Pojęcie „blockchain” (pol. *łańcuch bloków*) zostało wprowadzone po raz pierwszy około dekadę temu, jako określenie pewnego rozwiązania technicznego, pozwalającego na zwalczanie tak zwanego problemu podwójnego wydatkowania (ang. *double-spending*), które zastosowano w nowo zaproponowanej walucie „bitcoin”. Obecnie uważa się, że technologia ta ma szersze zastosowanie, znacznie wykraczające poza sferę finansów. Jedną z głównych zalet technologii blockchainowych jest fakt, że pozwalają one na „rozproszenie zaufania”, to znaczy użytkownicy systemów opartych o to narzędzie nie muszą ufać jednej wyróżnionej stronie, ale zamiast tego mogą polegać na innych (słabszych) założeniach, takich jak „uczciwa większość” czy „uczciwa większość mocy obliczeniowej”.

Jedną ze słabości tej technologii jest to, że (zmniejszając zaufanie do zewnętrznych serwerów) bardzo mocno opiera się ona na założeniu, że poszczególni użytkownicy są w stanie samodzielnie bezpiecznie przechowywać tajne dane i wykonywać na nich złożone algorytmy kryptograficzne. Dodatkowo, ponieważ użytkownicy blockchaina są zazwyczaj identyfikowani wyłącznie za pomocą swoich kluczy publicznych, to odpowiadające im klucze prywatne są bardzo atrakcyjnym celem cyberataków. Ponadto, istnieje realne ryzyko, że użytkownik na zawsze utraci dostęp do swojego konta z powodu utraty tajnego klucza (szacuje się, że łączna suma utraconych w ten sposób monet w latach 2011–2018 miała wartość ponad 2 mld dolarów). W związku z powyższym, w celu zwiększenia bezpieczeństwa, tajne klucze są często przechowywane w tak zwanych „(sprzętowych) portfelach”, a więc urządzeniach do przechowywania kluczy i wykonywania transakcji na blockchainie.

Jeśli taki portfel wykonany jest jako dedykowany samo-wystarczalny sprzęt (a nie program komputerowy), to nazywamy go *portfelem sprzętowym*. Takie urządzenie ma oczywiście swoją cenę, ponieważ generalnie sprzęt elektroniczny jest drogi. Dodatkowo, konieczność obsługi kolejnego urządzenia cyfrowego, obniża wygodę użytkowania. Z tego względu, część użytkowników zadawala się prostym (*software'owym*) portfelem, a więc zwyczajną aplikacją, którą można uruchomić na zwykłym komputerze bądź smartfonie. Inne popularne rozróżnienie między portfelami, to podział na „gorące” i „zimne” portfele. Te pierwsze są stale podłączone do Internetu, podczas gdy te drugie – są od niego świadomie odcięte (za pomocą techniki tzw. „air gapping”u). Korzystanie z portfeli wprowadza pewne dodatkowe założenia dotyczące zaufania. Zrozumienie ich jest istotne, ponieważ – w przeciwieństwie do tradycyjnych aplikacji (np. do bankowości internetowej) – systemy blockchainowe, ze względu na ich specyficzną, rozproszoną naturę, pseudonimowość oraz nieodwracalność transakcji, są znacznie bardziej podatne na ataki cybernetyczne skierowane przeciwko końcowemu użytkownikowi.

Celem tego projektu jest opracowanie nowych modeli i narzędzi do opisu i tworzenia bezpiecznych portfeli blockchainowych, ze szczególnym uwzględnieniem analizy podstawowych fundamentów teoretycznych tej dziedziny. Jego wynikami będą: nowe modele i nowe pojęcia w badanej dziedzinie, a także nowe rozwiązania, których bezpieczeństwo zostanie formalnie udowodnione. Przede wszystkim będziemy się skupiać na teoretycznych podstawach, ale spodziewamy się również, że nasze wyniki będą mieć także skutki praktyczne. Do celów modelowania rozważanych problemów, wykorzystamy formalizmy z kryptografii teoretycznej. Takie formalne podejście jest niezwykle ważne w dziedziny bezpieczeństwa cyfrowego. Wynika to z faktu, że bezpieczeństwa nie da się udowodnić „eksperymentalnie”, lub – innymi słowy – nie da się przeprowadzić żadnych eksperymentów, które mogłyby posłużyć jako dowód, że dany system jest bezpieczny. Nasze rozwiązania będą wykorzystywać narzędzia i metody z dziedziny kryptografii, a także algorytmów rozproszonych. Wykorzystamy również techniki znane z “kryptografii odpornej na wycieki” oraz “odpornej na modyfikacje” (ang. *leakage-* oraz *tamper-resilient cryptography*). Choć główne oczekiwane wyniki będą mieć charakter teoretyczny, możliwe również, że w ramach projektu zostaną stworzone prototypowe implementacje oraz rozwiązania o potencjale komercyjnym.