RESEARCH TOPIC DESCRIPTION

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: **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 4 "Economics and finance", Scholarship code: **D03**

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.

Curriculum 4 "Economics and finance", Scholarship code: **D06**

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 Valentinetti, University "G. d'Annunzio" of Chieti-Pescara, diego.valentinetti@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 pragmatical 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 5 “Law and Governance”, Scholarship code: **E03**

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.

Curriculum 6 “Industry 4.0”, Scholarship code: **F03**

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 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.