UNIVERSITY OF WARSAW

Press Office

31.03.2020

# ERC AWARDED ITS ADVANCED GRANT TO PROF. STEFAN DZIEMBOWSKI FROM UW

**Prof. Stefan Dziembowski from the UW Faculty of Mathematics, Informatics and Mechanics has been awarded an ERC Advanced Grant for his project entitled "Smart-Contract Protocols: Theory for Applications". PROCONTRA is an acronym for the project.**

The PROCONTRA project concerns so-called *smart contracts*. These contracts can be viewed as the "computer equivalent" of legal contracts. They are written in a language resembling a programming language, so they are always unambiguous and, unlike contracts written in natural language, their interpretation is not subject to dispute. This concept was introduced in the 90s and has gained immense popularity recently, mainly due to the development of the so-called blockchain technology that provides tools for writing down and executing these contracts.

## Prof. Dziembowski's second ERC grant

Prof. Stefan Dziembowski's field of expertise is cryptography. He is an author of numerous publications on this subject. He leads a research team at the University of Warsaw Faculty of Mathematics, Informatics and Mechanics which researches cryptographic aspects of the digital currency bitcoin.

For his achievements, Prof. Dziembowski received awards such as Best Paper Award at Eurocrypt 2014, Best Paper Award at IEEE S&P (Oakland) 2014 or Kazimierz Bartel Award 2016.

Awarded UW scientist was also associated with a few research institutions abroad. In years 2008-2010, he was an assistant professor at the University of Rome "La Sapienza". Working as a Marie-Curie Fellow at this university, he was awarded the ERC Starting Grant for the project "Cryptography and no-trusted machines". Prof. Dziembowski, however, decided to change the host institution and carry out the project at the University of Warsaw.

At the same time, he became the first laureate of this prestigious award at UW. Now, the European Research Council awarded the scientist for the second time. For his project PROCONTRA, Prof. Dziembowski will receive € 2.4 million.

phone: (+48) 22 55 20 990, 22 55 20 740, 22 55 24 066
e-mail: media(at)uw.edu.pl

## Smart contracts

The topics of the PROCONTRA project are *cryptographic protocols* that use such contracts. By this, we mean algorithms (executed by many independent parties) that interact with smart contracts. A simple example of such protocols can be a chess game in which a smart contract is responsible for the fairness of the game (e.g. that you cannot make unauthorized moves of figures), and the "protocol" contains instructions for each party on how to behave in order to make a move in the game. Of course, the protocols used in practice can be much more complicated than this example, and in particular, they can include scenarios in which the number of participants is much greater than 2. Protocols using smart contracts have a number of potential applications, especially in the so-called Internet of Things, where there is a need to conclude contracts directly between devices without human intervention.

Despite significant progress, this technology is still in a very early stage of development. The PROCONTRA project aims to transfigure this emerging field into a mature science. In particular, the goal of the grant is to create a formal theory of protocols based on smart contracts, along with security models, formal proofs, and a set of mathematical tools to analyze their security. As part of the project, we will also create new protocols of this type, and analyze existing protocols. For example, we will work on the so-called "off-chain protocols", which are used to move a significant part of blockchain operations outside the main blockchain while maintaining the same security guarantees. Another example of the applications, we will be working on, are solutions that increase the anonymity of the parties, taking part in such contracts.

The project will focus on mathematical formalism and formal security proofs of the proposed solutions. The project team will also engage in dialogue with the community of blockchain practitioners, and participate in efforts to standardize the protocols studied.

Also, this grant, along with other sources of financing, will be used to build, at the University of Warsaw, the first academic centre in Poland for blockchain and smart contract technology development.

The ERC Advanced Grants are awarded to researchers who have a track-record of significant research achievements in the last ten years. Advanced Grants may be awarded up to € 2.5 million for a period of 5 years.

phone: (+48) 22 55 20 990, 22 55 20 740, 22 55 24 066
e-mail: media(at)uw.edu.pl

UNIVERSITY OF WARSAW

**Press Office**

As yet ERC has awarded 37 grants to scientists working in Polish institutions, including 16 researchers from the University of Warsaw.

## Starting Grants:

2007 – Prof. Stefan Dziembowski

2009 – Prof. Mikołaj Bojańczyk

2009 – Prof. Natalia Letki

2010 – Prof. Piotr Sankowski

2012 – Prof. Justyna Olko

2013 – Prof. Piotr Sułkowski

2015 – Prof. Marek Cygan

2016 – Prof. Marcin Pilipczuk

2017 – Dr. Artur Obłuski

## Consolidator Grants:

2015 – Prof. Katarzyna Marciniak

2015 – Prof. Mikołaj Bojańczyk

2017 – Prof. Piotr Sankowski

2019 – Prof. Anna Matysiak

## Advanced Grants:

2009 – Prof. Andrzej Udalski

2019 – Prof. Stefan Dziembowski

## Proof of Concept:

2015 – Prof. Piotr Sankowski

Katarzyna Bieńko

Contact: media@uw.edu.pl