Generalnym tematem projektu są protokoły oparte na tzw. *inteligentnych kontraktach* (ang.: *smart contracts*). Nieformalnie rzecz ujmując, kontrakty te są umowami zapisanymi w formie przypominającej program komputerowy. Zwykle umieszczane są one na specjalnych platformach zwanych *blockchainami* i zintegrowane są z tzw. *kryptowalutami*. Najbardziej znanym przykładem takiej platformy jest *Ethereum*.

Inteligentne kontrakty mają własność „samo-wykonalności", tzn. ich realizacja opiera się wyłącznie na mechanizmie danej platformy i nie zależy od czynnika ludzkiego. W pewnym sensie blockchain pełni więc rolę cyfrowego notariusza odnotowującego zawarcie kontraktu i sędziego rozstrzygającego ewentualne spory. Cechy te czynią z inteligentnych kontraktów idealne narzędzie do wielu zastosowań informatycznych, zwłaszcza tych związanych z tzw. internetem rzeczy, w których kontrakty takie zawierane są bezpośrednio między urządzeniami i bez ingerencji człowieka.

Przez „*protokoły* oparte na inteligentnych kontraktach" rozumiemy algorytmy (wykonywane przez wielu niezależnych uczestników) które wchodzą w interakcje ze inteligentnymi kontraktami. Najprostszym przykładem takiego protokołu 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 jakie wiadomości ma wysyłać do kontraktu w celu wykonania ruchu w grze. Oczywiście, protokoły wykorzystywane w praktyce mogą być znacznie bardziej skomplikowane niż ten przykład i w szczególności mogą obejmować scenariusze w których liczba uczestników jest znacznie większa niż 2.

Celem grantu jest stworzenie formalnej teorii protokołów opartych na inteligentnych kontraktach, wraz z modelem bezpieczeństwa, formalnymi dowodami i zestawem narzędzi matematycznych służących analizie ich bezpieczeństwa. W ramach projektu będziemy też tworzyć nowe protokoły tego typu, oraz analizować protokoły istniejące. Przykładem protokołów, którymi będziemy się zajmować są tzw. „protokoły *off-chain*", które służą przeniesieniu znacznej części operacji blockchainowych poza główny blockchain, przy zachowaniu tych samych gwarancji bezpieczeństwa. Kierownik grantu opublikował niedawno kilka wstępnych prac na ten temat, które zostały przyjęte na najbardziej prestiżowe konferencje w tej dziedzinie (IEEE S&P, ACM CCS i Eurocrypt). Jest on też współtwórcą systemu o nazwie *Perun* który umożliwia tworzenie tzw. wirtualnych kanałów ze stanem (jest to jedna z technik „off-chain"). Oprócz dalszego rozwijania tych technik, duża część projektu poświęcona będzie szukaniu nowych rozwiązań i zastosowań inteligentnych kontraktów.

W projekcie duży nacisk postawiony będzie na matematyczny formalizm i dowody bezpieczeństwa proponowanych rozwiązań. Zespół realizujący projekt będzie również angażował się w dialog ze społecznością praktyków blockchainowych i współuczestniczył w wysiłkach mających na celu standaryzację badanych protokołów.