#	Research topics offered by IDEAS NCBR	Abstract	Group/team leader in IDEAS NCBR	E-mail
1	**More secure decentralized finance**	One of the main problems of cryptocurrencies is their highly fluctuating exchange rates with standard currencies. Decentralized finance (often abbreviated as DeFi) refers to blockchain solutions that address this problem. The most notable examples are the stable coins, where the internal currencies of a given blockchain are exchangeable with fiat money at a fixed rate. Several exciting proposals exist for constructing such coins, most coming from blockchain startups and lacking complete formal security analysis. This student will work on improving these protocols and understanding their security properties. DeFi protocols can also be used to replace financial institutions such as the stock market. One of the problems with this approach is the so-called front-running attacks. Unfortunately, most blockchain solutions allow such powerful participants to publish their transactions on the blockchain before the original transactions appear there. This can lead to considerable financial losses for such honest participants. This student will work on addressing this problem.	Stefan Dziembowski	stefan.dziembowski@ideas-ncbr.pl
2	**Proofs-of-Space in practice**	The most popular blockchain platforms use consensus based on the so-called Proofs-of-Work, where the participants are incentivized to constantly solve many computational puzzles (this process is also called mining). This leads to massive electricity consumption. Several alternatives to Bitcoin mining have been proposed in the past. Stefan Dziembowski (who leads this research at IDEAS) is one of the authors of another approach to this problem, called the Proofs-of-Space. In this solution, the computational puzzles are replaced with proofs that a given party contributed some disk space to the system. Several ongoing blockchain projects are based on these ideas. This student will work on improvements to these protocols.	Stefan Dziembowski	stefan.dziembowski@ideas-ncbr.pl

3	**Real-life side-channel security of blockchain wallets**	Another critical weakness in the vision of decentralizing internet services is that interacting with blockchains is more complicated than in the case of centralized solutions. Moreover, the decentralization makes it impossible to revert the transactions that were posted by mistake or as a result of an attack. Due to this, the users often rely on the so-called hardware wallets, which are dedicated devices protected against cyber-attacks. This student will work on analyzing the security of the existing hardware wallets. In particular, we will be interested in their side-channel security, i.e., security against attacks based on information such as power consumption or electromagnetic radiation.	Stefan Dziembowski	stefan.dziembowski@ideas-ncbr.pl
4	**Practice-oriented verification of blockchain protocols**	One of the main problems in the blockchain space is that decentralized solutions are typically more complex and error-prone than centralized ones. In particular, errors in smart contracts can lead to considerable financial losses. Furthermore, some blockchain algorithms in the past had serious mistakes that could be used to steal large amounts of money. This student will work on addressing these problems using tools from formal methods, in particular, proof assistants and provers such as Coq, Easycrypt, Why3, and others. Theoretical aspects of this work are one of the topics of the ongoing ERC grant of Stefan Dziembowski. This student will work on more technical aspects, especially making this approach usable in real life by blockchain developers.	Stefan Dziembowski	stefan.dziembowski@ideas-ncbr.pl
5	**Explainable Algorithmic Tools**	In this research project we aim to propose tools that would provide explanations for the different basic optimization problems, e.g., assignment problem, shortest paths, minimum cuts, or basic graphical neural networks. This research is motivated by the fact that even when faced with problems that can be solved exactly, we still would like to understand why this solutions was computed.	Piotr Sankowski	piotr.sankowski@ideas-ncbr.pl

6	**Learned Data-Structures**	ML tools enter as interior components into basic data structures or state-of-the-art approximation algorithms resulting in solutions that have better practical properties, e.g., indices. These new hybrid constructions are called learned data-structures. As the work on these ideas has just started we miss the right framework and tools for implementing state-of-art solutions and thus the research on new tools and models is hampered. This research aims to continue research on this problem and create new algorithms and data structures together with their implementations. This could prove tools to bridge the gap between theory and practice in algorithms and show that new theoretical advances can have practical implications.	Piotr Sankowski	piotr.sankowski@ideas-ncbr.pl
7	**Algorithmic Tools for Data Science and ML**	lthough, different parallel computation models have be studied for years already. A new model that describes real-world systems has been proposed recently - the Massively Parallel Computation (MPC) frameworks includes systes such as MapReduce, Hadoop, Spark, or Flume. It comes with a completely new possibilities as well as requirements. MPC computations are executed in synchronous rounds, but implementing these rounds on real-world systems takes considerable time. One round takes orders of magnitude longer than on classical Cray type system. Thus we would like to solve problems, in particular graph problems, in as few rounds as possible. With this challenge in mind, this project aims to design methods to break barriers that were impossible to overcome using classical techniques and models. More specifically, we are going to work on new algorithmic tools that would improve efficiency of both parallel and non-parallel algorithms used in data science.	Piotr Sankowski	piotr.sankowski@ideas-ncbr.pl
8	**Adversarial Social Network Analysis**	How can individuals and communities protect their privacy against social network analysis techniques, algorithms and other tools? How do criminals or terrorists organizations evade detection by such tools? Under which conditions can these tools be made strategy proof? These fundamental questions have recently attracted increasing attention in the literature as a new paradigm for social network analysis, whereby the strategic behaviour of network actors is explicitly modeled. Addressing this research challenge has various implications. For instance, it may allow two individuals to keep their relationship secret or private. It may also allow members of an activist group to conceal their membership, or even conceal the existence of their group from authoritarian regimes. Furthermore, it may assist security agencies and counter terrorism units in understanding the strategies that covert organizations use to escape detection, and give rise to new strategy-proof countermeasures.	Tomasz Michalak	tomasz.michalak@ideas-ncbr.pl

9	**Game-Theoretic Aspects of Blockchain Technologies**	The blockchain is a game changing technology and as such it has attracted enormous interest from both academia and industry. While there are countless potential application of blockchain, almost all of them share a common feature: the parties that use it are assumed to be, in principle, self-interested utility maximizing individuals. Given this, many aspects related to the blockchain technology should be analysed using the aparatus of game theory. These include such issues like: selfish mining, majority attacks and Denial of Service attacks, computational power allocation, reward allocation, and pool selection, and energy trading. While the literature that analyses game-theoretic aspects of blockchain is growing, there are many interesting open questions that have not yet been answered in a satisfactory way. For instance: how to design rules that lead to the development of payment channel networks that are secure, reliable and efficient.	Tomasz Michalak	tomasz.michalak@ideas-ncbr.pl
10	**Stackelberg Games for Security**	Various global threats, including terrorism, drug and human trafficking have led the researchers to look for more efficient way to utilize security resources. An interesting approach that delivered surprisingly good results is based on game theory. Instead of deploying security forces by expert decisions, an optimal solution of an appropriately constructed security game is used. This approach – based on Stackelberg Security Games – has proven to deliver substantially better results. It has been applied in numerous places in the USA (Los Angeles International Airport, the US Federal Air Marshals Service, Boston harbour) and all over the world (to endangered species in natural parks). In this research line, we would like to deploy such solutions in Poland. To this end, given the increasing number of threats and their changing nature, there is a need to extend the current theory of Stackelberg Security Games as well as the algorithms to compute them. We plan to deploy potential results in various critical places in Poland.	Tomasz Michalak	tomasz.michalak@ideas-ncbr.pl

11	**Explainability of Machine Learning Models Based on Game Theory**	One of the key research challenges regarding machine learning models is their explainability. When high-value decisions are taken, e.g., in medical diagnostic, understanding why a model made a specific prediction is often as important as the prediction's accuracy. Thus we need to develop methods to interpret the model's results in a transparent way so that humans are willing to follow model recommendations. As a result, recently, there has been a growing interest in the feature attribution problem, where, given some specific input x of features, one would like to attribute the model's prediction f(x) to the individual features. One of the most popular approaches to interpreting model predictions uses methods originating from cooperative game theory that are called solution concepts or values. They measure the importance of each player in, or contribution to, a coalitional game. While there exist many ways in which the importance of each player can be evaluated, some solution concepts are considered more fundamental than others due to underlying axiom systems that uniquely determine them. One important game-theoretic solution concept that attracted a lot of attention in the context of explainability is the Shapley value popularized by the SHAP library in python. However, the Shapley value is not the only solution concept that has been advocated for interpreting model predictions. Some papers suggest using other values. Each value has its own unique characteristics and should be used for specific applications and types of machine learning models. It is then a very pressing to do a thorough study of game-theoretic solution concepts for explainability of machine learning models. The challenge involves: (a) the study of theoretical aspects of applying various game-theoretic solution concepts; (b) the computational analysis---given the inherent computational challenges related to game-theoretic solution concepts it is paramount to look for tractable approaches to the problem; and (c) experimental analysis in chosen applications; and (d) possible implementation as a software library.	Tomasz Michalak	tomasz.michalak@ideas-ncbr.pl