EIT Digital – Industrial PhD position proposal

PhD thesis information

PhD Thesis – Title	Blockchain oracles
PhD Thesis – Short summary	How can we provide data privately and securely to smart contracts outside of the blockchain? Smart contracts live in a walled garden. As such, they starve for meaningful, authenticated data from the off-chain world. Authenticated data exchange between smart contracts and the off-chain world (oracles) has the potential to provide powerful services for businesses and organizations. This PhD is geared towards researching and proposing new solutions and protocols which will enable smart contracts to gather authenticated data from outside the blockchain. These off-chain data providers (oracles) include: web APIs, other blockchains, WolframAlpha etc.
Rationale/challenge – *describe the problem and why it is relevant*	Smart contracts are autonomous agents on the Blockchain. Therefore, any application that requires the use of an incorruptible third party, which is most applications, may use a smart contract in place of a centralized trusted third party. The main advantage smart contracts provide apart from not requiring any user intervention is that trust scales better with smart contracts as compared to centralized environments. However, the most compelling use cases of smart contracts, such as financial instruments require data feed from oracles outside the Blockchain (e.g. stock quotes). Since smart contracts execute in an adversarial environment, the potential financial gains from an attack provide a strong incentive to rational adversaries to subvert the smart contracts or the services on which they rely. Consequently, it is of critical importance that in such cases data exchange between smart contracts and oracles are authenticated, untampered (integrity), and in some cases intelligible only to desired entities (confidentiality). The global smart contracts market is expected to reach approximately 300M USD by the end of 2023 with 32% compound aggregated growth rate during the forecasted period from 2017 – 2023.[1] Apart from the fintech applications, smart contracts will play a significant role (among others) in the e-government, healthcare, real estate sector as well. For the citizens it offers applications based on the concept of data sovereignty. Therefore, it is crucial to fuel the smart contracts economy with trusted data – this is exactly what blockchain oracles do.
Innovation – *describe what is the intended solution and the advance w.r.t. the state-of-the-art*	The goal of this PhD is to develop a cryptographically provable protocol / service that has high interoperability with existing off-chain systems (E.g. web servers communicating with TLS). Such a solution could be used in the financial sector with financial instruments as well as in Identity Management Systems where

[1] https://www.marketresearchfuture.com/reports/smart-contracts-market-4588

	Identity providers serve as the trusted oracles feeding smarts contracts with information about some digital identities. In essence, the expected solution should extend smart contracts to the real world, creating an ecosystem where real world situations can act as secure input to a smart contract. The following design objectives are proposed for the solution: 1. Solution should be able to securely authenticate oracles outside the environment of the smart contract. 2. Solution should be able to verify the trustworthiness (data authenticity) of data fed into the smart contract by an oracle. 3. Data feed between smart contract and oracle should be confidential when necessary. 4. Solution should be decentralized, thus, verifying the authenticity of information supplied by oracle should not rely on one entity. 5. Establish a formal model for evaluating the security of the solution. 6. A software product implementing the proposed blockchain oracle protocol/service will be developed. One state-of-the-art solution in this area is Town Crier. This relies heavily on a centralized Town Crier Server (Relay and Enclave). This centralization creates a trust bottleneck and a single point of failure, thus, effectively putting an economic limit on various use cases that employ Town Crier. The decentralization of our solution constitutes an improvement in the security, efficiency, and overall interoperability of the state-of-the-art.
Research focus/topics – *describe <u>how</u> you are going to solve the problem*	The objectives listed for this PhD will be achieved through continuous research, seminars, and experimentation. The research into the current state of the art is conducted by a team of PhD students. At regular intervals, design proposals for a potential solution is shared and discussed at a seminar with at least one expert in the field. Experiments are then performed to test the validity of the proposed design, and lessons learnt are documented. This process is performed repeated until an optimal solution is found. We define an optimal solution in this context as a solution that achieves most of the project objectives with the least resources. The blockchain oracle will be implemented during the program, and refined, utilising the results of the scientific research. If the developed blockchain oracle reaches the necessary maturity, a **software product will be created and marketed**, thus leveraging the results of the PhD program, and on the other hand, providing user feedback to the research.
Deadlines/milestones (Gantt chart)	Complete review of all related literature (Distributed Ledger Technologies, Zero Knowledge Proofs, Private Function Evaluation, Smart Contracts, etc.)
	First draft of whitepaper containing 3 key details:

	1. A clear and concise protocol for achieving secure and private information exchange between a smart contract **(S)**, and an off-chain oracle **(O)**. 2. Supporting security and cryptographic proofs for the protocol in **(1)** above to ensure the confidentiality of the information exchange, authenticity of the off-chain oracle, and integrity / availability of exchanged information. 3. A clear and concise method for decentralizing the trust provided by off-chain oracles.
	Share white paper with experts and prepare first draft of yellow paper Software prototype developed and deployed.
	Make necessary corrections and additions to whitepaper, and prepare final yellow paper. Release of the final version (v1) of the software package implementing the protocol/service.
	Synchronisation of the content of the yellow paper and the developed software component. Transfer of the software package for industrial exploitation.
Expected outcome – *describe the expected results of the PhD*	At the end of the PhD, 2 papers are expected to be produced: 1. A whitepaper detailing a protocol or service that achieves the listed design objectives written in the innovation section of this document. This paper should contain a security model and all supporting cryptographic proofs. 2. A yellow paper detailing a real life implementation of the protocol with analysis on sustainability, security, and performance. The PhD topic is a logical extension of E-Group's existing identity management product line, connecting it to the blockchain world. During the course of the PhD program the blockchain oracle will be implemented as a software product (with the collaboration of E-Group's development team and the PhD student) and thus the results of the research will be channelled back to the industry.

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)*	Current proposals: DIMS (Call #19151) in Digital Finance AL, where E-Group is technology provider – during the evaluation phase this proposal got an A score.

	DIMS (Distributed Identity Management System) aims to offer KYC (know your customer) processes shared among companies, based on user consent. The eIDAS onboarding feature includes a blockchan oracle that connects the blockchain to government backed identity information. This application is a prime candidate to implement the PhD topic proposal in a real-world scenario. (However, the PhD topic includes deep scientific research that reaches beyond the scope of the EIT project.)

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*	Peter Ligeti is assistant professor on the Department of Computer Algebra at the Faculty of Informatics, ELTE Eötvös Loránd University Budapest. He obtained his master degree as applied mathematician in 2001 and as teacher of mathematics in 2003 at ELTE, a mathematics and computer science PhD degree in 2008. He has worked at ELTE since 2007, giving lectures and practice seminars in Hungarian and English for bachelor, master and PhD students as well as in the EIT Master School, mainly in mathematics and computer science. Recently, he is the supervisor of 2 PhD students, one of them is within the framework of Stipendium Hungaricum Programme. His main research interests are combinatorics and cryptography. He has participated in several academic and industrial R&D research projects, mainly focusing on the area of cryptology, security and privacy. Especially, he has been involved in 4 projects funded by the EIT.
HEI granting the title	ELTE
DTC location	Budapest
Geographical mobility plan	
No. of PhD positions	1
PhD duration	4
Co-funding percentages: - Industry - Academia - EIT Digital	20 30 50