EIT Digital – Industrial PhD position proposal

PhD thesis information

PhD Thesis – Title	Cryptographically secure, on-chain pseudorandom number generation (PRNG)
PhD Thesis – Short summary	Securely generating pseudorandom numbers on a blockchain is a challenging open problem. Since the Ethereum Virtual Machine is a deterministic Turing-complete machine it is extremely difficult to obtain pseudorandomness in this execution environment.
Rationale/challenge – *describe the problem and why it is relevant*	This research aims to examine and evaluate existing on-chain PRNGs as well as design and propose new secure on-chain PRNG protocols.
Innovation – *describe what is the intended solution and the advance w.r.t. the state-of-the-art*	Currently only workarounds, off-chain solutions and insecure on-chain solutions exist. These makeshifts do not suffice for applications like probabilistic payment channels, consensus algorithms (ie. Proof-of-stake) and gambling.
Research focus/topics – *describe how you are going to solve the problem*	After an initial research the chosen or proposed protocol will be implemented as a smart contract for the Ethereum Virtual Machine. Later to present the practicability of the protocol, also the off-chain accompanying components will be developed to demonstrate the feasibility of cryptographically secure on-chain pseudorandom number generation.
Deadlines/milestones (Gantt chart)	Finding the protocol to generate on-chain pseudo-randomness
	Finishing implementing the protocol as a proof-of-concept
	Research and select the best possible application area for it in cooperation with E-Group
	Implement and showcase on-chain pseudo-randomness in various decentralized applications chosen in agreement with E-Group
	Production-ready applications using on-chain pseudo-randomness transferred to E-Group for exploitation in its portfolio
Expected outcome – *describe the expected results of the PhD*	Our research will enable E-Group to reinforce their position in the e-commerce field by deploying micropayments based on the to-be-developed (researched and designed) probabilistic payment channels. Micropayments can reduce costs, provide security, confidentiality and are convenient. This alternative payment option is going to revolutionize the way we purchase products and services from energy sector, digital media, gambling etc. The topic of the PhD is directly connected to E-Group's planned blockchain activities, and can be an extension of E-Group's existing Abaqoos payment service product. During the course of

	the PhD program the results of the research will be channelled back to the industry, thus providing constant feedback on their practical applicability of the research results.

Relevance for the Action Line (section to be filled out by the Action Line Leader)

Action Line	Digital Finance
Alignment with Action Line – *statement from the Action Line Leader indicating the relevance for the AL from his perspective*	
Relevant IA – *List any relevant Innovation Activity (if applicable)*	

Partnership/financial information

Action Line Leader	Antonio García-Hortal
Industrial partner	E-Group ICT Software Zrt.
Industry advisor – *name and short bio*	Zoltán Hattyasy (MSc Computer Science – BME, Hungary) He has 25 years of experience in software development and 20 years in project management (Certified Scrum Master). He has been working in various domains (automotive, banking, military, e-government) as software architect designing complex software solutions, and coordinating the implementation as PM. He has experience in managing R&D projects, on national and EU level as well. He is acting as a PM for E-Group's running EIT Digital projects.
Academic/research partner	ELTE
Academic/research supervisor – *name and short bio*	Péter Burcsi is associate professor and head of the Department of Computer Algebra at the Faculty of Informatics, ELTE Eötvös Loránd University Budapest. He obtained his master degree as mathematician at ELTE in 2002, a PhD degree in 2009 and habilitation in 2015. He has worked at ELTE since 2005, giving lectures and practice seminars in Hungarian and English, mainly in mathematics and computer science. He is the supervisor of 4 PhD students, 2 of whom are expected to defend their theses in 2019. His main research interests are combinatorics on words and algorithms on strings. He has participated in several research projects, innovation activities and industrial projects, mainly focusing on the area of cryptology,

	security and privacy. He has been involved in 4 projects funded by the EIT and in giving courses in the EIT Master Program.
HEI granting the title	ELTE-IK
DTC location	Budapest
Geographical mobility plan	
No. of PhD positions	1
PhD duration	4
Co-funding percentages: - Industry - Academia - EIT Digital	20
	30
	50