



UNIwersytet
Warszawski

Biuro Prasowe

31.03.2020

ERC ADVANCED GRANT DLA PROF. STEFANA DZIEMBOWSKIEGO Z WMIM UW

Inteligentne kontrakty są – w uproszczeniu – umowami, których forma zapisu przypomina program komputerowy. Konieczne jest opracowanie zaawansowanych technik kryptograficznych wykorzystujących ich działanie. Kwestia ta poruszona zostanie w ramach projektu PROCONTRA, który nagrodzony został właśnie prestiżowym ERC Advanced Grant. Jego kierownikiem jest prof. Stefan Dziembowski z Wydziału Matematyki, Informatyki i Mechaniki UW.

Świat realny współistnieje obecnie z wirtualnym. Postępująca informatyzacja, usieciowienie i rosnące znaczenie nowoczesnych technologii informacyjno-komunikacyjnych wpływają na poszerzenie perspektyw działalności oraz zwiększenie „mocy obliczeniowych” człowieka. Z drugiej jednak strony, mogą wiązać się z ryzykiem wycieku poufnych danych. Jego zmniejszeniu sprzyjają m.in. badania naukowe w zakresie kryptologii. To dyscyplina będąca na pograniczu matematyki i informatyki, która wielu osobom kojarzy się przede wszystkim ze złamaniem w czasie II wojny światowej przez grupę polskich matematyków szyfru Enigmy.

Grant ERC po raz drugi

Jedną z gałęzi kryptologii jest kryptografia obejmująca wiedzę dotyczącą metod utajniania wiadomości. Autorem licznych publikacji poruszających tę tematykę jest prof. Stefan Dziembowski z Instytutu Informatyki UW. Na Uniwersytecie pod jego kierownictwem działa zespół badaczy z WMIM, których prace dotyczą m.in. kryptograficznych aspektów cyfrowej waluty bitcoin. Prace prof. Dziembowskiego otrzymały m.in. nagrody „Best Paper Awards” podczas konferencji Eurocrypt oraz IEEE Symposium on Security & Privacy.

Prof. Dziembowski związany był z kilkoma zagranicznymi instytucjami naukowymi. Staż podoktorski odbywał m.in. na Uniwersytecie La Sapienza w Rzymie. Jako pracownik tej uczelni w 2007 roku otrzymał Starting Grant Europejskiej Rady ds. Badań Naukowych. Wkrótce realizację projektu badawczego pt. „Cryptography and no-trusted machines” przeniósł na Uniwersytet Warszawski. Jednocześnie stał się pierwszym na UW laureatem tej prestiżowej nagrody.

ERC wyróżniła właśnie naukowca po raz kolejny – przyznając mu tym razem Advanced Grant w wysokości ponad 2,4 mln euro na realizację projektu pt. „Smart-Contract Protocols: Theory for Applications” (PROCONTRA).

O inteligentnych kontraktach

Inteligentne kontrakty (ang. *smart contracts*) można określić „informatycznym odpowiednikiem” umów prawnych. Pojęcie to pojawiło się w I. 90. XX w. W ostatnim czasie zyskało na popularności, głównie dzięki rozwojowi tzw. *technologii blockchain*, która dostarcza narzędzi do zapisywania i

wykonywania tych kontraktów. – Są one zapisywane w języku przypominającym język programowania, dzięki czemu zawsze pozostają jednoznaczne i, w przeciwieństwie do umów pisanych językiem naturalnym, ich interpretacja nie podlega sporom – tłumaczy prof. Stefan Dziembowski.

Przedmiotem badań w ramach projektu PROCONTRA będą protokoły kryptograficzne, czyli algorytmy wchodzące w interakcje z inteligentnymi kontraktami. – Prosty przykład takich protokołów może być gra w szachy, w której inteligentny kontrakt odpowiada za uczciwość rozgrywki, np. za to, żeby nie można było wykonać niedozwolonych ruchów figurami, a protokół zawiera instrukcje dla każdej ze stron dotyczącą tego, jak ma się zachowywać w celu wykonania ruchu w grze – mówi prof. Dziembowski. Dodaje przy tym, że w praktyce mogą być wykorzystywane znacznie bardziej skomplikowane protokoły, uwzględniające m.in. większą liczbę uczestników.

Mówiąc o potencjalnych zastosowaniach protokołów wykorzystujących inteligentne kontrakty, na myśl przychodzą zwłaszcza transakcje dokonywane w tzw. internecie rzeczy, gdzie pojawia się konieczność zawierania umów między urządzeniami – bez ingerencji człowieka.

– Projekt PROCONTRA ma celu przekształcenie tej rodzącej się dziedziny w dojrzałą naukę. W szczególności celem grantu jest stworzenie teorii protokołów opartych na inteligentnych kontraktach, wraz z modelem bezpieczeństwa, formalnymi dowodami i zestawem narzędzi matematycznych służących analizie ich bezpieczeństwa – mówi prof. Dziembowski, dodając: – W ramach projektu będziemy też tworzyć nowe protokoły tego typu oraz analizować protokoły już istniejące. Przykładowo, będziemy zajmować się tzw. protokołami *off-chain*, które służą przeniesieniu znacznej części operacji poza główny *blockchain*, przy zachowaniu tych samych gwarancji bezpieczeństwa.

Realizacja projektu PROCONTRA w ramach grantu ERC oraz dzięki wykorzystaniu innych źródeł finansowania przyczyni się do powstania na Uniwersytecie Warszawskim pierwszego w Polsce akademickiego centrum rozwoju *blockchaina* oraz technologii inteligentnych kontraktów.

[Dotychczas ERC 37 razy przyznała granty naukowcom pracującym w krajowych ośrodkach, w tym – 16 razy naukowcom z Uniwersytetu Warszawskiego.](#)

[Starting Grants:](#)

2007 – prof. Stefan Dziembowski

2013 – prof. Piotr Sułkowski

2009 – prof. Mikołaj Bojańczyk

2015 – prof. Marek Cygan

2009 – dr hab. Natalia Letki

2016 – prof. Marcin Pilipczuk

2010 – prof. Piotr Sankowski

2017 – dr Artur Obluski

2012 – dr hab. Justyna Olko

Consolidator Grants:

2015 – prof. Katarzyna Marciniak

2015 – prof. Mikołaj Bojańczyk

2017 – prof. Piotr Sankowski

2019 – dr hab. Anna Matysiak

Proof of Concept:

2015 – prof. Piotr Sankowski

Advanced Grants:

2009 – prof. Andrzej Udalski

2019 – prof. Stefan Dziembowski

Daiwa Maksimowicz

kontakt: media@uw.edu.pl