returns for farmers through the exploration and development potential of the use of blockchain in the agri-food sector.

The doctoral path will include studying new business and cost models with blockchain-based tracking systems and re-distributing the value of accurate and validated data along the whole supply chain. Also in focus will be implementing a farm-to-fork case study using public and private blockchain networks. The doctoral student will be directed toward solving fundamental challenges, such as identifying what data to record on the blockchain to be meaningful, assigning data consistency levels, mapping the production disciplinaries in smart contracts, guaranteeing trusted data through innovative validation methodologies, identifying groups of visibility of information. Finally, the traceability system under study must comply with agri-food and other regulations, such as those on privacy and security.

Research Team and environment:

The candidate will work in the SNAPPlab (Security, Network Applications and Positioning Laboratory), a small and vibrant research environment with many projects on blockchain applications, mainly in the agri-food and energy sectors. Furthermore, the team spans the whole research supply chain; low TRLs (1-5) are tackled by the SNAPP lab, and higher TRLs (6-9) with SEEDS srl, an academic spin-off of the University of Palermo that focuses on blockchain and smart contracts for the agri-food sector. Thanks to the collaboration with several national and international research groups, the candidate will work in cooperation with multi-disciplinary contexts: cryptographic integrations with the blockchain (with cryptographers), the intelligible smart contracts (with lawyers and linguists), agri-food fingerprinting (with geneticists and agronomists).

Suggested Skills:

Ideally, the successful candidate should have a good background in distributed systems, blockchain, smart contracts and general programming. Experience in system modelling and simulation (Matlab), data analysis (python, bash, UNIX), scripting and virtualization environments (Docker, compose, Kubernetes, Istio, ...) are considered an asset.