Università
Ca'Foscari
Venezia

PROJECT ACRONYM AND TITLE: **NiRvAna - Noninterference and Reversibility Analysis in Private Blockchains**

FUNDING PROGRAMME: **PRIN 2020**

HOST DEPARTMENT: **Department of Environmental Sciences, Informatics and Statistics**

SCIENTIFIC RESPONSIBLE: **Sabrina Rossi**

FINANCIAL DATA:

Project total costs	Overall funding assigned to UNIVE
€622.811,00	€ 132.007,00

ABSTRACT:
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 the excessive energy consumption required by the consensus protocol and 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.
Developing complex distributed systems like private blockchains is extremely challenging in terms of guaranteeing high levels of proper functioning, data protection, and quality of service. It even becomes a critical issue in CBDC platforms, where errors, data breaches, and poor performance may have economical and social consequences hard to estimate. This calls for a model-based approach in the early design stages so as to enable system property prediction.
The NiRvAna project 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, we will focus on relevant properties such as noninterference and reversibility. 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. This will be accomplished by developing or extending modeling languages, analysis techniques, and software tools according to an integrated view of correctness, security, and performance objectives.

PARTNERSHIP:

1 Università degli Studi di Urbino Carlo Bo	**Urbino (IT)**	**Coordinator**
2 Università "Ca' Foscari" VENEZIA	**Venezia (IT)**	**Partner**
3 Università degli Studi di UDINE	**Udine (IT)**	**Partner**