POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 40th cycle

Research Area n. 1 - Computer Science and Engineering

THEMATIC Research Field: BLOCKCHAIN AND CRYPTOGRAPHIC ENGINEERING

Monthly net income of PhDscholarship (max 36 months)
€ 1400.0 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	Horizen Labs is dedicated to elevating blockchain technology to unprecedented efficiency by significantly reducing proof verification costs without compromising security. Focusing on building next-gen, modular architecture enhanced with composable zero-knowledge proofs, Horizen Labs is advancing the field, setting new benchmarks for performance, security and cost-effectiveness.
Methods and techniques that will be developed and used to carry out the research	The components of the areas mentioned above will be assigned to a researcher, who will be integrated into the company's cryptographic team and contribute to the development of the company's research and software development roadmap. The researcher will work at the office daily, while also having the option to work remotely part-time.
Educational objectives	1. **Privacy in Blockchains** •Privacy-preserving smart contracts (e.g., homomorphic encryption, secure multi-party computation) •Scalable privacy solutions for Layer 2 and ZK apps. •Decentralized identity (e.g., selective disclosure, credential verification) •Privacy-preserving DeFi protocols (e.g., private swaps, confidential lending, shielded staking)

	•Confidential asset transfers (e.g., stealth addresses, ring signatures) •Cross-chain privacy solutions (e.g., anonymous bridges, interoperability with private chains) •Privacy-enhancing technologies for regulatory compliance (e.g., GDPR-friendly ZK proofs, AML-compliant selective disclosures) •Selective disclosure mechanisms for enterprises (e.g., ZK proofs for audits) 2. **AI and Its Intersection with Cryptography** •Privacy-preserving federated learning (e.g., differential privacy, homomorphic encryption) •AI-driven anomaly detection for blockchain security (e.g., fraud detection using machine learning models) •Verifiable AI models using zero-knowledge proofs (e.g., ZK-based proof of model integrity) •Decentralized identity with AI-based fraud detection (e.g., biometric verification with privacy guarantees) •Secure AI-driven credit scoring for DeFi applications (e.g., privacy-preserving creditworthiness assessment) •Private reputation systems on blockchain (e.g., ZK-proofs for trust scores without data exposure) •Lightweight proof generation for AI agents 3. **Zero-Knowledge Proofs (ZKPs) and Advanced Cryptographic Protocols** •Recursive proof composition for scalability (e.g., ZK-SNARK recursion, folding schemes) •Lightweight ZKPs for IoT and mobile devices (e.g., efficient proof generation on constrained hardware) •Efficient proof aggregation and compression methods (e.g., batching proofs, recursive verification •Fully homomorphic encryption for blockchain privacy (e.g., computation on encrypted blockchain data) •Secure multi-party computation (MPC) for decentralized applications (e.g., collaborative key management) •Threshold cryptography for secure key management (e.g., distributed key generation, threshold signatures) •Privacy-preserving sharding techniques (e.g., zk-SNARK-

	based shard verification)
Job opportunities	Possible employment with the company following the completion of the PhD.
Composition of the research group	1 Full Professors 0 Associated Professors 3 Assistant Professors 2 PhD Students
Name of the research directors	Prof. Francesco Bruschi

Contacts
Francesco Bruschi - francesco.bruschi@polimi.it Raffaella Lixi - raffaella@horizenlabs.io

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	700.0 €
By number of months	6

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

EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student.
5.707,20 Euro per student

TEACHING ASSISTANTSHIP: availability of funding in recognition of supporting teaching activities by the PhD student.
There are various forms of financial aid for activities of support to the teaching practice.
The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations.

COMPUTER AVAILABILITY:
1st year: Yes
2nd year: Yes
3rd year: Yes


POLITECNICO
MILANO