POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 38th cycle

Research Area n. 1 - Computer Science and Engineering

PNRR_352 Research Field: METHODOLOGIES FOR THE DESIGN, DEVELOPMENT AND TESTING OF DECENTRALIZED APPLICATIONS ON BLOCKCHAIN

Monthly net income of PhDscholarship (max 36 months)
€ 1250.0 In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity	
Motivation and objectives of the research in this field	Distributed applications based on blockchain represent a rapidly evolving and growing sector, due to the availability of blockchains, that allow to execute code in a public, credible, verifiable, guaranteed way, making it possible to develop credible coordination mechanisms, with applications in the financial, insurance, cultural, management of public assets, digital identity fields. Two of the main limitations presented by current blockchain technologies relate to data protection and scalability. The research aims to analyze the cryptographic tools available, and to define methodologies and engineering software tools that allow the definition of data access control mechanisms that do not compromise decentralization, and that allow to maximize throughput and minimize operating costs.
Methods and techniques that will be developed and used to carry out the research	The research will use cryptography and software engineering techniques and tools for the development and analysis of the results. Patterns that represent the peculiar interactions of the elements of a decentralized system (front-end, on-chain components) will be identified and defined with a view to controlling access to data. Tools will be developed that allow abstracting the technological implementation (e.g. use of verifiable computation) for the developer. In addition, tools and libraries will be

	developed for the automation of verification, development and deployment in particular, interesting application areas.
Educational objectives	1. development of a deep knowledge of blockchain technologies, of their technological presuppositions (cryptography, distributed systems, network infrastructures), of the possible economic and social impacts 2. development of critical capacity in evaluating the opportunity of using distributed technologies, with respect to different dimensions (complexity, energy costs, impact on regulatory compliance) 3. development of analytical skills for assessing the security of distributed systems, from an adversarial point of view 4. development of desig
Job opportunities	Il campo delle applicazioni su blockchain è in forte sviluppo, e con esso il mercato della domanda di professionisti che sappiano valutare l'opportunità e implementare applicazioni distribuite. Alcune tra le principali opportunità lavorative sono: 1. come analisti, sviluppatori, project manager presso società di consulenza in ambito blockchain 2. presso enti e amministrazioni pubbliche che intendano utilizzare queste tecnologie per lo sviluppo di servizi 3. presso organi di controllo che vogliano internalizzare competenze volte a valutare l'impatto non solo tecnologico della decentralizzazione di applicazioni per esempio finanziarie 4. presso società non tecnologiche che intendano sviluppare competenze interne di analisi dell'opportunità di utilizzo di tecnologie decentralizzate (e.g. NFT) per lo sviluppo della propria missione
Composition of the research group	1 Full Professors 1 Associated Professors 2 Assistant Professors 1 PhD Students
Name of the research directors	Prof. Francesco Bruschi

Contacts
francesco.bruschi@polimi.it, +390223993411

Additional support - Financial aid per PhD student per year (gross amount)	
Housing - Foreign Students	--
Housing - Out-of-town residents (more than 80Km out of Milano)	--

Scholarship Increase for a period abroad	
Amount monthly	625.0 €
By number of months	6

National Operational Program for Research and Innovation	
Company where the candidate will attend the stage (name and brief description)	Knobs s.r.l. Link: https://knobs.it/
By number of months at the company	6
Institution or company where the candidate will spend the period abroad (name and brief description)	Nchain, https://nchain.com/
By number of months abroad	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information

Attinenza alla tematiche, alle missioni/componenti prescelte del bando PNRR v. D.M. 352, art.6

La ricerca presenta attinenza alle tematiche del bando PNRR, in particolare alla missione 1, nei punti:
- incentivi per la transizione digitale e per l'adozione di tecnologie innovative e le competenze digitali da parte del settore privato;
La ricerca riguarda difatti lo sviluppo di strumenti e metodologie che consentano di utilizzare tecnologie blockchain per l'implementazione di applicazioni decentralizzate, potenzialmente inclusive, resilienti
- la digitalizzazione della Pubblica Amministrazione e rafforzamento delle competenze digitali;
Le tecnologie oggetto dello studio nella ricerca possono rappresentare uno strumento significativo per digitalizzare in modo trasparente e democratico una frazione importante dei servizi pubblici

Impresa, presso cui si svolgerà l'attività esterna

Knobs s.r.l.
Settore attività: consulenza informatica, iot, sviluppo di applicazioni blockchain
L'attività riguarderà lo sviluppo di applicazioni blockchain, con particolare attenzione ai

meccanismi di protezione di accesso ai dati e alla scalabilità
Collaborazioni pregresse: Knobs ha finanziato in precedenza progetti di ricerca con il dipartimento

Ente, università, azienda, centro di ricerca presso cui si svolgerà il periodo di studio e ricerca all'estero.

azienda: nchain,
settore attività: sviluppo di applicazioni blockchain
link: https://nchain.com/
mesi previsti: 6
descrizione sintetica: l'attività consisterà nello sviluppo di meccanismi di controllo basati su threshold signature in applicazioni blockchain

All information regarding educational activities, personal funding, regulations and obligations of Ph.D. candidates are available on the web site https://dottoratoit.deib.polimi.it/